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

(11) PI 0912971-5 B1

(22) Data do Depósito: 17/04/2009

(45) Data de Concessão: 10/11/2020

(54) Título: PROCESSO PARA ATIVAÇÃO E PERSONALIZAÇÃO DE UM MÓDULO DE IDENTIFICAÇÃO DE ASSINANTE EM UMA REDE DE RÁDIO MÓVEL

(51) Int.Cl.: H04W 8/26; H04W 12/00; H04W 12/04.

(52) CPC: H04W 8/265; H04W 12/0023; H04W 12/04.

(30) Prioridade Unionista: 23/05/2008 DE 10 2008 024 798.7.

(73) Titular(es): DEUTSCHE TELEKOM AG.

(72) Inventor(es): STEFAN KALINER.

(86) Pedido PCT: PCT EP2009002827 de 17/04/2009

(87) Publicação PCT: WO 2009/141035 de 26/11/2009

(85) Data do Início da Fase Nacional: 23/11/2010

(57) Resumo: PROCESSO PARA PERSONALIZAÇÃO OVER-THE-AIR DE CARTÕES DE CHIP EM TELECOMUNICAÇÕES. A presente invenção refere-se a um processo para ativação e personalização de um módulo de identificação de assinante SIM, sendo que o SIM, antes da primeira ativação, é equipado com um conjunto (S*) não individual e provisório de parâmetros de identificação e autenticação, que contém pelo menos uma identificação e autenticação, que contém pelo menos uma identificação de assinante (IMSI*) não individual e provisória e uma chave secreta (K*) não individual e provisória, sendo que o conjunto de parâmetros (S*) permite uma primeira ativação do SIM em uma rede de rádio móvel por meio de um aparelho terminal de rádio móvel, sendo que, depois da primeira ativação do SIM, é realizada uma personalização, seno que um conjunto de dados de assinante (S) individual e definitivo é transmitido e armazenado no SIM, contendo, particularmente, uma identificação de assinante (IMSI) definitiva, claramente definida, e uma chave de secreta (K) definitiva, claramente definida, particularmente, que o conjunto de dados de assinantes (S) definitivo, claramente definido, particularmente que o conjunto de dados de assinante (S) é transmitido através de uma conexão normal do sistema de rádio móvel, sob uso do conjunto (...).

Relatório Descritivo da Patente de Invenção para **"PROCESSO PARA ATIVAÇÃO E PERSONALIZAÇÃO DE UM MÓDULO DE IDENTIFICAÇÃO DE ASSINANTE EM UMA REDE DE RÁDIO MÓVEL".**

[001] A invenção refere-se a um processo para ativação e personalização de um módulo de identificação de assinante SIM.

[002] Cartões de chip são usados na telecomunicação, particularmente, por exemplo, nos sistemas de GSM ou UMTS móveis, para a identificação claramente definida e segura dos assinantes, bem como para por à disposição muitas funções especiais e serviços de mais valia. Os cartões de chip, designados, por exemplo, como UICC, SIM, USIM, R-UIM ou também ISIM, dependendo da geração e tipo do padrão de sistema que serve de base, ou aplicações de cartão de chip (abreviadamente designadas como "SIM" ou, de forma equivalente, como módulo de identificação de assinante), incluem, para esse fim, uma pluralidade de parâmetros especiais, chaves secretas e outros elementos dos mais diversos tipos, por exemplo, com referência ao operador de rede, provedor, produto ou assinante.

[003] Para ativação de um aparelho terminal móvel e participação no serviço de rádio móvel, é forçosamente necessário um sim com determinados dados individuais – pelo menos a identidade do assinante IMSI, chave secreta K e parâmetros individuais para o algoritmo de autenticação. Elementos coincidentes precisam estar presentes nos bancos de dados de assinante (por exemplo, HLR/AC ou HSS) da rede de origem, de outro modo, não é possível o estabelecimento de uma conexão, nem por parte do assinante, nem por parte da rede.

[004] O carregamento dos SIMs e a marcação dos dados individuais ocorre no âmbito da produção do cartão, por ocasião da chamada personalização, em todo o caso, bem antes da utilização do módulo de identificação do assinante. A cadeia de criação de valores da pre-

paração do cartão apresenta-se, em geral, tal como se segue:

- Produtor do chip: produz o chip com (partes do) software de operação.
- Produtor do cartão: produz o corpo do cartão, implanta o chip, carrega, opcionalmente, outras partes não individuais do software de operação e os dados correspondentes.
- Agente de personalização: carrega dados individualizados mais altos, características de assinante individuais, chave secretas e, opcionalmente, outras partes do software (aplicações) troca dados individuais com o operador de rede. Em geral, é idêntico ao produto de cartão.
- Agente de embalagem/logística: embala e expede os cartões de chip personalizados ao operador de rede ou a outros locais de destino. Pode ser idêntico ao produtor de cartão e/ou ao agente de personalização.
- Operador de rede: opera a rede de comunicação. Define a personalização para seus produtos, fornece todas as especificações ao agente de personalização, recebe dados individuais (pelo menos IMSI, K e parâmetros individuais do algoritmo de autenticação) do agente de personalização para adaptação das relações de assinante em seus bancos de dados.

[005] No final do processo de preparação, os SIMs encontram-se nos pontos de venda do operador de rede. Só na conclusão de um contrato de rádio móvel, dá-se no contexto da chamada ativação, a associação ao cliente concreto e a atribuição de um número de chamada. A ativação pressupõe a existência das relações de assinante nos bancos de dados do operador de rede.

[006] Como desvantagens dessa cadeia de processo, particularmente da personalização centralizada, podem ser relacionados:

- Especialização e individualização do produto precoce-

mente na cadeia de preparação, a necessidade efetiva só pode ser estimada nesse momento.

- Fixação de recursos (capacidade do banco de dados e números) no operador de rede dá-se, em parte, muito tempo antes da necessidade efetiva.

- Prestação de serviços muito especial com soluções tecnicamente complexas e flexibilidade limitada. Alta complexidade para monitoramento do agente de personalização externo. Modificações são, em geral, encomendadas de acordo com a oferta, depois desenvolvidas, testadas e recebidas, com uma necessidade de tempo correspondente. A flexibilidade necessária requer interfaces complexas.

- Consideráveis dificuldades no manuseio de novas formas de construção de SIM, por exemplo, variantes não retiráveis ou de "machine-to-machine" (M2M). Leva a uma especialização desfavorável já em produtos preliminares. Freia a inovação.

- Conceitos de "soft" alternativos são totalmente impossíveis na personalização convencional.

[007] É, portanto, tarefa da invenção aprimorar um processo para ativação e personalização de um módulo de identificação de assinante SIM de tal modo que ele supera as desvantagens do estado da técnica e permite que, sem uma fixação de recursos prematura, tal como, por exemplo, a capacidade do banco de dados e números, é possível, a qualquer momento, um fornecimento adaptado à necessidade momentânea de módulos de identificação de assinante personalizados e liberados para operação em uma rede de rádio móvel.

[008] No processo de acordo com a invenção para ativação e personalização de um módulo de identificação de assinante SIM, é particularmente vantajoso que, antes da primeira ativação, o SIM é equipado com um conjunto (S*) não individual e provisório de parâmetros de identificação e autenticação iniciais, que contêm pelo menos

uma identificação de assinante (IMSI*) não individual e provisória e uma chave secreta (K*) não individual e provisória, sendo que o conjunto de parâmetros (S*) permite uma primeira ativação do SIM em uma rede de rádio móvel por meio de um aparelho terminal de rádio móvel, sendo que, depois da primeira ativação do SIM, é realizada uma personalização, sendo transmitido um conjunto de dados de assinante (S) individual e definitivo e armazenado no SIM, que contém, particularmente, uma identificação de assinante (IMSI) claramente definida, definitiva, e uma chave secreta (K), particularmente, que o conjunto de dados de assinante (S) é transmitido através de uma conexão regular do sistema de rádio móvel, sob uso de (S*).

[009] O conjunto (S*) provisório de parâmetros de identificação e autenticação contém, portanto, pelo menos uma identificação de assinante não individual e provisória (IMSI*) e uma chave secreta não individual e provisória (K*), sendo que o conjunto de parâmetros (S*) permite uma primeira ativação do SIM em uma rede de rádio móvel por meio de um aparelho terminal de rádio móvel, isto é, que tanto a identificação de assinante como também a chave secreta são não-individuais e apenas provisórias, como componentes do conjunto provisório (S*) de parâmetros de identificação e autenticação iniciais.

[0010] Desse modo, inicialmente, é possível equipar uma pluralidade de módulos de identificação de assinante SIM (Subscriber Identity Module), que permitem o uso dos serviços de uma rede de rádio móvel, com conjuntos de dados de parâmetro não individuais e provisórios, sem que já seja preciso associar um número correspondente de recursos, tais como, por exemplo, identidades de assinante e números de chamada de rádio móvel, associados de modo claramente definido, uma vez o conjunto de parâmetros provisório permite uma primeira ativação, isto é, um registro em uma rede de rádio móvel, e, depois, á realizada, por parte da rede, a personalização do SIM, sendo

gerado um conjunto de dados de assinante definitivo, transmitido através da conexão de rádio existente ou através de uma conexão de rádio particularmente segura e armazenada no SIM. Os dados de assinante definitivos, que são armazenados no SIM, e que servem para a identificação do assinante no uso de serviços da rede de rádio móvel, são, portanto, transmitidos ao SIM no âmbito de um processo padronizado (Over The Air – OTA). Também com isso, são utilizados de modo vantajoso os recursos e capacidades de rede existentes.

[0011] A presente invenção possibilita o deslocamento da personalização, espacialmente, do agente de personalização externo para os domínios do operador de rede e, temporalmente, no final da cadeia de fornecimento, para momento ideal da primeira ativação do aparelho.

[0012] Pelo processo proposto, é possível produzir os módulos de identificação de assinante (SIM) para um sistema de comunicação móvel, completamente, sem dados individuais (exceto, por exemplo, por um número de série contínuo) e levar os mesmos à entrega. Nesse momento, incluem-se, em vez disso, dados de identificação especiais, não individuais e temporários, mas que, apesar disso, possibilitam uma conexão de acordo com os padrões para a rede do operador. Com mecanismos de OTA dá-se, depois, a personalização individual dos parâmetros definitivos da relação de assinante e o equipamento adicional de finalidade específica do SIM com dados e aplicações. A configuração da técnica por parte do cartão possibilita, ainda, a repetição ilimitada do processo (repersonalização, também no âmbito de uma troca de operador de rede) e a possibilidade de mudança a qualquer tempo de todos os dados relevantes da mesma maneira. As vantagens são individualmente:

- A configuração individual do SIM se dá no momento mais tarde possível, até então, continua mantida a maior flexibilidade no que

se refere ao uso do SIM.

• Como não há nenhuma personalização no âmbito da produção do cartão, esse passo de processo pode ser dispensado sem substituição. As desvantagens do estado da técnica citadas são evitadas.

• A interface com o produtor de cartão é consideravelmente simplificada, uma vez que não mais precisam ser transmitidos quaisquer parâmetros de personalização e não são mais retornados dados individuais críticos para a segurança.

• No âmbito da produção do cartão não se dá nenhum ajuste nos bancos de dados do operador de rede, com isso, também nenhuma fixação de recursos muito tempo antes da necessidade efetiva.

• Em princípio, não é necessário nenhum armazenamento de dados individuais, nem no produtor de cartão, operador de rede ou um terceiro.

• Alternativas modernas para o SIM convencional são possibilitadas e ganham um atrativo adicional: no uso de módulos "M2M" ou não retiráveis, o papel do produtor de cartão pode ser adicionalmente economizado, uma vez que o produtor de chip pode fazer o fornecimento diretamente. Em conceitos soft (macio), é dispensado até mesmo o papel do produtor de chip na cadeia de preparação.

• A infraestrutura, que de qualquer modo é mantida à disposição pelo operador de rede, para customização seletiva de OTA do SIM, depois da ativação (quando, por exemplo, o aparelho terminal e a tarifa do cliente estão fixados), assume adicionalmente a tarefa da personalização e é usada de modo mais eficiente. Com isso, formam-se efeitos sinérgicos.

[0013] Formas de construção de SIM modernas, que, de qualquer modo pressupõem ou causam implicitamente modificações no modelo de rolo relatado (por exemplo, variantes usadas por máquina, soldas

ou realizadas em software), podem manifestar suas vantagens tanto melhor quanto mais tarde forem individualizadas e especializadas. Essas variantes, em geral, não chegam mais às mãos do usuário e tornam-se componente fixo de um aparelho terminal muito tempo antes de ser conhecido o operador de rede. Além disso, o mesmo pode mudar durante o ciclo de vida do aparelho terminal. Assim, no âmbito da discussão sobre formas futuras do SIM, surge, regularmente, a pergunta sobre possibilidade de repersonalização. Além disso, seria ideal uma ampla independência de um operador de rede até o momento da ativação, para permitir uma produção mais simples possível, sem interfaces complexas, a administração de espaços para números específicos do operador, algoritmos de autenticação registrados etc.

[0014] A presente invenção possibilita, exatamente, essas características importantes, sendo que o operador de origem (ou o grupo operador) a qualquer momento está estabelecido, mas não requer, além disso, nenhuma necessidade de sintonização para dados individuais. Apesar disso, o operador de rede continua a ter possibilidades totais de influência e configuração sobre a personalização do alvo – que ninguém, além dele, pode realizar.

[0015] Os cartões de chip de acordo com a invenção estão equipados, de preferência, com um conjunto não individual de parâmetros de identificação e autenticação

$$S^*_i=\{IMSI^*_i, K^*_i, OPc^*_i, Qc^*_i, OK^*_i\} \text{ com } i = 0, 1, ...,N-1 \text{ e } N<<M;$$

[0016] sendo que $IMSI^*_i$ pode conter a identificação de rede válida MCC e MNC do operador. Com N é designada a quantidade total dos S^*_i e com M, a quantidade dos SIM, produzidos desse modo, no total, para um operador de rede. Dentro de M repetem-se os S^*_i, portanto, MIN vezes e, com isso não são claramente definidos e não são individuais.

[0017] Como única característica individual é acrescentado, por

exemplo, o número de série (ICCID) usual, que é associado continuamente pelo fabricante durante a produção. É importante que todos os dados a ser associados ao processo de produção corrente pelo fabricante sejam fornecidos de modo totalmente automático e sem especificações especiais (individuais) do operador de rede.

[0018] Particularmente, além disso, também não ocorre nenhum armazenamento ou transferência de dados individuais pelo fabricante de SIM, pelo operador de rede ou por um terceiro.

[0019] Na rede de rádio móvel do operador existe um banco de dados especial (THLR) com o valor fixo N com os S*i e, em cada caso, um número de chamada MSISDN*i fixamente associado. As relações de assinante nesse banco de dados são inalteradas, particularmente, não há nenhuma conexão com o fabricante de cartões de chip.

[0020] Um respectivo SIM é agora posto em funcionamento pela primeira vez em um aparelho terminal móvel totalmente de acordo com o padrão (isto é, não dotado de medidas especiais no que se refere ao processo aqui descrito. Depois da primeira ativação com S*i, dá-se a transmissão dos dados de assinante (S) definitivos, que são armazenados no módulo de identificação de assinante SIM. Simultaneamente, esses dados de assinante definitivos também são depositados no registro de origem HLR. O módulo de identificação de assinante SIM está, depois, pronto para funcionamento com os dados definitivos.

[0021] De preferência, na primeira ativação dá-se a formação de uma conexão com um servidor de personalização (PS) dentro da rede de rádio móvel, sendo que por parte do servidor de personalização (PS), o conjunto de dados de assinante (S) individual e definitivo para a personalização é gerado e transmitido ao SIM, particularmente, sob uso dos dados de assinante não individuais e provisórios (S*i).

[0022] De preferência, a identificação de assinante provisória (IMSI*i) não está claramente definida e pode ser associada provisori-

amente a vários módulos de identificação de assinante (SIM). Desse modo, é possível preservar os recursos existentes, sendo que conjuntos de parâmetros podem ser, por exemplo, reutilizados ciclicamente, sendo que os SIM, no entanto, podem continuar identificáveis e diferenciáveis por meio de uma identificação claramente definida, tal como, por exemplo, o número de série.

[0023] Em uma modalidade preferida, antes da realização da personalização, é realizada uma verificação do número de série do SIM (ICCID) e/ou do aparelho terminal de rádio móvel, por meio do número de identidade do aparelho (IMEI), através do qual o aparelho terminal de rádio móvel é identificável de modo claramente definido, e/ou pode ser realizada uma verificação de outros parâmetros de segurança do SIM. Desse modo, a segurança do processo pode ser aumentada.

[0024] De preferência, o número dos conjuntos de dados de assinante não individuais e provisórios (S*), que contêm pelo menos uma identificação de assinante não individual e provisória (IMSI*) e uma chave secreta não individual e provisória (K*), está fixado e, particularmente, de modo muito menor do que o número dos módulos de identificação de assinante (SIM), equipados, no total, com esses conjuntos de dados (S*), sendo que a qualquer momento existem muitos módulos de identificação de assinante (SIM) com dados provisórios (S*) idênticos.

[0025] De modo particularmente preferido, os conjuntos de dados de assinante não individuais e provisórios (S*), que contêm pelo menos uma identificação de assinante não individual e provisória (IMSI*) e uma chave secreta não individual e provisória (K*), são reutilizados ciclicamente no equipamento inicial dos módulos de identificação de assinante (SIM), particularmente, independentemente do fato de se ou quantos dos SIM já foram personalizados com dados de assinante individuais e definitivos (S).

[0026] Desse modo, pode ser garantida uma distribuição uniforme dos conjuntos de dados de assinante provisórios, não individuais (S*), de modo que não ocorre, inadvertidamente, um acúmulo de um ou mais desses conjuntos de dados de assinante não individuais (S*). Desse modo, pode ser reduzido o risco de uma colisão por uso simultâneo, casual, do mesmo conjunto de dados de assinante provisório em dois cartões de SIM, isto é, módulos de identificação de assinante, diferentes.

[0027] De preferência, depois de concluída a recepção e o armazenamento do conjunto de dados definitivo (S) sobre o SIM, é transmitida uma confirmação do recebimento do conjunto de dados de assinante (S) pelo aparelho terminal de rádio móvel à rede de rádio móvel. De preferência, é realizada, então, uma partida a quente do aparelho de rádio móvel, sob uso do novo conjunto de dados de assinante (S). Pela confirmação da recepção de dados correta, a rede de rádio móvel recebe uma comunicação de retorno sobre a personalizada realizada no SIM, de modo que o processo pode ser concluído.

[0028] De preferência, o conjunto de dados de assinante definitivo (S) gerado na personalização é armazenado no registro de origem (HLR). O armazenamento do conjunto de dados de assinante (S) e dos respectivos dados de assinante no registro de origem (HLR) permite a utilização dos serviços da rede de rádio móvel.

[0029] A relação de assinante pode nesse caso, estar dotada inicialmente de limitações de serviço específicas que só mais tarde são removidas, depois da constatação dos dados de cliente, desejos de serviço etc.

[0030] De preferência, na primeira ativação com o conjunto de parâmetros (S*), a relação de cliente dada pelo (IMSI*), é posta, por parte da rede em um estado de "em uso", enquanto isso, só é liberada uma utilização limitada, particularmente, a realização da personaliza-

ção, sendo que depois de concluída a personalização do SIM com o conjunto de dados de assinante individual e definitivo (S), a relação de assinante dada pelo (IMSI*) é posta em um estado de "liberada", que permite a nova utilização da relação de assinante dada pelo (IMSI*) por um outro módulo de identificação de assinante (SIM).

[0031] De modo particularmente preferido, em uma tentativa de ativação de um ou mais outros SIM com um conjunto de parâmetros provisório, idêntico (S*) de um primeiro SIM, já registrado na rede de rádio móvel, dá-se um enfileiramento em uma fila de espera e um atendimento de acordo com a prioridade das tentativas de ativação.

[0032] De preferência, em uma tentativa de ativação de um ou mais outros módulos de identificação de assinante (SIM) com uma identificação de assinante provisória (IMSI*) idêntica a um primeiro módulo de identificação de assinante (SIM), já registrado na rede de rádio móvel, é identificado pelo módulo de identificação de assinante (SIM) um eventual bloqueio do processo de personalização (ausência dos dados de personalização) e leva à repetição automática da solicitação de personalização.

[0033] De preferência, em uma tentativa de ativação de um ou mais outros módulos de identificação de assinante (SIM) com uma identificação de assinante provisória (IMSI*) idêntica a um primeiro módulo de identificação de assinante (SIM), já registrado na rede de rádio móvel, é identificada pelo módulo de identificação de assinante (SIM) uma eventual linha defeituosa dos dados de personalização, os dados são descartados e dá-se uma repetição automática da solicitação de personalização.

[0034] De modo particularmente preferido, na ausência de confirmação do aparelho terminal de rádio móvel à rede de rádio móvel, dá-se, automaticamente, uma nova expedição dos dados de personalização. De preferência, só depois da confirmação do aparelho terminal de

rádio móvel à rede de rádio móvel, dá-se o armazenamento do conjunto de dados definitivo (S) no registro de origem (HLR).

[0035] De preferência, só depois da confirmação do aparelho terminal de rádio móvel à rede de rádio móvel, dá-se a ativação e/ou liberação da relação de assinante (assinatura) caracterizada pelo conjunto de dados de assinante definitivo (S) no registro de origem (HLR).

[0036] De modo particularmente preferido, os conjuntos de dados de assinante definitivos (S) já estão colocados em reserva de curto prazo no registro de origem (HLR). Desse modo, está garantido que uma personalização de módulos de identificação de assinante (cartões de SIM) possa dar-se a curto prazo, a qualquer momento.

[0037] De preferência, as relações de assinante (assinaturas), caracterizadas pelos conjuntos de dados de assinante definitivos (S) no registro de origem (HLR), já estão colocados em reserva de curto prazo.

[0038] De modo particularmente preferido, as relações de assinante (assinaturas), caracterizadas pelos conjuntos de dados de assinante definitivos (S) no registro de origem (HLR), estão dotadas de limitações de serviço específicas.

[0039] De preferência, subsequentemente à personalização realizada, ocorrem, automaticamente, outros processos de carregamento, para configuração do cartão de SIM com propriedades e/ou serviços especiais.

[0040] De preferência, subsequentemente à personalização realizada, ocorre, automaticamente, um diálogo por máquina ou pessoal, de preferência, iniciado através do aparelho terminal de rádio móvel, com o cliente, para determinação dos dados de cliente, desejos de serviço etc., e particularmente, só depois são removidas eventuais limitações de serviço específicas.

[0041] Um exemplo de trabalho do processo de acordo com a in-

venção está representado nas figuras e é subsequentemente explicado. Mostram:

[0042] Figura 1- um exemplo de trabalho do processo de acordo com a invenção da personalização por OTA de um módulo de identificação de assinante SIM;

[0043] Figura 2- o esquema na ativação simultânea de vários SIM, particularmente, com conjunto de parâmetros provisório idêntico.

[0044] Cartões de chip (SIM) estão equipados com estão equipados, de preferência, com um conjunto não individual de parâmetros de identificação e autenticação

$S^*_i=\{IMSI^*_i, K^*_i, OPc^*_i, Qc^*_i, OK^*_i\}$ com i = 0, 1, ...,N-1 e N<<M;

[0045] sendo que $IMSI^*_i$ pode conter a identificação de rede válida MCC e MNC do operador. Com N é designada a quantidade total dos S^*_i e com M, a quantidade dos SIM, produzidos desse modo, no total, para um operador de rede. Dentro de M repetem-se, portanto, os S^*_i MIN vezes e, com isso, não estão claramente definidos e não são individuais.

[0046] Como única característica individual é acrescentado, por exemplo, o número de série (ICCID) usual, que é associado continuamente pelo fabricante durante a produção. É importante que todos os dados a ser associados ao processo de produção corrente pelo fabricante sejam fornecidos de modo totalmente automático e sem especificações especiais (individuais) do operador de rede.

[0047] Na rede de rádio móvel do operador existe um banco de dados especial (THLR) com o valor fixo N com os S^*_i e, em cada caso, um número de chamada $MSISDN^*_i$ fixamente associado. As relações de assinante nesse banco de dados são inalteradas, particularmente, não há nenhuma conexão com o fabricante de cartões de chip.

[0048] Um respectivo SIM é agora posto em funcionamento pela primeira vez em um aparelho terminal móvel totalmente de acordo com

o padrão (isto é, não dotado de medidas especiais no que se refere à presente proposta). Para simplificação do procedimento do sistema usual no registro em uma rede de rádio móvel, dá-se a personalização de acordo com a representação de acordo com a figura 1:

(1) O IMSI* é lido pelo aparelho terminal móvel e transmitido de acordo com o padrão à rede de rádio móvel recebida, e, opcionalmente retransmitida pela mesma à rede de origem e, na mesma, transmitida ao THLR. A informação de roteamento necessária para esse fim é tirada do IMSI*. O IMSI* é conhecido no THLR e é iniciada, de acordo com o protocolo normal, a autenticação entre cartão e THLR com os dados S^*_1. O resultado é positivo e a relação de assinante passa de acordo com o padrão para o estado, no qual é possível uma formação de conexão dos dois lados.

[0049] Como função especial, o THLR dota o $IMSI^*_i$, no momento mais cedo possível, do estado "em uso". Esse estado continua a existir até a liberação do $IMSI^*_i$, quer pela conclusão regulamentar da personalização subsequente, quer pela ocorrência de um caso especial (vide abaixo).

(2) Por parte da rede, é iniciada, então, a personalização por OTA, isto é, a transmissão dos dados de assinante personalizados através de uma conexão de rádio, na qual o índice i é entregue ao servidor de personalização PS. O PS conhece o $MSISDN_i$ que combina com o índice i, e a chave de OTA OK^*_i. Com isso, ele forma, então, uma sessão de OTA segura de acordo com o estado da técnica para o SIM correspondente.

[0050] Pode, agora, ser inicialmente testado, por exemplo, o ICCID do cartão ou o IMEI do aparelho (por exemplo, por meio de um black or white listing (listagem preto e branco)) e]ou outros parâmetros de segurança do cartão podem ser solicitados (por exemplo, um certificado), antes de iniciar-se a efetiva personalização. Para esse fim, são

gerados no PS dados de assinante definitivos

S = {IMSI, K, OPc, Qc, OK},

[0051] enviados ao SIM através do canal de OTA existente e ali armazenados – com isso, o cartão personalizado individualmente.

3) O processo é apoiado de modo apropriado por parte do cartão e protegido de tal modo que erros de conexão ou uma recepção apenas parcial não podem levar a uma personalização incompleta (com isso, inválida). Só depois da recepção completa e correta e o armazenamento de todos os dados necessários, o SIM confirma o processo para o PS e, subsequentemente, ativa, finalmente, uma partida a quente (full refresh) [atualização completa] do aparelho terminal, agora, com os dados de assinante definitivos S.

4) Paralelamente à personalização do SIM, o PS ativa a instalação da relação de assinante S no HLR definitivo. Com isso, é atingido pelos dois lados um estado tal como depois da personalização e instalação convencionais. O SIM pode ser usado agora para a operação padrão.

[0052] De preferência, o armazenamento e ativação das relações de assinante definitivas S no registro de origem HLR pode dar-se somente depois do recebimento da confirmação do SIM para a rede de rádio móvel e ser dotadas provisoriamente de limitações de serviço específicas.

[0053] Para aceleração do processo, as relações de assinante definitivas S no HLR já podem estar colocada em reserva de curto prazo, por exemplo, pelo fato de que o PS armazena e ativa regularmente um número de relações de assinante S, prevendo a necessidade próxima (por exemplo, para a próxima hora ou o próximo dia).

(5) A confirmação do SIM recebida em (3), leva no PS e no THLR à liberação imediata da relação de assinante S_i, particularmente, do $IMSI_i$*. Ele muda do estado "em uso" para o estado "livre" e, com

isso está pronto para a próxima utilização.

[0054] Efetivamente, devido à não definição clara dos conjuntos de dados de parâmetro S_i* e da coincidência das ativações, mesmo na distribuição uniforme dos S_i na quantidade total produzida (que é obtida por simples contagem incremental de i durante a produção), podem ser esperadas colisões na personalização por OTA.Esse é o caso quando, durante o processamento a relação de assinante S_i*, isto é, quando o $IMSI_i$* está caracterizado como "em uso", ocorre uma segunda ou até mesmo outras tentativas de registro de SIM com conjuntos de dados de parâmetro S_i* idênticos. Esse caso está representado na figura 3. Mas, essas colisões representam um caso de operação normal, que é levado em consideração do seguinte modo:

- Tentativas de registro com $IMSI_i$*, que não podem ser processadas de modo igual, são enfileiradas em uma fila de espera e processadas na seqüência da entrada.
- O número N dos conjuntos de parâmetros S_i* deve ser selecionado de tal modo que a probabilidade de uma colisão (e, mais ainda, de uma colisão múltipla) fica suficientemente pequena. Como N continua a valer << M, as vantagens da presente proposta permanecem mantidas completamente, mesmo a N = 1.000 ou N = 10000.
- A velocidade da personalização por OTA deve ser configurada por sistemas otimizados, de tal modo que o período, no qual um $IMSI_i$* está em uso, fica o menor possível.
- Casos de erro durante o ciclo de personalização, por exemplo,, na ausência da confirmação do SIM, devem ser limitados por time-out [tempo esgotado], de modo que o $IMSI_i$* é novamente liberado o mais rapidamente possível.
- Um eventual bloqueio do processo de personalização (ausência dos dados de personalização) é identificado pelo SIM e leva à repetição automática da solicitação de personalização.

- Uma eventual linha defeituosa dos dados de personalização é identificada pelo SIM, os dados são descartados e dá-se uma repetição automática da solicitação de personalização.

- Na eventual ausência da confirmação do SIM à rede de rádio móvel, pode dar-se, automaticamente, uma nova expedição dos dados de personalização.

[0055] Ao processo de personalização segue-se, automaticamente, uma partida a quente e tentativa de registro com os dados de assinante definitivos. Pode, agora, ser realizada, sem pressão de tempo, em um novo processo de OTA, a outra configuração, por parte do cartão da relação de assinante.

[0056] Isso se refere à configuração adicional do cartão de SIM com propriedades e serviços especiais, bem como a determinação dos dados de cliente e desejados de serviço por meio de um diálogo pessoal ou automático, de preferência, através do aparelho terminal de rádio móvel. Por fim, limitações de serviço especiais, opcionalmente, existentes previamente, são removidas.

[0057] A aplicação do conceito proposto não está limitada ao canal de OTA (mas que para aplicação em redes de rádio móvel deve ser o mais interessante), mas também é concebível em variantes ligadas por fio. Por exemplo, quando a personalização deve dar-se de modo descentralizado, mas ainda nos pontos de venda (POS) do operador de rede ou do fornecedor. Através da Internet e de um leitor de cartão conectado, isso é concebível até mesmo em qualquer local desejado. Os princípios, tal como a reutilização do IMSIi*, valem, nesse caso, de modo inalterado, assim como as vantagens a ser obtidas em relação ao estado da técnica.

[0058] São apresentadas aqui, em forma de anotação, as seguintes configurações vantajosas:

- todos os sistemas, por exemplo, GMS, UMTS, IMS,

WLAN, WIMAX, LTE/SAE/EPS, NGMN, NGN, CDMA

- todos os cartões de chip da telecomunicação, por exemplo, UICC, SIM, USIM, ISIM, RUIM e futuros
- todos os fatores de formação, por exemplo, , ID-1, ID-000, MiniUICC, M2M, IFF e futuros
- todas as modalidades, por exemplo, removable, semi-removable, non-removable, soft
- todos os canais de OTA, por exemplo, SMS, BIP/CAT-TP, TCP/P, também RDM
- todos os canais ligados por linha, por exemplo, LAN, WAN, Internet
- todos os aparelhos terminais, por exemplo, telefones móveis ou fixos, PCs e PCs de Notebook, módulos de dados
- todos os leitores de cartão descentralizados, por exemplo, no POS
- todos os perímetros, por exemplo, de (IMSI, K) até personalização/individualização completa e download de software
- com proteção adicional por processos de PKI, certificados e/ou senha de personalização
- com derivação de determinados parâmetros
- com avaliação do IMEI (personalização específica para o aparelho)
- com avaliação do ICCID (personalização específica para o cartão)
- como prestação de serviços por terceiros
- como personalização inicial ou repersonalização, também com troca de operador de rede
- integrado no diálogo on-line, inclusive fechamento de contrato e ativação

[0059] Vista geral e traduções dos termos utilizados e sua designação e abreviatura internacionalmente usuais:

- módulo de identificação de assinante (Subscriber Identity Module, SIM)
- identificação de assinante (International Mobile Subscriber Identity, IMSI)
- número de identidade do aparelho (International Mobile Equipment Identity, IMEI)
- número de rádio móvel (Mobile Subscriber Integrated Services Digital Network Number, MSISDN)
- número de série do SIM (CCID)
- conexão de rádio ao SIM (Over The Air, OTA)
- registro de origem ou registro de origem temporário(Home Location Register, HLR ouTHLR)
- comunicação de máquina para máquina (Machine to Machine, M2M)
- read – ler
- check – teste verificação, testar
- network – rede
- attach, attached –anexar, anexado
- hold and buffer – armazenar intermediariamente
- authenticate, authentication- autenticar, autenticação
- auth. – abreviatura para authenticate, authentication
- bad – deficiente
- failure – erro
- send – enviar, transmitir
- update – atualização
- generate – gerar
- session – sessão

- secured – protegido
- release – liberação, liberar
- personalisation – personalização
- Perso Cycle – processo de personalização
- install – instalar
- target – alvo, região de alvo
- confirmation – confirmação
- full refresh – atualização completa, atualizar completamente
- ack. – abreviatura de acknowledgement – mensagem de retorno
- timeout –tempo excedido

REIVINDICAÇÕES

1. Processo para ativação e personalização de um módulo de identificação de assinante (SIM) em uma rede de rádio móvel, caracterizado pelo fato de que uma pluralidade de módulos de identificação de assinante (SIM), antes de uma primeira ativação, é equipado com um conjunto de parâmetros de dados (S*) idêntico, não individual, não inequívoco e provisório de parâmetros de identificação e autenticação iniciais, que contêm pelo menos uma identificação de assinante provisória (IMSI*) e uma chave secreta (K*) não individual e provisória, sendo que o conjunto de dados de parâmetros (S*) permite a primeira ativação do módulo de identificação de assinante (SIM) na rede de rádio móvel por meio de um aparelho terminal de rádio móvel e o número de conjunto de dados de parâmetros (S*) é menor que o número do total de módulos de identificação de assinante (SIM) dotados de conjunto de dados de parâmetros (S*), sendo que depois da primeira ativação de um módulo de identificação de assinante (SIM), é realizada uma personalização, onde um conjunto de dados de assinante (S) individual e definitivo é transmitido e armazenado no módulo de identificação de assinante (SIM), que contém uma identificação de assinante (IMSI) inequívoca e definitiva, e uma chave secreta (K).

2. Processo de acordo com a reivindicação 1, caracterizado pelo fato de que na primeira ativação da formação de uma conexão para um servidor de personalização (PS) dá-se dentro da rede de rádio móvel, sendo que por parte do servidor de personalização (PS), o conjunto de dados de assinante (S) para a personalização é gerado e transmitido ao módulo de identificação de assinante (SIM), particularmente, sob uso conjunto de parâmetros de dados (S*) não individuais e provisórios.

3. Processo de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que, antes da realização da personalização, é reali-

zada uma verificação do número de série (ICCID) do módulo de identificação de assinante (SIM) e/ou do número de identidade do aparelho (IMEI), através do qual o aparelho terminal de rádio móvel pode ser identificado de modo claramente definido, e/ou uma verificação de outros parâmetros de segurança do módulo de identificação de assinante (SIM).

4. Processo de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que que o conjunto de dados de assinante (S) definitivo é transmitido através de uma conexão OTA do sistema de rádio móvel, sob uso do conjunto de parâmetros de dados (S*) provisório.

5. Processo, de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que os conjuntos de dados de assinante (S*) não individuais e provisórios são reutilizados ciclicamente no equipamento inicial dos módulos de identificação de assinante (SIM), particularmente, independentemente do fato de se ou quantos dos SIM já foram personalizados com conjunto de dados de assinante (S) individuais e definitivos.

6. Processo, de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que o conjunto de dados de assinante (S) gerado na personalização, e os dados de assinante correspondentes só são armazenados na primeira ativação do módulo de identificação de assinante (SIM), no registro de local de origem (HLR).

7. Processo, de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que, depois de realizados a recepção e o armazenamento do conjunto de dados de assinante (S) individual e definitivo no módulo de identificação de assinante (SIM), é transmitida uma confirmação pelo aparelho terminal de rádio móvel à rede de rádio móvel, particularmente, que é realizada uma

partida a quente do aparelho terminal de rádio móvel, sob uso do conjunto de dados de assinante (S).

8. Processo, de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que na primeira ativação com o conjunto de parâmetros de dados (S*) não individual e provisório, a relação de assinante dada pelo (IMSI*) é posta, por parte da rede, em um estado de "em uso", enquanto é liberada apenas uma utilização limitada, e que, depois de concluída a personalização do SIM com o conjunto de dados de assinante (S) individual e definitivo, a relação de assinante dada pelo (IMSI*) é posta em um estado de "liberado", que permite novamente a utilização da relação de assinante dada pelo (IMSI*) por um outro módulo de identificação de assinante SIM.

9. Processo, de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que em uma tentativa de ativação de um ou mais outros módulos de identificação de assinante (SIM), com uma identificação de assinante (IMSI*) provisória, idêntica a um primeiro módulo de identificação de assinante (SIM), já registrado na rede de rádio móvel para personalização, dá-se um alistamento em uma fila de espera e um tratamento de acordo com a prioridade das tentativas de ativação.

10. Processo, de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que em uma tentativa de ativação de um ou mais outros módulos de identificação de assinante (SIM), com uma identificação de assinante (IMSI*) provisória, idêntica a um primeiro módulo de identificação de assinante (SIM), já registrado na rede de rádio móvel para personalização, um bloqueio eventual do processo de personalização (ausência dos dados de personalização) é identificado pelo módulo de identificação de assinante (SIM) e leva à repetição automática da consulta de personalização.

11. Processo, de acordo com qualquer uma das reivindica-

ções precedentes, caracterizado pelo fato de que na tentativa de ativação de um ou mais outros módulos de identificação de assinante (SIM), com uma identificação de assinante (IMSI*) provisória, idêntica a um primeiro módulo de identificação de assinante (SIM), já registrado na rede de rádio móvel para personalização, uma linha errada dos dados de personalização é identificada pelo módulo de identificação de assinante (SIM), os dados são descartados e dá-s uma repetição automática da consulta de personalização.

12. Processo, de acordo com qualquer uma das reivindicações 7 a 11, caracterizado pelo fato de que na ausência da confirmação do aparelho terminal de rádio móvel à rede de rádio móvel dá-se, automaticamente, uma nova expedição do conjunto de dados de assinante (S).

13. Processo, de acordo com qualquer uma das reivindicações 6 a 12, caracterizado pelo fato de que só depois da confirmação do aparelho terminal de rádio móvel à rede de rádio móvel, dá-se o armazenamento do conjunto de dados de assinante (S) definitivo no registro do local de origem (HLR).

14. Processo, de acordo com qualquer uma das reivindicações 6 a 13, caracterizado pelo fato de que só depois da confirmação do aparelho terminal de rádio móvel à rede de rádio móvel, dá-se a ativação e/ou liberação da relação de assinante (assinatura), caracterizada pelo conjunto de dados de assinante (S) definitivo no registro do local de origem (HLR).

15. Processo de acordo com qualquer uma das reivindicações 6 a 14, caracterizado pelo fato de que os conjuntos de dados de assinante (S) definitivos no registro do local de origem (HLR) já estão previstos como reserva.

16. Processo de acordo com qualquer uma das reivindicações 6 a 15, caracterizado pelo fato de que as relações de assinante

(assinaturas), caracterizadas pelos conjuntos de dados de assinante (S) definitivos no registro do local de origem (HLR) já estão previstas como reserva.

17. Processo de acordo com qualquer uma das reivindicações 6 a 16, caracterizado pelo fato de que as relações de assinante (assinaturas), caracterizadas pelos conjuntos de dados de assinante (S) definitivos no registro do local de origem (HLR), estão dotadas de restrições de serviço específicas.

18. Processo de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que subsequentemente à personalização realizada, dão-se, automaticamente, outros processos de carga para configuração do módulo de identificação de assinante (SIM) com propriedades e/ou serviços especiais.

19. Processo de acordo com qualquer uma das reivindicações precedentes, caracterizado pelo fato de que subsequentemente à personalização realizada, é iniciado, automaticamente, um diálogo por máquina ou pessoal, através do aparelho terminal de rádio móvel, com o cliente para determinação dos dados de cliente e/ou desejos de serviços.

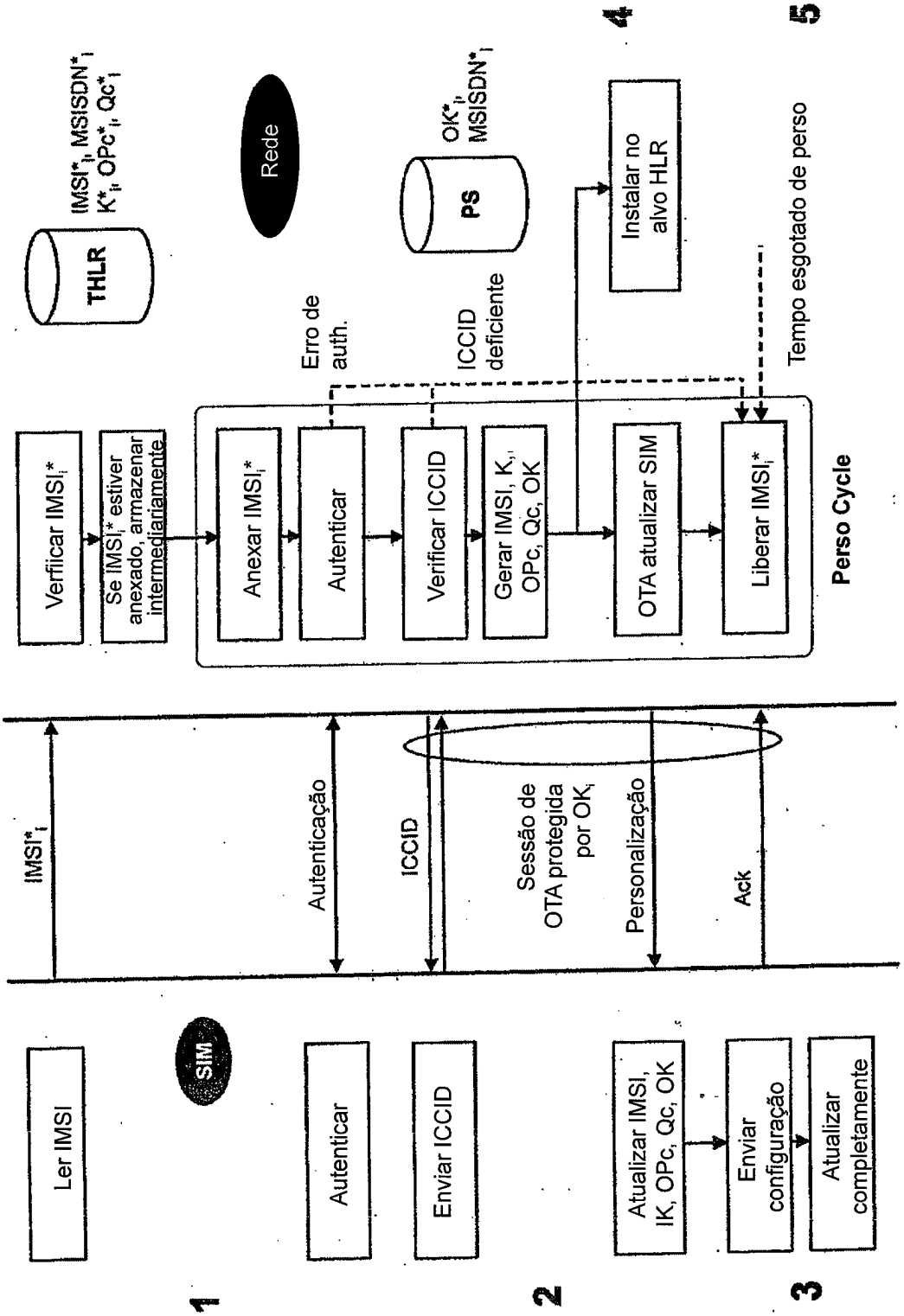
1
Ler IMSI
SIM
Autenticar
Enviar ICCID
2
Atualizar IMSI, IK, OPc, Qc, OK
Enviar configuração
Atualizar completamente
3
IMSI*i
Autenticação
ICCID
Sessão de OTA protegida por OKi
Personalização
Ack
4
5
THLR
IMSI*i, MSISDN*i
K*i, OPc*i, Qc*i
Rede
PS
OK*i, MSISDN*i
Instalar no alvo HLR
Erro de auth.
ICCID deficiente
Tempo esgotado de perso
Verificar IMSI*i
Se IMSI*i estiver anexado, armazenar intermediariamente
Anexar IMSI*i
Autenticar
Verificar ICCID
Gerar IMSI, Ki, OPc, Qc, OK
OTA atualizar SIM
Liberar IMSI*i
Perso Cycle

Fig. 1

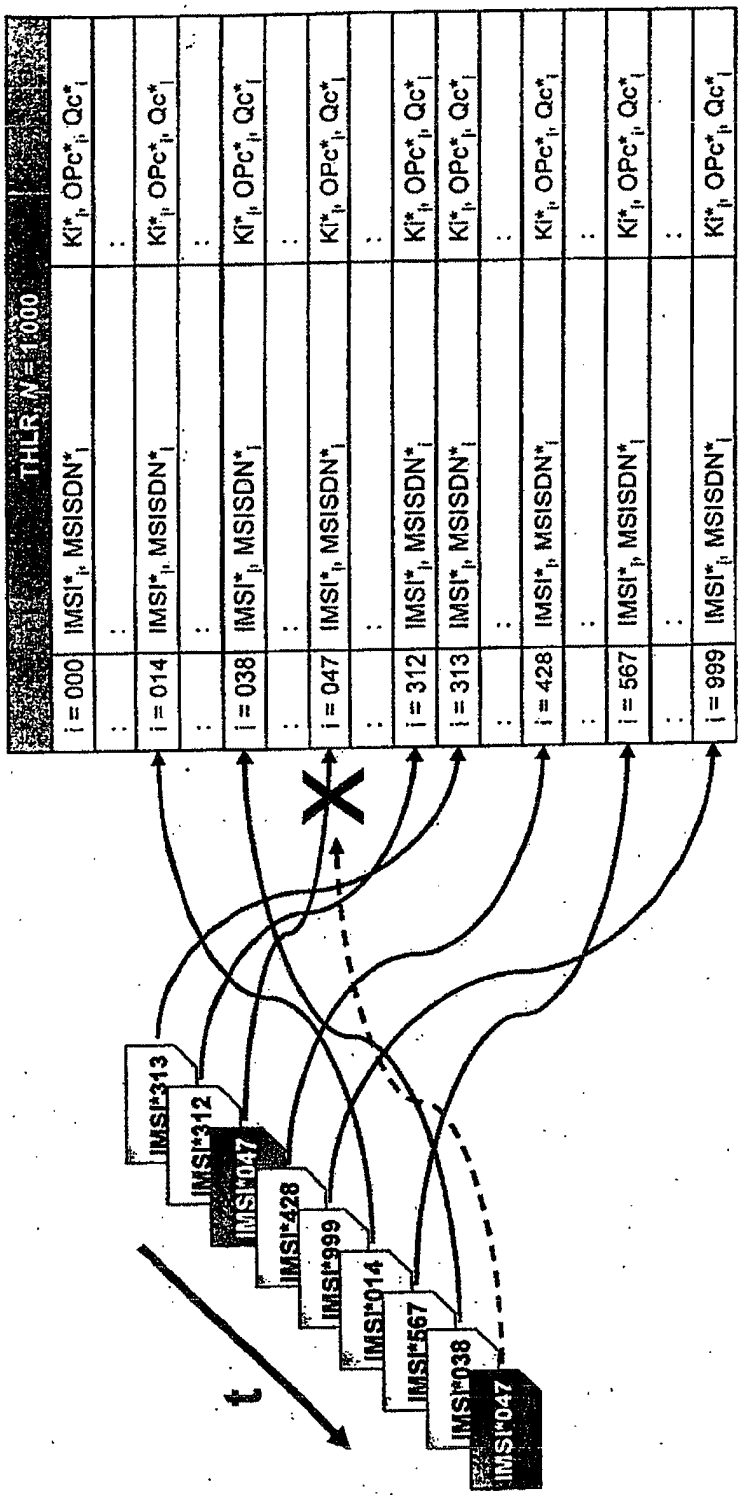
THLR N = 1'000
i = 000
IMSI*i, MSISDN*i
Ki*i, OPc*i, Qc*i
i = 014
i = 038
i = 047
i = 312
i = 313
i = 428
i = 567
i = 999
IMSI*313
IMSI*312
IMSI*047
IMSI*428
IMSI*999
IMSI*014
IMSI*567
IMSI*038
IMSI*047
t

Fig. 2