Universidade do Minho
Escola de Engenharia

Emanuel José da Silva Freitas

Solução de controlo para redes WLAN em convivência com redes 3GPP

Outubro de 2009

Solução de controlo para redes WLAN em convivência com redes 3GPP
Emanuel José da Silva Freitas
UMinho | 2009

Universidade do Minho
Escola de Engenharia

Emanuel José da Silva Freitas

Solução de controlo para redes WLAN em convivência com redes 3GPP

Mestrado em Engenharia Informática

Trabalho efectuado sob a orientação do
Prof. Doutor Paulo Manuel Martins de Carvalho
e do
Eng. Paulo Jorge Rolo Ferreira

Outubro de 2009

Agradecimentos

Em primeiro lugar, gostaria de exprimir a minha gratidão ao meu orientador, Professor Paulo Carvalho, por toda a ajuda e disponibilidade, quer no desenvolvimento desta dissertação, quer ao longo de todo o Mestrado.

Depois, a nível profissional, queria agradecer ao Engenheiro Paulo Rolo, por todo o apoio e orientação dados na realização deste trabalho, ajudando na sua concretização.

Gostaria também de agradecer aos meus amigos, especialmente ao Filipe Leitão, por todo o encorajamento e amizade ao longo deste tempo. Por fim, queria agradecer aos meus pais e ao resto da família por toda a compreensão e suporte.

Resumo

As redes 3G[1] possibilitam uma grande mobilidade e vasta cobertura, no entanto as taxas de transmissão são reduzidas e sua utilização é cara quando comparadas com as WLANs[2], que apesar de permitirem altas taxas de transmissão têm uma cobertura bastante reduzida. O sucesso das redes 3G e das WLANs e as diferenças entre ambas tem vindo a criar a necessidade da integração destas duas tecnologias.

O principal objectivo da integração das redes 3G com as redes WLANs é permitir a partir da rede WLAN o acesso aos serviços oferecidos pela rede 3G potenciando assim ao operador novos mercados e novas oportunidades de negócio. A partilha de serviços e a utilização de um meio comum de controlo de acesso são também factores importantes na convergência fixo-móvel.

Tendo em vista estes objectivos, este trabalho a ser realizado numa empresa de I&D de uma das principais operadoras de telecomunicações portuguesas propõe uma solução de controlo para redes WLAN permitindo estender os serviços de autenticação, autorização e *accounting* das redes 3G às redes WLAN.

Neste contexto, será realizado um estudo do estado da arte, das normalizações propostas pelo 3GPP[3] e uma análise dos requisitos existentes. De seguida será feito o desenho e implementação da solução seguindo as normalizações já referidas e descritos os testes para validação do seu funcionamento. Por fim são apresentadas algumas conclusões e enunciado o trabalho futuro.

[1] Third Generation Network
[2] Wireless Local Area Network
[3] 3rd Generation Partnership Project

Abstract

3G[4] networks allow great mobility and wide coverage, however the transmission rates are low and their use is too expensive when compared with the WLANs[5] that despite high transmission rates have a very low coverage. The success of 3G networks and WLANs and the differences between them created the need for integration of these two technologies.

The main objective of the integration of 3G networks with WLANs is to allow the services offered by 3G network to be accessed from the WLAN. This integration gives to the operators new markets and new opportunities business. The sharing of services and use of a common mean of access control are also important factors in fixed-mobile convergence.

To achieve these objectives, this work carried out in a R&D company of the Portuguese leading telecom operator, proposes a control solution for WLAN networks enabling to extend the services of authentication, authorization and accounting of 3G networks to to WLANs. In this context, this work covers initially a detailed study of the state of the art and of the standards proposed by the 3GPP[6] and the analysis of the existing requirements. After that, it is presented the design,implementation and tests of the proposed solution following the regulations cited above.

[4]Third Generation Network
[5]Wireless Local Area Network
[6]3rd Generation Partnership Project

Conteúdo

Lista de Figuras

Lista de Tabelas

Glossário

3G	Third Generation Network
3GPP	3rd Generation Partnership Project
AAA	Authorization, Authentication e Accounting
AES	Advanced Encryptation Standard
AK	Anonymity Key
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
APN	Access Point Name
AuC	Authentication Centre
AV	Authentication Vector
CDR	Charging Data Record
CK	Cipher Key
CS	Circuit Switched
DSCF	Data Service Control Function
DSGW	Diameter Signaling Gateway
EAP	Extensible Authentication Protocol
EAP-AKA	EAP Method for UMTS Authentication and Key Agreement
EAP-SIM	EAP Method for GSM Subscriber Identity
ECB	Electronic Code Book

ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
HLR	Home Location Register
HN	Home Network
HSS	Home Subscriber Server
I&D	Investigação e Desenvolvimento
I-WLAN	3GPP-WLAN Interworking
IDS	Intelligent Diameter Stack
IK	Integrity Key
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
Kc	Cipher Key
Ki	Individual Subscriber Authentication Key
MAC	Message Authentication Code
MMS	Multimedia Messaging Service
MSK	Master Session Key
NAI	Network Access Identifier
NASREQ	Network Access Server Application
NIC	Network Interface Card
OCS	Online Charging System
OFCS	Offline Charging System
PDG	Packet Data Gateway
PDN	Packet Data Network
PS	Packet Switched

QoS	Quality of Service
R&D	Research and Development
RADIUS	Remote Authentication Dial In User Service
RTDAP	Real Time Data Application Part
SIM	Subscriber Identity Module
SLF	Subscriber Locator Function
SQN	Sequence Number
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
UE	User Equipment
UICC	Universal Integrated Circuit Card
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunications System
VN	Visited Network
W-APN	Wireless APN
WAG	Wireless Access Gateway
WLAN	Wireless Local Area Network
WLAN AN	WLAN Access Network
WLAN UE	WLAN User Equipment
XAF	eXtensible Architecture Framework

Capítulo 1

Introdução

Se analisarmos as características das redes 3G [1] e das WLANs podemos verificar que as duas redes se complementam. Por um lado as redes 3G possibilitam uma grande mobilidade e têm uma vasta cobertura permitindo um *roaming* praticamente global, no entanto as taxas de transmissão que permitem para acesso a dados são bastante baixas e a utilização é cara quando comparadas com as WLANs. Por outro lado, as WLANs permitem taxas de transmissão elevadas a baixo custo, mas têm uma cobertura e mobilidade bastante reduzidas e algumas vulnerabilidades a nível de segurança. Estas diferenças complementares têm vindo a criar a necessidade da integração das duas redes tentando desta forma permitir a utilização da tecnologia de acesso que mais se adeqúe a cada situação diminuindo assim as desvantagens de cada rede.

A integração das duas redes permite estender os serviços da rede 3G às redes WLAN trazendo desta forma vantagens quer para o utilizador, uma vez que poderá aceder a estes serviços de uma forma simples pois praticamente não precisa de intervir, segura e desfrutando das altas taxas de transmissão que a rede oferece, quer para o operador que poderá combinar mais uma tecnologia de acesso à sua rede e assim oferecer serviços em mais situações potenciando novas oportunidades de negócio.

A autenticação[1], autorização[2] e *accounting*[3] (AAA) das redes WLAN passam a ser efectuadas utilizando a rede 3G tornando assim estes processos mais seguros, uma vez que estendem os algoritmos de autenticação da rede 3G à rede WLAN, e mais simples porque passa a existir

[1] Autenticação consiste em verificar a identidade de determinado utilizador.

[2] Autorização consiste em verificar se o utilizador tem acesso a determinado recurso ou serviço.

[3] *Accounting* é o acto de recolher informação de consumo de recursos para efeitos de planeamento de capacidade, alocação de recursos, cobrança, etc.

apenas um único perfil de utilizador para as duas redes. Estender os serviços de AAA da rede 3G à rede WLAN facilita também o processo de *roaming* entre redes WLAN.

No âmbito deste tema, depois de efectuados diversos estudos ([2], [3], [4] e [5]), surgiram duas principais abordagens: a do *3rd Generation Partnership Project* (3GPP) que define componentes e interfaces especificamente para a integração das redes 3G com as WLANs e a do *Telecoms & Internet converged Services & Protocols for Advanced Networks* (TISPAN) [6] que é mais genérica e define uma arquitectura onde diversos meios de acesso são suportados. Como o foco deste trabalho são apenas as WLANs foi adoptada a abordagem do 3GPP.

1.1 Objectivos

O objectivo deste trabalho será desenvolver uma solução de controlo para redes WLAN em convivência com redes 3GPP denominada *3GPP AAA Server*. De forma a cumprir este objectivo será necessário fazer o levantamento dos requisitos do sistema em questão para posteriormente ser realizado o desenho da arquitectura e implementação. Durante este processo serão seguidas todas as normalizações propostas pela entidade 3GPP referentes a este sistema.

Esta solução será um componente que posteriormente será integrado num operador de telecomunicações. Por este motivo é necessário analisar a integração deste novo componente na arquitectura global já existente definindo interfaces de interligação com os componentes já existentes.

Finalmente, serão efectuados testes previamente definidos com base nos requisitos à solução apresentada, de modo a garantir a qualidade da mesma.

Enumerando os objectivos para a realização deste trabalho temos:

- Análise dos requisitos da solução;
- Estudo das normalizações propostas pela entidade 3GPP relativas a esta solução;
- Estudo da integração da solução na arquitectura já existente tendo em conta as normalizações propostas;
- Desenho da solução;
- Implementação da solução;

- Testes da solução desenvolvida.

1.2 Enquadramento Normativo

A solução elaborada deverá respeitar as normalizações propostas pela entidade *3rd Generation Partnership Project* (3GPP). Estas estão agrupadas por *Releases* e cada *release* contém centenas de normalizações dos mais variados temas organizadas por assunto (ex. aspectos de serviço, protocolos, segurança, etc). A primeira referência à integração das redes 3G com as redes WLAN aparece na *Release* 6 com as normas [7], [8], [9], [10], [11] e [12]. Estas normas especificam vários componentes, interfaces, questões de segurança e de tarifação que permitem aos utilizadores WLAN aceder aos serviços disponibilizados por as redes 3G, sendo que a componente a desenvolver neste projecto é denominada pelo 3GPP como *3GPP AAA Server*.

De forma a possibilitar as várias funcionalidades que estão especificadas, o *3GPP AAA Server* deverá interagir com diversos componentes, sendo eles a *WLAN Access Network* (WLAN AN) onde o cliente WLAN está directamente ligado, o *WLAN Access Gateway* (WAG) que é o ponto de entrada na rede 3G, o *Packet Data Gateway* (PDG) que irá permitir aceder aos serviços da rede 3G, o *Home Subscriber Server* (HSS) que contém toda a informação dos clientes, o *Online Charging System* (OCS) e o *Offline Charging System* (OFCS) que são responsáveis pela tarifação do serviço.

Na *Release* 7 foram feitas algumas correcções e acrescentado o suporte para Qualidade de Serviço. Na *Release* 8 não houve alterações para além de pequenas correcções. O estudo desta dissertação foi focado apenas na *Release* 8.

1.3 Principais contribuições

Um estudo de mercado efectuado, provou que, apesar das primeiras normas do 3GPP relativas a este tema já datarem de 2003, ainda não existem muitos produtos no mercado e os que existem não suportam totalmente as especificações propostas. Assim, a principal contribuição deste trabalho é oferecer um produto que permita a integração das redes 3G com as redes WLAN e que siga na sua totalidade todas as especificações propostas. Como este trabalho foi realizado num ambiente empresarial esta nova solução irá proporcionar também novas oportunidades de negócio.

1.4 Organização da dissertação

Esta dissertação está organizada em cinco capítulos da seguinte forma:

Introdução Neste capítulo é feito o enquadramento do tema da dissertação e são apresentados os seus objectivos e organização.

Interligação 3GPP-WLAN Apresenta o estudo feito sobre o tema da dissertação. Numa primeira parte são identificados vários cenários de integração entre as redes 3G e WLAN identificados pelo 3GPP. Na secção seguinte é descrita a arquitectura proposta pelo 3GPP e detalhados os seus componentes e interfaces. Por fim são apresentados alguns casos de uso.

Desenvolvimento da solução Este capitulo contém todos os detalhes relativos ao requisitos, arquitectura e concepção da solução.

Validação da solução Contém o resultados e análise dos testes efectuados à solução implementada.

Conclusão Neste capítulo são apresentadas as principais conclusões acerca da dissertação e discutido algum trabalho futuro.

Capítulo 2

Interligação 3GPP-WLAN

2.1 Introdução

Neste capítulo será apresentado o estado da arte relativamente ao tema de integração das redes 3G e WLAN (3GPP-WLAN *Interworking* ou I-WLAN) com base em diversos estudos já efectuados sobre o tema ([2], [3], [4] e [5]) e nas normas propostas pela entidade 3GPP (*Release* 8). Inicialmente serão descritos seis cenários de integração que foram identificados por um estudo realizado pelo 3GPP [7]. De seguida será apresentada a arquitectura de referência proposta também pelo 3GPP com todos os componentes que fazem parte desta e as interfaces entre eles. Por fim serão apresentados alguns casos de uso do sistema.

2.2 Cenários de integração

Em [7] foram identificados diversos requisitos e descritos seis cenários de integração entre redes 3G e WLAN. Cada cenário é uma evolução do anterior na integração das duas redes. Esta evolução parte de um cenário em que praticamente não existe integração até ao cenário em que os serviços da rede 3G são disponibilizados sem limitações aos utilizadores WLAN.

2.2.1 Cenário 1 – Tarifação e atendimento comuns

Este é o nível de integração mais simples. O utilizador recebe do operador credenciais específicas para aceder à rede WLAN. Apenas o serviço de atendimento e de tarifação são partilhados pelos

dois tipos de acesso, por outras palavras, apenas o serviço de apoio ao cliente e a factura final são comuns. Não existe integração real entre as duas redes.

Este cenário não acrescenta nenhum requisito novo e por isso está fora do âmbito das especificações do 3GPP.

2.2.2 Cenário 2 – Controlo de acesso e contabilização sob o sistema 3GPP

Neste cenário a autenticação, autorização e *accounting* para o acesso WLAN são fornecidos pelo sistema 3G, aplicando desta forma os mecanismos de segurança do sistema 3G à WLAN. Neste cenário o utilizador terá que possuir uma carta WLAN equipada com um UICC (cartão SIM ou USIM) associado à sua conta 3G. O utilizador não nota diferenças significativas na forma em que o acesso é disponibilizado, à excepção de não possuir e ter de inserir credenciais específicas para aceder à WLAN, a sua identificação é realizada com base no SIM ou USIM.

Este cenário permite aos utilizadores terem conectividade IP via WLAN (*WLAN Direct IP Access*) e ao operador uma gestão mais simples dos clientes nas duas redes.

2.2.3 Cenário 3 – Acesso aos serviços *Packet Switched* do sistema 3GPP

O objectivo deste cenário é permitir ao utilizador WLAN aceder a serviços baseados em *Packet Switched* (PS) (ex. IMS, MMS, *Instant Messaging*) da rede 3G. Este processo foi denominado "*WLAN 3GPP IP Access*". Os serviços aos quais o utilizador WLAN poderá aceder serão definidos pelo operador.

Neste cenário não existe continuidade dos serviços entre as duas redes, ou seja, quando o utilizador comuta da rede 3G para a WLAN, ou vice-versa, todas as sessões activas irão ser terminadas. Actualmente as normas do 3GPP (*Release* 8) estão definidas de forma a suportar este cenário.

2.2.4 Cenário 4 – Continuidade dos serviços

O objectivo deste cenário é permitir a possibilidade de comutação entre as duas redes sem exista falha no fornecimento dos serviços referidos no cenário anterior. A comutação do serviço entre redes poderá ser notada pelo utilizador (ex. interrupção na transferência dos dados), no entanto, não existe a necessidade de intervenção manual para restabelecer o serviço. Como exemplo

temos uma ligação ftp iniciada na rede WLAN e transferida para a rede 3G, sem necessidade de reiniciar a ligação ftp.

A qualidade de serviço poderá sofrer mudanças devido à diferença de capacidades e características das duas redes por exemplo, taxas de transferência mais baixas quando o serviço fornecido inicialmente sobre a rede WLAN passa a ser fornecido pela rede 3G. Para que este cenário seja possível é necessário criar mecanismos de *handover*.

2.2.5 Cenário 5 – Continuidade dos serviços sem interrupção

O objectivo deste cenário é permitir a continuidade dos serviços tal como no cenário anterior, no entanto, a transição entre redes não deverá ser perceptível ao utilizador. Deste modo, a perda de pacotes e o tempo de *handover* deverão ser mínimos para não causar disrupção dos serviço.

2.2.6 Cenário 6 – Acesso aos serviços *Circuit Switched*

Este cenário permite o acesso aos serviços *Circuit Switched* (CS) da rede 3G, como por exemplo chamadas de voz, através da WLAN. A comutação entre redes deverá ser imperceptível ao utilizador.

2.3 Arquitectura

O *European Telecommunications Standards Institute* (ETSI) especificou duas aproximações genéricas de integração entre as redes WLAN e 3G denominadas *tight coupling* e *loose coupling* [13]. As duas soluções diferem no nível de integração requerido entre as duas redes.

Na arquitectura *tight coupling* a WLAN está directamente ligada à rede 3G obrigando a que todo o tráfego passe obrigatoriamente por a rede 3G, por outras palavras, a rede 3G passa a ser a rede core para a WLAN. Nesta arquitectura há necessidade de efectuar alterações na rede 3G de forma a suportar maiores taxas de transmissão e por isso é pouco apelativa. A vantagem desta arquitectura é que a WLAN seria vista como outro meio de acesso e por isso a mobilidade entre redes seria simplificada e seria possível garantir a Qualidade de Serviço (*Quality of Service* - QoS).

Na arquitectura *loose coupling* as WLANs são implementadas como uma rede de acesso

complementar aos sistemas do 3GPP, sendo operadas de forma independente. Nesta arquitectura apenas a base de dados dos utilizadores é partilhada não sendo necessárias grandes alterações na rede. O tráfego é enviado directamente para a rede IP. A desvantagem nesta arquitectura é que os problemas relacionados com o *handover* (ex. latência, perda de pacotes) são mais notados.

A arquitectura adoptada pelo 3GPP é baseada em *loose coupling* e está descrita na norma [9]. Neste documento podemos encontrar os componentes e interfaces necessários para que a integração entre redes WLAN e 3GPP seja possível.

2.3.1 Modelos de referência

Na norma 3GPP TS 23.234 [9] estão definidos três modelos de referência de forma a suportar os cenários 1, 2 e 3. Na secção 2.4 e 2.5 encontra-se, respectivamente, uma descrição mais detalhada dos vários componentes e interfaces respectivamente.

Modelo de referência *Non-Roaming*

Na Figura 2.1 está representado o modelo de referência mais simples onde o utilizador se liga a uma rede de acesso WLAN que está directamente ligada à *Home Network* do seu operador.

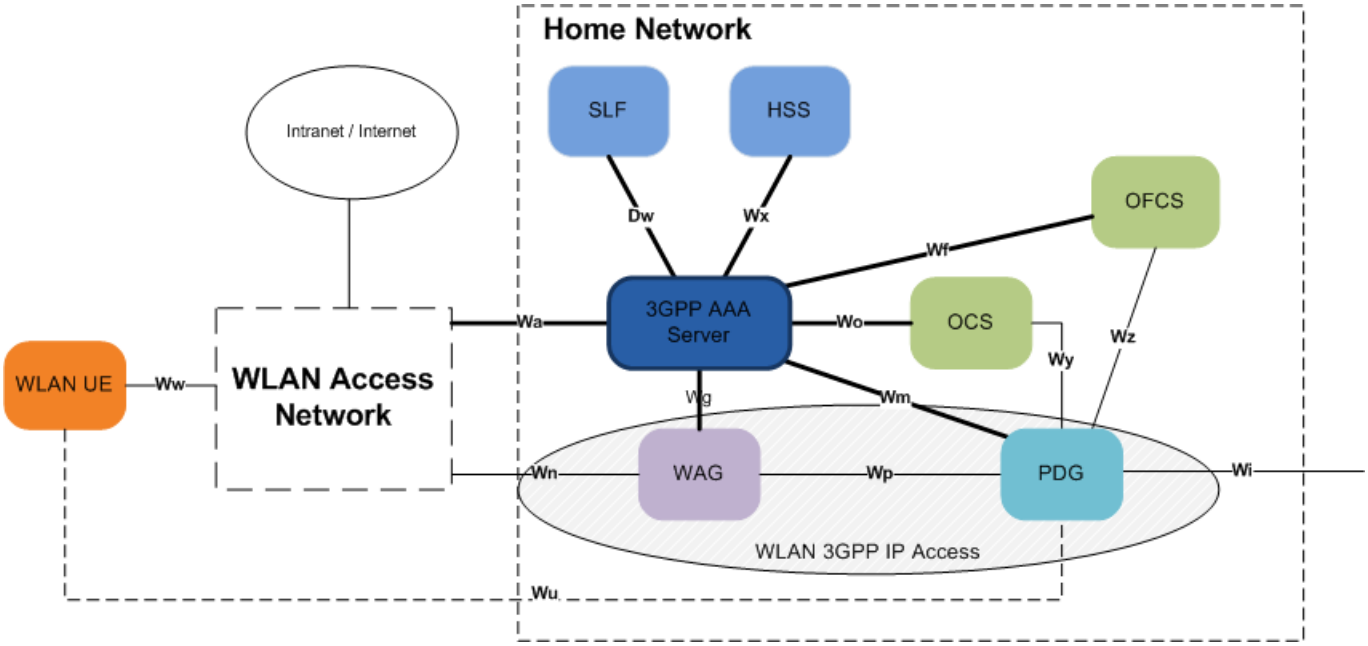

Figura 2.1: Modelo de Referência *Non-Roaming*

Modelo de referência *roaming*

Na Figura 2.2 e Figura 2.3 estão representados os modelos de referência para o cenário em que o utilizador se encontra em *roaming* e a rede de acesso WLAN à qual se liga não está directamente ligada à *Home Network* do seu operador. Em ambos os casos a *Home Network* faz o controlo de acesso à WLAN e a informação relativa ao *charging* poderá ser gerada na *Home* e/ou na *Visited Network*. Os dois modelos contemplam o caso dos serviços PS serem disponibilizados pela *Home* ou pela *Visited Network*.

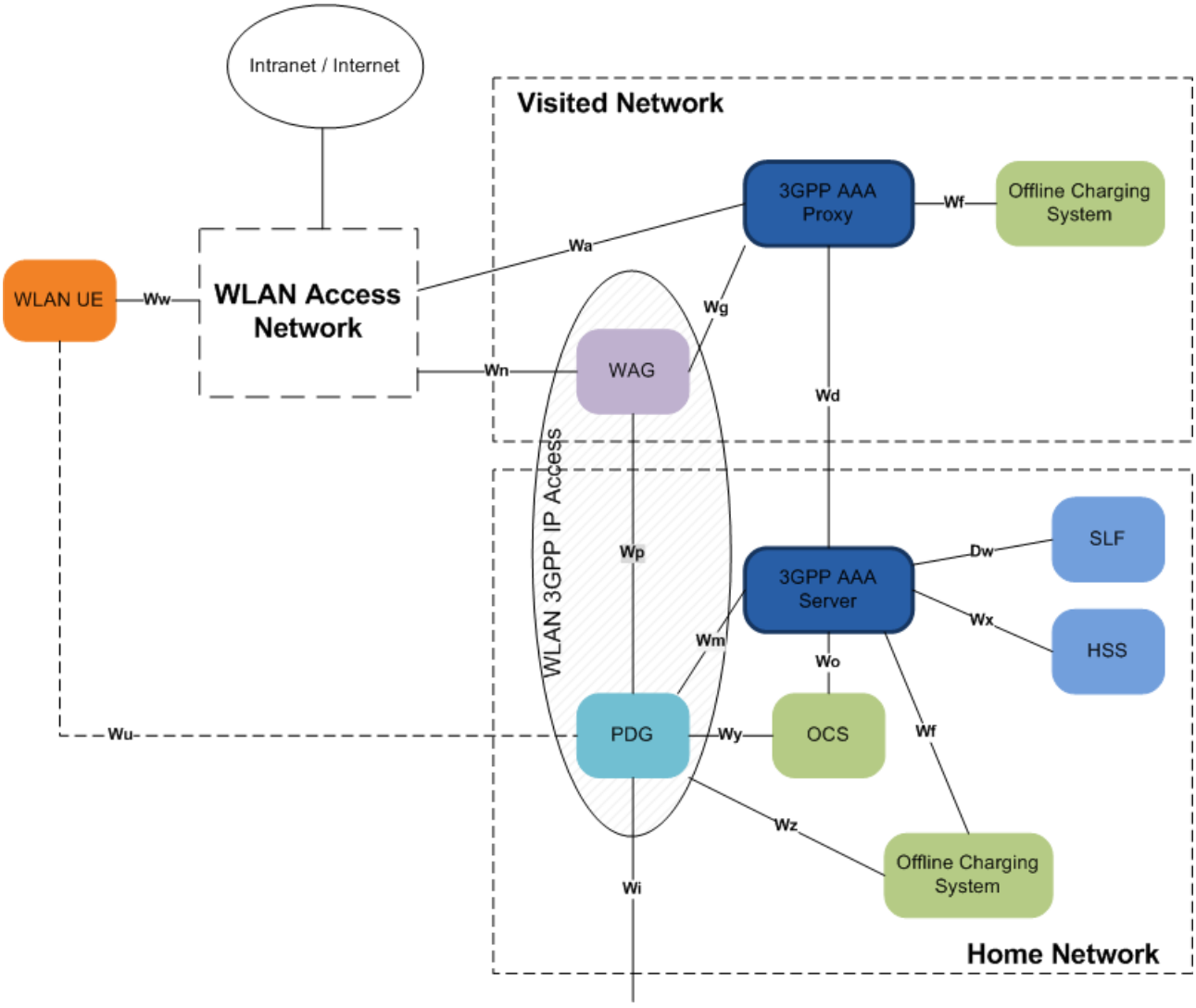

Figura 2.2: Modelo de Referência *roaming* (1)

Neste caso os serviços baseados em PS são disponibilizados pela *Home Network*.

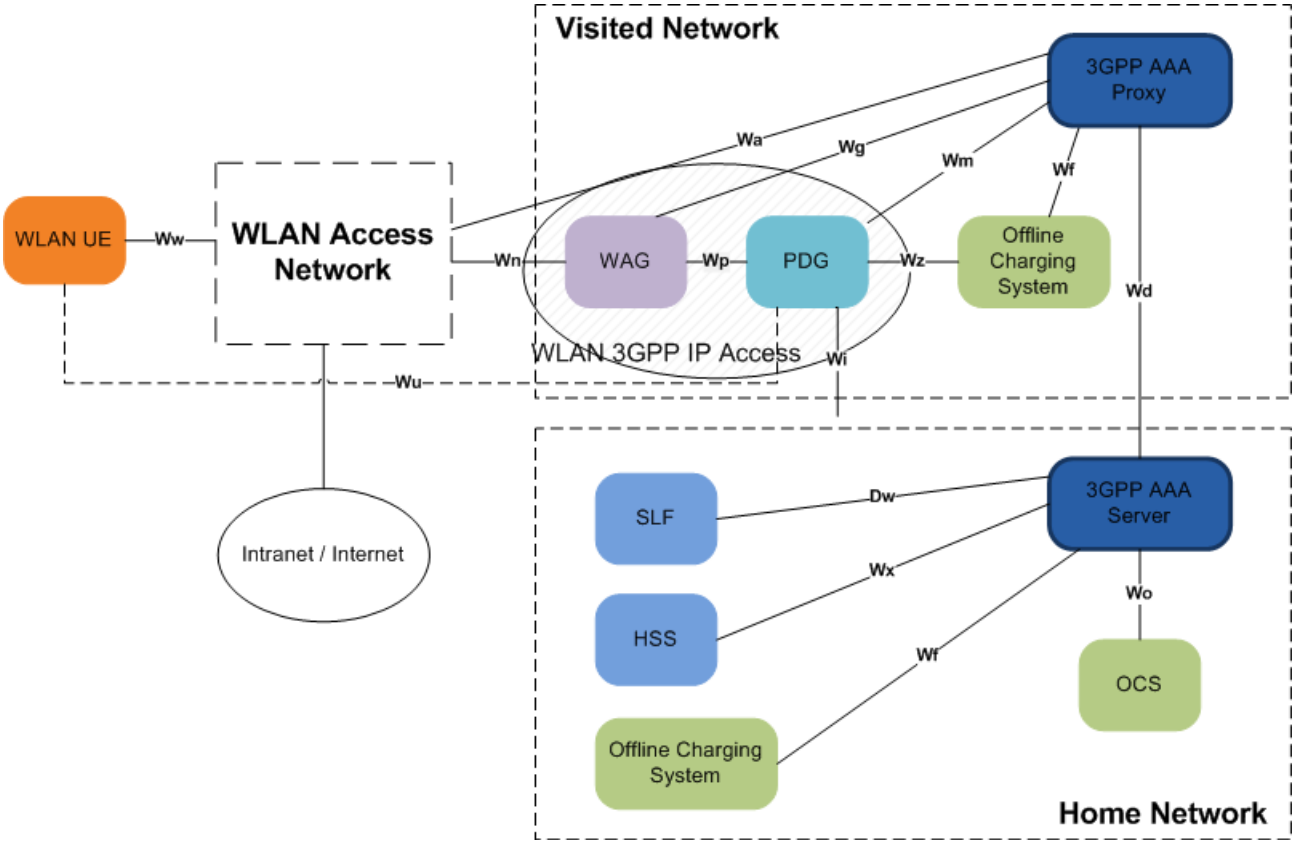

Figura 2.3: Modelo de Referência *roaming* (2)

Neste caso os serviços baseados em PS são disponibilizados pela *Visited Network*.

2.4 Componentes

2.4.1 WLAN UE

O WLAN UE é o equipamento do utilizador (*smart phone, laptop*, PDA, etc) que contém uma carta de rede WLAN (WLAN NIC). Esta deverá possuir um leitos de cartão SIM ou USIM, que armazena a informação do utilizador (UICC), de forma a permitir o acesso à WLAN com o propósito de integração com a rede 3G. Este equipamento poderá permitir o acesso apenas à WLAN ou simultaneamente a WLAN e 3G e poderá estar ligado à *Home Network* (HN) ou a uma *Visited Network* (VN).

Cada equipamento é identificado pelo IMSI (presente no (U)SIM) e pelo endereço físico da carta WLAN (MAC Address). Para aceder à WLAN o UE necessita de uma conta, sendo que esta é representada pelo *Network Access Identifier* (NAI) que permite identificar o utilizador e a *Home Network*.

O WLAN UE deverá permitir autenticação utilizando o protocolo EAP (SIM ou AKA conforme seja um utilizador GSM ou UMTS), gerar W-APNs [14] de acordo com as normas, obter o endereço do PDG a partir do W-APN e criação de túneis IPSec com o PDG. A descrição de todas as funcionalidades do WLAN UE pode ser consultada em [15].

2.4.2 *3GPP AAA Server*

O *3GPP AAA Server* está localizado na *Home Network*. Realiza as funções de autenticação, autorização e *accounting* de utilizadores WLAN e de túneis do *Packet Data Gateway* (PDG). O *3GPP AAA Server* funciona como um EAP *Authenticator*.

Durante o processo de autenticação e autorização de cada utilizador, o *3GPP AAA Server* requisita informação de autenticação e perfil do utilizador ao HSS. Depois de o utilizador estar correctamente autenticado e autorizado, o *3GPP AAA Server* envia para a WLAN AN informações de autorização e para o WAG as políticas de *routing*.

Quando o perfil do utilizador é alterado no HSS, o *3GPP AAA Server* é notificado sendo responsável por propagar as alterações necessárias a todos os componentes. Estas alterações podem eventualmente levar ao término da sessão de um utilizador ou a uma re-autorização.

O *3GPP AAA Server* poderá ter que gerar informação relativa a *charging online* e *offline* caso a rede de acesso WLAN não suporte esta funcionalidade. Pode também actuar como um *3GPP AAA Proxy*, encaminhando as mensagens para outro servidor.

2.4.3 *3GPP AAA Proxy*

O *3GPP AAA Proxy* está localizado na *Visited Network*. A sua principal função é transmitir a informação proveniente da WLAN AN, do PDG e do WAG para o *3GPP AAA Server* e vice-versa. Permite também o acesso aos W-APNs da *Visited Network* de acordo com as políticas locais.

Poderá haver a necessidade do *3GPP AAA Proxy* fazer a conversão entre os protocolos

RADIUS[16] e Diameter[17] na interface Wd quando a rede de acesso WLAN apenas suporta RADIUS.

2.4.4 *Home Subscriber Server* (HSS)

O HSS está localizado na *Home Network* e contém dois componentes distintos:

- *Home Location Register* (HLR) que consiste numa base de dados dos utilizadores. Esta possui informação sobre a identificação, perfil, localização e *charging* dos utilizadores que será usada por diversos serviços.
- *Authentication Centre* (AuC) utilizado para autenticar e autorizar os utilizadores. Este componente guarda as credenciais de segurança e gera os vectores de autenticação, designados *triplets* e *quintuplets*, que serão utilizados pelos protocolos EAP-SIM e EAP-AKA.

Quando um utilizador WLAN se liga e o processo de autenticação e autorização é concluído com sucesso, o *3GPP AAA Server* guarda no HSS informação de sessão relativa ao utilizador como por exemplo informação de estado, endereço IP, nome do *3GPP AAA Server*, etc.

2.4.5 *Subcription Locator Function* (SLF)

O SLF está localizado na *Home Network* e permite ao *3GPP AAA Server* encontrar o endereço do HSS que contém a informação do utilizador, num cenário onde são utilizados vários HSS. O 3GGP AAA dirige em primeiro o pedido ao SLF e este responde com o redireccionamento para o HSS que contém esse informação desse utilizador.

2.4.6 *WLAN Access Gateway* (WAG)

O WAG está localizado na *Visited Network* no caso de o utilizador se encontrar em *roaming* e na *Home Network* caso contrário. É o *gateway* para o qual os dados da WLAN AN devem ser enviados para que se consiga disponibilizar os serviços baseados em PS da rede 3GPP.

Durante o processo de autenticação e autorização de utilizadores WLAN, o *3GPP AAA Server* envia ao WAG políticas de encaminhamento para que este possa realizar as suas principais funções que são:

- *Routing enforcement*, que consiste em encaminhar o tráfego para o PDG apropriado que pode estar na *Home* ou na *Visited Network*, dependendo das políticas locais e do serviço ao qual o utilizador está a tentar aceder;

- *Policy enforcement*, funcionando de forma semelhante a uma *firewall* garantindo que apenas tráfego autorizado é enviado. O tráfego poderá ser filtrado por IP, protocolo, porto e direcção (entrada ou saída).

2.4.7 *Packet Data Gateway* (PDG)

O PDG pode estar situado na *Visited Network* ou na *Home Network* dependendo das políticas locais. A sua principal funcionalidade é terminar os túneis que são estabelecidos a partir do WLAN UE. O conceito destes túneis é similar às APNs (*Access Point Name*) nas redes GPRS/UMTS e, por este motivo, são denominados por W-APNs (WLAN APN). Quando um utilizador pretende aceder a um serviço da rede 3G uma W-APN é activada e é estabelecido um túnel IPSec a partir do equipamento do utilizador para o PDG. Um utilizador pode ter mais que uma W-APN no ser perfil, podendo estas ser activadas simultaneamente. Durante o processo de estabelecimento de uma W-APN, o PDG contacta o servidor 3GPP AAA a fim de efectuar a sua autenticação, aceitando ou rejeitando a W-APN de acordo com a decisão do *3GPP AAA Server*.

O PDG tem também a função de gerar informação de *charging offline* e *online* que permite contabilizar a utilização do acesso WLAN 3GPP IP e poderá fazer *Policy Control* (ex. controlo de QoS por serviço) de acordo com TS 23.203 [18].

2.4.8 *Online Charging System* (OCS)

Existem dois tipos de cobranças nas redes 3G: o pré-pago onde o cliente compra créditos que depois serão gastos conforme a sua utilização e o pós-pago onde o cliente é cobrado pela utilização dos serviços passado um período de tempo estipulado. A cobrança poderá ser feita por tempo, volume de dados, etc.

A gestão dos créditos dos clientes pré-pagos deverá ser feita em tempo real (*online*) e para isso foi introduzido na rede o *Online Charging System*. A informação relativa a *online charging* que chega da WLAN AN ou PDG ao *3GPP AAA Server* é reenviada para o OCS, este irá responder permitindo ou negando o pedido conforme o crédito do cliente. Este componente

encontra-se localizado na *Home Network*. É responsável por realizar o controlo, em tempo real, do acesso aos serviços do operador, pelo que existe apenas no operador ao qual o cliente pertence.

2.4.9 *Offline Charging System* (OFCS)

A informação relativa ao *offline charging* obtida nos diferentes componentes (3GPP AAA ou PDG) é enviada para o *Offline Charging System*, na forma de mensagens de *accounting*. Este componente está localizado na *Home Network* e poderá também existir na *Visited Network*. É responsável pela geração que CDRs que permitam ao operador realizar a taxação do cliente após os serviços terem sido consumidos (pós-pago). Pode servir também para o operador visitado poder gerar CDRs para efeitos de confrontação com o operador de origem.

2.5 Interfaces

Nos modelos de referência podemos ver várias interfaces entre os diversos componentes, com diversas funcionalidades distintas que serão descritas nesta secção. Uma descrição mais detalhada das funcionalidades de cada interface pode ser encontrada em [9].

A maior parte das interfaces directamente ligadas ao *3GPP AAA Server* deverão suportar o protocolo RADIUS [16] e/ou Diameter [17]. Nesta dissertação foi apenas focado o protocolo Diameter pois é uma evolução do RADIUS e é o protocolo de eleição sugerido pelas normas. O Diameter Base [17] é um protocolo que contém os requisitos mínimos para autenticação autorização e *accounting*, no entanto, existem diversas *Diameter Applications* (ex. EAP [19], NASREQ [20] e Credit-Control [21]) que estendem o protocolo base adicionando novos comandos e/ou atributos. A descrição dos protocolos e procedimentos que cada interface deverá suportar encontra-se em [10].

2.5.1 Interface Wa

Interface entre a WLAN AN e o *3GPP AAA Server/Proxy*.

O principal objectivo desta interface é transportar informação de autenticação, autorização e *accounting* de forma segura. Para isto deverá suportar o protocolo RADIUS com extensões que permitam transportar frames EAP, desligar utilizadores, etc., e o protocolo Diameter que

para além do protocolo base deverá suportar as Aplicações Diameter EAP, NASREQ e Credit-Control.

A implementação do protocolo RADIUS nesta interface tem o objectivo suportar um maior número de WLAN ANs, no entanto, é esperado que as WLAN ANs evoluam para o protocolo Diameter. Na descrição dos procedimentos desta interface apenas serão mencionadas as mensagens utilizadas no protocolo Diameter. De forma a garantir a interoperabilidade com redes WLAN *legacy*, poderá ser usado um *gateway* protocolar RADIUS-Diameter, entre a rede WLAN e o 3GPP AAA.

Procedimentos

WLAN Access Authentication and Authorization

Este procedimento é utilizado para transportar entre a WLAN AN e o *3GPP AAA Server/Proxy* a informação relativa à autenticação, re-autenticação e autorização. Neste procedimento são utilizadas as mensagens Diameter-EAP-Request e Diameter-EAP-Answer definidas em [19], sendo que estas mensagens irão conter os pacotes EAP encapsulados.

Immediate Purging of a User from WLAN Access

Este procedimento é usado pelo *3GPP AAA Server* para comunicar à WLAN AN que um determinado WLAN UE deverá ser desligado do serviço I-WLAN.

Neste procedimento são utilizadas as mensagens Abort-Session-Request e Abort-Session-Answer definidas em [20].

Ending a Session

Este procedimento é usado pela WLAN AN para comunicar ao *3GPP AAA Server* que um determinado utilizador se desligou.

Neste procedimento são utilizadas as mensagens Session-Termination-Request e Session-Termination-Answer definidas em [20].

WLAN Access Authorization Information Update Procedure

O procedimento de actualização da informação de acesso é utilizado para modificar os parâmetros de autorização fornecidos à WLAN AN. Este procedimento é utilizado pelo *3GPP AAA Server* quando a informação de autorização é modificada (por exemplo modificação do perfil do utilizador no HSS) e é necessário fazer a actualização na WLAN AN. O procedimento

de actualização deverá dar origem a um novo procedimento de autenticação e autorização no WLAN UE.

Neste procedimento são utilizadas as mensagens Re-Auth-Request e Re-Auth-Answer definidas em [20].

Offline Accounting

Este procedimento é utilizado para transportar informação de *offline charging* entre a WLAN AN e o *3GPP AAA Server/Proxy*.

Neste procedimento são utilizadas as mensagens Accounting-Request e Accountging-Answer definidas em [19].

Online Charging

Este procedimento é utilizado para transportar informação de *online charging* entre a WLAN AN e o *3GPP AAA Server/Proxy*.

Neste procedimento são utilizadas as mensagens AA-Request e AA-Answer definidas em [17].

2.5.2 Interface Wx

Interface entre o *3GPP AAA Server* e o HSS. O objectivo desta interface é permitir operações entre os dois componentes, tais como:

- Obter do HSS os vectores de autenticação e perfil do utilizador;
- Registar/remover o estado dos utilizadores I-WLAN no HSS;
- Notificar alterações no perfil do utilizador.

Esta interface deverá suportar o protocolo *Diameter Application for Cx interface* definido em [22].

Procedimentos

Authentication Procedures

Este procedimento é iniciado pelo *3GPP AAA Server* quando é necessário obter informação do HSS necessária para realizar a autenticação de um determinado utilizador. A informação contida na resposta do HSS varia conforme o protocolo utilizado (EAP-SIM ou EAP-AKA).

Neste procedimento são utilizadas as mensagens Multimedia-Auth-Request e Multimedia-Auth-Answer definidas em [22].

WLAN Registration/DeRegistration Notification

Este procedimento é iniciado pelo *3GPP AAA Server* para registar um novo utilizador, para remover o registo ou para obter o perfil de um utilizador.

Neste procedimento são utilizadas as mensagens Server-Assignment-Request e Server-Assignment-Answer definidas em [22].

Network Initiated De-Registration by HSS, Administrative

Este procedimento é usado pelo HSS quando um determinado utilizador deve ser desligado por algum motivo.

Neste procedimento são utilizadas as mensagens Registration-Termination-Request e Registration-Termination-Answer definidas em [22].

HSS Initiated Update of User Profile

Este procedimento é utilizado pelo HSS quando o perfil de um utilizador é modificado e precisa de ser enviado para o *3GPP AAA Server* para que este tome as medidas necessárias consoante as modificações.

Neste procedimento são utilizadas as mensagens Push-Profile-Request e Push-Profile-Answer definidas em [22].

2.5.3 Interface Wg

Interface entre o WAG e o *3GPP AAA Server* ou Proxy dependendo se o WAG se encontra na *Home* ou na *Visited Network* respectivamente. A sua principal função é permitir a inserção e remoção de *routing policies* no WAG.

Esta interface deverá suportar o protocolo Diameter base e Diameter NASREQ.

Procedimentos

Policy Download Procedures

Este procedimento é usado pelo *3GPP AAA Server* para enviar para o WAG as políticas de *routing*, relativas a um determinado utilizador.

Neste procedimento são utilizadas as mensagens AA-Request e AA-Answer definidas em [19].

Routing Policy Cancellation Procedure

Este procedimento é utilizado pelo *3GPP AAA Server* quando este pretende remover do WAG as políticas de *routing* de um determinado utilizador.

Neste procedimento são utilizadas as mensagens Abort-Session-Request e Abort-Session-Answer definidas em [20].

WAG Initiated Routing Policy Cancellation Procedure

Este procedimento é executado pelo WAG quando uma sessão específica foi removida do WAG sem que tenha sido usado o procedimento "*Routing Policy Cancellation Procedure*".

Neste procedimento são utilizadas as mensagens Session-Termination-Request e Session-Termination-Answer definidas em [20].

2.5.4 Interface Wm

Interface entre o *3GPP AAA Server/Proxy* e o PDG que permite autenticar, autorizar e remover túneis iniciados pelo WLAN UE.

Esta interface deverá suportar os protocolos Diameter EAP para autenticação, Diameter NASREQ para autorização e Diameter Base para remoção de túneis.

Procedimentos

Authentication Procedure

Este procedimento é iniciado pelo PDG quando recebe do WLAN UE um pedido de estabelecimento de um túnel. É utilizado para autenticar o utilizador que pretende estabelecer o túnel.

Neste procedimento são utilizadas as mensagens Diameter-EAP-Request e Diameter-EAP-Answer definidas em [19].

Autorization Procedure

Este procedimento é executado pelo PDG depois do "*Authentication Procedure*" estar concluído com sucesso. É utilizado para autorizar um determinado túnel.

Neste procedimento são utilizadas as mensagens AA-Request e AA-Answer definidas em [19].

PDG Initiated Session Termination Procedure

Este procedimento é usado pelo PDG quando um túnel associado a um determinado W-APN é desligado por parte do utilizador.

Neste procedimento são utilizadas as mensagens Session-Termination-Request e Session-Termination-Answer definidas em [20].

***3GPP AAA Server* Initiated Tunnel Disconnect Procedure**

Este procedimento é executado pelo *3GPP AAA Server* quando um determinado túnel deve ser desligado no PDG por iniciativa do 3GPP AAA.

Neste procedimento são utilizadas as mensagens Abort-Session-Request e Abort-Session-Answer definidas em [20].

Access and Service Authorization information Update Procedure

Este procedimento é usado pelo *3GPP AAA Server* quando há uma actualização no perfil do utilizador no HSS e é necessário voltar a autorizar os túneis activos.

Neste procedimento são utilizadas as mensagens Re-Auth-Request e Re-Auth-Answer definidas em [20].

Depois deste pedido o PDG inicia novamente o "*Autorization Procedure*".

2.5.5 Interface Wd

Este interface liga o *3GPP AAA Proxy* ao *3GPP AAA Server*, possivelmente por redes intermédias. O objectivo desta interface é transportar informação de autenticação, autorização e accounting de forma segura.

O *3GPP AAA Proxy* reenvia por esta interface todas as mensagens que lhe chegam com

destino ao *3GPP AAA Server*.

Esta interface deverá suportar o protocolo Diameter Base e as Diameter Applications EAP, NASREQ e Credit-Control e deverá suportar todos os procedimentos definidos para as interfaces Wa, Wg e Wm.

2.5.6 Interface Wo

Interface entre o *3GPP AAA Server* e o OCS utilizada para transportar informação relativa a *online charging* para isso deverá suportar a Diameter Credit-Control Application.

Procedimentos

Online Charging

Este procedimento é utilizado para enviar do *3GPP AAA Server* para o OCS informação de *online charging*. Para isto são utilizadas as mensagens Credit-Control-Request e Credit-Control-Answer definidas em [21].

2.5.7 Interface Wf

Interface entre o *3GPP AAA Server/Proxy* e o OFCS utilizada para transportar informação relativa a *offline charging* para isso deverá suportar o protocolo Diameter base.

Procedimentos

Offline Accounting

Este procedimento é utilizado para enviar do *3GPP AAA Server/Proxy* para o OFCS informação de *offline charging*. Para isto são utilizadas as mensagens Accounting-Request e Accounting-Answer definidas em [20].

2.5.8 Interface Ww

Interface entre o WLAN UE e a WLAN AN utilizando IEEE 802.1x ou outro sistema de acesso.

Esta interface deverá suportar os protocolos IKEv2 [23] e EAP-SIM [24] ou EAP-AKA [25].

Procedimentos

WLAN Access Authentication and Authorization

Este procedimento é utilizado para autenticar e autorizar um WLAN UE. Ao receber uma mensagem de EAP-Request da rede o WLAN UE envia uma EAP-Response com a sua identificação. A rede voltará a enviar um EAP-Request e o WLAN UE deverá enviar a sua identificação e os dados de autenticação.

O número de mensagens trocadas no decorrer deste procedimento varia conforme o protocolo utilizado (EAP-SIM ou EAP-AKA).

WLAN Re-Authentication

Este procedimento invocado pela WLAN AN com o objectivo de re-autenticar o WLAN UE.

A WLAN AN envia ao WLAN UE uma das seguintes mensagens: EAP-Request/AKA-Challenge, EAP-Request/AKA-Reauthentication, EAP-Request/SIM-Challenge ou EAP-Request/SIM-Reauthentication. O WLAN UE responde com um EAP-Response contendo a sua identificação e informação de autenticação.

WLAN UE Initiated Tunnel Establishment

Este procedimento é executado pelo WLAN UE quando pretende iniciar um túnel com o PDG de forma a aceder a uma determinada W-APN. Para isso, o WLAN UE envia ao PDG a mensagem IKE-AUTH-REQ contendo a sua informação assim como a W-APN ao qual pretende aceder. O PDG responde com um IKE-AUTH-RESP.

WLAN UE Initiated Tunnel Disconnection

Este procedimento é usado pelo WLAN UE quando pretende desligar um túnel no PDG. Para isso o WLAN UE envia ao PDG a mensagem IKE INFORMATIONAL com DELETE no *payload*, ao que o PDG responde com IKE INFORMATIONAL RESPONSE.

PDG Initiated Tunnel Disconnection

Este procedimento é invocado pelo PDG quando pretende desligar um túnel. Para isso o PDG envia ao WLAN UE a mensagem IKE INFORMATIONAL com DELETE no *payload*, e o WLAN UE responde com IKE INFORMATIONAL RESPONSE.

2.5.9 Interface Wn

Interface entre a WLAN AN e o WAG. O objectivo desta interface é forçar o tráfego dos túneis iniciados no WLAN UE a passar pelo WAG.

Esta interface deverá suportar o protocolo IKEv2 [23]. Deverá ainda suportar os procedimentos "*WLAN UE Initiated Tunnel Establishment*", "*WLAN UE Initiated Tunnel Disconnection*" e "*PDG Initiated Tunnel Disconnection*" definidos para a interface Ww.

2.5.10 Interface Wp

Interface entre o WAG e o PDG.

Esta interface deverá suportar o protocolo IKEv2 [23]. Deverá ainda suportar os procedimentos "*WLAN UE Initiated Tunnel Establishment*", "*WLAN UE Initiated Tunnel Disconnection*" e "*PDG Initiated Tunnel Disconnection*" definidos para a interface Ww.

2.5.11 Interface Wz

Interface entre o PDG e o *Offline Charging System* que permite transportar informação relativa a *offline charging*. Esta interface deverá suportar o protocolo Diameter base.

Na *Release* 8 das normas 3GPP ainda não está completamente definido o funcionamento desta interface, obrigando a que a informação relativa a *offline charging* gerada no PDG seja enviada para o *3GPP AAA Server* pela interface Wm e só posteriormente o *3GPP AAA Server* a reenviar para o OFCS utilizando a interface Wf.

2.5.12 Interface Wi

Interface entre o PDG e a *Packet Data Network* (PDN).

Esta interface é semelhante à interface Gi do domínio PS e é baseada em IP. Os serviços oferecidos via esta interface podem ser globalmente endereçados pelo sistema de endereçamento público do operador ou através de um sistema de endereçamento privado.

2.5.13 Interface Wu

Interface entre o WLAN UE e o PDG.

Esta interface representa o túnel estabelecido entre o WLAN UE e o PDG. O transporte do tráfego nesta interface é fornecido pelas interfaces Ww, Wn e Wp, fazendo com que o tráfego passe pelo WAG onde são aplicadas políticas de *routing*.

2.5.14 Interface Dw

Interface entre o *3GPP AAA Server* e o SLF que permite ao *3GPP AAA Server* obter o endereço do HSS que contém a informação de um determinado utilizador num cenário com vários HSSs.

2.6 Casos de uso

Analisando os requisitos do *3GPP AAA Server*, que teve especial foco neste estudo, foram identificados alguns casos de uso que envolvem a utilização de procedimentos de várias interfaces. O conteúdo das mensagens trocadas entre os vários componentes poderá ser visto em [10].

2.6.1 Autenticação e Autorização WLAN

Devido à natureza das WLANs existem diversas preocupações relativamente à segurança (ex. fácil captura e injecção de tráfego) e por isso é necessário que existam mecanismos que garantam a protecção da identidade, integridade e confidencialidade dos dados. Para este fim o 3GPP decidiu que para autenticar os utilizadores deverá ser utilizado o protocolo *Extensible Authentication Protocol* (EAP) [26]. O EAP é uma *framework* de autenticação fim-a-fim que disponibiliza funções comuns e negociação para diversos mecanismos de autenticação utilizando um método *challenge-response*.

No caso da autenticação de utilizadores WLAN são utilizados dois mecanismos distintos que deverão ser suportados por o WLAN UE e por o *3GPP AAA Server*:

- O *EAP for UMTS Authentication and Key Agreement* (EAP-AKA) [25] empregado para autenticar os utilizadores *Universal Mobile Telecommunications System* (UMTS)

utilizando o *Universal Subscriber Identity Module* (USIM).

- O *EAP for GSM Subscriber Identity* (EAP-SIM) [24] usado para autenticar os utilizadores *Global System for Mobile Communications* (GSM) utilizando o *Subscriber Identity Module* (SIM).

Os dois mecanismos garantem autenticação mutua entre o WLAN UE e o *3GPP AAA Server* através de uma chave privada (*Master Session Key*) que será gerada durante o processo de autenticação.

Identity

A identidade do utilizador que irá ser usada pelo protocolo EAP é baseada no *Network Access Identifier* (NAI), cujo formato está especificado em [27]. O NAI é composto por duas partes, o nome do utilizador (*username*) e o domínio (*realm*).

O *username* pode ser de três tipos:

- *Permanent username* - Derivado a partir do International Mobile Subscriber Identity (IMSI) [14] e permite identificar o utilizador. Está guardado no SIM/USIM.
- *Pseudonym username* - Utilizado para proteger a identidade do utilizador. Este username é gerado pelo 3GPP AAA Server e consiste no IMSI cifrado utilizando o *Advanced Encryptation Standard* (AES) [28] em modo *Electronic Code Book* (ECB) com uma chave de 128 bits. O *3GPP AAA Server* envia este *username* para o WLAN UE durante o processo de autenticação. A partir desse momento o WLAN UE deverá passar a usar esta identificação aumentando assim a protecção da sua identidade.
- *Fast re-authentication username* - Semelhante ao *Pseudonym username* mas apenas utilizado para re-autenticação rápida.

O *realm* deverá ter o formato especificado em [29] e permite identificar a *Home Network* do utilizador.

EAP-AKA

No processo de autenticação e autorização de utilizadores WLAN utilizando o protocolo EAP-AKA é utilizado o mecanismo AKA [30] já existente para o UMTS. Este mecanismo permite

gerar diferentes chaves que irão garantir a autenticação e segurança da transmissão de dados entre o *3GPP AAA Server* e o WLAN UE. Quando um utilizador se pretende autenticar o *3GPP AAA Server* pede ao HSS um vector de autenticação (AV) que consiste em cinco valores: RAND, XRES, CK, IK e AUTN. Para mais informações sobre estes valores deverá ser consultada a referência [31].

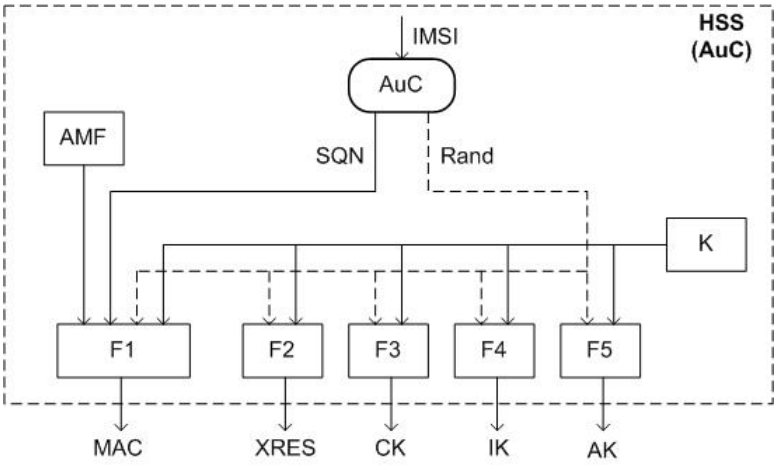

Figura 2.4: Protocolo AKA (HSS)

A Figura 2.4 representa a geração dos vários valores no HSS (AuC). Inicialmente o AuC obtém quatro valores para um determinado utilizador:

RAND Valor aleatório gerado pelo AuC;

***Sequence Number* (SQN)** Gerado pelo AuC para evitar ataques de *replay*;

***Authentication Management Field* (AMF)** Informação sobre a janela de sincronização entre o WLAN UE e a rede;

***Master Key* (K)** Chave privada do utilizador que está guardada no AuC e no USIM.

Estes valores são passados como parâmetros de acordo com a Figura 2.4 às funções F1, F2, F3, F4 e F5. Todas estas funções estão no AuC e no USIM e são privadas variando em cada operador.

Os valores obtidos são:

MAC Valor que irá permitir ao WLAN UE verificar a autenticidade do *3GPP AAA Server*;

XRES Valor que irá permitir ao *3GPP AAA Server* verificar a autenticidade do WLAN UE;

CK *Cipher Key* utilizada para cifrar a informação a ser transmitida;

IK *Integrity Key* utilizada para garantir que a integridade dos dados;

AK *Anonymity Key* utilizada para garantir que a identidade do utilizador não seja rastreada.

O valor do AUTN é o resultado da operação:

$$AUTN = SQN \oplus AK||AMF||MAC \tag{2.1}$$

A Figura 2.5 representa o mesmo processo no WLAN UE.

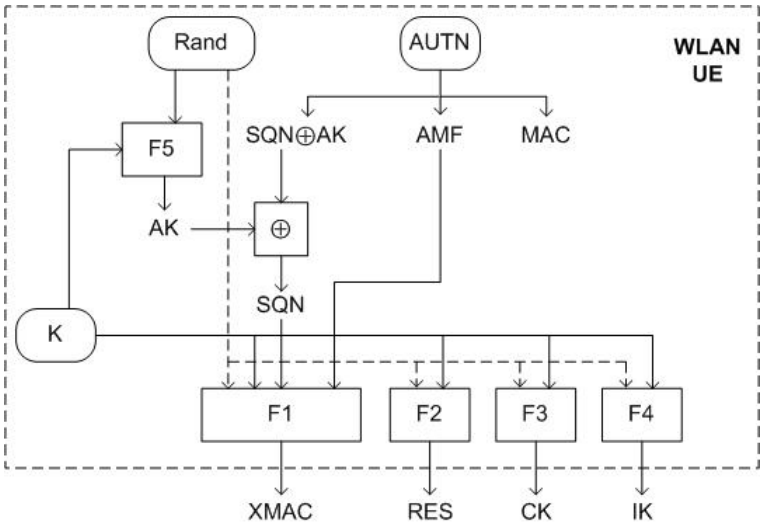

Figura 2.5: Protocolo AKA (WLAN UE)

Neste caso o WLAN UE recebe o valor do RAND e do AUTN a partir do *3GPP AAA Server* e utilizando o K que está guardado no USIM efectua as mesmas operações que o HSS. Desta forma tanto o HSS como o WLAN UE obtêm os mesmos valores para o XMAC (igual ao MAC), RES (igual ao XRES), CK e IK.

Na Figura 2.6 podemos ver o processo de autenticação e autorização completo utilizando o protocolo EAP-AKA. Quando o utilizador se encontra em *roaming* as mensagens entre a WLAN AN e o *3GPP AAA Server* são reenviadas utilizando o *3GPP AAA Proxy*.

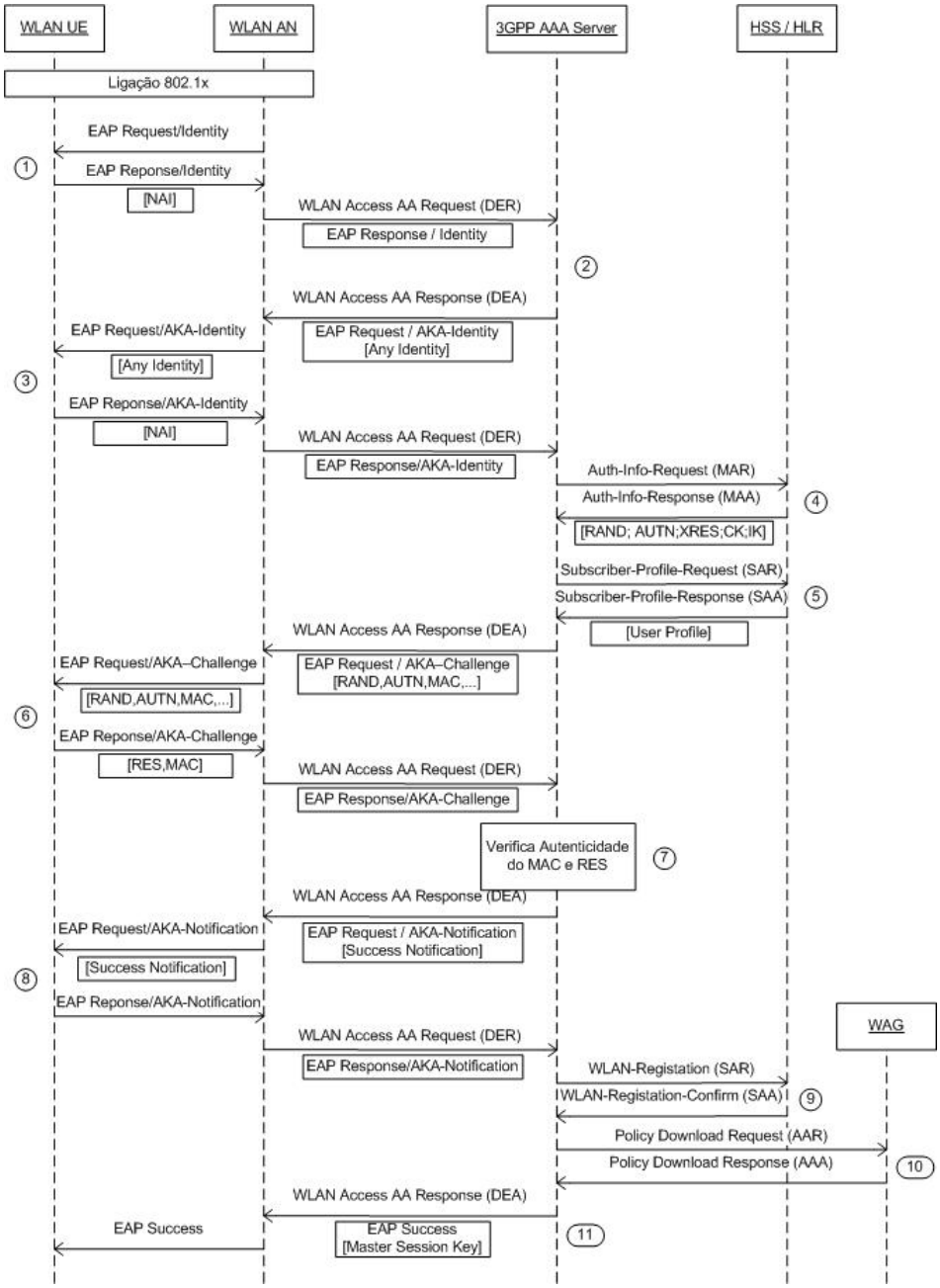

Figura 2.6: Autenticação e Autorização utilizando o protocolo EAP-AKA

1. A WLAN AN envia para o WLAN UE uma mensagem EAP com um pedido de identificação (EAP *Request Identity*). Se for a primeira autenticação o WLAN UE deverá responder com o seu *Permanent username* caso contrário deverá responder com o *Pseudonym username*. A mensagem é encapsulada numa mensagem Diameter pela

WLAN AN e enviada para o *3GPP AAA Server*.

2. A partir da identificação recebida o 3GPP AAA Sever identifica o protocolo que deverá ser utilizado (neste caso EAP-AKA) e envia para a WLAN AN um novo pedido de identificação, desta vez utilizando o protocolo EAP-AKA. Se o *3GPP AAA Server* receber um *Pseudonym username* e não conseguir identificar a identidade do utilizador envia um novo pedido obrigando o envio do *Permanent username*.

3. O pedido vindo do *3GPP AAA Server* é reenviado para o WLAN UE que responde mais uma vez com a identidade que tinha enviado previamente.

4. O *3GPP AAA Server* obtém o vector de autenticação (RAND, AUTN, XRES, CK e IK) do HSS.

5. O *3GPP AAA Server* obtém a informação de perfil do utilizador do HSS e verifica se o utilizador deverá ter acesso WLAN.

6. É enviado um EAP Request/AKA-Challenge para o WLAN UE contendo o valor do RAND, AUTN, MAC[1] e o *Pseudonym* e *Fast re-authentication username* que deverão ser utilizados nas próximas autenticações. O WLAN UE verifica a autenticidade do *3GPP AAA Server* analisando o valor do MAC recebido e o XMAC por ele calculado. Se os dois valores forem iguais envia uma resposta contendo o RES por ele calculado.

7. O *3GPP AAA Server* verifica a autenticidade do WLAN UE analizando o valor do MAC[2] e comparando o RES recebido com o XRES por ele calculado.

8. Se for comprovada a autenticidade é enviada uma notificações de sucesso para o WLAN UE ao qual este deverá responder.

9. O *3GPP AAA Server* efectua o registo do novo utilizador no HSS.

10. As routing policies são enviadas para o WAG.

11. Finalmente é enviada uma mensagem de sucesso para a WLAN AN contendo a *Master Session Key* (MSK). A MSK é calculada utilizando a função SHA1 com vários valores concatenados passados como parâmetro, conforme a operação seguinte:

[1]Este valor não deverá ser confundido com o MAC do protocolo AKA. Neste caso o MAC significa *Message Authentication Code* e é calculado aplicando a função SHA1 com a chave IK à mensagem EAP garantindo assim a autenticidade e integridade dos dados

[2]Message Authentication Code

$$MSK = SHA1(Identity|IK|CK) \tag{2.2}$$

EAP-SIM

Para os utilizadores GSM é utilizado o protocolo EAP-SIM no processo de autenticação e autorização WLAN usando o mecanismo SIM já existente para o GSM. Neste caso o processo é mais simples em relação ao EAP-AKA pois o vector de autenticação que o HSS gera apenas contêm três valores: RAND, SRES e Kc. O *3GPP AAA Server* pode solicitar mais que um vector de autenticação ao HSS.

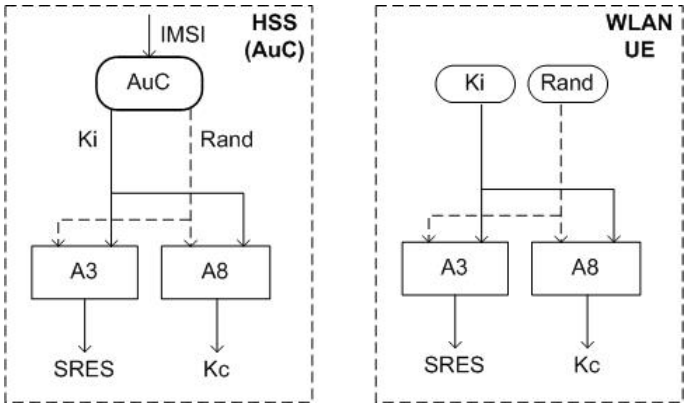

Figura 2.7: Protocolo SIM

A Figura 2.7 representa a geração dos valores no HSS (AuC). A partir do IMSI o AuC obtêm dois valores:

RAND Valor aleatório gerado pelo AuC;

Ki *Individual Subscriber Authentication Key* que está guardada no AuC e no SIM.

Estes valores são passados como parâmetros às funções A3 e A8 que estão no AuC e no SIM e são privadas variando em cada operador. Os resultados das funções são:

SRES Valor que irá permitir ao *3GPP AAA Server* verificar a autenticidade do WLAN UE e vice-versa;

Kc *Cipher Key* utilizada para cifrar a informação a ser transmitida.

Na Figura 2.8 podemos ver o processo de autenticação e autorização completo utilizando o protocolo EAP-SIM. Quando o utilizador se encontra em *roaming* as mensagens entre a WLAN AN e o *3GPP AAA Server* são reenviadas utilizando o *3GPP AAA Proxy*.

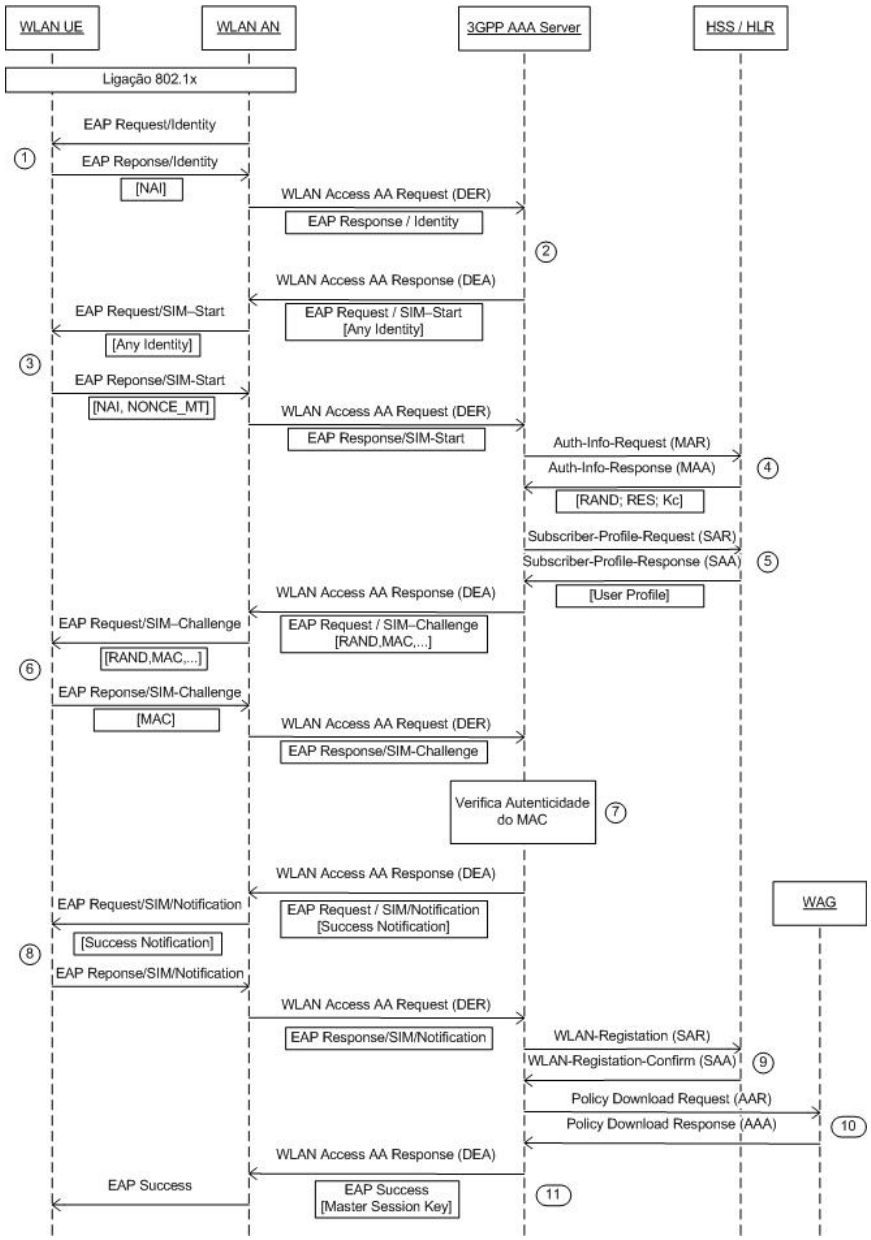

Figura 2.8: Autenticação e Autorização utilizando o protocolo EAP-SIM

1. A WLAN AN envia para o WLAN UE uma mensagem EAP com um pedido de identificação (EAP *Request Identity*). Se for a primeira autenticação o WLAN UE deverá responder com o seu *Permanent username* caso contrário deverá responder com o *Pseudonym username*. A mensagem é encapsulada numa mensagem Diameter pela WLAN AN e enviada para o *3GPP AAA Server*.

2. A partir da identificação recebida o 3GPP AAA Server identifica o protocolo que deverá ser utilizado (neste caso EAP-SIM) e envia para a WLAN AN um novo pedido de identificação, desta vez usando o protocolo EAP-SIM. Esta nova mensagem contém a lista das versões EAP que o *3GPP AAA Server* suporta (*VersionList*). Se o *3GPP AAA Server* receber um *Pseudonym username* e não conseguir identificar a identidade do utilizador envia um novo pedido obrigando o envio do *Permanent username*.

3. O pedido vindo do *3GPP AAA Server* é reenviado para o WLAN UE que responde mais uma vez com a identidade que tinha enviado previamente, com a versão EAP por ele escolhida (*SelectedVersion*)e com um valor aleatório (NONCE_MT) por ele gerado que irá servir para a geração da *Master Session Key*.

4. O *3GPP AAA Server* obtém o vector de autenticação (RAND, SRES, Kc) do HSS.

5. O *3GPP AAA Server* obtém a informação de perfil do utilizador do HSS e verifica se o utilizador deverá ter acesso WLAN.

6. É enviado um EAP Request/SIM-Challenge para o WLAN UE contendo o valor do RAND, MAC[3] e o *Pseudonym* e *Fast re-authentication username* que deverão ser utilizados nas próximas autenticações. O WLAN UE verifica a autenticidade do *3GPP AAA Server* analisando o valor do MAC recebido. Se estiver correcto envia uma resposta com um novo MAC.

7. O *3GPP AAA Server* verifica a autenticidade do WLAN UE analizando o valor do MAC.

8. Se for comprovada a autenticidade é enviada uma notificações de sucesso para o WLAN UE ao qual este deverá responder.

9. O *3GPP AAA Server* efectua o registo do novo utilizador no HSS.

10. As routing policies são enviadas para o WAG.

[3] *Message Authentication Code* calculado a partir da mensagem EAP e do SRES garantindo assim a autenticidade e integridade dos dados

11. Finalmente é enviada uma mensagem de sucesso para a WLAN AN contendo a *Master Session Key* (MSK). A MSK é calculada utilizando a função SHA1 com vários valores concatenados passados como parâmetro, conforme a operação seguinte:

$$MSK = SHA1(Identity|n * Kc|NONCE\_MT|VersionList|SelectedVersion) \tag{2.3}$$

2.6.2 Fim de Sessão

Quando um utilizador se desliga da rede a WLAN AN notifica o *3GPP AAA Server* conforme a Figura 2.9.

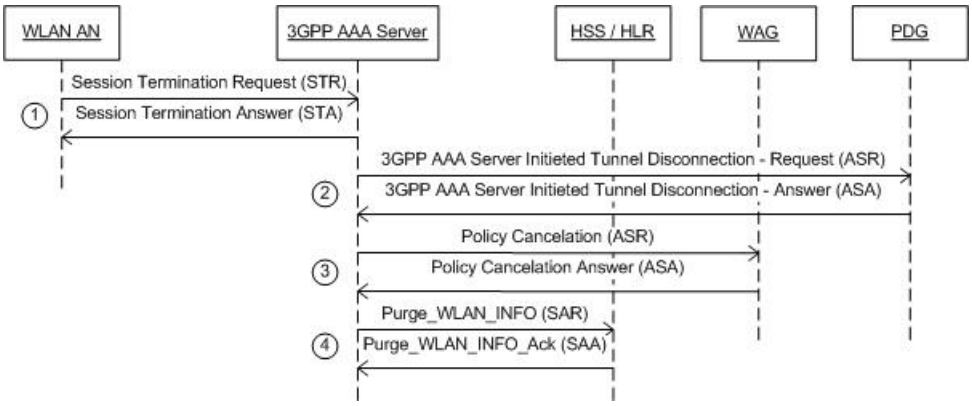

Figura 2.9: Fim de Sessão

1. Um pedido de fim de sessão é enviado para o *3GPP AAA Server*;
2. Os túneis que possam estar activos no PDG são removidos;
3. As routing policies definidas para o utilizador são removidas do WAG;
4. O estado do utilizador é removido do HSS.

2.6.3 Cancelamento da Sessão

Quando a rede decide que um utilizador deverá ser desligado, seja por ordem do *3GPP AAA Server*, seja por ordem do HSS ou mesmo quando o pedido de charging é recusado o *3GPP AAA*

Server deverá proceder como está representado na Figura 2.10.

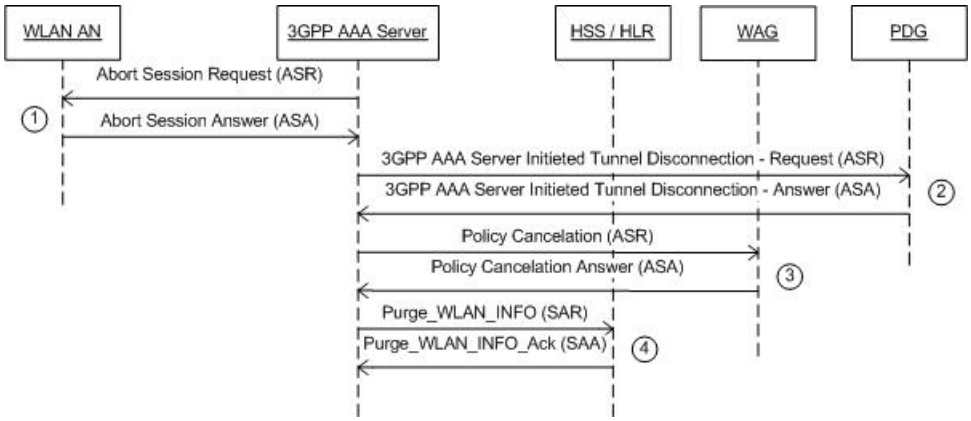

Figura 2.10: Cancelamento da Sessão

1. O *3GPP AAA Server* notifica a WLAN AN que a sessão de um determinado utilizador deverá ser desligada;

2. Os túneis que poderão estar activos no PDG são removidos;

3. As routing policies do utilizador são removidas do WAG;

4. É removido o estado do utilizador no HSS.

2.6.4 Actualização de perfil

Quando o perfil do utilizador é actualizado no HSS o *3GPP AAA Server* deverá fazer as alterações necessárias consoante o tipo de alteração como está representado na Figura 2.11.

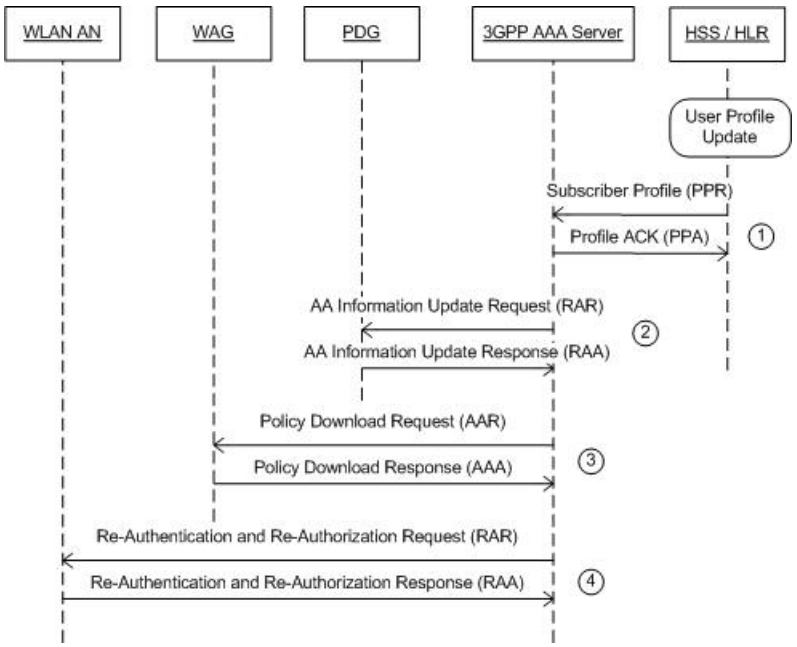

Figura 2.11: Actualização de perfil

1. O HSS notifica o *3GPP AAA Server* das alterações no perfil do utilizador;

2. Caso as alterações estejam relacionadas com os túneis activos o *3GPP AAA Server* deverá notificar o PDG destas actualizações;

3. Se as alterações forem relacionada com as *routing policies* o *3GPP AAA Server* deverá enviar as novas *routing policies* para o WAG;

4. Se as alterações forem relacionada com a autenticação e/ou autorização do utilizador o *3GPP AAA Server* deverá enviar um pedido de re-autenticação para a WLAN AN para que esta inicie o processo de autenticação e autorização novamente.

2.6.5 Estabelecimento de Túneis

Quando um utilizador pretende aceder a um determinado serviço é estabelecido um túnel IPSec com o PDG utilizando o protocolo *Internet Key Exchange* (IKEv2) como especificado em [23].

A Figura 2.12 representa o processo completo de estabelecimento do túnel.

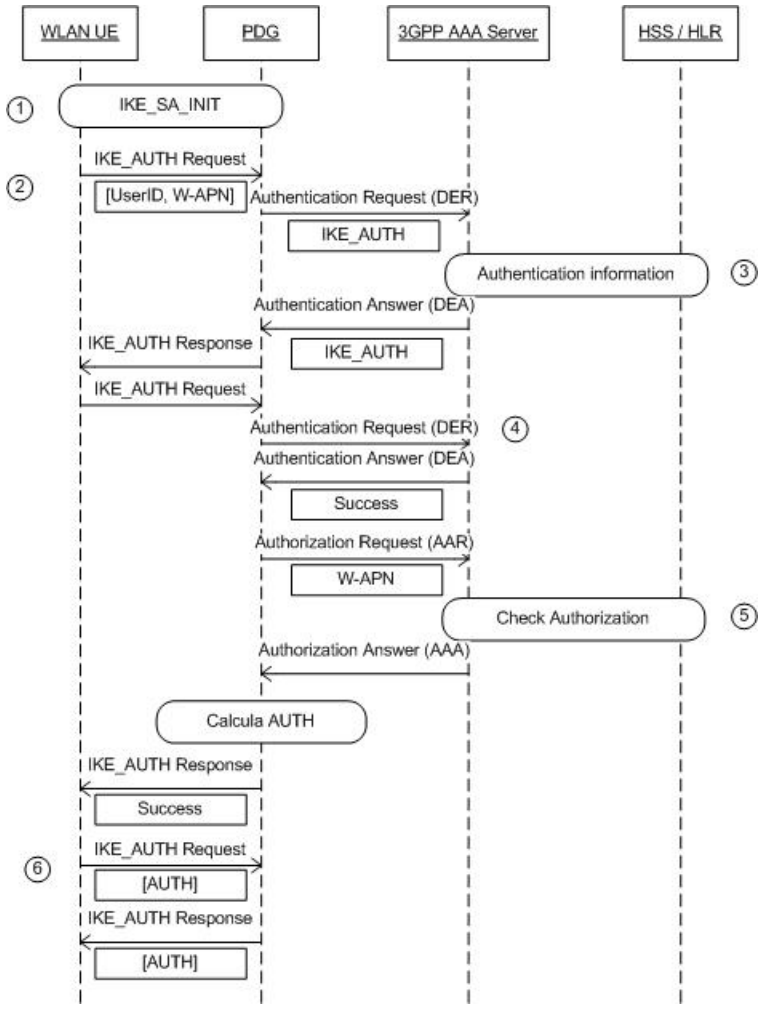

Figura 2.12: Estabelecimento de Túneis

1. O WLAN UE e o PDG trocam informações relativas ao protocolo IKEv2 de forma a que possam estabelecer uma ligação segura;

2. O WLAN UE envia para o PDG a sua identificação e qual o W-APN a que está a tentar aceder;

3. Se o *3GPP AAA Server* não tiver os vectores de autenticação faz um pedido ao HSS para que este os envie;

4. O utilizador é autenticado utilizando o protocolo EAP-AKA ou EAP-SIM conforme seja uma rede UMTS ou GSM respectivamente;

5. O PDG verifica no *3GPP AAA Server* se o utilizador tem permissões para aceder à W-APN, se essa informação não estiver no *3GPP AAA Server* é feito um novo pedido ao HSS;

6. O processo de estabelecimento do túnel entre o PDG e o WLAN UE é concluido.

2.6.6 Término de Túnel

A Figura 2.13 representa o processo de término de túneis. Este processo ocorre quando um utilizador deixa de aceder a uma determinada W-APN.

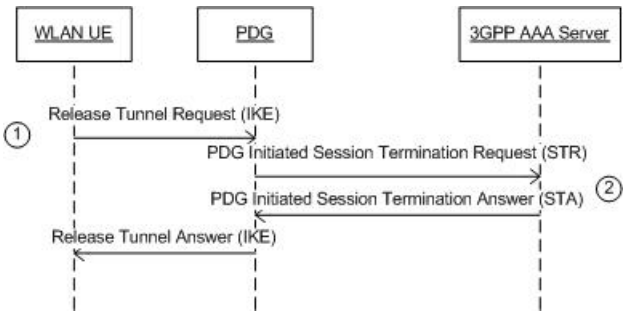

Figura 2.13: Término de Túnel

1. O WLAN UE envia um pedido para terminar o túnel.

2. O PDG notifica o *3GPP AAA Server* que o túnel deverá ser terminado.

2.6.7 *Offline Charging*

A WLAN AN poderá ou não suportar *accounting*, pelo que existem duas formas de realizar *charging offline*. Se a WLAN AN suportar *Offline Charging* esta gera mensagens de *Accounting* e envia para o *3GPP AAA Server* para que este as reenvie para o OFCS conforme está representado na Figura 2.14. Se a WLAN AN não suportar geração de mensagens de *Accounting*, estas serão geradas pelo *3GPP AAA Server* quando o utilizador se autentica, re-autentica e termina a sessão como está representado na Figura 2.15.

As mensagem de *Accounting* poderão ser do tipo START usadas no inicio da sessão, INTERIM utilizadas para enviar informação sobre uma sessão que já está em curso e STOP utilizadas para terminar a sessão.

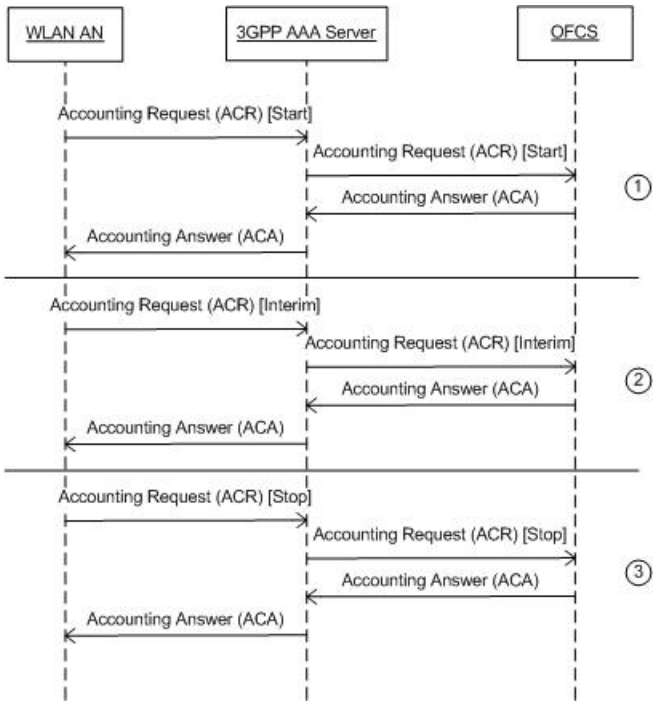

Figura 2.14: Offline Charging (1)

1. A WLAN AN gera e envia para o *3GPP AAA Server* uma mensagem de *Accounting* START quando o utilizador se autentica com sucesso, o *3GPP AAA Server* deverá reenviar esta mensagem para o OFCS;

2. Depois de um tempo estipulado a WLAN AN gera e envia para o *3GPP AAA Server* uma mensagem de *Accounting* INTERIM, o *3GPP AAA Server* deverá reenviar esta mensagem para o OFCS;

3. Quando o utilizado se desliga a WLAN AN gera e envia para o *3GPP AAA Server* uma mensagem de *Accounting* STOP, o *3GPP AAA Server* deverá reenviar esta mensagem para o OFCS.

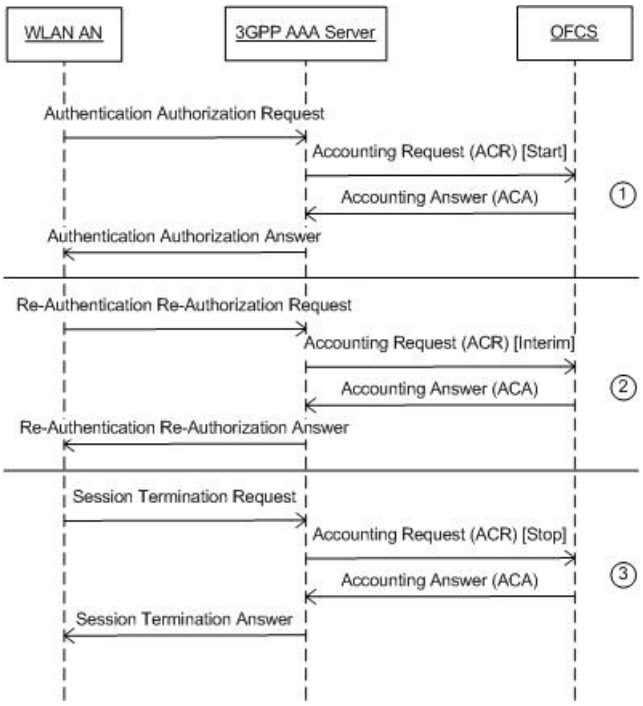

Figura 2.15: Offline Charging (2)

1. Durante o processo de autenticação e autorização o *3GPP AAA Server* gera e envia uma mensagem de *Accounting* START para o OFCS;

2. Quando um utilizador se re-autentica o *3GPP AAA Server* gera e envia uma mensagem de *Accounting* INTERIM para o OFCS;

3. Quando um utilizador termina a sessão o *3GPP AAA Server* gera e envia uma mensagem de *Accounting* STOP para o OFCS;

2.6.8 *Online Charging*

Para *Online Charging* existem três cenários possíveis. Quando a WLAN AN suporta *Online Charging* é esta que gera e envia para o *3GPP AAA Server* as mensagens relativas a *Online Charging* para que este as reenvie para o OCS (Figura 2.16). Se não suportar *Online Charging* mas suportar *Offline Charging* o *3GPP AAA Server* sempre que recebe uma mensagem relativa ao *Offline Charging* gera e envia para o OFS uma mensagem de *Online Charging* (Figura 2.17). Por fim se a WLAN AN não suportar nem *Online Charging* nem *Offline Charging* o *3GPP AAA*

Server deverá gerar e enviar mensagens de *Online Charging* para o OCS quando o utilizador se autentica, re-autentica e termina a sessão (Figura 2.18).

As mensagem de *Online Charging* poderão ser do tipo START e são usadas no inicio da sessão, UPDATE utilizadas para enviar informação sobre uma sessão que já está em curso e TERMINATE utilizadas para terminar a sessão.

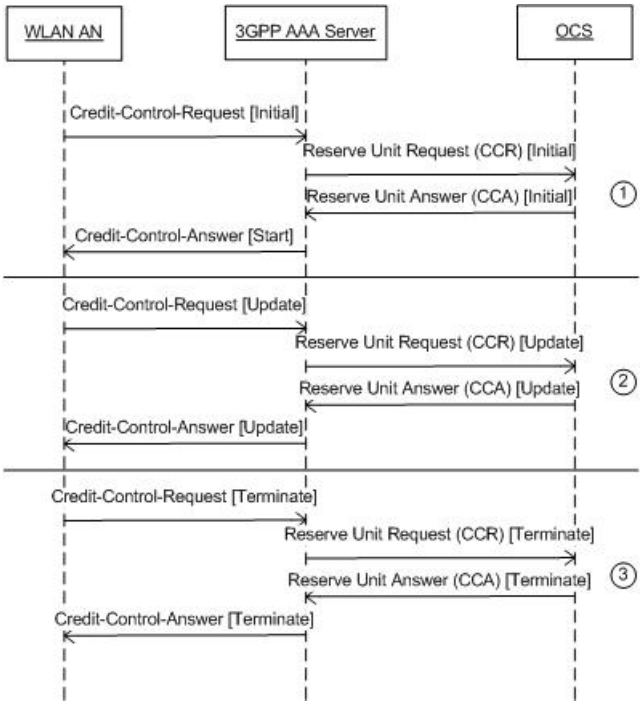

Figura 2.16: Online Charging (1)

1. A WLAN AN gera e envia para o *3GPP AAA Server* uma mensagem de textitOnline Charging do tipo START quando o utilizador se autentica com sucesso, o *3GPP AAA Server* deverá reenviar esta mensagem para o OCS;

2. Depois de um tempo estipulado a WLAN AN gera e envia para o *3GPP AAA Server* uma mensagem de *Online Charging* do tipo INTERIM, o *3GPP AAA Server* deverá reenviar esta mensagem para o OCS;

3. Quando o utilizado se desliga a WLAN AN gera e envia para o *3GPP AAA Server* uma mensagem de *Online Charging* do tipo STOP, o *3GPP AAA Server* deverá reenviar esta mensagem para o OCS.

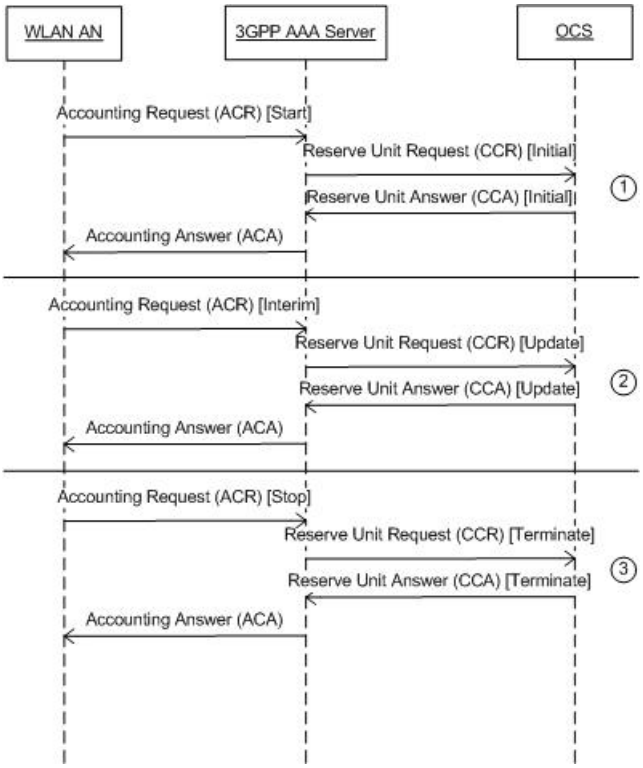

Figura 2.17: Online Charging (2)

1. Quando recebe uma mensagem de *Offline Charging* do tipo START o *3GPP AAA Server* gera e envia para o OCS uma mensagem de *Online Charging* to tipo START.

2. Quando recebe uma mensagem de *Offline Charging* do tipo INTERIM o *3GPP AAA Server* gera e envia para o OCS uma mensagem de Online Charging to tipo UPDATE.

3. Quando recebe uma mensagem de *Offline Charging* do tipo STOP o *3GPP AAA Server* gera e envia para o OCS uma mensagem de *Online Charging* to tipo TERMINATE.

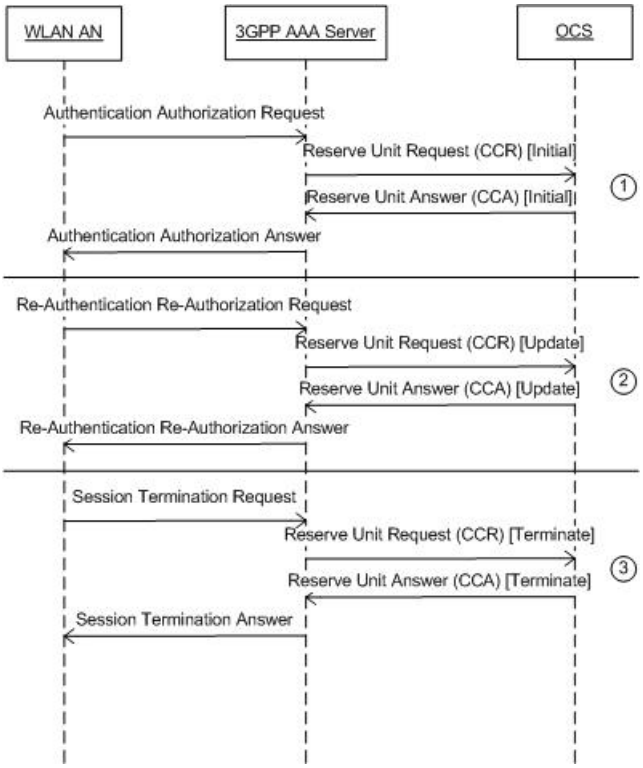

Figura 2.18: Online Charging (3)

1. Durante o processo de autenticação e autorização o *3GPP AAA Server* gera e envia uma mensagem de *Online Charging* do tipo START para o OCS;

2. Quando um utilizador se re-autentica o *3GPP AAA Server* gera e envia uma mensagem de *Online Charging* do tipo INTERIM para o OCS;

3. Quando um utilizador termina a sessão o *3GPP AAA Server* gera e envia uma mensagem de *Online Charging* do tipo STOP para o OCS;

2.7 Conclusão

Neste capítulo foram apresentados os estudos realizados e exposto o estado da arte das normas do 3GPP sobre o tema da dissertação. Na primeira parte foram identificados seis cenários de integração, de seguida foi apresentada a arquitectura de referência proposta pelo 3GPP com todos os seus componentes e interfaces. Por fim, foram apresentados alguns casos de uso do sistema que foram previamente identificados.

No próximo capítulo será apresentado o desenvolvimento da solução com base nos conceitos descritos neste capítulo.

Capítulo 3

Desenvolvimento da solução

3.1 Introdução

Uma vez completo o estudo preliminar sobre as normas existentes relativas ao tema de integração das WLANs com a rede 3G, será agora descrita a elaboração do *3GPP AAA Server*. Inicialmente serão identificados os requisitos que a solução desenvolvida deverá cumprir sejam estes funcionais ou de interface com sistemas externos. De seguida será feito o enquadramento da solução com os restantes produtos da PT Inovação. Depois disto serão apresentados os seus detalhes de concepção. Neste ponto será apresentada a perspectiva lógica da solução onde serão explicados todos os módulos que fazem parte do sistema e serão apresentados os diagramas de robustez e de actividade de forma a explicar mais detalhadamente o comportamento de toda a solução.

3.2 Análise de requisitos

A solução desenvolvida deverá cumprir diversos requisitos, alguns funcionais, que dizem respeito ao funcionamento do sistema em si, e outros de interface com sistemas externos, que dizem respeito à forma de como o sistema deverá interagir com outros componentes.

3.2.1 Requisitos Funcionais

Use Cases O sistema deverá suportar totalmente os use cases "Autenticação e Autorização WLAN", "Fim de Sessão", "Cancelamento da Sessão", "Actualização de perfil", "*Online Charging*"e "*Offline Charging*"definidos na secção 2.6 deste documento.

Integração com stack Diameter IDS A Intelligent Diameter Stack® (IDS) é um produto da PT Inovação que consiste em uma pilha protocolar que implementa o protocolo Diameter Base definido em [17] com o objectivo de disponibilizar as funcionalidades do protocolo Diameter Base e outras Diameter *Applications*. A IDS deverá suportar todas as mensagens e AVPs definidos para todas as interfaces.

Alta disponibilidade A alta disponibilidade para os clientes Diameter deverá ser assegurada.

Escalabilidade O componente fazendo parte de um sistema altamente escalável deverá também ele ser o mais escalável possível.

Robustez Sendo um ponto sensível e fundamental no sistema, o 3GPP AAA deverá ser o mais robusto possível. O sistema deverá apresentar uma arquitectura *Active/StandBy*, devendo ser mantido sincronismo entre ambas instâncias. Em caso de comutações induzidas (paragem do *Active*) ou devido a problemas (*crash* da aplicação) o *downtime* deverá ser o mais reduzido possível.

Integração com a framework XAF A *framework eXtensible Architecture Framework*®(XAF) é um produto da PT Inovação que, entre outras coisas, disponibiliza um gestor de configurações (XMan) e um gestor de eventos (*Event Manager*).

3.2.2 Requisitos de Interface com Sistemas Externos

Interface com *WLAN Access Network* (Wa) Interface entre a rede de acesso (WLAN AN) e o 3GPP AAA. O principal objectivo desta interface é transportar informações de autenticação, autorização e *accounting* de forma segura. Deverá suportar os protocolos: Diameter Base, Diameter-EAP, Diameter-NASREQ, Diameter Credit Control.

Interface com *3GPP AAA Proxy* (Wd) Esta interface liga o *3GPP AAA Proxy* ao *3GPP AAA Server* por redes intermédias. O objectivo desta interface é transportar informação de autenticação, autorização e accounting de forma segura. Deverá suportar os protocolos: Diameter Base, Diameter-EAP, Diameter-NASREQ, Diameter Credit Control.

Interface com *Online Charging System* (Wo) Esta interface é utilizada para transportar informação de online charging entre o 3GPP AAA e o Online Charging System. Deverá suportar o protocolo Diameter Credit Control.

Interface com *Offline Charging System* (Wf) Esta interface é utilizada para transportar informação de offline charing entre o 3GPP AAA e o Offline Charging System. Deverá suportar o protocolo Diameter Base.

Interface com HSS (Wx) Interface entre o 3GPP AAA e o HSS. Esta interface permite obter informação de autenticação e perfil dos utilizadores, registar e remover utilizadores WLAN no HSS e notificar alterações no perfil dos utilizadores. Deverá suportar o protocolo Diameter Application for Cx interface.

3.3 Enquadramento da solução com outros produtos PT Inovação

Na figura 3.1 está representado o enquadramento da solução desenvolvida com alguns produtos já existentes na PT Inovação.

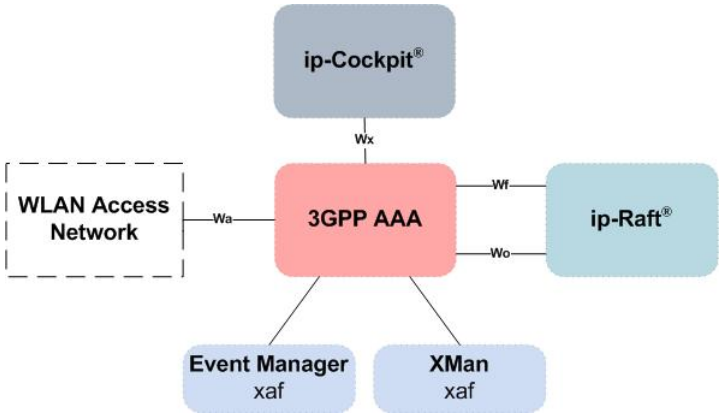

Figura 3.1: Integração com os Produtos PT Inovação

ip-Cockpit é a solução de HSS existente na PT Inovação.

ip-Raft é a solução para *Charging* existente na PT Inovação. Contém as funções de *Online* e *Offline Charging*.

Event Manager é um módulo de gestão de eventos. Quando um evento chega ao *Event Manager* é processado de acordo com regras pré-configuradas, o que permite executar diferentes operações sobre cada evento. É utilizado sobretudo para armazenar os eventos em base de dados ou em ficheiro.

XMan é um servidor de ficheiros, utilizado armazenar as configurações de diversas plataformas permitindo que estas possam aceder aos seus parâmetros de configuração remotamente. A administração destes parâmetros é efectuada via interface WEB.

3.4 Detalhes de concepção

3.4.1 Perspectiva Lógica

A solução desenvolvida está divida em níveis funcionais como está representado na figura 3.2. A camada *Diameter Applications* é a implementação da *stack* IDS e tem como objectivo receber/enviar as mensagens Diameter e armazená-las no local correcto para que depois possam ser processadas. O *Controller* sendo o bloco principal do sistema, é responsável por fazer a gestão dos restantes blocos e gerir configurações e *logs*. Os *Managers* são responsáveis por processar as mensagens recebidas e tomar acções conforme a situação.

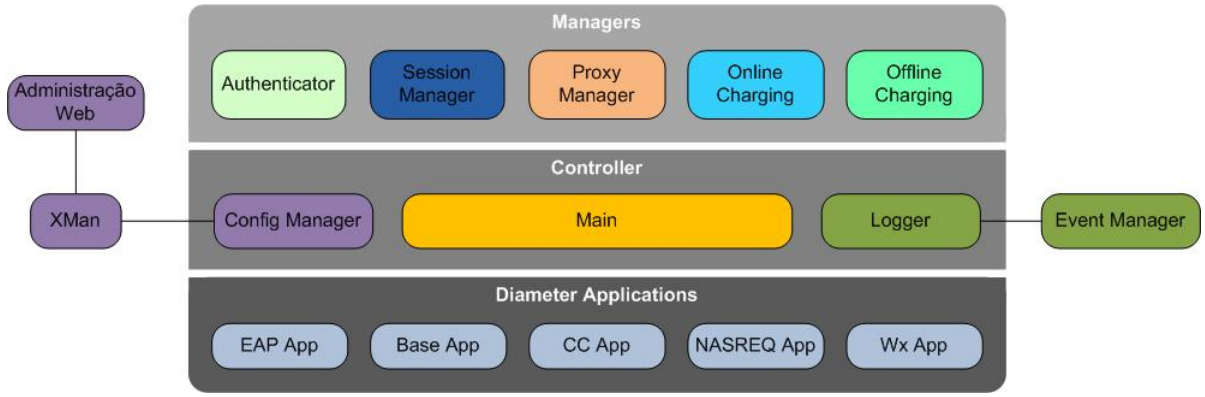

Figura 3.2: Perspectiva Lógica

Controller

Main O *Main* é o módulo central do 3GPP AAA. É a ele que cabe coordenar as acções dos restantes blocos funcionais. Durante o arranque do sistema o *Main* é responsável por obter as configurações, iniciar as restantes *threads* e fazer a sua gestão. Este bloco também é responsável por instanciar as várias *Diameter Applications* (EAP App, Base App, NASREQ App, CC App e Cx App) e irá conter diversas *queues* de mensagens:

- *Auth Queue* – Contém mensagens relativas à autenticação e/ou autorização de utilizadores WLAN e de túneis. Estas mensagens serão processadas pelos *Authenticators*.
- *Session Queue* – Contém mensagens relativas à sessão dos utilizadores (ex. fim de sessão, actualização de perfil, etc). Estas mensagens serão processadas pelos *Session Managers*.
- *Proxy Queue* – Contém mensagens recebidas ou que deverão ser enviadas para outro servidor 3GPP AAA. Estas mensagens serão processadas pelos *Proxy Managers*.
- *Offline Charging Queue* – Contém mensagens relativas a *Offline Charging*. Estas mensagens serão processadas pelos *Offline Charging*.
- *Online Charging Queue* – Contém mensagens relativas a *Online Charging*. Estas mensagens serão processadas pelos *Online Charging*.

A utilização deste módulo permite uma gestão mais simples e eficaz de todo o sistema uma vez que é centralizada.

Config Manager Este bloco é responsável gerir as configurações dos diversos blocos. Sempre algum bloco necessite de obter algum parâmetro de configuração efectua um pedido a este módulo centralizando assim toda a informação. De forma a obter as configurações do módulo é feita uma ligação ao gestor de configurações (XMan) . Caso esta ligação não seja possível as configurações são lidas a partir de um ficheiro de configuração que é passado como parâmetro no arranque do módulo. A estrutura das configurações no XMan poderá ser vista no anexo A.

Logger Este bloco é responsável pela actividade de *logging* do módulo. Os blocos funcionais enviam para este bloco todas as acções de *logging* que necessitam. É efectuada uma ligação a um servidor *Event Manager* onde irão ser guardados os diversos eventos. Caso não exista nenhum servidor *Event Manager* configurado os eventos serão guardados num ficheiro de *logging* local. A utilização de um módulo apenas para gerir os eventos tem como objectivo

simplificar o trabalho dos outros módulos, não tendo estes que se preocupar com o tipo e para onde é que a informação que deverá ser enviada. Existem diversos tipos de eventos que poderão ser enviados para o *Event Manager*:

DiameterApp Para eventos relacionados com as várias *Diameter Applications*. Este tipo de eventos deverá conter informação sobre qual aplicação gerou o evento, o tipo de mensagem que foi recebida/enviada, o *username* que está associado à mensagem, a origem e o destino da mesma, possíveis erros, etc;

Auth, Session, Proxy, Offline, Online Para eventos relacionados com o *Authenticator, Session Manager, Proxy Manager, Offline Charging* e *Online Charging* respectivamente. Deverá conter informação sobre o *username* que está associado ao evento, a sessão em questão, possíveis erros, informação específica sobre o evento, etc;

Controller Para eventos relacionados com todo o bloco *Controller*. Contém informação sobre o módulo que gerou o evento, possíveis erros, informação específica sobre o evento, etc;

Estes eventos têm vários níveis, nomeadamente *debug*, *info*, *warn* e *error* podendo ou não ser tomadas acções consoante o nível. A divisão dos eventos por tipo e nível permite ainda simplificar a pesquisa de eventos e estatísticas.

Diameter Applications

A utilização de várias instâncias da classe *Application* da *stack Diameter* IDS permite separar logo à partida as mensagens podendo tomar diferentes acções consoante o seu tipo.

EAP App Este bloco irá implementar a *Diameter EAP Application*, para isto irá estender a classe *Application* da *stack Diameter* IDS. Quando uma mensagem Diameter EAP é recebida, este bloco é responsável por verificar se a origem da mensagem é correcta e qual o 3GPP AAA para o qual a mensagem se destina. Caso a mensagem se destine a outro 3GPP AAA a mensagem irá ser colocada na *Proxy Queue*, caso contrário a mensagem irá ser colocada na *Auth Queue*.

Base App Este bloco irá implementar o Diameter Base, para isto irá estender a classe *Application* da *stack Diameter* IDS. Quando uma mensagem Diameter Base é recebida este bloco é responsável por verificar se a origem da mensagem é correcta e qual o 3GPP AAA para o qual a mensagem se destina. Caso a mensagem se destine a outro 3GPP AAA a mensagem

irá ser colocada na Proxy Queue, caso contrário irá verificar se a mensagem é relativa a *Offline Charging* ou é relativa à sessão. Caso seja de *Offline Charging* a mensagem será colocada na *Offline Charging Queue* e na *Session Queue* caso contrário.

NASREQ App Este bloco irá implementar a *Diameter NASREQ Application*, para isto irá estender a classe *Application* da *stack Diameter* IDS. Quando uma mensagem Diameter NASREQ é recebida este bloco é responsável por verificar se a origem da mensagem é correcta e qual o 3GPP AAA para o qual a mensagem se destina. Caso a mensagem se destine a outro 3GPP AAA a mensagem irá ser colocada na *Proxy Queue*, caso contrário irá verificar se a mensagem é relativa a *Offline Charging*, se é relativa à sessão ou se é relativa a autorização. Caso seja de *Offline Charging* a mensagem será colocada na *Offline Charging Queue*, na *Session Queue* caso seja relativa à sessão e na *Auth Queue* se for relativa à autorização.

CC App Este bloco irá implementar a *Diameter Credit Control(CC) Application*, para isto irá estender a classe *Application* da *stack Diameter* IDS. Quando uma mensagem Diameter CC é recebida este bloco é responsável por verificar se a origem da mensagem é correcta e qual o 3GPP AAA para o qual a mensagem se destina. Caso a mensagem se destine a outro 3GPP AAA a mensagem irá ser colocada na *Proxy Queue*, caso contrário irá ser colocada na *Online Charging Queue*.

Wx App Este bloco irá implementar a *Diameter Wx Application*, para isto irá estender a classe *Application* da *stack Diameter* IDS. Quando uma mensagem Diameter Wx é recebida este bloco é responsável por verificar se a origem da mensagem é correcta. Caso a mensagem seja uma resposta a um pedido do *Authenticator* deverá ser colocada na *Auth Queue*, caso contrário deverá ser colocada na *Session Queue*.

Managers

Foram criados diferentes tipos de *Managers* com o objectivo de dividir o processamento de mensagens de um forma lógica, consoante o tipo de operação a que a mensagem se destina. Desta forma o desenvolvimento de cada bloco é facilitado. Poderão existir mais do que um *Manager* de cada tipo, sendo o seu número configurável.

Authenticator Este bloco é responsável por efectuar operações de autenticação e autorização, para isso irá obter mensagens da *Auth Queue* e irá processá-las conforme o estado da

sessão em curso.

Session Manager Este bloco é responsável por efectuar operações relativas às sessões em curso. Para isso irá obter mensagens da *Session Queue* e irá processá-las conforme o estado da sessão em curso.

Proxy Manager Este bloco é responsável por enviar as mensagens de utilizadores em *roaming* para o 3GPP AAA correcto, o estado das sessões em curso é guardado. Este bloco irá obter as mensagens da *Proxy Queue*.

Online Charging Este bloco é responsável pela gestão do *Online Charging*, para isso irá obter mensagens da *Online Charging Queue* e caso seja um pedido irá reenvia-lo para o OCS, caso seja uma resposta irá reenvia-la para o componente (WLAN AN ou 3GPP AAA) correcto.

Offline Charging Este bloco é responsável pela gestão do *Offline Charging*, para isso irá obter mensagens da *Offline Charging Queue* e caso seja um pedido irá reenvia-lo para o OFCS, caso seja uma resposta irá reenvia-la para o componente (WLAN AN ou 3GPP AAA) correcto.

3.4.2 Diagramas de Robustez

A metodologia de desenvolvimento de *software* Iconix [32] define vários tipos de diagramas baseados em *Unified Modeling Language* (UML). Esta metodologia pode ser vista como um processo que vai desde a representação dos casos de uso até ao desenvolvimento do código em si. Um dos diagramas definidos é o "Diagrama de Robustez"que permite representar o funcionamento do sistema, de uma forma simples, utilizando os objectos (figura 3.3) definidos pela metodologia.

Neste tipo de diagramas, e tal como pode ser visto nas figuras 3.4 e 3.5, é possível identificar facilmente os objectos de entrada/saída do e a sequência das acções de todo o sistema.

Figura 3.3: Objectos do diagrama de robustez

Objectos Fronteira permitem às entidades externas comunicar com o sistema, poderão ser interfaces, páginas, etc;

Objectos Controlo são integradores entre os objectos de fronteira e os objectos de entidade, normalmente são convertidos em métodos;

Objectos Entidade correspondem geralmente a objectos onde a informação é guardada, poderão ser uma classe, uma base de dados, etc.

Nas seguintes figuras existem mais do que um Objecto Fronteira com o mesmo nome, na realidade são o mesmo objecto. A razão dos objectos estarem repetidos é simplesmente para facilitar a organização do diagrama.

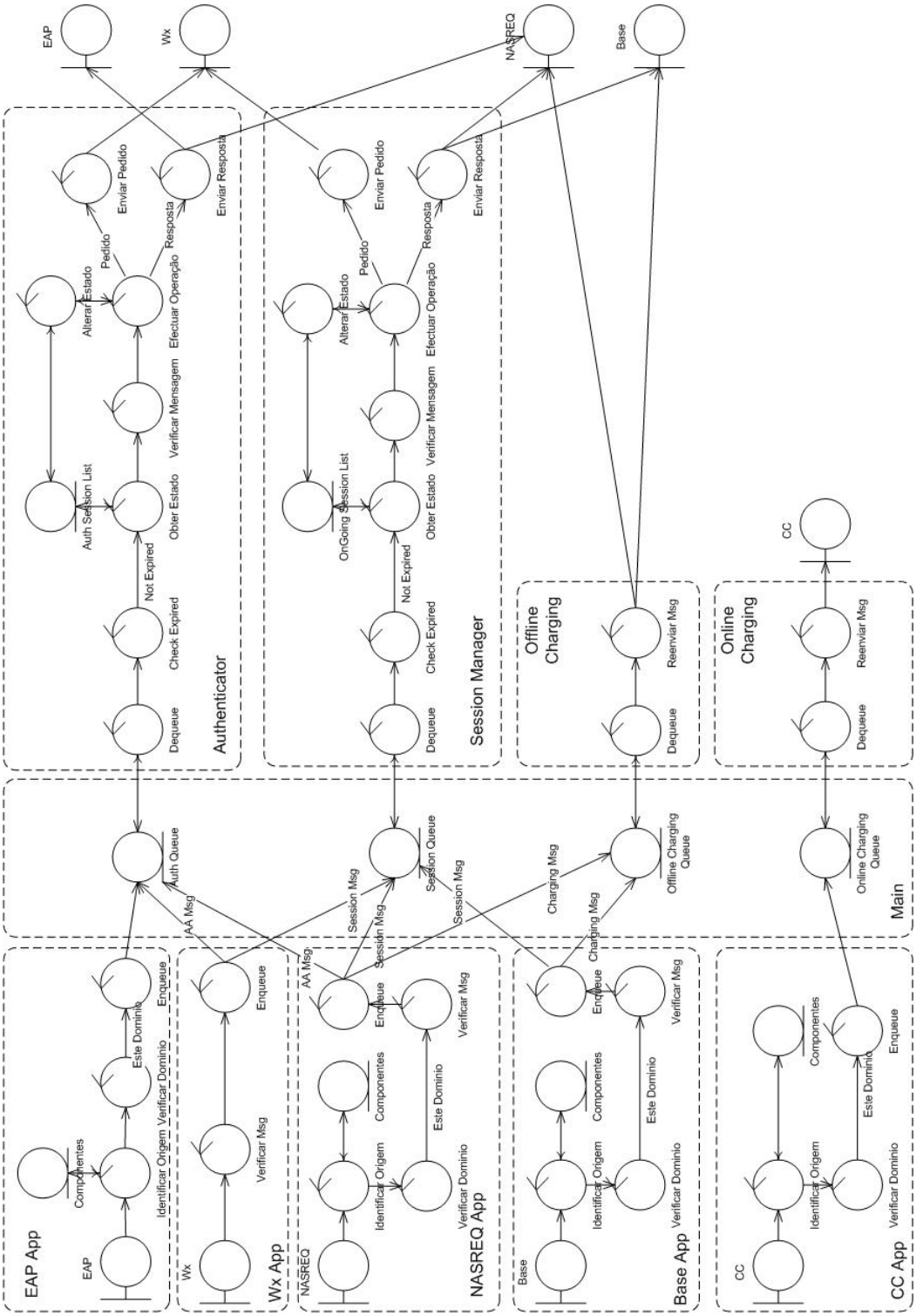

Figura 3.4: Diagramas de Robustez (1)

O funcionamento das várias *Diameter Applications* (EAP App, Wx App, NASREQ App, Base App, e CC App) é semelhante: quando uma mensagem é recebida é verificada a sua origem pois apenas determinados componentes é que tem permissão para enviar certas mensagens, posteriormente é analisado o domínio para o qual a mensagem se destina e, por fim, é analisado o tipo da mensagem para que a mensagem seja colocada na *queue* correcta para depois ser processada.

Nos *managers*s "*Authenticator*"e "*Session Manager*"o funcionamento também é semelhante: quando uma mensagem chega à *queue* é verificada a validade da mensagem pois poderá não fazer sentido processar uma mensagem já muito antiga. Posteriormente a mensagem é analisada de forma a obter o estado actual da sessão e são efectuadas operações conforme esse estado e a mensagem recebida. Estas operações podem resultar no envio de uma resposta ou no envio de um pedido para outro componente. No caso dos *managers* "*Offline Charging*"e "*Online Charging*"o processo é mais simples pois apenas tem que reenviar as mensagens recebidas para o OFCS e OCS respectivamente.

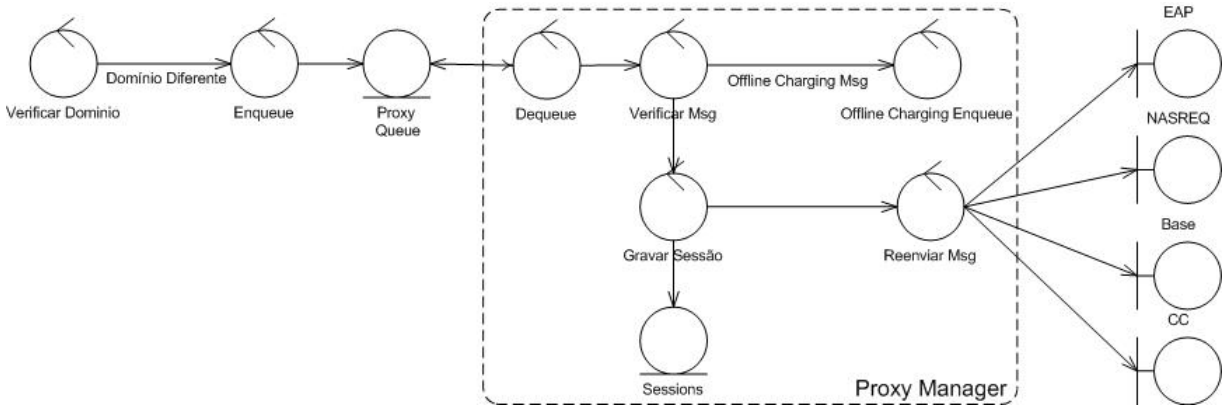

Figura 3.5: Diagramas de Robustez (2)

A figura acima representa o caminho alternativo do Objecto Controlo "Verificar Domínio". Neste caso a mensagem não se dirige a este *3GPP AAA Server* e por isso ele deverá funcionar como um *3GPP AAA Proxy* e reenviar a mensagem para o *3GPP AAA Server* correcto. O *3GPP AAA Proxy* é *stateful* e por isso deverá guardar o estado actual da sessão.

Uma versão mais detalhada do funcionamento dos *Managers* poderá ser visto nos diagramas de actividade na secção seguinte.

3.4.3 Diagramas de actividade

Nesta secção são apresentados os diagramas de actividade dos vários *Managers*. Neles podemos ver a sequência das actividades a partir do momento que uma mensagem é recebida. O comportamento que o sistema irá ter varia, por exemplo, com a mensagem recebida, a origem da mensagem e o estado actual da sessão em curso.

Authenticator

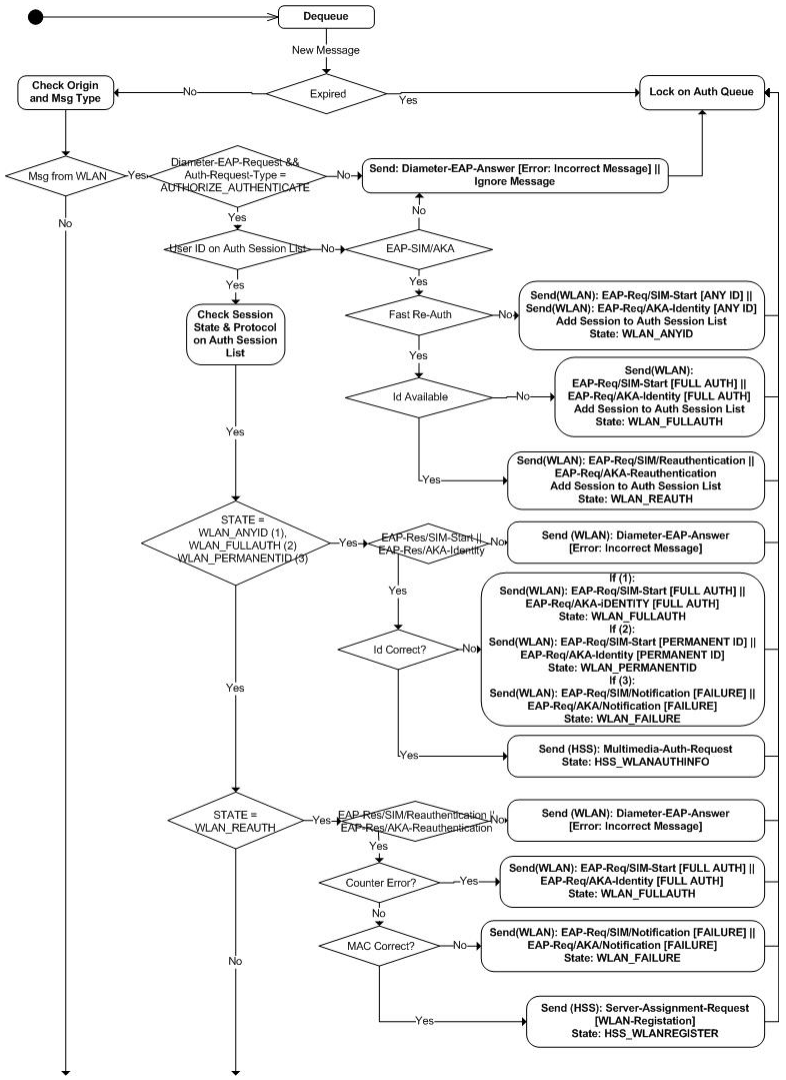

Figura 3.6: Authenticator (1)

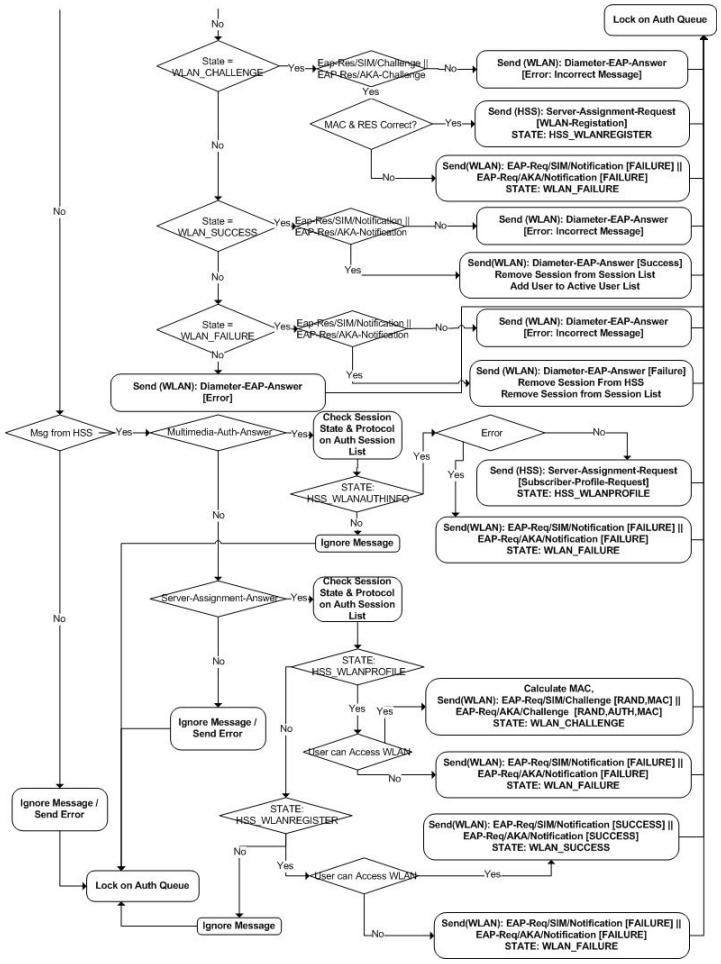

Figura 3.7: Authenticator (2)

Quando um *Authenticator* retira uma mensagem da *Auth Queue* analisa a sua validade pois poderá não fazer sentido processar uma mensagem já muito antiga. De seguida verifica a origem da mensagem. As mensagens processadas pelos *Authenticators* apenas poderão ter dois tipos de origem: WLAN AN ou HSS, se a mensagem tiver outro tipo de origem é enviada uma mensagem de erro ou é ignorada. Posteriormente o *Authenticator* tenta obter o estado actual da sessão, se não conseguir significa que é uma nova sessão e deverá dar inicio ao processo de autenticação utilizando o protocolo EAP-SIM ou EAP-AKA conforme o tipo de utilizador em questão. Uma vez obtido o estado actual da sessão é verificada mais uma vez a mensagem para ver se esta está de acordo com o que era suposto ter sido recebido consoante o estado actual. Se tudo estiver correcto, consoante o estado actual, o *Authenticator* irá enviar uma resposta ou irá fazer um pedido a outro componente.

Session Manager

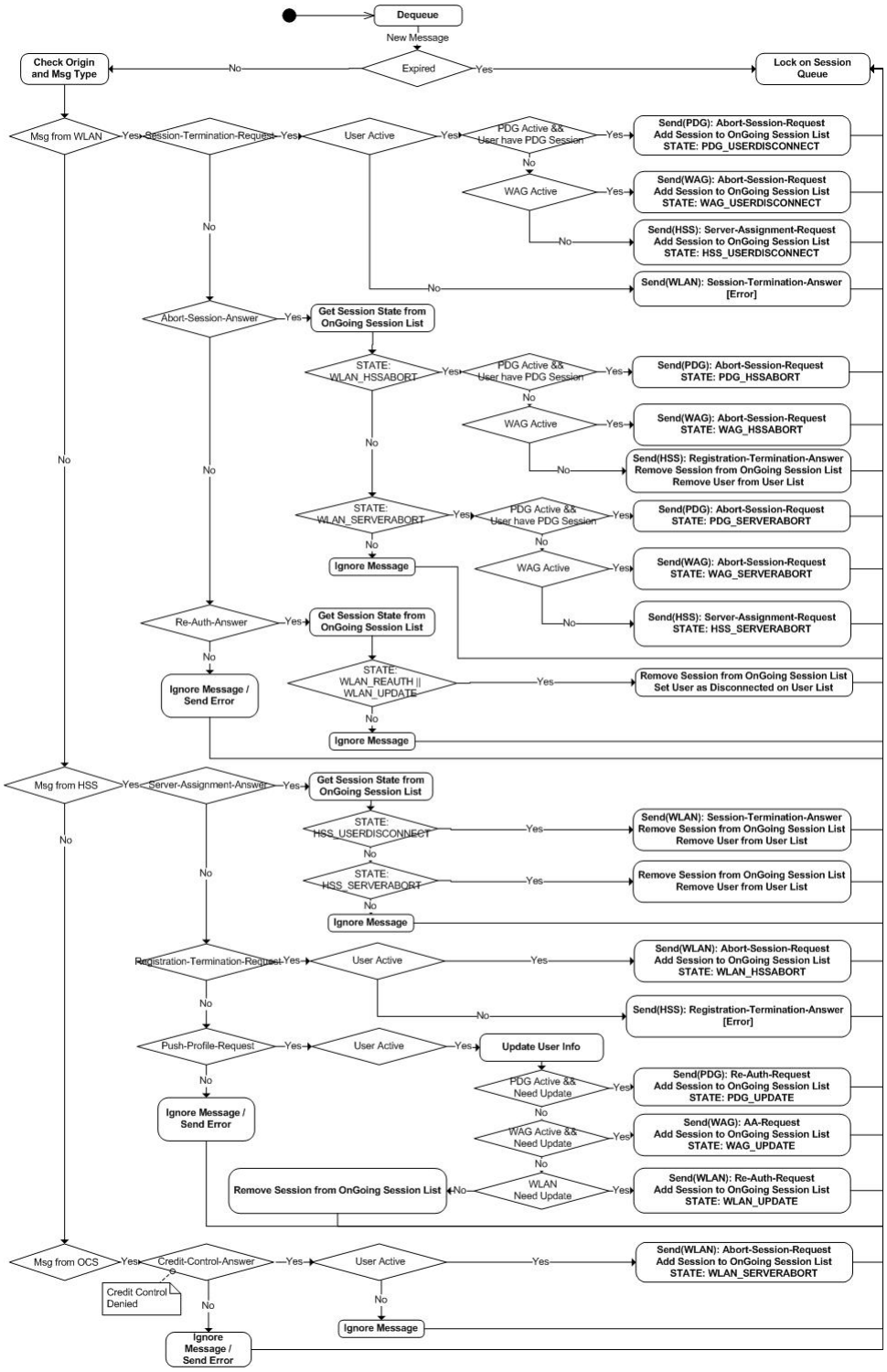

Figura 3.8: Session Manager

O sistema de processamento de mensagens do *Session Manager* é similar ao *Authenticator*. Neste caso, para além de processar mensagens provenientes de componentes do tipo WLAN AN e HSS também poderá processar mensagens vindas do OCS. Isto acontece quando um pedido de *charging* é recusado e é necessário que o *3GPP AAA Server* tome as medidas necessárias para remover a sessão do utilizador em questão.

Proxy Manager

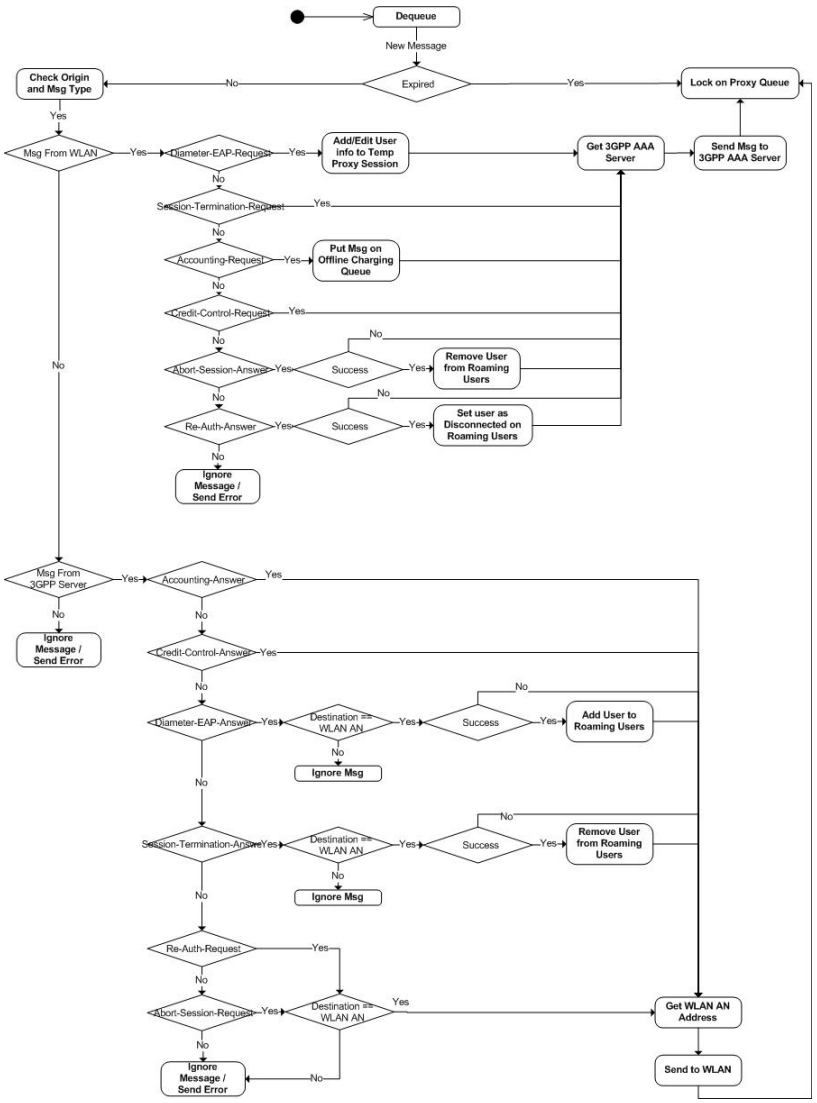

Figura 3.9: Proxy Manager

O *3GPP AAA Server* quando actua como um *Proxy* deverá ser *stateful*, para tal, sempre que recebe uma mensagem deverá fazer uma análise para verificar qual é o estado actual da sessão em curso. Quando verifica que determinado utilizador foi autenticado com sucesso ou a sua sessão terminou por algum motivo deverá, respectivamente, inserir o utilizador numa lista de utilizadores em *roaming* ou removê-lo dessa lista.

Offline/Online Charging

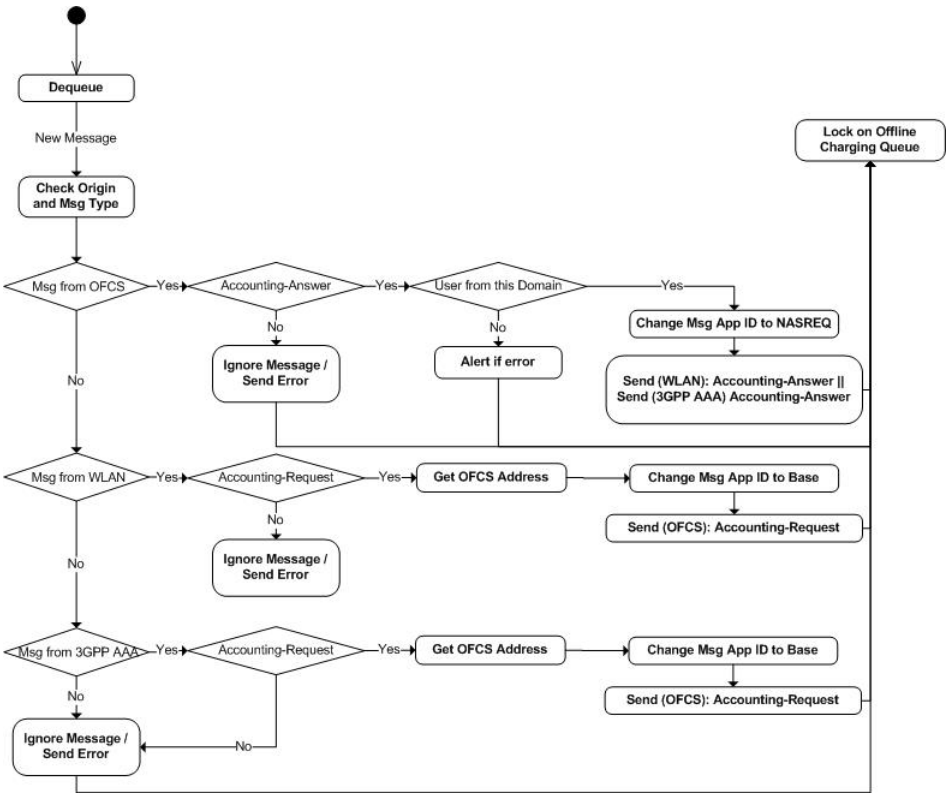

Figura 3.10: Offline Charging

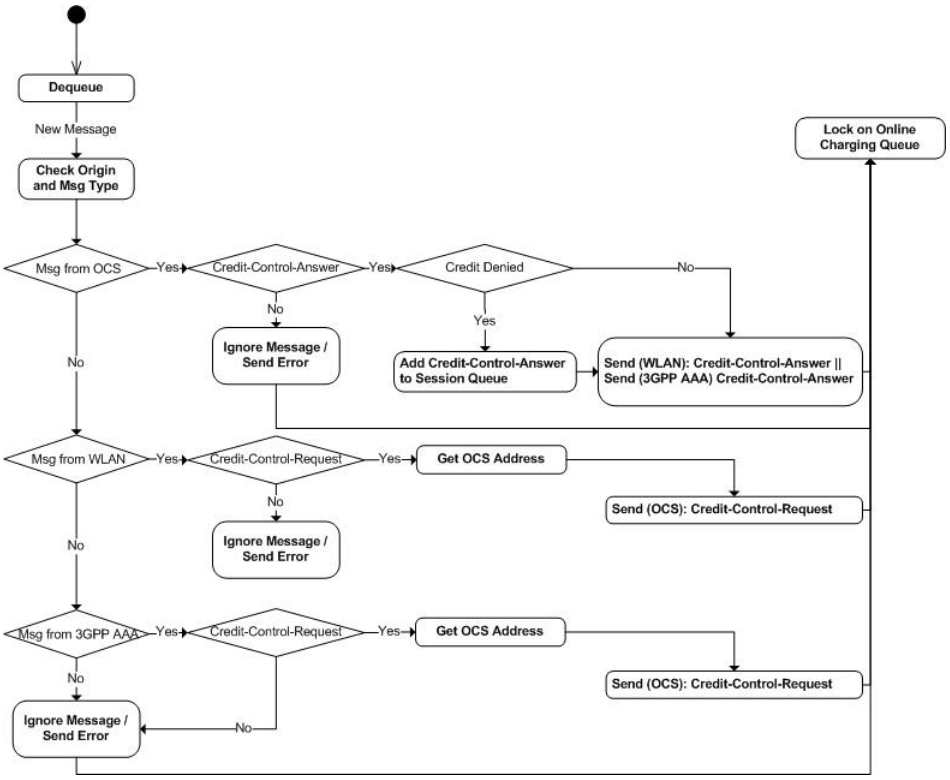

Figura 3.11: Online Charging

O funcionamento destes dois *Managers* é bastante semelhante. Em ambos é feito o reenvio da mensagem recebida para outro componente. No caso do *Offline Charging*, mesmo que a mensagem recebida não seja dirigida ao domínio do *3GPP AAA Server* (no caso do utilizador se encontrar em *roaming*) deverá ser enviada para o OFCS local para efeitos de confrontação com o operador de origem.

3.5 Conclusão

Neste capítulo foram apresentados todos os detalhes relativos ao desenvolvimento da solução. Neste sentido foi feita uma análise dos requisitos funcionais e de interface da solução. De seguida foi feito um enquadramento da solução com os produtos já existentes e por fim foram apresentados os detalhes de concepção onde foi apresentada a perspectiva lógica, diagramas de robustez e de actividade da solução, conforme o processo de desenvolvimento baseado em Iconix e UML.

No próximo capítulo será apresentado o protótipo da solução bem como os principais resultados obtidos.

Capítulo 4

Validação da solução

4.1 Introdução

Neste capítulo serão descritos os testes efectuados à solução e os resultados obtidos. Na primeira parte será apresentado o cenário de testes que foi utilizado descrevendo os diversos componentes que o constituem. De seguida serão apresentados alguns exemplos de eventos resultantes de diversas operações que um utilizador poderá realizar.

4.2 Cenário de Testes

Para testar a solução desenvolvida foi criado um cenário de testes de acordo com a representação da figura 4.1. Devido à dificuldade em obter alguns componentes foi recorrido à simulação no caso da WLAN AN, OCS e OFCS. Os componentes *ip-Cockpit*, *Event Manager* e *XMan* são proprietários da PT Inovação e já foram apresentados na secção 3.3 e por este motivo não serão referidos novamente. No caso do OCS e OFCS a simulação é feita utilizando os componentes *Diameter Signaling Gateway* (DSGW) e *Data Service Control Function* (DSCF).

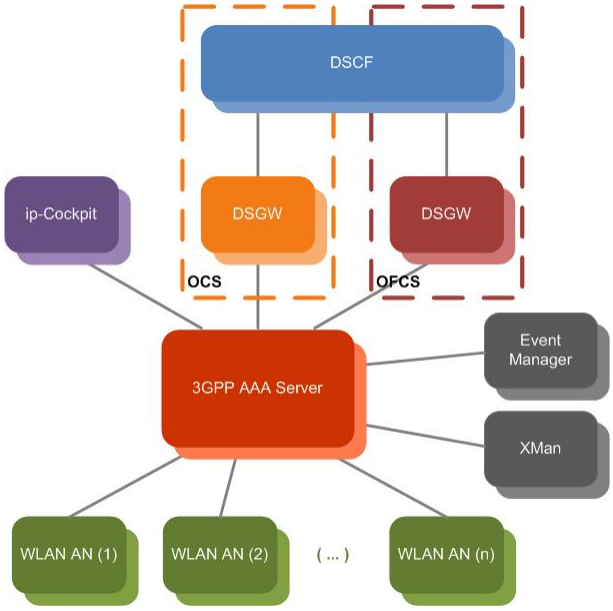

Figura 4.1: Cenário de Testes

Os componentes introduzidos de forma a possibilitar os testes de simulação foram:

DSGW Este componente serve como *gateway* e permite transformar mensagens Diameter em mensagens *Real Time Data Application Part* (RTDAP) (protocolo interno da PT Inovação) e vice-versa.

DSCF Este componente recebe mensagens RTDAP e depois de as analisar envia uma resposta consoante o que esteja configurado.

WLAN AN Este componente pretende simular uma WLAN AN e permite realizar todas as operações suportadas pelo *3GPP AAA Server* desenvolvido. Suporta o protocolo EAP-SIM e EAP-AKA de forma a simular os clientes GSM e UMTS respectivamente. É possível instanciar mais do que um componente deste tipo para que seja possível testar o *3GPP AAA Server* num cenário com múltiplas WLAN ANs. Também é possível configurar este componente de forma a suportar *Online Charging* e/ou *Offline Charging*.

Para cada um dos *n* clientes configurados, este componente tenta simular o comportamento dos clientes, isto é, inicialmente faz a autenticação e autorização normal e, caso a WLAN AN esteja configurada para simular *Online* e/ou *Offline Charging*, envia também pedidos de *Online* e *Offline Charging*. Depois desta fase inicial poderá continuar a enviar

pedidos de *charging* ou poderá iniciar novamente o processo de autenticação e autorização, contudo, desta vez poderá novamente ser normal ou utilizando o *Pseudonym* ou mesmo utilizando a autenticação e autorização rápida. O sistema poderá ainda simular o fim de sessão de um utilizador e reiniciar todo o processo.

Quando recebe um pedido de cancelamento de sessão proveniente do *3GPP AAA Server* este componente desliga o cliente e inicia novamente o processo de autenticação e autorização normal.

A utilização dos componentes DSGW e DSCF permite simular facilmente um componente com uma interface Diameter. Isto deve-se ao facto de serem totalmente configuráveis permitindo assim, através de vários parâmetros, construir uma resposta consoante os valores contidos no pedido. Este tipo de solução foi adoptada uma vez que, como se trata de uma simulação, não surgiu a necessidade de acrescentar mais complexidade ao processamento das mensagens.

4.3 Testes de funcionalidade

Neste secção são apresentados alguns eventos que são enviados para o *Event Manager* quando um determinado utilizador efectua algum tipo de operação. Devido à grande quantidade de eventos que o *3GPP AAA Server* poderá enviar apenas são aqui representados os mais significativos, de modo a facilitar a sua leitura.

Nos exemplos que se seguem um utilizador GSM com o *username* 71156781 irá ligar-se a uma WLAN AN cujo *hostname* é wlan2 e o domínio tst3.ims.drp2. O *3GPP AAA Server* ao qual esta WLAN AN está ligada tem como *hostname* aaa e o domínio é tst3.ims.drp2. Existem ainda o OFCS com *hostname* ofcs e o OCS com *hostname* ocs, ambos têm como domínio tst3.ims.drp2.

A sequência das mensagens trocadas poderá ser vista com mais detalhe na secção 2.6.

Autenticação e Autorização Normal

Neste exemplo o utilizador irá iniciar o processo de autenticação e autorização normal, isto é, irá enviar o NAI contendo o IMSI.

```
Oct 12 16:49:25: evtype=DiameterApp, app=EAPApp, msgtype=DER, session_id=1, username=171156781@tst3.ims.drp2, origin_host=wlan2,
origin_realm=tst3.ims.drp2, destination_host=aaa, destination_realm=tst3.ims.drp2, info=Message Added to Auth Queue
Oct 12 16:49:25: evtype=DiameterApp, app=EAPApp, msgtype=DEA, session_id=1, username=171156781@tst3.ims.drp2, origin_host=aaa,
origin_realm=tst3.ims.drp2, destination_host=wlan2, destination_realm=tst3.ims.drp2, info=Message sent
```

```
Oct 12 16:49:25: evtype=DiameterApp, evsrc=3gppaaa, app=EAPApp, msgtype=DER, session_id=1, username=171156781@tst3.ims.drp2,
origin_host=wlan2, origin_realm=tst3.ims.drp2, destination_host=aaa, destination_realm=tst3.ims.drp2, info=Message Added to Auth Queue
```

Esta primeira troca de mensagens irá permitir ao *3GPP AAA Server* saber qual a identidade do utilizador e qual o protocolo que deverá ser utilizado para além de informação relativa ao próprio protocolo que está a ser utilizado.

```
Oct 12 16:49:25: evtype=DiameterApp, app=WxApp, msgtype=MAR, session_id=2, username=71156781, origin_host=aaa,
origin_realm=tst3.ims.drp2, destination_host=hss, info=Message sent
Oct 12 16:49:25: evtype=DiameterApp, app=WxApp, msgtype=Answer, session_id=2, username=71156781, origin_host=hss,
origin_realm=tst3.ims.drp2, info=Message Added to Auth Queue
Oct 12 16:49:25: evtype=DiameterApp, app=WxApp, msgtype=SAR, session_id=2, username=71156781, origin_host=aaa,
origin_realm=tst3.ims.drp2, destination_host=hss, info=Message sent
Oct 12 16:49:25: evtype=DiameterApp, app=WxApp, msgtype=Answer, session_id=2, username=71156781, origin_host=hss,
origin_realm=tst3.ims.drp2, info=Message Added to Auth Queue
```

Depois de obter a identidade do utilizador o *3GPP AAA Server* irá pedir ao HSS os vectores de autenticação e o perfil do utilizador.

```
Oct 12 16:49:27: evtype=DiameterApp, app=EAPApp, msgtype=DEA, session_id=1, username=171156781@tst3.ims.drp2, origin_host=aaa,
origin_realm=tst3.ims.drp2, destination_host=wlan2, destination_realm=tst3.ims.drp2, info=Message sent
Oct 12 16:49:28: evtype=DiameterApp, app=EAPApp, msgtype=DER, session_id=1, username=171156781@tst3.ims.drp2, origin_host=wlan2,
origin_realm=tst3.ims.drp2, destination_host=aaa, destination_realm=tst3.ims.drp2, info=Message Added to Auth Queue
```

Com as chaves contidas no vector de autenticação o *3GPP AAA Server* irá enviar um *challenge request* para a WLAN AN ao qual esta responde.

```
Oct 12 16:49:29: evtype=DiameterApp, app=WxApp, msgtype=SAR, session_id=2, username=71156781, origin_host=aaa,
origin_realm=tst3.ims.drp2, destination_host=hss, info=Message sent
Oct 12 16:49:29: evtype=DiameterApp, app=WxApp, msgtype=Answer, session_id=2, username=71156781, origin_host=hss,
origin_realm=tst3.ims.drp2, info=Message Added to Auth Queue
```

Uma vez analisada a resposta da WLAN AN o *3GPP AAA Server* regista o estado do utilizador no HSS.

```
Oct 12 16:49:29: evtype=DiameterApp, app=EAPApp, msgtype=DEA, session_id=1, username=171156781@tst3.ims.drp2, origin_host=aaa,
origin_realm=tst3.ims.drp2, destination_host=wlan2, destination_realm=tst3.ims.drp2, info=Message sent
Oct 12 16:49:29: evtype=DiameterApp, evsrc=3gppaaa, app=EAPApp, msgtype=DER, session_id=1, username=171156781@tst3.ims.drp2,
origin_host=wlan2, origin_realm=tst3.ims.drp2, destination_host=aaa, destination_realm=tst3.ims.drp2, info=Message Added to Auth Queue
Oct 12 16:49:29: evtype=DiameterApp, app=EAPApp, msgtype=DEA, session_id=1, username=171156781@tst3.ims.drp2, origin_host=aaa,
origin_realm=tst3.ims.drp2, destination_host=wlan2, destination_realm=tst3.ims.drp2, info=Message sent
Oct 12 16:49:29: evtype=Auth, session_id=1, username=71156781, info=User Authenticated
```

Por fim é enviada a notificação de sucesso bem como a *Master Session Key* para a WLAN AN terminando assim o processo de autenticação e autorização.

Autenticação e Autorização com *Pseudonym*

A autenticação e autorização utilizando o *Pseudonym* como *Identity* é igual à autenticação e autorização normal tirando o facto de ser enviado o *Pseudonym* em vez do IMSI.

```
Oct 12 16:52:17: evtype=DiameterApp, app=EAPApp, msgtype=DER, session_id=3,
username=L1nzJPz0vzX55dnA7N2Q0eO8hdJ02LwoRgSxUbVU0YLZUtgbAAv642O3lm4NHervWtQURX@tst3.ims.drp2,
origin_host=wlan2, origin_realm=tst3.ims.drp2, destination_host=aaa, destination_realm=tst3.ims.drp2, info=Message Added to Auth Queue
```

Este exemplo apenas contém uma mensagem pois a única variação em relação ao anterior é o *username*.

Autenticação e Autorização Rápida

No caso da autenticação e autorização rápida o processo é bastante mais simples pois o *3GPP AAA Server* já tem os vectores de autenticação e o perfil do utilizador, não sendo por isso necessário requisita-los ao HSS.

```
Oct 12 16:51:58: evtype=DiameterApp, app=EAPApp, msgtype=DER, session_id=5,
username=8pj8S9qJoLx3221pQBYWTf7D3l908k3w5QXzjrfsJGKG9yN41pwxW710o3F37483w7u9Y0@tst3.ims.drp2,
origin_host=wlan2, origin_realm=tst3.ims.drp2, destination_host=aaa, destination_realm=tst3.ims.drp2, info=Message Added to Auth Queue
Oct 12 16:51:58: evtype=DiameterApp, app=EAPApp, msgtype=DEA, session_id=5,
username=8pj8S9qJoLx3221pQBYWTf7D3l908k3w5QXzjrfsJGKG9yN41pwxW710o3F37483w7u9Y0@tst3.ims.drp2, origin_host=aaa,
origin_realm=tst3.ims.drp2, destination_host=wlan2, destination_realm=tst3.ims.drp2, info=Message sent
Oct 12 16:51:58: evtype=DiameterApp, app=EAPApp, msgtype=Diameter_EAP_Request, session_id=5,
username=8pj8S9qJoLx3221pQBYWTf7D3l908k3w5QXzjrfsJGKG9yN41pwxW710o3F37483w7u9Y0@tst3.ims.drp2, origin_host=wlan2,
origin_realm=tst3.ims.drp2, destination_host=aaa, destination_realm=tst3.ims.drp2, info=Message Added to Auth Queue
```

O *3GPP AAA Server* identifica a *Identity* do utilizador como sendo uma *Fast re-authentication* e inicia o processo de autenticação rápida enviando para a WLAN AN um *challenge request* contendo, entre outros, o novo *Fast re-authentication username* que deverá ser usado na próxima autenticação e autorização rápida.

```
Oct 12 16:51:58: evtype=DiameterApp, app=WxApp, msgtype=SAR, session_id=2, username=71156781, origin_host=aaa,
origin_realm=tst3.ims.drp2, destination_host=hss, info=Message sent
Oct 12 16:51:58: evtype=DiameterApp, app=WxApp, msgtype=Answer, session_id=2, username=71156781, origin_host=hss,
origin_realm=tst3.ims.drp2, info=Message Added to Auth Queue
```

Depois de analisada a resposta e verificada a autenticidade do utilizador é efectuado o registo do estado no HSS.

```
Oct 12 16:51:58: evtype=DiameterApp, app=EAPApp, msgtype=DEA, session_id=5,
username=8pj8S9qJoLx3221pQBYWTf7D3l908k3w5QXzjrfsJGKG9yN41pwxW710o3F37483w7u9Y0@tst3.ims.drp2,
origin_host=aaa, origin_realm=tst3.ims.drp2, destination_host=wlan2, destination_realm=tst3.ims.drp2, info=Message sent
Oct 12 16:51:58: evtype=DiameterApp, app=EAPApp, msgtype=DER, session_id=5,
username=8pj8S9qJoLx3221pQBYWTf7D3l908k3w5QXzjrfsJGKG9yN41pwxW710o3F37483w7u9Y0@tst3.ims.drp2,
origin_host=wlan2, origin_realm=tst3.ims.drp2, destination_host=aaa, destination_realm=tst3.ims.drp2, info=Message Added to Auth Queue
Oct 12 16:51:58: evtype=DiameterApp, app=EAPApp, msgtype=DEA, session_id=5,
username=8pj8S9qJoLx3221pQBYWTf7D3l908k3w5QXzjrfsJGKG9yN41pwxW710o3F37483w7u9Y0@tst3.ims.drp2,
origin_host=aaa, origin_realm=tst3.ims.drp2, destination_host=wlan2, destination_realm=tst3.ims.drp2, info=Message sent
Oct 12 16:51:58: evtype=Auth, session_id=5, username=71156781, info=User Authenticated
```

Por fim é enviada a notificação de sucesso bem como a *Master Session Key* para a WLAN AN terminando assim o processo de Autenticação e Autorização.

Offline Charging

Neste exemplo a WLAN AN suporta *Offline Charging* por isso o processo é bastante simples.

```
Oct 12 16:49:29: evtype=DiameterApp, app=BaseApp, msgtype=AR, session_id=7,
username=L1nzJPz0vzX55dnA7N2Q0eO8hdJ02LwoRgSxUbVU0YLZUtgbAAv642O3lm4NHervWtQURX@tst3.ims.drp2,
origin_host=wlan2, origin_realm=tst3.ims.drp2, destination_realm=tst3.ims.drp2, info=Message Added to Offline Charging Queue
Oct 12 16:49:29: evtype=OfflineCharging, session_id=8, username=71156781, info=Message Accounting_Request sent to OFCS
Oct 12 16:49:29: evtype=DiameterApp, app=BaseApp, msgtype=AR, session_id=8, username=71156781, origin_host=ofcs,
origin_realm=tst3.ims.drp2, info=Message Added to Offline Charging Queue
Oct 12 16:49:29: ,evtype=OfflineCharging,session_id=7, username=71156781, info=Message Accounting_Answer sent to WLAN
```

Ao receber uma mensagem de *Accounting* proveniente da WLAN AN o 3GPP reenvia-a para o OFCS. Com a resposta o procedimento é semelhante sendo esta reenviada para a WLAN AN.

Online Charging

Tal como no exemplo anterior também neste caso a WLAN suporta *Online Charging*.

```
Oct 12 16:49:30: evtype=DiameterApp, app=CCApp, msgtype=CCR, session_id=5, origin_host=wlan2, origin_realm=tst3.ims.drp2,
destination_realm=tst3.ims.drp2, info=Message Added to Online Charging Queue
Oct 12 16:49:30: evtype=OnlineCharging, session_id=10, username=71156781, info=Message Credit_Control_Request sent to OCS
Oct 12 16:49:30: evtype=DiameterApp, app=CCApp, msgtype=CCA, session_id=10, origin_host=ocs, origin_realm=tst3.ims.drp2,
info=Message Added to Online Charging Queue
Oct 12 16:49:30: evtype=OnlineCharging, session_id=5, username=71156781, info=Message Credit_Control_Answer sent to WLAN
```

A mensagem de *Credit-Control* recebida da WLAN AN é reenviada para o OCS. Neste casso o *request* foi aceite com sucesso por isso a resposta foi reenviada para a WLAN AN sem outro tipo de acções.

Session Termination

No exemplo que se segue um determinado utilizador desliga-se e por isso a WLAN AN notifica o *3GPP AAA Server* do sucedido.

```
Oct 12 17:02:43: evtype=DiameterApp, app=BaseApp, msgtype=STR, session_id=8,
username=L1nzJPz0vzX55dnA7N2Q0eO8hdJ02LwoRgSxUbVU0YLZUtgbAAv642O3lm4NHervWtQURX@tst3.ims.drp2, origin_host=wlan2,
origin_realm=tst3.ims.drp2, destination_host=aaa, destination_realm=tst3.ims.drp2, info=Message Added to Session Queue
```

A WLAN AN envia uma notificação de fim de sessão para o *3GPP AAA Server*.

```
Oct 12 17:02:43: evtype=DiameterApp, app=WxApp, msgtype=SAR, session_id=7, username=71156781, origin_host=aaa,
origin_realm=tst3.ims.drp2, destination_host=hss, info=Message sent
Oct 12 17:02:43: evtype=DiameterApp, app=WxApp, msgtype=Answer, session_id=7, username=71156781, origin_host=hss,
origin_realm=tst3.ims.drp2, info=Message Added to Session Queue
```

O estado do utilizador é removido do HSS.

```
Oct 12 17:02:43: evtype=DiameterApp, app=BaseApp, msgtype=STA, session_id=8,
username=L1nzJPz0vzX55dnA7N2Q0eO8hdJ02LwoRgSxUbVU0YLZUtgbAAv642O3lm4NHervWtQURX@tst3.ims.drp2, origin_host=aaa,
origin_realm=tst3.ims.drp2, destination_host=wlan2, destination_realm=tst3.ims.drp2, info=Mensagem sent
Oct 12 17:02:43: evtype=Session, session_id=8, username=71156781, info=User Disconnected
```

É enviada uma resposta para a WLAN AN terminando assim o processo de fim de sessão.

4.4 Conclusão

Neste capítulo foi apresentado o cenário de testes que foi utilizado para testar o protótipo desenvolvido descrevendo os componentes utilizados. De seguida foram apresentados algum exemplos de eventos que são gerados quando a WLAN AN interage com o *3GPP AAA Server* para efectuar algum tipo de operação.

Apesar dos testes serem bastante preliminares e se ter recorrido à simulação considera-se que os resultados permitiram, com um grau razoável de confiança, validar o correcto funcionamento da solução.

Capítulo 5

Conclusões

Este capítulo será dedicado ao relato das conclusões mais importantes do trabalho desenvolvido assim como apresentação de perspectivas de trabalho futuro.

5.1 Interligação 3GPP-WLAN

A necessidade de integração das redes 3G com as WLANs tem vindo a crescer com o passar do tempo. Isto deve-se ao aparecimento de *hotspots* nos mais variados locais e as diversas vantagens que este integração traz quer para os utilizadores, que poderão aceder aos serviços da rede 3G tomando partido das velocidades permitidas por as redes WLAN, quer para os operadores móveis que prestam o serviço pois criam novas oportunidades de negócio. Neste sentido foram efectuados vários estudos de normalizações de forma a possibilitar a integração destas duas redes.

Foram apresentados o estudo e as normalizações levados a cabo pela entidade 3GPP e que serviram de base no desenvolvimento desta solução de controlo para redes WLAN em convivência com redes 3GPP. Inicialmente foram apresentados os vários cenários de integração possíveis. De seguida foi apresentada a arquitectura de referência proposta, sendo descritos todos os componentes e interfaces que a constituem. Por fim, foram apresentados alguns casos de uso do sistema que envolvem a utilização de procedimentos em várias interfaces.

5.2 Desenvolvimento da Solução

A solução desenvolvida consistiu num *3GPP AAA Server* capaz de autenticar, autorizar e realizar a contabilização de utilizadores WLAN utilizando os serviços e protocolos das redes 3G.

No capítulo 3 são os pormenores da várias fases da elaboração da solução. Inicialmente foi realizado o levantamento de requisitos que a solução deveria cumprir. Numa segunda fase foram apresentados os componentes já existentes na PT Inovação com os quais esta nova solução irá interagir. Por fim, foi descrita a solução propriamente dita apresentando todos os seus módulos e explicado o seu funcionamento através de vários diagramas.

A solução desenvolvida no âmbito desta dissertação consiste na primeira fase do que será o produto final. Por este motivo ficou decidido que nesta primeira fase seria implementado até ao cenário dois (2.2.2) e que nas fazes posteriores seria implementado o terceiro cenário de interligação. Todas as funcionalidades necessárias de forma a suportar o cenário dois estão implementadas, assim como todas as interfaces e respectivos protocolos. Desta forma, podemos afirmar que a solução desenvolvida está em conformidade com todas as normalizações existentes.

5.3 Testes da Solução

Devido à impossibilidade de obter equipamento real os testes realizados à solução desenvolvida passaram por simular alguns componentes com os quais o sistema interage.

Foi delineado e apresentado o cenário de testes utilizado para testar o protótipo e alguns resultados obtidos. Numa primeira parte foram apresentando os vários módulos utilizados de forma a poder simular os diversos componentes. De seguida foram apresentados os eventos resultantes de algumas operações possíveis: autenticação e autorização normal, com *pseudonym* e rápida, *online* e *offline charging* e fim de sessão.

Apesar dos testes terem sido realizados num ambiente simulado considera-se que foram um sucesso pois o sistema respondeu conforme o esperado em todas as situações. No entanto, seria bastante prematuro afirmar que o sistema se irá comportar correctamente num sistema real, uma vez que, os módulos base (ex. Diameter IDS) utilizados para as simulações são os mesmos utilizados no *3GPP AAA Server* podendo existir algumas incompatibilidades quando integrados com diferentes componentes.

5.4 Trabalho Futuro

Uma vez terminada esta fase do projecto foram identificados alguns pontos para trabalho futuro:

1. Teste da solução com componentes reais: Apesar dos testes efectuados, é necessário testar esta nova solução num ambiente real onde os vários componentes que interagem com o sistema e os próprios clientes sejam reais.

2. Suporte do cenário 3: Irão ser acrescentadas novas funcionalidade à solução de forma a suportar o cenário 3 descrito na secção 2.2. Ao completar esta fase espera-se que a solução fique completamente compatível com o estado da arte das normalizações do 3GPP.

Apêndice A

Configurações do Sistema

As tabelas seguintes representam a configuração do sistema que está guardada no XMan com uma pequena descrição. As configurações estão organizadas por directórios e cada ficheiro representa um parâmetro.

Tabela A.1: Configurações do Sistema (Parte 1)

host	Hostname do *3GPP AAA Server*	
realm	Domínio do *3GPP AAA Server*	
port	Porto utilizado por o *3GPP AAA Server*	
command_line _port	Porto para aceder à linha de comandos	
general	auth_session _timeout	Tempo máximo que uma sessão de autenticação poderá ficar inactiva
	msg_timeout	Tempo máximo das mensagens Diameter até serem ignoradas
	authenticators _number	Número de *threads Authenticator* que serão iniciadas
	sessionManagers _number	Número de *threads Session Manager* que serão iniciadas
	proxyManager _number	Número de *threads Proxy Manager* que serão iniciadas
	offlineCharging _number	Número de *threads Offline Charging* que serão iniciadas
	onlineCharging _number	Número de *threads Online Charging* que serão iniciadas

Tabela A.2: Configurações do Sistema (Parte 2)

components	3gppaaa	3gppaaa.list	Lista com a identificação de todos os *3GPP AAA Server*s que estão directamente ligados	
		<id>	host	*Hostname*
			realm	Domínio
			port	Porto
	hss	hss.list	Lista com a identificação de todos os HSSs que estão directamente ligados	
		default_hss _host	*Hostname* do HSS por omissão do sistema	
		default_hss _realm	Domínio do HSS por omissão do sistema	
		<id>	host	*Hostname*
			realm	Domínio
			port	Porto
	ocs	ocs.list	Lista com a identificação de todos os OCSs que estão directamente ligados	
		default_ocs _host	*Hostname* do OCS por omissão do sistema	
		default_ocs _realm	Domínio do OCS por omissão do sistema	
		<id>	host	Hostname
			realm	Domínio
			port	Porto
	ofcs	ofcs.list	Lista com a identificação de todos os OFCSs que estão directamente ligados	
		default_ofcs _host	*Hostname* do OFCS por omissão do sistema	
		default_ofcs _realm	Domínio do OFCS por omissão do sistema	
		<id>	host	Hostname
			realm	Domínio
			port	Porto

Tabela A.3: Configurações do Sistema (Parte 3)

	wlan_an	wlan_an.list	Lista com a identificação de todas as WLAN AN que estão directamente ligadas	
		<id>	host	*Hostname*
			realm	Domínio
			port	Porto
			IPv4	Endereço IPv4 da WLAN AN
			IPv6	Endereço IPv6 da WLAN AN
			offlinecharging	Suporte de *Offline Charging*
			onlinecharging	Suporte de *Online Charging*
event_manager	host	Endereço do *Event Manager*		
	port	Porto		
ids	auth_application _id	*Auth Application ID* utilizado nas mensagens Diameter		
	ids_conf	Configuração da IDS		
	service_context_id	*Service Context ID* das mensagens de *Credit Control*		
log	append	Indica se cada ver que o módulo arranca deve fazer *append* para o antigo ficheiro de *logs*		
	count	Número máximo de ficheiros de *logs* que serão mantidos		
	level	Número de níveis de *log* que estarão activos		
	limit	Limite de tamanho dos ficheiros de *logs*		
	pattern	*Path* e nome base dos ficheiros de *logs*		

Bibliografia

[1] 3GPP. General Packet Radio Service (GPRS); Service description. TS 23.060, 3rd Generation Partnership Project (3GPP), June 2009.

[2] J. Ala-Laurila, J. Mikkonen, and J. Rinnemaa. Wireless LAN Access Network Architecture for Mobile Operators. *IEEE Communications Magazine*, pages 82–89, November 2001.

[3] Pahlavan, K. Krishnamurthy, P. Hatami, A. Ylianttila, M. Makela, J.P. Pichna, R. Vallstron, J. Worcester Polytech. Inst., MA. Handoff in hybrid mobile data networks. *Personal Communications, IEEE*, pages 34–47, April 2000.

[4] Buddhikot, M. Chandranmenon, G. Han, S. Lee, Y.W. Miller, S. Salgarelli, L. Lucent Technol. Bell Labs, Holmdel, NJ, USA. Integration of 802.11 and third-generation wireless data networks. *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, pages 503– 512, April 2003.

[5] Millind M. Buddhikot, Girish Chandranmenon, Seungjae Han, Yui-Wah Lee, Scott Miller, And Luca Salgarelli. Design and Implementation of WLAN/CDMA 2000 Interworking Architecture. *IEEE Communications Magazine*, November 2003.

[6] Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN). http://www.etsi.net/tispan/.

[7] 3GPP. Feasibility study on 3GPP system to Wireles Local Area Network (WLAN) interworking. TR 22.934, 3rd Generation Partnership Project (3GPP), June 2007.

[8] 3GPP. Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking. TS 22.234, 3rd Generation Partnership Project (3GPP), June 2007.

[9] 3GPP. 3GPP system to Wireless Local Area Network (WLAN) interworking; System description. TS 23.234, 3rd Generation Partnership Project (3GPP), June 2008.

[10] 3GPP. 3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3. TS 29.234, 3rd Generation Partnership Project (3GPP), June 2008.

[11] 3GPP. Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging. TS 32.252, 3rd Generation Partnership Project (3GPP), June 2008.

[12] 3GPP. 3G security; Wireless Local Area Network (WLAN) interworking security. TS 33.234, 3rd Generation Partnership Project (3GPP), March 2008.

[13] European Telecommunications Standards Institute (ETSI). Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Requirements and Architectures for Interworking between HIPERLAN/2 and 3rd Generation Cellular systems. TR 101 957, ETSI, August 2001.

[14] 3GPP. Numbering, addressing and identification. TS 23.003, 3rd Generation Partnership Project (3GPP), September 2008.

[15] 3GPP. 3GPP system to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3. TS 24.234, 3rd Generation Partnership Project (3GPP), September 2008.

[16] C. Rigney, S. Willens, A. Rubens, and W. Simpson. Remote Authentication Dial In User Service (RADIUS). RFC 2865, Internet Engineering Task Force, June 2000.

[17] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko. Diameter Base Protocol. RFC 3588 (Proposed Standard), September 2003.

[18] 3GPP. Policy and charging control architecture. TS 23.203, 3rd Generation Partnership Project (3GPP), September 2008.

[19] P. Eronen, T. Hiller, and G. Zorn. Diameter Extensible Authentication Protocol (EAP) Application. RFC 4072 (Proposed Standard), August 2005.

[20] P. Calhoun, G. Zorn, D. Spence, and D. Mitton. Diameter Network Access Server Application. RFC 4005 (Proposed Standard), August 2005.

[21] H. Hakala, L. Mattila, J-P. Koskinen, M. Stura, and J. Loughney. Diameter Credit-Control Application. RFC 4006 (Proposed Standard), August 2005.

[22] 3GPP. Cx and Dx interfaces based on the Diameter protocol; Protocol details. TS 29.229, 3rd Generation Partnership Project (3GPP), September 2008.

[23] C. Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306 (Proposed Standard), December 2005. Updated by RFC 5282.

[24] H. Haverinen and J. Salowey. Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM). RFC 4186 (Informational), January 2006.

[25] J. Arkko and H. Haverinen. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA). RFC 4187 (Informational), January 2006. Updated by RFC 5448.

[26] B. Aboba, D. Simon, and P. Eronen. Extensible Authentication Protocol (EAP) Key Management Framework, August 2008.

[27] B. Aboba and M. Beadles. The Network Access Identifier. RFC 2486, Internet Engineering Task Force, January 1999.

[28] S. Frankel, R. Glenn, and S. Kelly. The AES-CBC Cipher Algorithm and Its Use with IPsec. RFC 3602, Internet Engineering Task Force, September 2003.

[29] P.V. Mockapetris. Domain names - implementation and specification. RFC 1035, Internet Engineering Task Force, November 1987.

[30] A. Niemi, J. Arkko, and V. Torvinen. Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA). RFC 3310, Internet Engineering Task Force, September 2002.

[31] 3GPP. 3G security; Security architecture. TS 33.102, 3rd Generation Partnership Project (3GPP), June 2008.

[32] Mark Collins-Cope, Doug Rosenberg, and Matt Stephens. *Agile Development with ICONIX Process: People, Process, and Pragmatism*. Apress, Berkely, CA, USA, 2005.