
UNIVERSIDADE DE ÉVORA

Mestrado em Engenharia Informática

# Um Sistema de Pagamentos Electrónicos para Serviços e Conteúdos Móveis com Garantias Fortes de Acessibilidade

*David Luís Fernandes de Araújo*

orientador: *Prof. Doutor António Eduardo Dias*

Março de 2005

*Esta dissertação não inclui as criticas e sugestões feitas pelo júri.*

# Prefácio

Este documento contém uma dissertação intitulada *"Um Sistema de Pagamentos Electrónicos para Serviços e Conteúdos Móveis com Garantias Fortes de Acessibilidade"*, um trabalho do aluno David Luís Fernandes de Araújo[1], estudante de Mestrado em Engenharia Informática na Universidade de Évora.

O orientador deste trabalho é o Professor Doutor António Eduardo Dias[2], do Departamento de Informática da Universidade de Évora.

O autor do trabalho é licenciado em Engenharia Informática, pela Universidade de Évora. A presente dissertação foi entregue em Março de 2005.

[1]david.araujo@isp.novis.pt
[2]aed@di.uevora.pt

# Agradecimentos

O trabalho de Mestrado constitui um eminente desafio que obriga o aluno a uma profunda dedicação. Na recta final do trabalho, dedico umas palavras a algumas pessoas, que de uma ou de outra forma, contribuíram para eu alcançar este objectivo a que me propus.

Em primeiro lugar quero agradecer do fundo do meu coração à minha querida amiga Francisca Azevedo e ao meu querido amigo Artur Romão. Sem vocês não teria conseguido. Espero um dia poder retribuir o que fizeram por mim.

Helena Prinxipeza, obrigado pela tua força e carinho nos momentos mais difíceis, e por teres aturado aqui o maluquinho.

Aos meus pais e irmão, obrigado pelo apoio incondicional que me deram, como sempre!

Ao resto da minha família, particularmente os meus avós, obrigado por gostarem tanto de mim e eu de vocês.

Ao Professor Eduardo Dias, obrigado pela disponibilidade demonstrada ao aceitar ser meu orientador e pela ajuda ao longo do meu trabalho.

Aos Professores Gonçalo Jacinto e Luís Arriaga, obrigado pelas valiosas contribuições que deram a este trabalho.

Um grande abraço de obrigado aos meus amigos e colegas Miguel Reis, José Saias, José Carlos, Nuno Palma, Rui Gomes, Luís Martins e Gonçalo Santos. Um beijinho de obrigado à minha coleguinha Teresa Pereira.

# Sumário

O mercado emergente de aplicações e serviços disponibilizados através de dispositivos móveis, em particular os terminais de redes celulares (vulgo telemóveis), potencia um conjunto de modelos de negócio baseados no pagamento destes serviços por parte dos utilizadores.

Mas se este potencial é uma realidade, é também paralelamente um desafio em que se tornam visíveis um conjunto de incógnitas e problemas, sobretudo técnicos, mas também ao nível dos modelos de negócio, que fazem com que a área de pagamentos móveis seja ainda imatura.

Esta dissertação apresenta um sistema de pagamentos móveis para serviços e conteúdos de baixo valor, que tem como principais objectivos: 1) ser independente do operador móvel como meio de acesso; 2) cobrar os serviços e conteúdos móveis adquiridos pelos consumidores através das contas dos respectivos operadores e 3) permitir a partilha da mesma conta por vários utilizadores, independentemente do operador móvel que utilizam.

# An Electronic Payment System For Services and Contends With Strong Guarantees of Accessibility

*ABSTRACT*

The emergent market of applications and services available through mobile devices, in particular mobile phones, enables a set of business models based on the payment of these services by the users.

But if this potential is a reality, it is also a challenge in that a set of unanswered questions and problems, mostly technical, but also concerning business models level, still make mobile payments an immature area.

The work described in this thesis includes the development and implementation of a mobile payment system for low value services and contends, whose main goals are: 1) to be independent of the mobile operator as the access means; 2) to charge the mobile services and contents acquired by consumers through their respective operators accounts and 3) to allow the sharing of the same account by several users, regardless of the mobile operator they use.

# Conteúdo

# Lista de Figuras

# Lista de Tabelas

# Capítulo 1

# Introdução

Este primeiro capítulo apresenta uma introdução sobre as áreas abrangidas pelo trabalho desenvolvido nesta dissertação. Mais concretamente, na secção 1.1 é apresentado o enquadramento do trabalho proposto e descrita a motivação que levou à realização do mesmo. Na secção 1.2 são descritos os objectivos definidos para o trabalho. Finalmente, na secção 1.3 é apresentada a estrutura do documento.

## 1.1 Enquadramento e Motivação

Um dos fenómenos tecnológicos dos últimos tempos, que veio alterar hábitos, atitudes e modos de vivência foi a Internet. O enorme e rápido crescimento da utilização da Internet nos últimos anos, apenas pode ser comparado com a rápida adopção das tecnologias móveis. Com o amadurecimento da Internet surgiram novas formas de fazer negócios, aproveitando assim as características peculiares e favoráveis desta rede de redes. Foi então que surgiu o termo Comércio Electrónico, que se pode definir sumariamente como a condução de transacções financeiras através da Internet.

Posteriormente, o aparecimento das tecnologias móveis veio reforçar e acelerar a comunicação entre as pessoas. A adopção destas tecnologias é um fenómeno ímpar, e hoje em dia a maior parte de nós não dispensa o uso do telemóvel, a face visível desta tecnologia. Segundo a Eurostat (2004), nove em cada dez portugueses usam telemóvel. Pode eventualmente nomear-se o telemóvel como um dos objectos de culto dos nossos tempos.

O desenvolvimento destas tecnologias proporcionou novas oportunidades no desenvolvimento de serviços e conteúdos para ambientes móveis. Consequentemente,

surgiu a necessidade de adaptar os mecanismos de pagamento utilizados para cobrar os serviços e conteúdos adquiridos pelos consumidores a esta realidade. Novos desafios surgiram assim na área dos Pagamentos Móveis, particularmente na vertente de micro-pagamentos, pois a maior parte dos serviços e conteúdos disponibilizados são de baixo valor, e.g., toques para telemóvel, imagens, jogos, músicas e serviços informativos.

De entre as questões e problemas levantados por esta área, há principalmente dois que merecem destaque: o facto de as quantias a pagar serem, tendencialmente muito baixas, e a forte dependência do operador móvel que suporta a comunicação.

No primeiro caso, estamos perante um cenário de micro-pagamentos, para o qual já existe um conjunto alargado de propostas de solução. As mais realistas apontam sempre para um modelo de conta corrente pré-paga, em que os montantes gastos nos pagamentos móveis são debitados nessa conta.

Este facto leva-nos ao segundo problema: em geral, estas contas estão associadas às contas correntes (também elas, na maioria, pré-pagas) que os utilizadores possuem junto dos respectivos operadores móveis. Ao contrário do comércio electrónico na Internet, em que geralmente não é relevante qual o provedor de acesso que se utiliza para se poder desfrutar de pagamentos electrónicos, os modelos preconizados para o mundo móvel têm, quase todos, uma forte associação aos operadores.

Assim, não é viável que um utilizador, que seja cliente de mais do que um operador, possa pagar por serviços móveis sem ter que possuir duas contas correntes para o efeito. Ou, num cenário ainda mais complexo, não é viável que um conjunto de pessoas (e.g., uma família), que utilizem diferentes operadores entre eles, possam pagar por serviços móveis usando uma conta corrente comum. Por outras palavras, não existem garantias fortes de acessibilidade, entendendo-se tais garantias como a independência do meio de acesso aos bens e serviços que se pretendem consumir (comprar).

## 1.2 Objectivos

O objectivo do trabalho realizado no âmbito desta tese de mestrado é definir e implementar um sistema de pagamentos móveis, que proporcione as funcionalidades necessárias para acomodar os requisitos de um sistema de micro-pagamentos, ao mesmo tempo que evita a dependência relativamente a um operador móvel específico (ou qualquer outro meio de acesso). Um objectivo fundamental deste

trabalho é desenvolver o sistema acima referido, sem perder de vista a sua componente prática, tanto do ponto de vista técnico como, sobretudo, de modelo viável de negócio em face das tendências actuais nas áreas de negócio móvel (exceptuando eventuais resistências estratégicas dos próprios operadores).

## 1.3 Organização do Documento

O capítulo 2 apresenta uma série de conceitos relacionados com as áreas nas quais este trabalho se insere, nomeadamente conceitos de comércio electrónico e móvel, assim como de pagamentos móveis.

O capítulo 3 apresenta alguns sistemas de pagamentos electrónicos existentes na área dos micro-pagamentos e pagamentos móveis.

O capítulo 4 propõe um novo sistema de pagamentos electrónicos, para serviços e conteúdos móveis com garantias fortes de acessibilidade.

O capítulo 5 apresenta a implementação do sistema proposto no capítulo 4, seguida de uma análise de desempenho e respectivas conclusões.

Finalmente, no capítulo 6 são apresentadas as conclusões deste trabalho e feita referência a trabalho futuro.

# Capítulo 2

# Pagamento Móveis

## 2.1 Enquadramento do Comércio Móvel

O termo Comércio Electrónico foi definido em [29] como:

"Qualquer sistema tecnológico e económico que potencia ou facilita a actividade comercial de um conjunto variado de participantes através de mecanismos electrónicos."

A explosão e "popularização" da Internet nos últimos anos, veio fomentar o desenvolvimento e a acessibilidade ao Comércio Electrónico. Práticamente ao mesmo tempo, um outro fenómeno de sucesso veio acentuar e modificar a forma como as pessoas comunicavam: o telemóvel. De facto, se existem dois fenómenos tecnológicos que caracterizaram a última década, eles são claramente a Internet e as tecnologias de telecomunicações móveis. Assim, foi de forma "natural" que se juntaram as duas tecnologias, dando origem a um novo canal de negócios, o Comércio Móvel.

O Comércio Móvel, consiste na condução de transacções financeiras, utilizando para tal uma rede móvel e um dispositivo móvel. De forma muito simplista, podemos resumidamente referir que o Comércio Móvel é o Comércio Electrónico sem fios.

O termo Comércio Móvel foi definido em Dezembro de 1997 no *Global Mobile Commerce Forum*, como: *"Providing the Mobile Consumer with the ability to purchase and receive goods and services securely, via wireless technology"*

O conceito de Comércio Electrónico, digitalizou o processo de pagamento, tornando desnecessário o contacto físico entre o comprador e vendedor. A conversão do físico para o virtual trouxe consigo enormes benefícios, tanto para os consumidores como para os comerciantes [31].

O Comércio Móvel, para além das vantagens oferecidas pelo Comércio Electrónico, permite o pagamento de bens e serviços, tanto físicos como digitais, independentemente do local em que o consumidor se encontra, i.e., proporciona mobilidade.

Devido às características particulares das tecnologias envolvidas no Comércio Móvel, a sua emergência opera num ambiente muito diferente do Comércio Electrónico conduzido via Internet. Embora os estudos e análises (*benchmarks*) indiquem um enorme potencial de negócio para o Comércio Móvel (ver secção 2.4), o seu caminho para o esperado sucesso está ainda a esbarrar em vários obstáculos e desafios. Se por um lado as especificidades do Comércio Móvel o tornam complexo, por outro tornam-no extremamente apelativo e levam a acreditar que será um negócio sem precedentes em termos de potencial de mercado. Assim, o Comércio Móvel terá que assentar em modelos, quer técnicos, quer de negócio, de valor acrescentado que alavanquem esse mesmo potencial.

Para os vários intervenientes na cadeia de valor do Comércio Móvel, este, em termos teóricos, já representa vantagens:

- Para os Consumidores representa conveniência.
- Para os Comerciante representa uma nova fonte de receitas e um mercado inexplorado.
- Para os Operadores Móveis representa um aumento do tráfego de dados.

Entre as vantagens e oportunidades oferecidas pelo Comércio Móvel, destacamse as seguintes [30]:

- **Ubiquidade**: O Comércio Móvel possibilita aos consumidores o acesso à informação, independentemente da sua localização física e da altura do dia, garantido-lhes mobilidade total. A informação está disponível quando e onde é mais necessária.
- **Alcance**: O Comércio Móvel potencia o negócio dos comerciantes, oferecendo-lhes a possibilidade de chegarem aos consumidores independentemente da sua localização física e da altura do dia. Por outro lado, acrescenta-lhes um novo canal de vendas, a juntar ao *off-line* e *on-line*.

- **Localização**: O conhecimento da localização física dos consumidores num momento particular, adiciona valor acrescentado ao Comércio Móvel. Através da disponibilização desta informação, muitas aplicações e serviços baseados na localização poderão ser desenvolvidas.

- **Oportunidade**: As potencialidades presentes no Comércio Móvel geram oportunidades de negócio em cima da hora, e.g., compra de bilhetes *"last-minute"*. Desta forma é fomentado o acto de comprar de forma impulsiva.

- **Personalização**: Uma enorme quantidade de informação, serviços e aplicações está disponível actualmente na Internet, o que pode levar à dispersão e consequentemente pouco eficaz e eficiente acesso à informação de facto relevante para o consumidor. Assim, cada vez mais se torna importante a informação ser relevante e filtrada para os consumidores. Através do Comércio Móvel, um consumidor pode personalizar o tipo de serviços e aplicações que deseja ter no seu dispositivo móvel, de forma a espelhar a informação para ele mais relevante, i.e., aumentando a eficiência.

- **Disseminação**: Algumas infraestruturas sem fios possibilitam a entrega de informação de forma simultânea a um conjunto de utilizadores, numa região geográfica específica. Desta forma, consegue-se disseminar informação a uma grande população de consumidores.

Comércio Móvel é um termo que serve de "chapéu" para transacções financeiras móveis. No entanto, este pode ser dividido em vários segmentos:

- *M-Trading*
- *M-Banking*
- *M-Downloads*
- *M-Adveirdising*
- *M-Retail*
- *M-Payments*

Esta dissertação irá concentrar-se no último segmento, os Pagamentos Móveis, nomeadamente a utilização de um dispositivo móvel e de uma rede publica móvel, num cenário de pagamento de bens e serviços.

## 2.2 Um Caso de Sucesso no Comércio Móvel

O maior caso de sucesso no mercado do Comércio Móvel é o serviço iMode [8] do operador Japonês de telecomunicações móveis NTT DoCoMo. A taxa de crescimento deste serviço tem sido impressionante, passando dos 5.5 milhões de subscritores em 2000, para os 42 milhões em 2004[1].

O iMode fornece serviços de voz, correio electrónico e serviços Web aos utilizadores de telemóveis. Os utilizadores pagam uma subscrição para aceder ao serviço iMode, sendo depois cobrado uma pequena quantia por cada pacote de dados descarregados (um pacote tem 128 bytes de dados). Como os telemóveis possuem capacidade de navegação na Internet, os utilizadores podem utilizá-los para fazer compras, da mesma forma que fariam através do seu computador pessoal ligado à Internet.

A maior parte do tempo despendido pelos utilizadores do iMode é a enviar e receber correio electrónico (ver figura 2.1), com uma média de nove mensagens por dia. No entanto, as maiores receitas vêm de pacotes de dados descarregados da Web (ver figura 2.2). Para além disto, os utilizadores pagam taxas adicionais de 1 a 3 dólares por mês, para acederem a serviços *"premium"*, tais como informação, jogos e horóscopo.

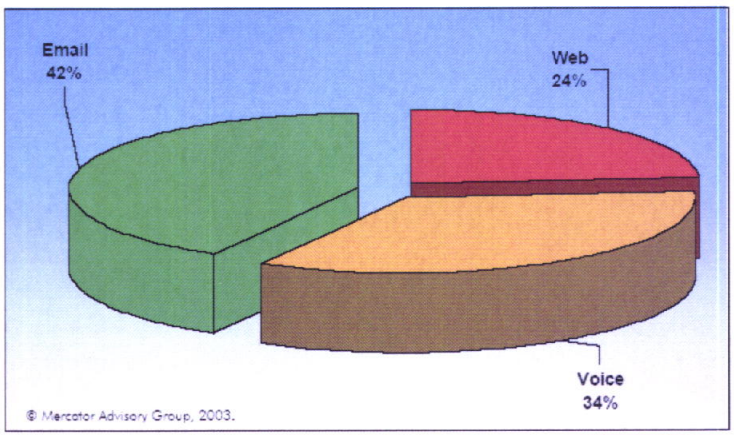


Figura 2.1: Tempo despendido no iMode

[1]Fonte: NTT DoCoMo.

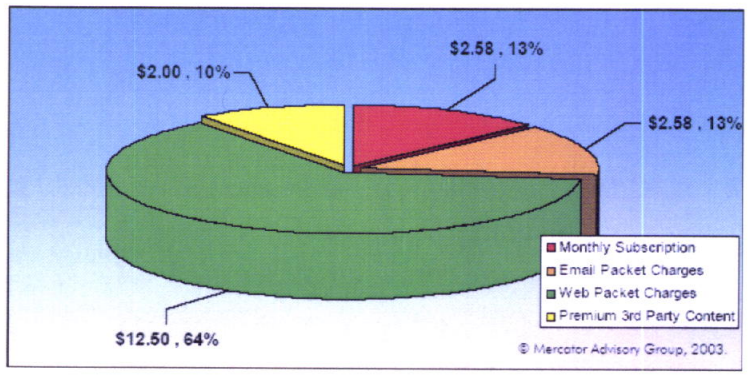


Figura 2.2: Gastos por mês no iMode por utilizador

As particularidades do ambiente em que o iMode subsiste podem em parte explicar o seu sucesso. Entre os factores de sucesso do iMode, destacam-se três que diferenciam o ambiente do Comercio Electrónico Japonês do resto do mundo:

- A baixa taxa de utilização de Internet no Japão. O país tem cerca de 67 milhões de utilizadores de Internet, numa população de 128 milhões[2].
- O Japão tem uma taxa de penetração de telemóveis muito alta (cerca de 79% no final de 2002[3]). A Docomo tem cerca de 59% do mercado[4].
- A maior parte dos Japoneses vive em áreas densamente povoadas, o que leva a que uma grande parte dos subscritores acedam à rede através de um número relativamente baixo de antenas. Consequentemente, os *upgrades* à rede são relativamente fáceis e baratos quando comparados com países onde a densidade populacional é menor.

O sucesso do serviço iMode é um exemplo que os Operadores Móveis que adquiriram as licenças da terceira geração gostariam de seguir. No entanto, os mercados Europeus e Americanos têm pouco em comum com o mercado Japonês, particularmente no que se refere ao contexto cultural. Nomeadamente, o mercado dos Estados Unidos é quase o oposto, i.e., uma alta penetração de computadores pessoais ligados à Internet e uma relativamente baixa penetração de telemóveis. Mais detalhes da estratégia de sucesso da NTT DoCoMo para o Comércio Móvel, podem ser encontrados em [38].

[2]Fonte: Nielsen - Novembro 2004.
[3]Fonte: CommsDesign.
[4]Fonte: NTT DoCoMo.

## 2.3 Novos Processos de Pagamento

Por pagamento entende-se a condução de uma transacção de valor monetário entre duas partes, um comprador e um vendedor. Os processos de pagamento têm vindo a sofrer várias alterações ao longos dos tempos, consequência essencialmente do desenvolvimento tecnológico nesta área.

No inicio, os pagamentos eram conduzidos face-a-face, i.e., com o comprador e o vendedor fisicamente no local da venda e recorrendo a dinheiro físico. Com o aparecimento dos cartões de crédito e débito, as transacções sem dinheiro físico (remotas) tornaram-se mais populares. Posteriormente, as possibilidades criadas com a Internet, levaram ao aparecimento de uma nova geração de pagamentos, os chamados pagamentos electrónicos. Mais recentemente, a crescente utilização de dispositivos móveis por parte das pessoas e o desenvolvimento das tecnologias de Comércio Móvel, levaram ao aparecimento dos chamados Pagamentos Móveis. Um estudo acerca da evolução dos sistemas de pagamentos electrónicos pode ser encontrado em [41].

Pagamento Móvel define-se como: "Utilização de um dispositivo móvel (telemóvel, *Personal Digital Assistant*, etc) na condução de transacções financeiras de uma forma *wireless*, entre um comprador e um vendedor."[33]

Com a chegada das redes de terceira geração, muitos dos problemas enfrentados pelo Comércio Móvel puderam ser ultrapassados, e começaram a criar-se condições para o desenvolvimento de novas e mais apelativas aplicações móveis. Paralelamente, é expectável que os mecanismos de pagamento acompanhem esta evolução, adaptando-se assim a novas realidades. Esta evolução terá como consequência uma crescente utilização, por parte dos consumidores, dos dispositivos móveis em cenários de pagamentos.

De entre os dispositivos móveis existentes, como já referido, os telemóveis são os que representam uma maior fatia do mercado. Assim, no decurso desta dissertação, os telemóveis serão apresentados como o dispositivo móvel de eleição.

A ubiquidade dos telemóveis, que ultrapassam em número os computadores pessoais a nível mundial, torna-os particularmente apelativos como dispositivos de pagamento, sobretudo devido aos atributos que partilham com os veículos de pagamento actuais [33]:

- Os telemóveis GSM contêm um cartão SIM (*Subscriber Identification Module*), i.e., um *Smart Card* com informações acerca da rede, do subscritor

e espaço suficiente em memória para guardar umas centenas de contactos telefónicos. Uma vez que os cartões SIM partilham muitas das características de um *Smart Card* embebido num cartão de pagamento, estes podem facilmente também tornar-se num cartão de crédito ou débito.

- O teclado numérico de um telemóvel permite introduzir números com facilidade, e com alguma dificuldade nomes e moradas de contacto (caracteres alfanuméricos). De uma perspectiva puramente de hardware, não é muito diferente do PIN (*Personal Identification Number*) Pad dos POS (*Point Of Sale*), ou do teclado das ATM (*Automatic Teller Machine*) - um dispositivo de input básico que permite comunicar com uma aplicação de software. Por outro lado, o ecrã do telemóvel é um dispositivo de output que facilita a comunicação do utilizador com o software, e pode apresentar o mesmo tipo de interfaces que o ecrã de uma ATM. À medida que a tecnologia vai evoluindo e se torna mais centrada nos dados, os telemóveis vão assumindo novas formas, com ecrãs maiores e com melhor definição, e os teclados mais próximos do tradicional QWERTY.

- Ultimamente é frequente falar-se de dispositivos *contactless* nos POS, sejam eles dispositivos RFID (*Radio Frequence Identification*) como o ExxonMobil Speedpass [6], ou cartões *Smart Card* com tecnologia RFID como o PayPass da MasterCard [18] ou o ExpressPay da American Express [1]. Os telemóveis sempre foram dispositivos *contactless*, i.e, não precisam de contacto físico para comunicarem com outros dispositivos. Tecnologias como o Bluetooh permitem o estabelecimento de comunicação entre dispositivos de forma automática.

- Os Operadores Móveis têm sistemas de facturação bastante maduros e nos quais os clientes confiam. Os subscritores são normalmente cobrados através de factura mensal (conta pós-paga), ou via uma conta pré-paga. Estes esquemas não são muito diferentes do modo de funcionamento dos cartões de crédito e débito, largamente utilizados em cenários de pagamento.

A figura 2.3 ilustra alguns dos atributos partilhados entre os veículos de pagamento actuais e as tecnologias móveis.

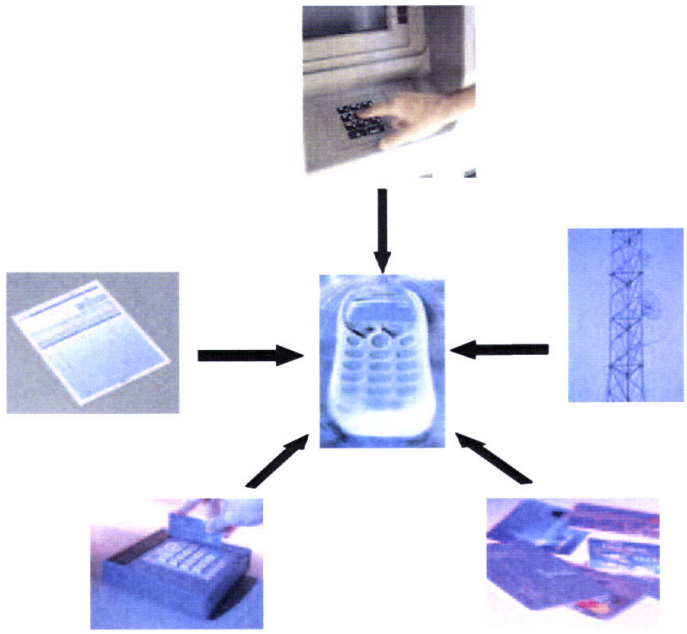

Figura 2.3: Atributos partilhados com os veículos de pagamento

Com tantas funcionalidade e processos em comum com as tecnologias bancárias existentes, reforçamos então que os telemóveis parecem ser candidatos perfeitos a ocupar um lugar de destaque como dispositivo de pagamento.

## 2.4 Tendências e Expectativas

Desde a fase da "bolha" da Internet que os analistas diminuíram fortemente as suas primeiras previsões relativamente ao crescimento do mercado do Comércio Móvel. Existem várias razões para o arranque lento do Comércio Móvel:

- Limitações dos dispositivos e da rede móvel,
- Falta de maturidade das soluções de pagamento, e
- Falta de interesse dos utilizadores.

No entanto, grande parte dos estudos de mercado e *benchmarks* actuais indicam que o Comércio Móvel e as tecnologias envolvidas, continuam a representar uma enorme oportunidade de negócio:

- Segundo a *European Electronic Communications Regulation and Markets* (2004), a taxa de penetração telemóveis na Europa em 2004 foi de 87%.
- Em Setembro de 2004 existiam em Portugal 9,636 milhões de utilizadores de telemóveis, segundo dados que os operadores móveis entregaram à Anacom.
- Segundo a *Internet World Stats* (2005), a taxa de penetração da Internet é actualmente de 66.5% nos Estados Unidos, 52.8% no Japão e 25.2% na Europa.
- A *Jupiter Research* (2004) estima que o Comércio Móvel gere receitas na ordem dos 88 biliões de dólares em todo mundo, no ano de 2009.
- A *Media Capital Telecom* prevê que o mercado da produção de conteúdos para telemóveis valerá em Portugal no ano de 2005, cerca de 370 milhões de euros.

A figura 2.4 ilustra as previsões para receitas provenientes de conteúdos móveis, divididas por regiões.

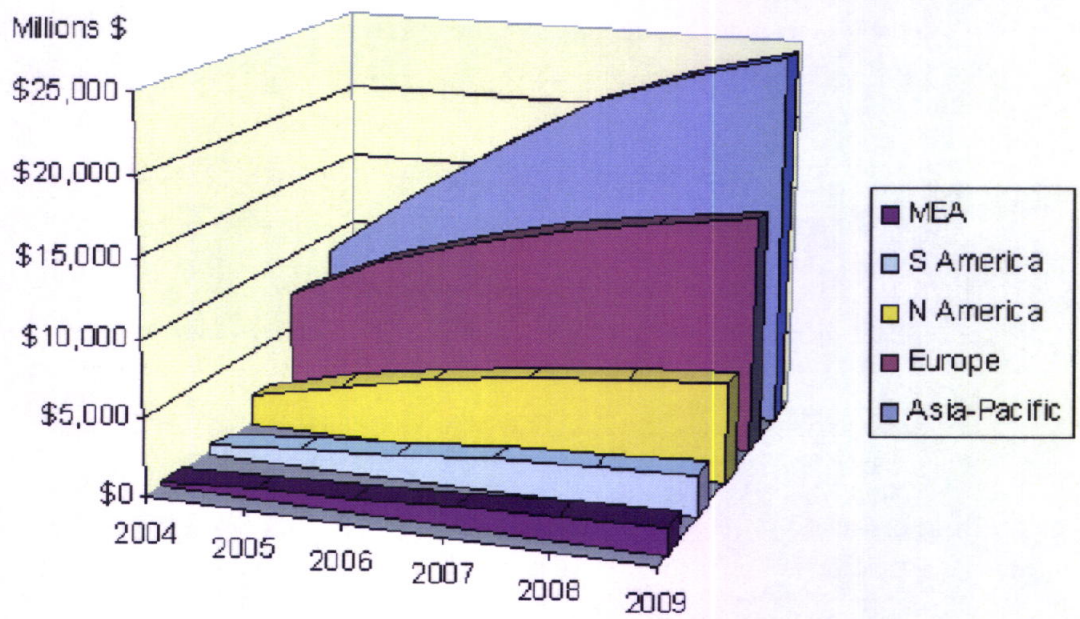


Figura 2.4: Receitas esperadas para conteúdos móveis por região. Fonte:[39]

## 2.5 Características

Os Pagamentos Móveis possuem várias características que os distinguem [37]. Entre tais características destacam-se as seguintes:

- Partes envolvidas
- Montante das transacções
- Local versus Remoto
- Tipo de bens e serviços
- Método de pagamento
- Método de atribuição de preço

De seguida são exploradas as características acima enunciadas, que permitem distinguir as várias categorias de Pagamentos Móveis.

### Partes envolvidas

As partes envolvidas num pagamento permitem diferenciar o tipo de pagamento em causa. Assim, existem as seguintes associações entre os vários intervenientes num processo de pagamento:

- Entre uma empresa e uma pessoa (denominado por *Business-to-Consumer*, B2C).
- Entre duas empresas (denominado por *Business-to-Business*, B2B).
- Entre duas pessoas (denominado por *Person-to-Person*, P2P).

### Montante das transacções

Os montantes envolvidos nos Pagamentos Móveis permitem dividi-los em dois tipos distintos:

- Micro-pagamentos, que abrange pagamentos com quantias inferiores a aproximadamente 10 euros.
- Macro-pagamentos, ou seja pagamentos com quantias superiores a aproximadamente 10 euros.

A quantia de 10 euros é normalmente apresentada na literatura como o ponto de separação entre os micro e macro pagamentos.

A filosofia dos sistemas de pagamentos é normalmente diferente, consoante os pagamentos a processar sejam micro ou macro pagamentos. Para os macro-pagamentos, os aspectos de segurança são mais importantes que para os micro-pagamentos, pois o risco de não pagamento assume outra dimensão. Para os micro-pagamentos, a experiência de compra deverá ser fácil e rápida para o utilizador. Por outro lado, o custo de processamento de um micro-pagamento deverá ser o mais baixo possível, pois as margens de lucro são extremamente baixas.

A vertente dos micro-pagamentos em Pagamentos Móveis é especialmente interessante, pois a maior parte dos serviços e conteúdos disponibilizados em ambientes móveis pertence a esta categoria.

### Local versus Remoto

A localização da compra é outra das características dos Pagamentos Móveis. Assim, existem dois ambientes diferentes:

- Remotos, em que o vendedor e o comprador acordam efectuar uma transacção comercial sobre uma rede móvel (não se encontram na presença um do outro). Este tipo de Pagamento Móvel é semelhante ao pagamento electrónico efectuado através de um computador pessoal conectado à Internet, sendo o computador pessoal substituído pelo dispositivo móvel. Pagamentos de toques, imagens, noticias ou serviços de trânsito, enquadram-se neste tipo de Pagamentos Móveis.

- Locais, em que o vendedor e o comprador trocam informações e bens através de uma canal físico (encontram-se na presença um do outro), mas utilizam tecnologias móveis para efectuar o pagamento. Este tipo de Pagamentos Móveis é similar aos pagamentos face-a-face, com a informação do pagamento a ser transmitida na rede móvel. Pagamentos de parquímetros, de bebidas numa máquina automática, ou de serviços de taxi, enquadram-se neste tipo de Pagamentos Móveis.

### Tipo de bens e serviços

Os Pagamentos Móveis podem ser utilizados para cobrar diversos bens e serviços diferenciados, tais como:

- Bens e serviços físicos, e.g. bebidas, chocolates, bilhetes de cinema e serviços de taxi.
- Bens e serviços digitais, e.g. ficheiros de música ou vídeo e serviços de informação.

No resto da dissertação, o termo "bens" será utilizado para descrever tanto bens e serviços físicos como digitais.

### Método de pagamento

O momento em que o consumidor efectivamente paga pelos bens que comprou, varia entre:

- "Pagar agora" (débito), em que o consumidor paga no momento em que recebe os bens.
- "Pagar depois" (crédito), em que o consumidor paga posteriormente a ter recebido os bens. Por exemplo, um consumidor compra um toque para o seu telemóvel e só o paga no final do mês, através da factura do seu Operador Móvel.
- "Pagar antes", em que o consumidor paga adiantado para obter os bens que deseja. Os cartões pré-pagos de voz, são exemplos deste método de pagamento.

### Método de atribuição de preço

O preço de determinado bem envolvido num Pagamento Móvel pode ser calculado com base nos seguintes modelos:

- Pagamento por visualização, em que o consumidor é cobrado por cada visualização do bem. Enquadra-se neste modelo o *download* de um ficheiro de música, ou a visualização de uma notícia.

- Pagamento por unidade, em que o consumidor é cobrado por cada unidade do bem disponibilizada pelo vendedor. A unidade em questão poderá ser quantificada em termos de volume de dados transmitidos, ou tempo de visualização. Enquadra-se neste modelo o *streaming* de vídeo.
- Subscrição, em que o consumidor paga uma quantia fixa, e pode aceder aos bens de uma forma ilimitada, por um período limitado de tempo. Enquadra-se neste esquema o acesso a artigos de um jornal on-line.

A figura 2.5, ilustra vários tipos de bens, divididos por algumas das características acima referidas.

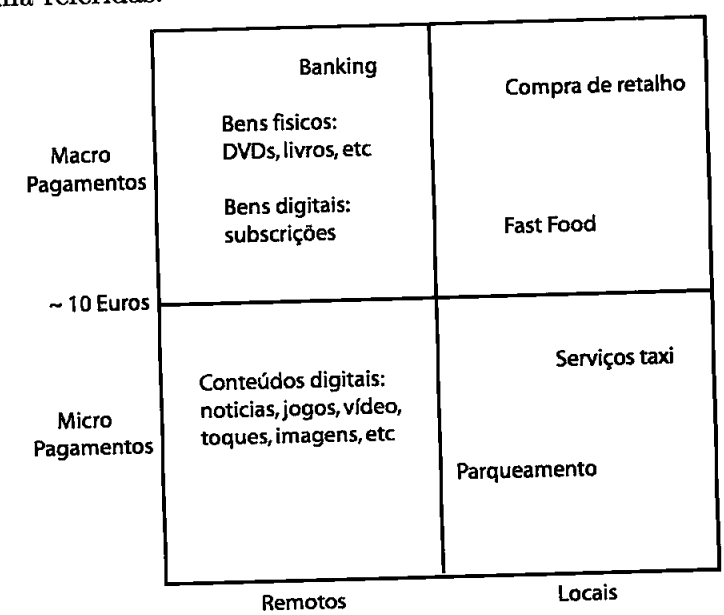


Figura 2.5: O panorama dos Pagamentos Móveis. Fonte: [49]

## 2.6 Intervenientes

Em todos os cenários de pagamento, nomeadamente nos Pagamentos Móveis, existem pelo menos três intervenientes envolvidos:

- Utilizador, é a pessoa que possui um dispositivo móvel e o utiliza para efectuar pagamentos móveis. Também conhecido como consumidor, comprador ou cliente, nesta dissertação será denominado simplesmente por Utilizador. Para realizar Pagamentos Móveis, os Utilizadores precisam de subscrever serviços a um provedor de serviços de pagamento.

- Comerciante, é uma pessoa ou empresa que disponibiliza bens para vender aos Utilizadores. No universo do Comércio Electrónico também é conhecido como provedor de serviços e conteúdos. Os Comerciantes precisam de subscrever serviços a um provedor de serviços de pagamento, que tratará de processar os seus pedidos de pagamento.

- Provedor de Serviços de Pagamento (daqui por diante designado simplesmente por PSP), é uma terceira entidade responsável pelo processo de pagamento entre os Utilizadores e Comerciantes. Nas suas funções inclui-se a autenticação dos Utilizadores e Comerciantes, o início, a autorização e condução de processos de pagamento. O PSP pode verificar o crédito e risco de fraude do Utilizador, assim como efectuar o *customer care* e disputas de pagamento. Uma das maiores responsabilidades do PSP é reportar e consolidar todas as transacções aos Comerciantes.

Um dos candidatos naturais a assumir o papel de PSP em cenários de pagamentos móveis, são os Operadores Móveis (daqui por diante designado simplesmente por Operadores), pois já têm experiência em cobrar pelos serviços de voz e dados. Por outro lado, os custos com as licenças das redes de terceira geração, e o desejo em rentabilizar esses enormes investimentos, faz com que os Operadores estejam bastante interessados em assumir o mercado dos Pagamentos Móveis. O papel de PSP pode também ser assumido por bancos e empresas cujo único foco de negócio seja a disponibilização de serviços de pagamentos a Utilizadores e Comerciantes.

Todas as transacções de pagamento passam pelo PSP, que mantém uma relação de confiança com os Utilizadores e Comerciantes. Os Utilizadores têm que estar confiantes que serão debitados apenas pelos bens recebidos e pelos montantes correctos. Por outro lado, também os Comerciantes têm que estar confiantes que todos os pagamentos serão consolidados de acordo com o contrato formalizado com o PSP. Estas relações de confiança são tipicamente estabelecidas e garantidas através de uma marca forte e da inexistência de erros no historial de processamento das transacções.

Para além dos intervenientes acima descritos, existem outros, que mesmo não interagindo directamente no processo de pagamento, contribuem de forma decisiva para o desenvolvimento do mercado dos Pagamentos Móveis - intervenientes passivos. Entre estes, destacam-se os seguintes:

- Reguladores, são organizações que têm a função de criar regras e controlar a sua aplicação. Este papel pode ser adoptado pelo Estado, entidades reguladoras de bancos ou grupos de normalização.

- Fabricantes, são empresas que desenvolvem e disponibilizam tecnologias para o mercado das telecomunicações móveis. O seu papel é crucial, visto estarem constantemente a efectuar *upgrades* aos dispositivos que permitem tornar o processo de pagamento mais fácil e seguro.

## 2.7 Tecnologias

As tecnologias envolvidas nos Pagamentos Móveis dividem-se em várias categorias. A figura 2.6, adaptada de [43], apresenta essa divisão.

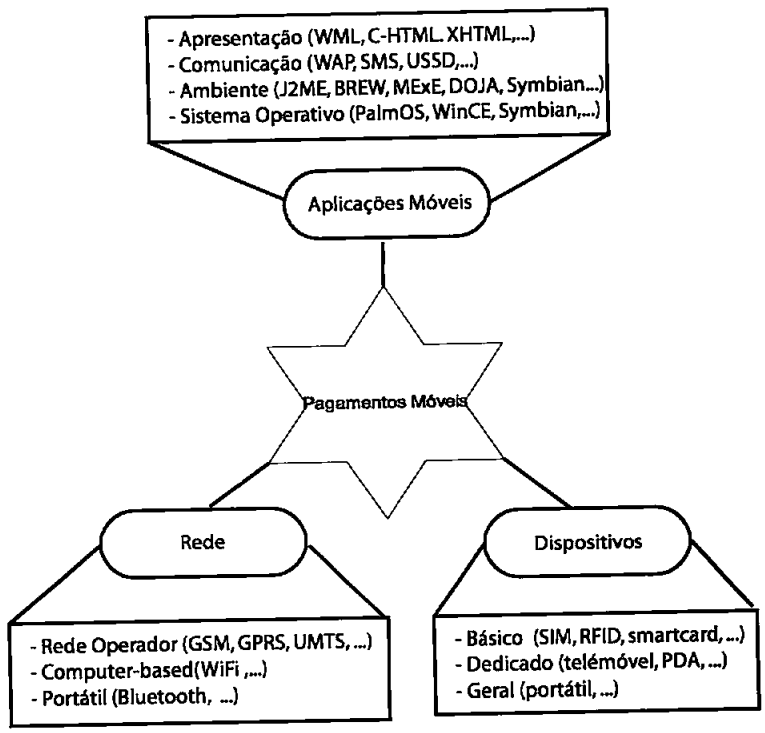


Figura 2.6: Tecnologias utilizados em Pagamentos Móveis [43]

A exposição das tecnologias envolvidas nos Pagamentos Móveis será apresentada de forma bastante superficial, pois não faz parte do foco da dissertação.

Foram consideradas três categorias de tecnologias:

- Rede, representa as tecnologias utilizadas nas infraestruturas de rede sem fios.

- Dispositivos, representa a infraestrutura sem fios utilizada pelo utilizador.
- Aplicações Móveis, representa as tecnologias usadas pelos provedores de serviços e conteúdos móveis.

Mais detalhes e descrições destas tecnologias, encontram-se em [46].

## 2.8 Desafios

Actualmente, é ainda desconhecido, pelo menos publicamente, qual vai ser o modelo de negócio de sucesso dos Pagamentos Móveis. O mercado dos Pagamentos Móveis está ainda na sua infância e a sua fase de maturidade ainda é uma incógnita.

Os desafios enfrentados pelos Pagamentos Móveis dividem-se em dois grupos: desafios de negócio e desafios técnicos [30].

### 2.8.1 Desafios de Negócio

De entre os desafios de negócio dos Pagamentos Móveis, destacam-se os seguintes:

- **Modelo de negócio**: Que tipo de bens vender, a que população, que esquema de pagamentos adoptar, que tipo de parceiros procurar? Estas são algumas das perguntas ainda por responder nesta nova área dos Pagamentos Móveis. As soluções disponibilizadas são ainda demasiado recentes para se conseguir analisar o efeito das escolhas efectuadas, nomeadamente é prematuro retirar ensinamentos destas primeiras experiências. No entanto, é um facto reconhecido, à semelhança de outros negócios no mundo "virtual", que estes modelos são claramente diferenciados em função da cultura de cada país e dos hábitos e vivências dos consumidores.

- **Custo**: O custo é outro dos factores que pode ser uma barreira no rápido desenvolvimento dos Pagamentos Móveis. Qual é o custo de utilizar um mecanismo de pagamento móvel na perspectiva dos consumidores? É suposto o consumidor ter que fazer um *upgrade* ao seu dispositivo móvel, antes de começar a utilizar o método de pagamento?

  Quando custará ao Comerciante a integração de um método de pagamento móvel nas suas aplicações de Comércio Móvel? Mecanismos de pagamento com interfaces simples, podem simplificar o processo de integração e diminuir os custos dessa integração. Estão os comerciantes preparados para pagar as taxas cobradas pelos PSP?

Finalmente, qual será o custo de montar um sistema de Pagamentos Móveis de sucesso? Os custos incluem, investimentos técnicos - hardware, software e integração - e custos de marketing e vendas, e.g. promover o sistema junto dos utilizadores e dos potenciais comerciantes.

- **Apatia dos Utilizadores**: A pouca permeabilidade dos utilizadores pode ser também uma das razões para o lento começo do Comércio Móvel. Os Pagamentos Móveis são um meio novo de pagamento, pouco divulgado e as pessoas sentem-se desconfiadas em utilizar os seus dispositivos móveis para pagar [21]. Por outro lado, ainda não foi desenvolvida uma ou mais *killer application* [28], i.e. uma aplicação atractiva o suficiente para motivar a adopção desta nova forma de pagamento.

### 2.8.2 Desafios Técnicos

De entre os desafios técnicos dos Pagamentos Móveis, destacam-se os seguintes:

- **Segurança**: O aumento da segurança num sistema de pagamentos minimiza o risco de fraudes e consequentemente o custo de manutenção do sistema. Por outro lado, os Utilizadores e Comerciantes sentem-se mais confiantes ao utilizarem um sistema de pagamentos que seja visto como seguro. Existem quatro grandes elementos de segurança que necessitam de ser cumpridos num sistema de Pagamentos Móveis:

  1. Autenticação, permite ao sistema determinar se o Utilizador e o Comerciante envolvidos no pagamento são quem dizem ser.
  2. Confidencialidade, garante que os dados sensíveis de um pagamento não são acedidos por entidades não autorizadas ao sistema.
  3. Integridade, garante que os dados de um pagamento não são alterados, depois do Utilizador os ter autorizado.
  4. Não-repudio, liga os intervenientes de um pagamento, de forma que posteriormente não possam negar a sua participação na transacção.

- **Interoperabilidade**: A interoperabilidade sustenta qualquer sistema de pagamentos global, assegurando que os Utilizadores têm acesso a um vasto leque de bens, e os Comerciantes uma forte base de Utilizadores. Por exemplo, os Operadores deverão passar de soluções proprietárias de pagamentos para ambientes abertos, disponibilizando aos seus clientes o acesso a uma vasta rede de Comerciantes. Várias iniciativas e consórcios estão presentemente a trabalhar para atingir este objectivo [4].

- **Usabilidade**: Estudos mostram que os consumidores são atraídos por produtos simples de usar e que não requerem mudanças de hábitos radicais. Qualquer sistema de pagamentos deverá preencher este requisito. Exemplos do passado [40], nomeadamente em sistemas de micro-pagamentos, mostram que os consumidores não adoptam soluções rebuscadas, mesmo que tecnicamente muito boas. Para os Pagamentos Móveis atingirem elevado potencial, será necessário que a utilização de dispositivos móveis como meio de pagamento, se torne tão ou mais simples que a utilização do "rei" dinheiro.

  A simplicidade apresenta-se assim como um dos desafios mais importantes: a expectativa do utilizador é que tudo funcione sem qualquer problema, sem a necessidade de manobras complexas, ao simples toque de uma tecla. Por outro lado, não basta ser fácil para o utilizador, este tem que entender quais os custos implicados e ficar com a impressão de estar a receber muito valor em troca do que paga.

## 2.9 Ciclo de Vida de um Pagamento Móvel

O ciclo de vida típico de um Pagamento Móvel, apresentado na figura 2.7, está dividido em várias fases [31]. As diversas fases em conjunto, e seguindo um determinado fluxo sequencial, possibilitam a realização de transacções financeiras móveis.

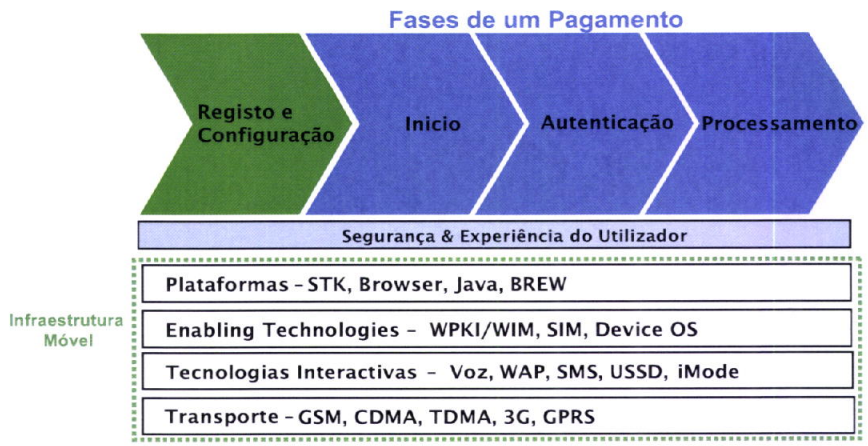


Figura 2.7: Ciclo de vida de um Pagamento Móvel

A primeira fase de um Pagamento Móvel típico consiste no **registo e configuração** do mecanismo de pagamento. O processo de registo pode consistir na abertura de uma conta por parte do Utilizador junto de um PSP, de forma a utilizar os seus serviços de pagamento. O processo de configuração pode incluir a instalação de uma aplicação e de dados de pagamento no dispositivo móvel do Utilizador. A fase de registo e configuração acontece normalmente uma só vez, e pode ser conduzido sobre a rede móvel, Internet, ou em pessoa.

Estando a fase de registo e configuração concluída, o Utilizador pode começar a efectuar Pagamentos Móveis. Assim, a segunda fase é o **início do pagamento**, e ocorre sempre que se processa uma transacção. Esta fase incluí o pedido de pagamento por parte do Utilizador junto do Comerciante, através de uma interface previamente definida, e onde são disponibilizados os dados do pagamento.

A terceira fase, **autenticação do utilizador**, é um dos passos mais importantes na transacção de um pagamento. É imperativo que o Utilizador esteja confiante que os detalhes do seu pagamento não serão comprometidos. É igualmente importante que o Comerciante esteja confiante que o cliente com quem está a negociar é válido.

A quarta e última fase, **processamento do pagamento**, ocorre assim que os detalhes do Utilizador estejam autenticados e consiste na autorização da transacção. No mundo físico, a parte final deste processo envolve a impressão de um recibo que confirme o pagamento. No ambiente móvel também podem ser emitidos recibos digitais, confirmando que a transacção foi efectuada com sucesso.

## 2.10 Cenários de Pagamento

Como foi descrito na secção 2.5, os Pagamentos Móveis apresentam diversas características que possibilitam a sua utilização em cenários de pagamento distintos [26]. Os três cenários apresentados de seguida, partilham as seguintes características:

- Os intervenientes no processo de pagamento são o Utilizador, Comerciante e PSP.
- O Utilizador e Comerciante registam-se junto do PSP, antes de começarem a utilizar os serviços de pagamento disponibilizados por este.
- O Utilizador pode escolher o método de pagamento que deseja (conta pré-paga, pós-paga ou pagar no momento) junto do PSP.

### 2.10.1 Conteúdos Digitais

O cenário "Conteúdos Digitais" apresenta as seguintes características (tal como definidas em 2.5):

- Montante das transacções: Micro-pagamentos
- Tipo de bens e serviços: Digitais
- Local versus Remoto: Remoto

Neste cenário de pagamento, o Utilizador usa o seu dispositivo móvel para comprar conteúdos digitais, e.g. ficheiros de músicas ou toques de telemóvel, junto de um Comerciante. Os pagamentos são cobrados através da conta do Utilizador no PSP. A figura 2.8 apresenta o diagrama de sequência do processo de pagamento.

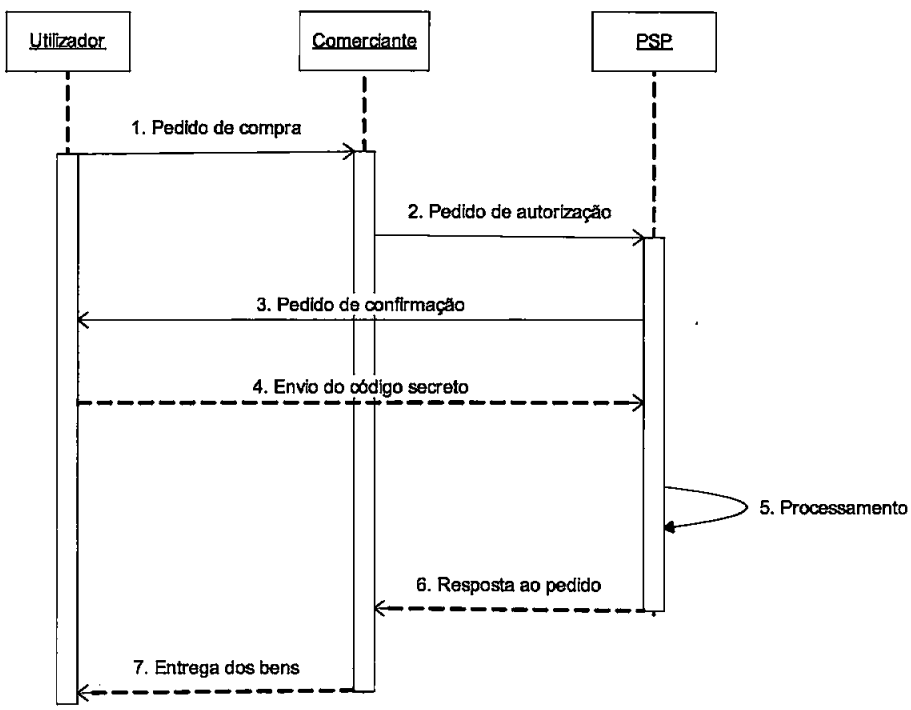


Figura 2.8: Diagrama de sequência do cenário Conteúdos Digitais

1. Pedido de compra por parte do Utilizador e indicação do desejo em realizar um pagamento móvel.
2. Pedido de autorização do pagamento junto do PSP.

3. Pedido de autenticação e confirmação do pagamento ao Utilizador.
4. Autenticação e confirmação do pagamento através da apresentação do código secreto do Utilizador.
5. Processamento do pedido de pagamento por parte do PSP.
6. Envio da resposta ao pedido de pagamento para o Comerciante.
7. Entrega do conteúdo requerido pelo Utilizador no passo 1.

Este cenário poderia igualmente ser aplicado à Internet de rede fixa, com o Utilizador a usar um computador pessoal para efectuar o pedido de pagamento, e o seu dispositivo móvel para se autenticar e confirmar o pagamento.

### 2.10.2 Local de Venda Assistido

O cenário "Local de Venda Assistido" apresenta as seguintes características (tal como definidas em 2.5):

- Montante das transacções: Micro e Macro pagamentos
- Tipo de bens e serviços: Físicos
- Local versus Remoto: Local

Neste cenário de pagamento, o Comerciante é uma pessoa que oferece os seus serviços ou bens ao Utilizador no local da venda, e.g. o pagamento de um serviço de táxi, ou o pagamento de uma refeição num restaurante. O processo de pagamento é inicializado pelo Comerciante no local da venda. Os pagamentos são cobrados através da conta do Utilizador no PSP. A figura 2.9 apresenta o diagrama de sequência do processo de pagamento.

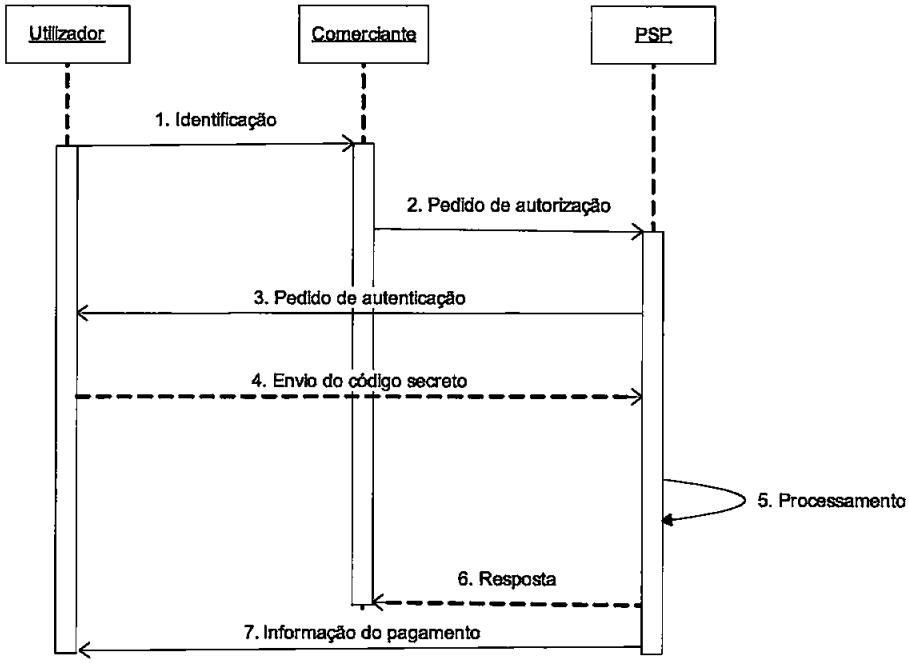


Figura 2.9: Diagrama de sequência do cenário Local de Venda Assistido

1. O Utilizador disponibiliza o seu número de telemóvel ao Comerciante.
2. O Comerciante envia os dados do pagamento e o número do telemóvel do Utilizador para o PSP. Para tal, o Comerciante poderá utilizar um telemóvel ou um dispositivo especifico disponibilizado pelo PSP para o efeito.
3. Pedido de autenticação e confirmação do pagamento ao Utilizador.
4. Autenticação e confirmação do pagamento através da apresentação do código secreto do Utilizador.
5. Processamento do pagamento por parte do PSP.
6. Envio da resposta ao pedido de pagamento para o Comerciante.
7. Envio da informação do estado do pagamento para o Utilizador.

### 2.10.3 Local de Venda Não Assistido

O cenário "Local de Venda Não Assistido" apresenta as seguintes características (tal como definidas em 2.5):

- Montante das transacções: Micro pagamentos
- Tipo de bens e serviços: Físicos
- Local versus Remoto: Local

Neste cenário, o Comerciante é uma máquina física, e.g. uma máquina de venda automática, e o Utilizador encontra-se fisicamente na sua presença. O pagamento de parquímetros, ou a venda de produtos alimentares no metro, são serviços adequados para este cenário. O processo de pagamento é inicializado pelo Utilizador no local da venda. Os pagamentos são cobrados através da conta do Utilizador no PSP. A figura 2.10 apresenta o diagrama de sequência do processo de pagamento.

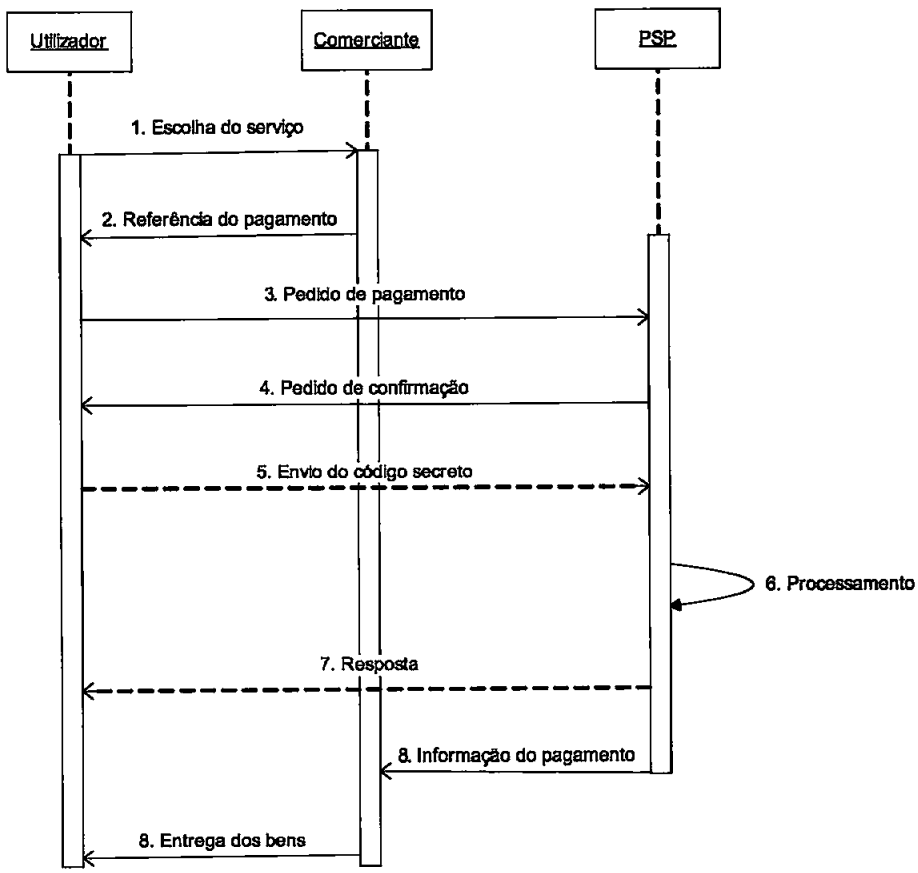


Figura 2.10: Diagrama de sequência no cenário Local de Venda Não Assistido

1. O Utilizador escolhe o bem ou serviço que deseja comprar junto do Comerciante (neste caso uma máquina).

2. O Comerciante disponibiliza uma referência de pagamento ao Utilizador.

3. O Utilizador envia os dados do pagamento para o PSP.

4. Pedido de autenticação e confirmação do pagamento ao Utilizador.

5. Autenticação e confirmação do pagamento através da apresentação do código secreto do Utilizador.

6. Processamento do pagamento por parte do PSP.

7. Envio da resposta ao pedido de pagamento para o Utilizador.

8. Envio da informação do estado do pagamento para o Comerciante.

9. Entrega do bem ou serviço requerido pelo Utilizador no passo 1.

## 2.11 Porquê Micro-Pagamentos?

A expansão registada no negócio de voz oferecido pelos Operadores levou a uma saturação do mercado e consequente estagnação em termos de receitas. Assim, os Operadores olham agora para novas oportunidades de negócio capazes de gerar receitas, por forma a aumentar o ARPU (*Average Revenue Per User*).

Nomeadamente, com a aquisição das dispendiosas licenças da terceira geração, os Operadores necessitam de rentabilizar os investimentos efectuados [36]. A área dos dados surge assim como uma aposta natural num mercado ainda por explorar, em que a maior parte dos bens e serviços disponibilizados enquadra-se na categoria dos micro-pagamentos. Este segmento de mercado é extremamente apetecível, pois para além de ser muito bem aceite pelos consumidores, comporta riscos reduzidos em termos de fraude, comparado com o mercado dos macro-pagamentos. A tecnologia SMS (*Short Message Service*) é um bom exemplo da forte apetência dos consumidores por serviços de dados.

O facto dos bens e serviços disponibilizados hoje em dia nesta área serem de baixo valor, potencia o acto de compra impulsiva por parte dos consumidores. A Ovum Research, prevê que o mercado dos toques (extremamente impulsivo) na Europa, passe dos actuais 16 milhões de euros para 721 milhões em 2008. Por outro lado, é extremamente importante que os consumidores sintam que estão a receber muito em troca do que pagam.

A relação de confiança que os clientes mantêm com os seus Operadores, nomeadamente a nível de facturação, torna-os em canais de cobrança privilegiados. A utilização das contas que os clientes possuem nos seus Operadores, surge assim como ideal para cenários de micro-pagamentos móveis.

# Capítulo 3

# Sistemas de Pagamentos Electrónicos

Este capítulo apresenta alguns sistemas de micro-pagamentos e pagamentos móveis disponibilizados no mercado.

## 3.1 Sistemas de Micro-pagamentos

As taxas elevadas a pagar pela utilização de cartões de crédito, tornam a sua utilização proibitiva para pagamentos de baixo valor (imagine-se a situação da taxa cobrada ser superior ao valor do próprio pagamento).

Outra das desvantagens inerentes à utilização de cartões de crédito em cenários de pagamento on-line, é o facto do utilizador ter que introduzir os seus dados confidencias cada vez que efectua uma compra. Esta questão, a da confidencialidade da informação, que é ainda um dos principais motivos da relativa baixa adesão ao Comércio Electrónico. Apesar de tudo, têm surgido ultimamente algumas iniciativas para tentar contornar estas dificuldades. O protocolo 3D Secure da VISA [25] e o sistema português MBNet da Sociedade Interbancária de Serviços (SIBS) [19], são disso exemplo.

Assim sendo, surgiu a necessidade de desenvolver sistemas apropriados ao processamento de micro-pagamentos, de forma a tornar rentável um segmento de mercado, pouco explorado e com enorme potencial.

Os dois sistemas de micro-pagamentos abaixo apresentados são soluções desenvolvidos para pagamentos sobre a Internet de rede fixa. No entanto, e sal-

vaguardando as diferenças evidentes entre rede fixa e rede móvel, estes sistemas poderiam ser migrados para um ambiente móvel.

### 3.1.1 Peppercoin

*"big change for small change"* - Peppercoin$^{TM}$

A PepperCoin$^{TM}$ [23] disponibiliza um sistema de pagamentos com o mesmo nome, que permite aos comerciantes vender os seus conteúdos digitais de uma forma rentável, aplicado a quantias tão pequenas como poucos cêntimos. Os consumidores podem usar uma única conta PepperCoin junto de vários comerciantes, o que torna o sistema universal e conveniente.

A tecnologia do PepperCoin, foi desenvolvida pelos professores Silvio Micali e Ronald L. Rivest do *Massachusetts Institute of Technology.*

Através de mecanismos de probabilidades matemáticas [24], a que a empresa chama de agregação universal, em detrimento dos tradicionais mecanismos de agregações de transacções, o PepperCoin reduz o volume de transacções que precisam de ser processadas por entidades terceiras ou instituições financeiras. Desta forma, evita-se a ineficiência subjacente à utilização de cartões de crédito em pagamentos de baixo valor, e reduz-se os custos imputados aos comerciantes, tornando o negócio mais rentável em toda a sua cadeia de valor.

A PepperCoin, utiliza tecnologias de cifra baseadas em certificados digitais, de forma a proteger os pagamentos dos seus clientes.

Antes de começar a vender os seus conteúdos digitais através do PepperCoin, o Comerciante terá que passar por duas fases:

1. **Registo**: O Comerciante regista-se perante a PepperCoin, fornecendo os dados necessários do processo contratual. Após o registo, o PepperCoin disponibiliza ao Comerciante uma aplicação, de nome PepperMilling, que este irá utilizar para vender os seus conteúdos.

2. **Preparação dos conteúdos**: Através do PepperMilling, o Comerciante empacota e cifra o conteúdo digital a vender. Como resultado, é gerado um ficheiro, designado PepperBox, que contém o conteúdo cifrado, a informação do seu montante e a identificação do Comerciante. O PepperBox é disponibilizado aos clientes no portal do Comerciante, ou via outro método de entrega, e.g. correio electrónico.

Quanto ao cliente, este também terá que passar por uma fase de registo e configuração, antes de começar a comprar via o sistema PepperCoin. No processo contratual, o cliente escolhe o(s) método(s) de pagamento da sua conta e disponibiliza os dados confidencias dessa(s) escolha(s), e.g. número de cartão de crédito ou NIB. Após o registo, o PepperCoin disponibiliza ao cliente uma aplicação, designada PepperPanel, que terá que ser instalada no computador de onde se irão realizar os pagamentos. O PepperPanel, serve para o cliente criar a moeda do sistema, designada por PepperCoins, no momento de pagar, e decifrar as PepperBox.

Na figura 3.1, é apresentado o diagrama de sequência do processo de pagamento através do sistema de micro-pagamentos PepperCoin.

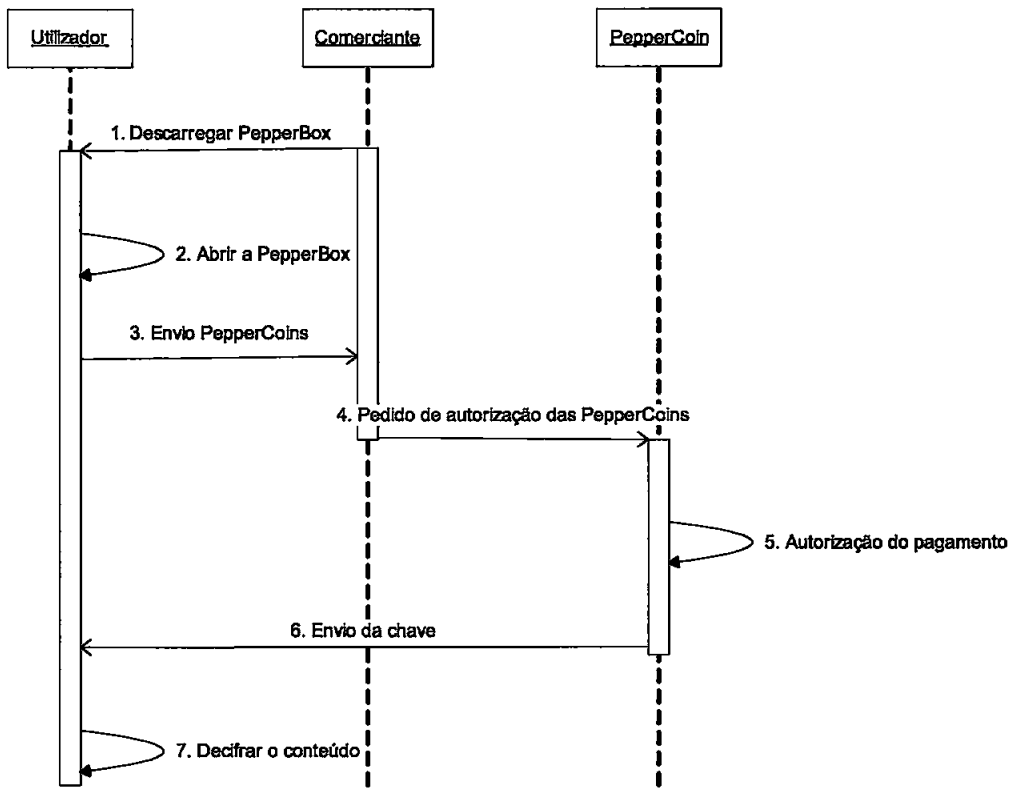


Figura 3.1: Diagrama de sequência do processo de pagamento no Peppercoin

1. Para ter acesso ao conteúdo pretendido, o Utilizador descarrega a PepperBox do portal do Comerciante, ou recebe via uma mensagem de correio electrónico.

2. O Utilizador abre a PepperBox através da sua PepperPanel, dando-lhe acesso aos detalhes da compra, tais como, preço, identificação do comerciante e descrição do conteúdo, assim como ao conteúdo cifrado.

3. Após confirmar os detalhes da compra, o Utilizador utiliza a sua PepperPanel para gerar as PepperCoins necessárias para efectuar o pagamento, enviando-as para o Comerciante. Cada uma das PepperCoin, é criada na altura da compra, e contém informação dos gastos acumulados do cliente (esta informação serve para cobrar o cliente de forma coerente).

4. O Comerciante reenvia as PepperCoins para o PepperCoin, para autorizar o pagamento.

5. O PepperCoin valida as PepperCoins, i.e. verifica o certificado digital, a assinatura do Utilizador, as datas de expiração e a autorização do Utilizador para comprar o tipo de conteúdo em questão. De seguida, executa os mecanismos de detecção de fraude.

6. Se o pagamento tiver sido autorizado com sucesso no passo anterior, o PepperCoin envia a chave que decifra o conteúdo cifrado para o Utilizador.

7. Ao receber a chave, e através da seu PepperPanel, o Utilizador decifra o conteúdo cifrado.

Periodicamente, o PepperCoin cobra os Utilizadores pelas suas compras, e paga aos Comerciantes pelos conteúdos vendidos.

### 3.1.2 FirstGate click&buy

*"FIRSTGATE click&buy is a revolutionary new payment channel for the Internet that empowers content providers to become content merchants, transforms Web surfers into customers, and translates clicks into transactions"* - FirstGate click&buy

Como já foi referido anteriormente, um dos grandes inconvenientes em utilizar cartões de crédito para compras on-line, é o facto de os consumidores terem que fornecer os dados confidencias do seu cartão de crédito por cada compra que fazem. Para minimizar este problema, têm surgido uma série de sistemas de pagamentos com base num conceito muito simples - guardar os dados confidenciais do cliente e fornecer-lhes um código secreto para se autenticarem no sistema.

Assim, os clientes podem carregar a sua conta com um montante pré-definido e ir gastando, ou serem cobrados numa base periódica pelas suas compras. O facto do uso de cartão de crédito ser proibitivo para transacções de baixo valor, torna este tipo de sistema ideal para cenários de micro-pagamentos. O sistema de micro-pagamentos Firstgate click&buy [7], funciona com base neste conceito, as chamadas contas *pre-arranged*.

Entre os serviços e conteúdos oferecidos pelos comerciantes aderentes ao First-Gate, encontra-se música, vídeo, jogos e serviços de informação. O FirstGate permite que os comerciantes escolham o método de pagamento que mais lhes convém, e.g., por clique, por item, por minuto, por visionamento ou subscrição.

O cliente ao registar-se no FirstGate, terá que indicar o(s) método(s) de pagamento para a sua conta e disponibilizar os dados confidencias dessa(s) escolha(s), e.g., número de cartão de crédito ou NIB. Como resultado, a FirstGate atribui ao cliente um código secreto que o identifica perante o sistema no momento de pagar.

Na figura 3.2, é apresentado o diagrama de sequência do processo de pagamento através do sistema de micro-pagamentos FirstGate.

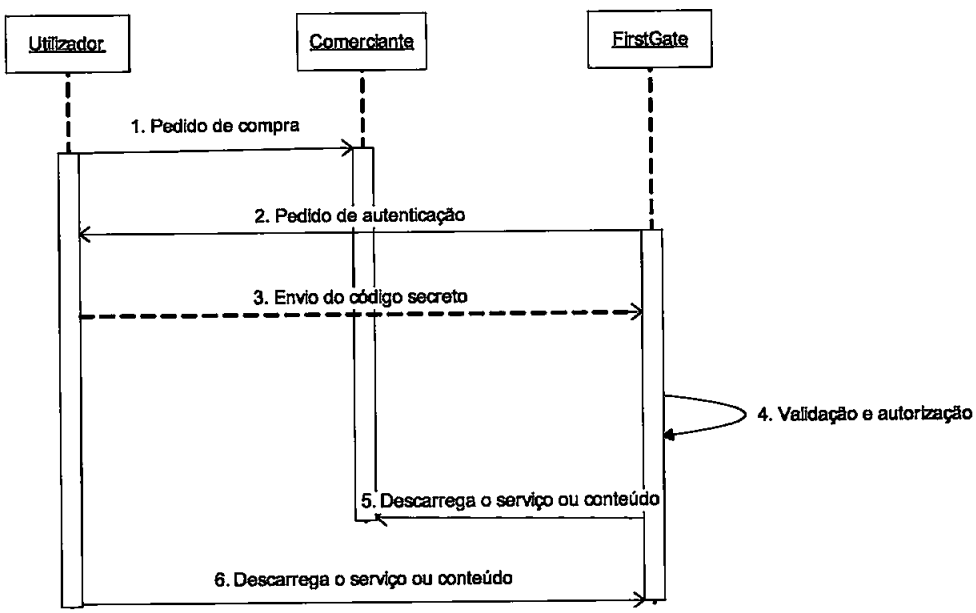


Figura 3.2: Diagrama de sequência do processo de pagamento na FirstGate

1. No momento de pagar, o Utilizador clica no logo da Firstgate da página do Comerciante.

2. O Comerciante redirecciona o Utilizador para a página da Firstgate, onde lhe são apresentados os detalhes da compra e lhe é solicitado a introdução do seu código secreto.

3. O Utilizador confirma os detalhes da compra e envia o seu código secreto.

4. A Firstgate valida o Utilizador e o pedido de pagamento.

5. Se o pagamento for autorizado, a Firstgate descarrega o conteúdo em questão do Comerciante.

6. O Utilizador descarrega o conteúdo da FirstGate.

Numa base mensal, a FirstGate cobra os clientes pelas suas compras, e paga aos comerciantes pelos serviços e conteúdos vendidos.

## 3.2 Sistemas de Pagamentos Móveis

Os sistemas de pagamentos móveis, caracterizam-se pela utilização de dispositivos móveis como telemóveis, *Personal Digital Assistant* (PDA) ou outros, para levar a cabo transacções comerciais.

Nesta secção, são apresentados dois sistemas de pagamentos móveis presentes actualmente no mercado.

### 3.2.1 PayBox

"Tens o teu telefone móvel, tens a tua carteira" - Paybox

No sistema de pagamentos móveis Paybox [44], o cliente necessita apenas de ter uma conta bancária e um telemóvel, independentemente do operadora móvel a que está associado. Tal como o sistema FirstGate, apresentado na secção 3.1.2, a Paybox é controlada por um PSP, e baseia-se no conceito de conta *pre-arranged*. O sistema suporta pagamentos remotos, e.g., compra de bilhetes na Internet, e pagamentos locais, e.g., pagamento em lojas.

Ao registar-se na Paybox, o cliente tem que indicar o(s) método(s) de pagamento para a sua conta e disponibilizar os dados confidencias dessa(s) escolha(s), e.g., número de cartão de crédito ou NIB. Para além dos métodos de pagamento, é pedido ao cliente um número de telemóvel para ficar associado à sua conta. Como resultado, a Paybox atribui ao cliente um código secreto que o identifica perante o sistema no momento de pagar.

Na figura 3.3, é apresentado o diagrama de sequência do processo de pagamento através do sistema de pagamentos móveis Paybox.

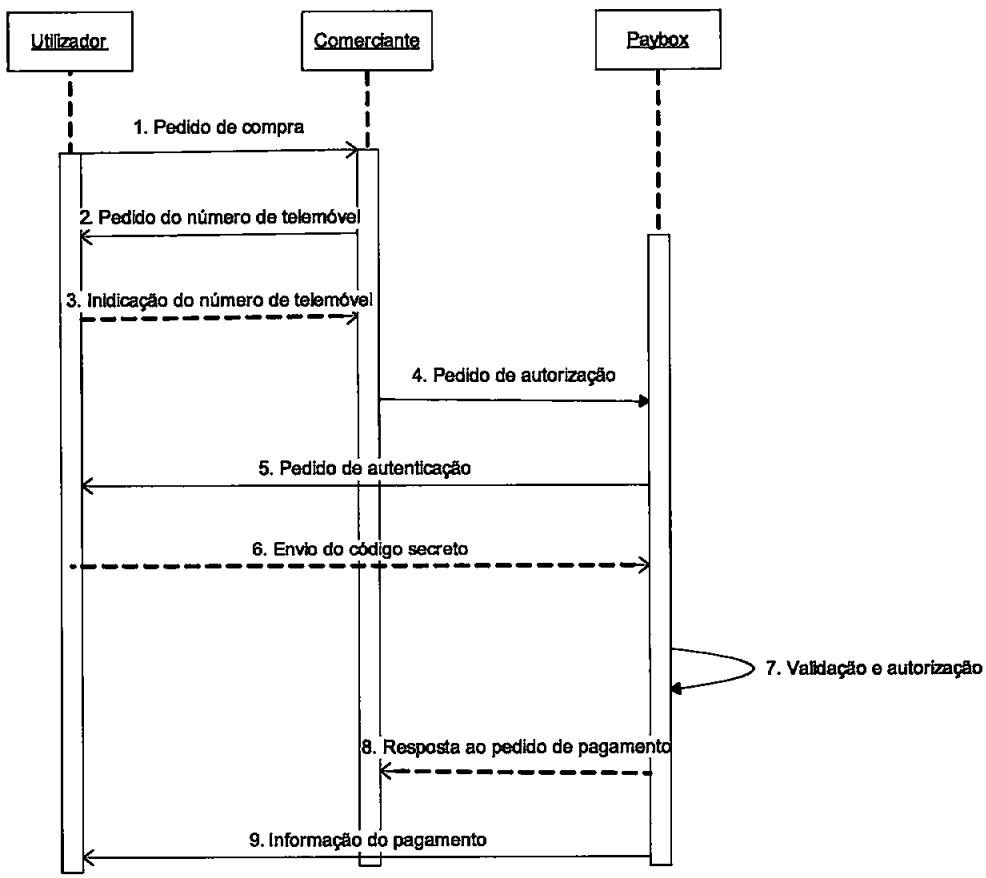


Figura 3.3: Diagrama de sequência do processo de pagamento na Paybox

1. Caso se trate de um pagamento remoto, o Utilizador clica no logo da Paybox da página do Comerciante no momento de pagar. Se for um pagamento local, o Utilizador diz ao Comerciante que deseja pagar através do sistema da Paybox.

2. O Comerciante pede ao Utilizador que indique o número de telemóvel associado à sua conta na Paybox.

3. O Utilizador indica o seu número de telemóvel.

4. O Comerciante envia o número de telemóvel do Utilizador e os dados de pagamento para a Paybox.

5. A Paybox envia uma mensagem de voz para o telemóvel do Utilizador, pedindo que este confirme os detalhes do pagamento.

6. O Utilizador confirma o pagamento, respondendo à mensagem anterior com a indicação do seu código secreto.

7. Validação do Utilizador e processamento do pagamento (transferência de fundos do banco do cliente para o do comerciante).

8. Envio da resposta ao pedido de pagamento para o Comerciante.

9. Envio da informação do estado do pagamento para o Utilizador.

O facto da Paybox processar os pagamentos junto das entidades bancárias dos intervenientes em tempo real, torna o sistema mais apropriados para utilização em cenários de macro-pagamentos.

### 3.2.2 Vodafone m-pay

*"Vodafone m-pay - The new way to shop"* - Vodafone

O sistema de pagamentos móveis Vodafone m-pay [51] é proprietário da gigante de telecomunicações móveis Vodafone, e restringe o acesso aos seus próprios clientes.

O sistema de pagamentos Vodafone m-pay, está dividido em duas vertentes:

1. Vodafone m-pay bill: Neste caso, os Utilizadores são cobrados pelos serviços e conteúdos adquiridos através da sua conta na Vodafone. Para além de ter que ser cliente da Vodafone, o Utilizador terá que criar uma conta Vodafone m-pay bill no portal da Vodafone. Este sistema, é apropriado para cenários de micro-pagamentos.

2. Vodafone m-pay cards: Funciona com base no conceito de carteira móvel, em que os Utilizadores registam os dados dos seus cartões de crédito e débito junto da Vodafone. No momento em que desejam efectuar os pagamentos, a Vodafone disponibiliza estes dados aos Comerciantes. Para além de ter que ser cliente da Vodafone, o Utilizador terá que criar uma conta Vodafone m-pay cards no portal da Vodafone. Este sistema, é apropriado para cenários de macro-pagamentos.

Ao registarem-se no sistema Vodafone m-pay, os Utilizadores recebem um identificador e um código secreto, para se autenticarem no momento de pagar.

Na figura 3.4, é apresentado o diagrama de sequência do processo de pagamento através do sistema de pagamentos móveis Vodafone m-pay bill.

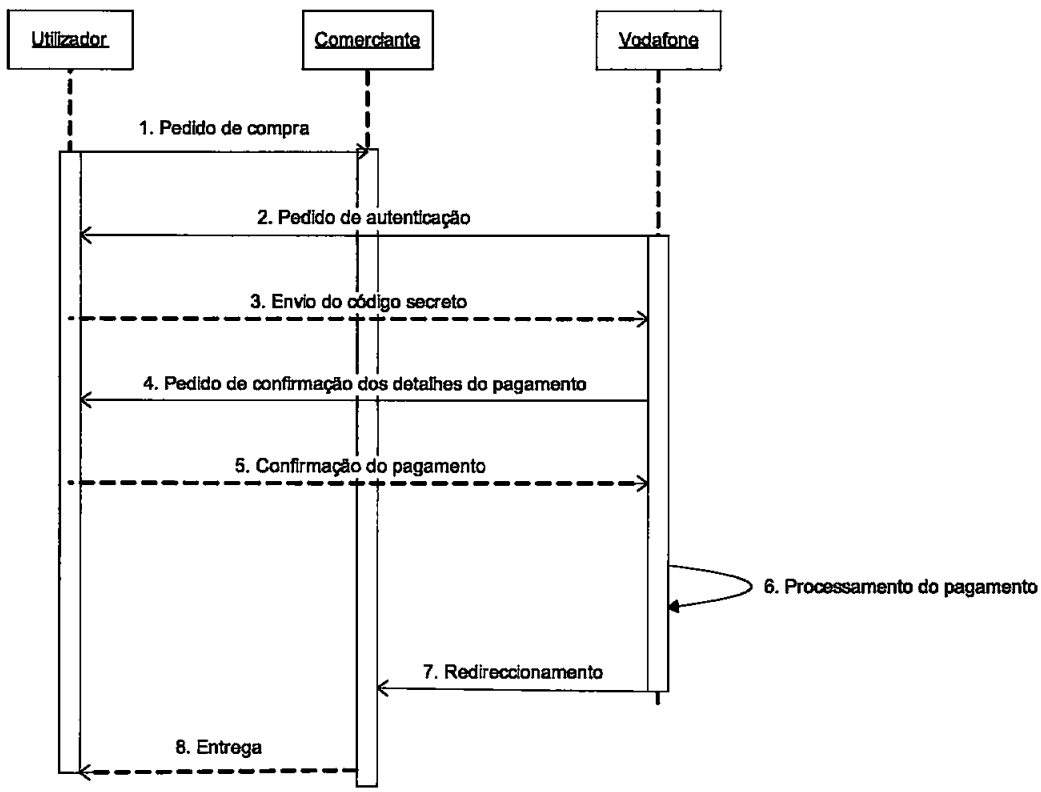


Figura 3.4: Diagrama de sequência do processo de pagamento no Vodafone m-pay bill

1. No momento de pagar, o Utilizador escolhe o Vodafone m-pay bill como método de pagamento na página do Comerciante.

2. O Utilizador é redireccionado para a página da Vodafone, onde lhe é solicitado a introdução da sua identificação e do seu código secreto.
3. O Utilizador autenticasse e entra na portal da Vodafone.
4. São apresentados ao Utilizador os detalhes do pagamento que está prestes a efectuar e é-lhe solicitada confirmação.
5. O Utilizador confirma o pagamento.
6. O Vodafone m-pay bill processa o pagamento.
7. O Utilizador é redireccionado novamente para a página do Comerciante, onde é apresentada a confirmação do pagamento.
8. O Comerciante entrega o serviço ou conteúdo requerido pelo Utilizador.

As compras efectuadas pelo Utilizador, vão aparecer na sua factura mensal da Vodafone, ou debitadas de uma conta pré-paga.

Na figura 3.5, é apresentado o diagrama de sequência do processo de pagamento através do sistema de pagamentos móveis Vodafone m-pay cards.

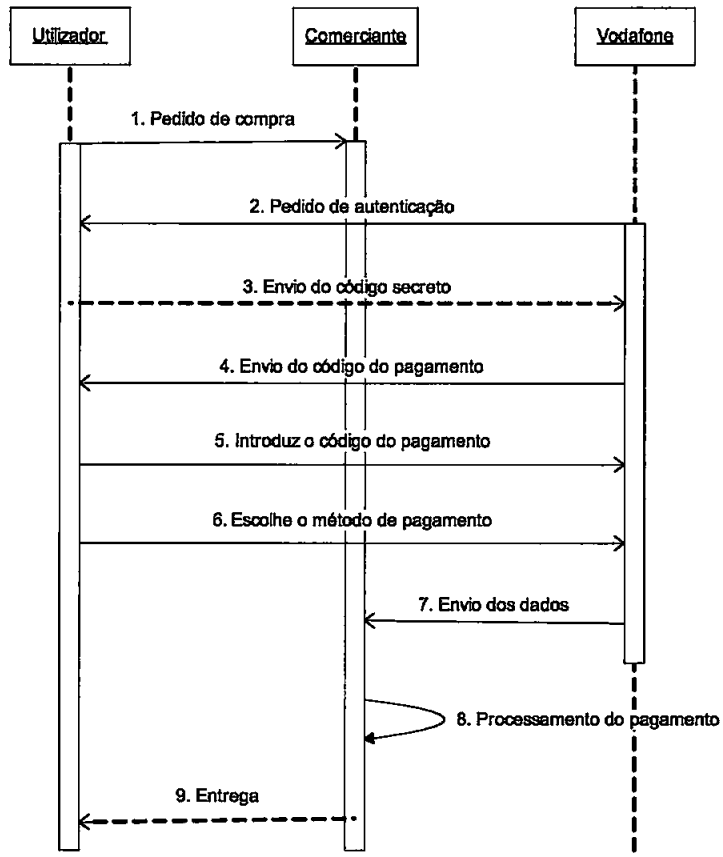


Figura 3.5: Diagrama de sequência do processo de pagamento no Vodafone m-pay cards

1. No momento de pagar, o Utilizador escolhe o Vodafone m-pay cards como método de pagamento na página do comerciante.

2. O Utilizador é redireccionado para a página da Vodafone, onde lhe é solicitado a introdução da sua identificação e do seu código secreto.

3. O Utilizador autentica-se e entra na portal da Vodafone.

4. A Vodafone envia um código para o telemóvel do Utilizador.

5. O Utilizador insere esse código na página da Vodafone, e são-lhe apresentados os vários métodos de pagamento disponíveis para a sua conta.

6. O Utilizador escolhe o método de pagamento.

7. A Vodafone disponibiliza ao Comerciante os dados confidenciais do método de pagamento escolhido, e redirecciona o Utilizador novamente para a página do Comerciante.

8. O Comerciante autoriza o pagamento junto das entidades bancárias.

9. O Comerciante apresenta a confirmação do pagamento na sua página e entrega o serviço ou conteúdo requerido pelo Utilizador.

As compras efectuadas pelo Utilizador, serão imediatamente debitadas da sua conta bancária.

## 3.3 Análise dos Sistemas de Pagamentos Móveis

Analisando os sistemas de pagamentos móveis existentes, alguns dos quais descritos anteriormente, conclui-se que tipicamente existem dois modelos distintos:

- Sistemas controlados por Operadores Móveis, e.g., Vodafone m-pay.
- Sistemas controlados por PSPs, e.g., PayBox.

Assim, podemos concluir que o tipo de entidade processadora do pagamento é uma característica extremamente relevante nos sistemas de pagamentos móveis. Torna-se assim importante analisar os dois modelos acima referidos, por forma a tentar perceber as vantagens e desvantagens de cada um.

### 3.3.1 Sistemas de Pagamentos Móveis Controlados por Operadores Móveis

Estes sistemas, uma vez que são proprietários dos Operadores, ficam restringidos aos seus clientes. Tipicamente este modelo utiliza as contas dos Utilizadores (pré-paga, pós-paga, etc) nos seus Operadores, para debitar os pagamentos móveis por estes efectuados.

Os Comerciantes aderentes a estes sistemas ficam restringidos aos clientes do Operador, e vice-versa. Nomeadamente, os clientes de um Operador não podem aceder a serviços e conteúdos de Comerciantes aderentes a sistemas de outro Operador.

O facto dos Operadores terem uma relação de confiança com os seus clientes, e nomeadamente mecanismos de facturação maduros, torna este modelo bastante bem aceite pelos consumidores.

### 3.3.2 Sistemas de Pagamentos Móveis Controlados por *Payment Service Providers*

Estes sistemas são geridos por entidades independentes que asseguram o processo de pagamento entre os Comerciantes e os Utilizadores de forma segura.

Os Utilizadores são cobrados pelos serviços e conteúdos adquiridos aos Comerciantes, através de uma conta no PSP. O método de pagamento pode ser através de uma conta pré-paga, conta pós-paga, pagamento em tempo real via cartões bancários, etc. Os Comerciantes conseguem chegar a todos os Utilizadores, independentemente do Operador a que estão associados.

Este modelo é independente do meio de acesso do Utilizador, i.e., Operador utilizado, e permite aos Comerciantes chegarem a todo o mercado. No entanto, o facto do Utilizador ter que pagar a uma terceira entidade, muitas vezes desconhecida, pode também servir de barreira à adopção deste modelo.

# Capítulo 4

# O Sistema de Micro-Pagamentos Móveis

Neste capítulo é apresentado um novo sistema de micro-pagamentos móveis. O sistema foi apresentado em [27].

Ao longo do capítulo, será utilizada notação *Unified Modeling Language* (daqui por diante designado simplesmente por UML) para descrever o sistema proposto. O UML é uma linguagem para especificação, construção, visualização e documentação de artefactos de um sistema de software [47].

## 4.1 O Conceito e a Relação com os Sistemas Existentes

As conclusões retiradas da secção 3.3 permitem concluir que os modelos adoptados pelos sistemas de pagamentos móveis apresentam limitações relevantes, e que as vantagens de uns são as desvantagens dos outros e vice-versa. A motivação desta dissertação prende-se, assim, com a percepção dessas mesmas limitações, e com as repercussões que daí advêm para o desenvolvimento do mercado dos pagamentos móveis.

O sistema de pagamentos proposto nesta dissertação (daqui por diante designado simplesmente por SP), tem por base a conjugação dos vários modelos existentes, de forma a capitalizar os pontos fortes detectados nesses modelos, e eliminar as características avaliadas como pontos fracos. O objectivo final é o desenvolvimento de um sistema que proporcione um cenário ideal para o processamento de micro-pagamentos em ambiente móvel.

Como referido anteriormente, o SP procura assim evitar as principais desvantagens dos modelos analisados na secção 3.3, nomeadamente a dependência relativamente a um Operador Móvel especifico, e o pagamento a uma terceira entidade, como um PSP. Por outro lado, vantagens como a utilização dos mecanismos de facturação dos Operadores Móveis e a gestão do sistema de pagamentos por parte de uma terceira entidade como um PSP, foram tomadas em consideração. Adicionalmente, a possibilidade de ter vários Utilizadores do SP a serem cobrados na mesma conta corrente, foi também prevista.

A figura 4.1 apresenta o conceito do SP como um diagrama de sequência, na perspectiva do comprador.

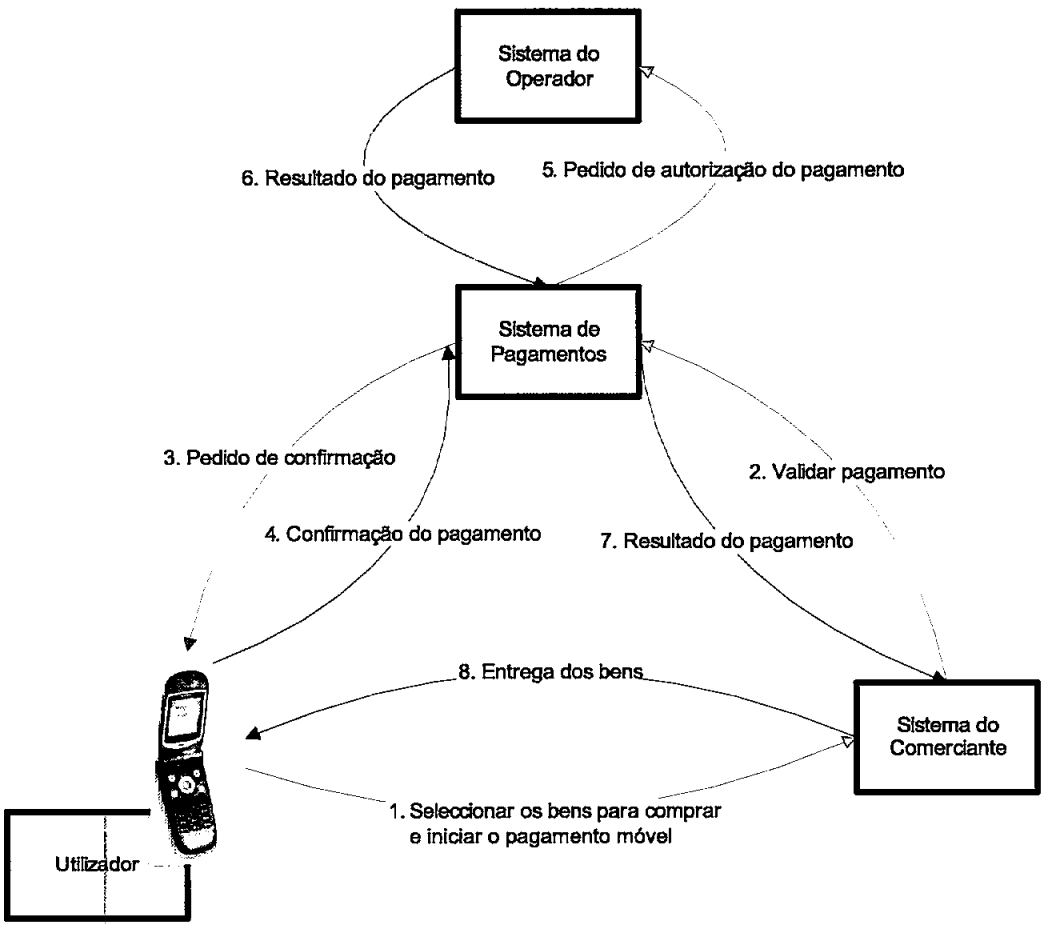


Figura 4.1: Esquema conceptual do Sistema de Pagamentos Móveis proposto

## 4.2 Critérios de Desenho e Implementação

Esta secção apresenta os critérios que o SP deve preencher. Existem três grupos de critérios que foram considerados relevantes: funcionais, arquitecturais (segurança, escalabilidade, desempenho e modularidade) e económicos. Os critérios funcionais definem o que o sistema deve ser capaz de fazer, enquanto os arquitecturais definem como o sistema deve ser construído.

### 4.2.1 Critérios Funcionais

Um dos objectivos desta tese, é o desenvolvimento de um sistema de micropagamentos móveis (SP), que seja independente do Operador Móvel que suporta a comunicação, mas que tire partido do seu mecanismo de facturação, i.e, que utilize as contas dos Utilizadores nos seus Operadores para debitar os pagamentos.

Os requisitos a observar pelo SP em termos de funcionalidades são:

- O SP deverá ser adequado para o pagamentos de baixo valor, i.e., micropagamentos.
- O SP deverá ser adequado para o pagamento de bens e serviços tanto digitais como físicos (daqui por diante designados simplesmente por bens).
- O SP não deverá estar associado a nenhum Operador Móvel especifico, i.e, deverá ser multi-operador.
- O SP deverá ser controlado e gerido por um PSP. O PSP deverá servir de ligação entre os Comerciantes e os Operadores, controlando todo o fluxo do processo de pagamento.
- O SP deverá disponibilizar mecanismos de registo para os Utilizadores, Comerciantes e Operadores, para criação das respectivas contas no sistema.
- O SP deverá utilizar a conta que o Utilizador tem no seu Operador (daqui por diante designadas por Carteira), para cobrar os pagamentos móveis. O método de pagamento utilizado (conta pré-paga, pós-paga, etc) para cobrar o Utilizador, é da responsabilidade do Operador responsável pela Carteira.
- Os Utilizadores deverão poder partilhar uma Carteira para efectuar os seus pagamentos no SP, independentemente do Operador Móvel a que estejam associados, garantindo assim uma forte acessibilidade ao SP.

- No caso de partilha de uma Carteira, terá que haver um proprietário da Carteira (no registo definiu a conta do seu Operador para debitar os pagamentos móveis), chamado de super-utilizador, e Utilizadores autorizados por este para usar a sua Carteira, chamados de sub-utilizadores.

- Os super-utilizadores devem poder definir regras de autorizações e restrições sobre os pagamentos dos seus sub-utilizadores. As regras de autorização representam onde e o quê um Utilizador pode comprar, enquanto que as regras de restrição representam as limitações em termos de compras a que o Utilizador está sujeito (explicado mais em detalhe na secção 4.4.3).

- Os Utilizadores deverão confirmar os seus pagamentos através da apresentação de um código secreto no SP, excepto se definido em contrário nas suas preferências.

- O SP deverá permitir que os Utilizadores tenham acesso ao historial das suas transacções.

- O SP deverá permitir que os Utilizadores, Comerciantes e Operadores possam adicionar, remover e modificar dados da sua conta.

- O SP deverá permitir que os Comerciantes efectuem pedidos de autorização de pagamento, acedam aos estados das suas transacções e consigam cancelar pagamentos já processados.

### 4.2.2 Segurança

A segurança é um elemento fundamental em qualquer sistema de pagamentos electrónicos e encarada como a principal preocupação dos consumidores.

O modelo de segurança do SP deverá tomar em consideração as limitações inerentes ao ambiente móvel (explicadas na secção 4.7.1), o tipo de pagamentos processados e o nível de desempenho desejado para o SP. Os critérios a preencher pelo SP em termos de segurança são:

- Entidades não autorizadas não deverão ter acesso ao SP, ou aos seus dados.

- As comunicações entre os vários intervenientes e o SP deverão ser cifradas com recurso a criptografia de chave simétrica (explicado em detalhe na secção 4.7). Deverá ser utilizada criptografia de chave pública para troca das chaves simétricas.

- Os Utilizadores deverão poder manter o anonimado perante os Comerciantes, i.e., quando efectuam uma compra junto de um Comerciante, deverá ser impossível a este conhecer a real identidade do Utilizador (explicado na secção 4.7).

### 4.2.3 Escalabilidade

O SP deverá ser escalável, i.e, os tempos de resposta a pedidos de pagamento deverão aumentar linearmente à medida que o número de pedidos no SP aumenta exponencialmente. Por outro lado, escalabilidade também se traduz na possibilidade de aumentar exponencialmente a capacidade de um sistema, à medida que se aumenta linearmente a capacidade dos servidores que albergam o sistema.

### 4.2.4 Desempenho

O desempenho é um aspecto especialmente importante em sistemas de micro-pagamentos. Como estão envolvidas baixas quantias, muitas vezes associadas a compras impulsivas, este tipo de sistema deve contribuir para fechar as transacções rapidamente, contribuindo para uma experiência agradável por parte dos Utilizadores.

No caso particular do SP, o desempenho em termos do tempo de resposta a pedidos de pagamento deverá merecer uma atenção muito especial. Tempos de resposta na ordem dos 2 a 3 segundos por pagamento, deverão ser obtidos em situações de carga normal. A medição do desempenho deverá ser efectuada com recurso a testes de carga sobre o sistema (ver secção 5.5).

### 4.2.5 Modularidade

O SP deverá ser construído de forma modular, i.e, como um conjunto de módulos independentes entre si, em que juntos possibilitam o processamento de pagamentos móveis. A adição de novas funcionalidade a um módulo do SP não deverá interferir com os restantes módulos. Esta característica torna-se especialmente importante no que respeita a interfaces com entidades externas ao SP. Por exemplo, a disponibilização de uma nova interface para o Comerciante, deverá ser transparente para os outros módulos do SP.

### 4.2.6 Custos

Em sistemas de micro-pagamentos, o custo de processamento por transacção é um aspecto fundamental para a viabilidade do negócio que se quer levar a cabo.

Caso o custo de processamento de um pagamento represente uma percentagem alta do montante envolvido, então o modelo de negócio adoptado torna-se inviável. Assim, o sucesso dos sistemas de micro-pagamentos passa em grande parte por conseguir controlar estes custos.

O SP deverá tomar em consideração os custos de processamento por transacção. Para tal, deverão ser criados mecanismos para optimizar os custos por transacção (ver secção 4.5), de forma a tornar o SP adequado para cenários de micro-pagamentos.

## 4.3 Actores

Um actor é uma entidade externa (fora do sistema) que interage com o sistema ao participar (ou iniciar normalmente) um caso de utilização (explicado na secção 4.4). Os actores poderão ser pessoas, outros sistemas informáticos ou eventos exteriores.

Consoante a forma como interagem com o sistema, os actores dividem-se em dois tipos diferentes:

- Actores principais, são aqueles que retiram um resultado observável do caso de utilização.
- Actores secundários, são aqueles que são requeridos para a obtenção de informações adicionais, i.e., apenas podem consultar ou informar o sistema quando o caso de utilização está a ser executado.

No caso do SP, são três os actores que com ele interagem, sendo que em acções distintas podem apresentar-se como actores principais ou secundários, como se poderá confirmar mais à frente. Os três actores presentes no SP são:

- Utilizador, é a pessoa que possui um dispositivo móvel e o utiliza para realizar pagamentos móveis em troca de bens.
- Comerciante, é alguém ou alguma empresa que vende os seus bens aos Utilizadores, e disponibiliza a opção de pagamento móvel. O termo Comerciante é aqui utilizado de uma forma mais geral que na linguagem comum. Mesmo que não estejam envolvidos bens físicos, e.g., um serviço informativo de trânsito, o provedor de serviços e conteúdos é considerado um Comerciante.

- Operador Móvel (daqui por diante designado simplesmente por Operador), é uma empresa de telecomunicações móveis que disponibiliza as contas dos seus clientes (denominadas por Carteiras) para cobrar pagamentos móveis.

## 4.4 Casos de Utilização

"Um caso de utilização especifica uma sequência de acções, incluindo variantes, que um sistema pode efectuar, interagindo com os actores do sistema"[42].

Os casos de utilização (daqui por diante designados simplesmente por CdU) descrevem as interacções típicas entre os utilizadores de um sistema e o sistema propriamente dito. Eles representam a interface externa do sistema e especificam um dado tipo de requisitos que o sistema deve suportar (note-se que é 'o quê' e não 'como').

O SP implementa vários CdU (descritos mais abaixo), dos quais se destacam três indispensáveis para a realização de pagamentos móveis:

- Registo
- Pagamento Móvel
- Consolidação

Juntando os três casos de utilização na sequência correcta, completa-se uma transacção de pagamento móvel. Para além destes, existem outros CdU relevantes, mas que saem do domínio do SP. Por exemplo, o CdU "Fazer Compras" presente no sistema do Comerciante é obrigatório para que o processo de pagamento se possa efectuar. É esperado que o Utilizador seleccione os bens que deseja comprar.

A figura 4.2 apresenta a sequência dos CdU acima referidos, através de uma cadeia de processos.

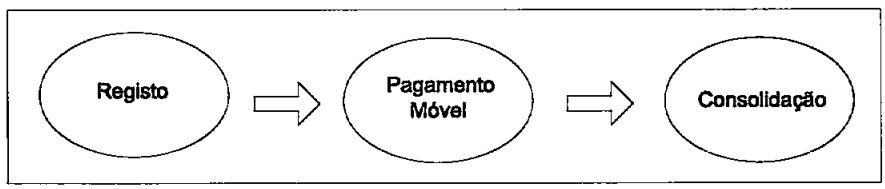


Figura 4.2: Fluxo de processos

De seguida são apresentados dois diagramas de CdU do SP, que representam as relações entre os actores e os CdU:

1. A figura 4.3 apresenta o diagrama de CdU do processo de pagamento móvel
2. A figura 4.4 apresenta o diagrama de CdU das restantes interacções dos actores com o SP[1]

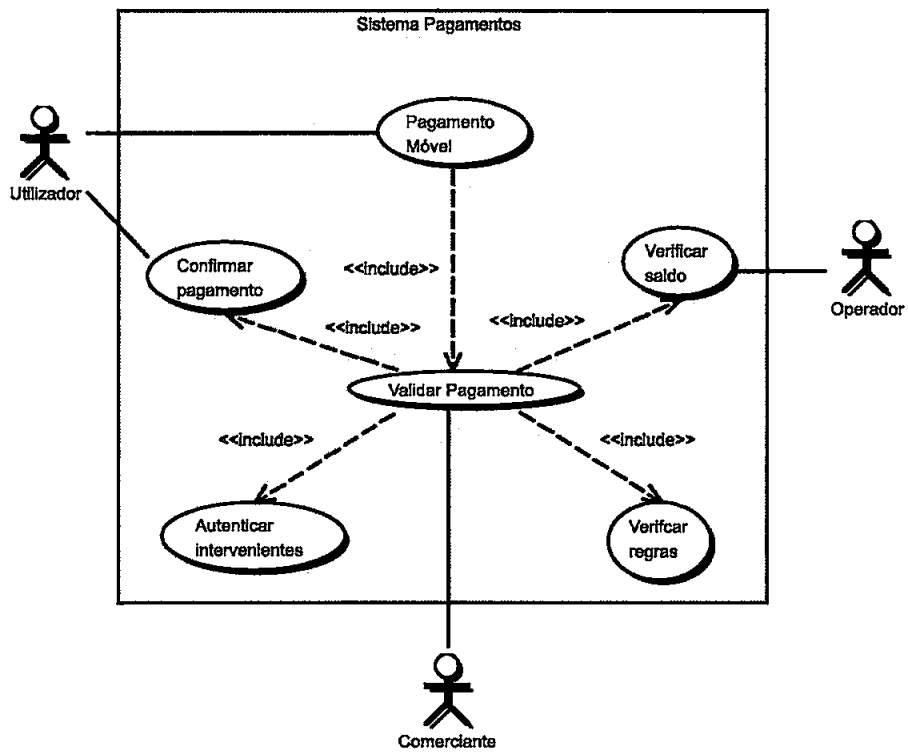


Figura 4.3: Diagrama de casos de utilização do SP - parte 1

[1]Para além dos CdU apresentados, existem outros de menor relevância, pelo que serão ignoradas

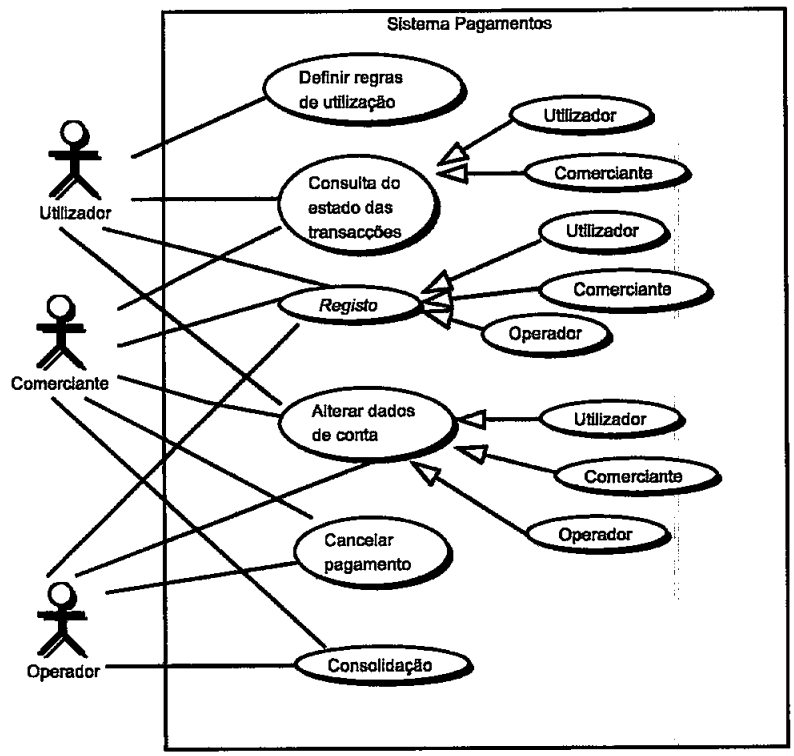


Figura 4.4: Diagrama de casos de utilização do SP - parte 2

De seguida descreve-se cada um dos CdU do SP, dando especial atenção ao CdU "Pagamento Móvel", que devido à sua importância e complexidade, é apresentado de uma forma mais detalhada, nomeadamente recorrendo a diagramas de interacção e de estados.

### 4.4.1 Registo

O CdU "Registo" é anterior a todas as outras interacções dos actores com o SP, e consiste na identificação e criação de contas dos vários actores no SP. Após esta fase, os vários actores podem começar a desempenhar o seu papel no SP. Este CdU está representado no diagrama da figura 4.4 como uma acção de registo genérica, com os CdU "Utilizador", "Comerciante" e "Operador" a implementarem-no nas diversas vertentes (registo do Utilizador, registo do Comerciante e registo do Operador).

Durante esta fase, os vários actores terão que disponibilizar alguns dados ao SP, tais como:

- Utilizador: dados pessoais; número de telemóvel donde irá efectuar os pagamentos móveis; Carteira onde serão debitados os seus pagamentos (poderá ser por exemplo o número de telemóvel associado a essa Carteira); código secreto para confirmar os seus pagamentos. Será nesta fase que o Utilizador poderá optar por definir uma Carteira que não a que possuí no seu Operador, para cobrar os seus pagamentos móveis. Nomeadamente a Carteira definida poderá pertencer a outro Operador que não o seu (uma garantia forte de acessibilidade).
- Comerciante e Operador: essencialmente dados de natureza financeira.

O CdU só ficará finalizado após o SP disponibilizar aos vários actores os seguintes elementos:

- Utilizador: aplicação de pagamentos para instalar no dispositivo móvel
- Comerciante e Operador: interfaces de comunicação

### 4.4.2 Alterar Dados de Conta

O CdU "Alterar dados de conta" representa a acção de alteração dos dados disponibilizados pelos vários actores no processo de registo (descrito acima). Da mesma maneira que o CdU "Registo", também este CdU está representado no diagrama de CdU da figura 4.4 como uma acção de alteração de dados de conta genérica, com os CdU "Utilizador", "Comerciante" e "Operador" a implementarem-na nas diversas vertentes.

### 4.4.3 Definir Regras de Utilização

O CdU "Definir regras de utilização", é utilizado exclusivamente por super-utilizadores, i.e., Utilizadores que utilizem a Carteira que possuem junto do seu Operador para debitar os seus pagamentos móveis. Este CdU representa a acção realizada por um super-utilizador na definição das regras de utilização da sua Carteira por parte dos seus sub-utilizadores. Assim, um super-utilizador pode definir as seguintes regras:

- Autorizar outros Utilizadores a usarem a sua Carteira para efectuar pagamentos móveis (criação de sub-utilizadores), independentemente do Operador a que pertençam.

- Criar regras de autorização e restrição à sua Carteira, por forma a controlar os pagamentos dos seus sub-utilizadores. As regras de autorização, definem os bens que um Utilizador pode comprar, e.g., autorizar compras de conteúdos infantis num determinado Comerciante. Por outro lado, as regras de restrições definem as limitações em termos de compras a que o Utilizador está sujeito, e.g., não permitir gastar mais que 1 euro por dia, ou não permitir efectuar pagamentos antes das 16h00.

- Criar regras de confirmação de pagamentos. As regras de confirmação de pagamentos definem a periodicidade com que o Utilizador tem que confirmar os seus pagamentos (apresentar o seu código secreto). A periodicidade definida será utilizada pelo mecanismo de sessão do SP (explicado em detalhe na secção 4.5), para determinar se o Utilizador precisa de confirmar o pagamento ou não. Por exemplo, o Utilizador pode definir que para pagamentos inferiores a 1 euro, tem uma periodicidade de 1 hora, o que quer dizer que após um primeiro pagamento confirmado com código secreto, o Utilizador fica dispensado de confirmar os próximos pagamentos abaixo de um euro durante 1 hora. Várias regras podem ser adicionadas para situações distintas.

### 4.4.4 Consulta do Estado das Transacções

O CdU "Consulta do estado das transacções" permite aos vários aos Utilizadores e Comerciantes consultarem o estado das transacções em que estão envolvidos no SP. Tal como o CdU "Registo" e "Alterar dados da conta" também este é apresentado no diagrama de CdU da figura 4.4 como uma acção genérica, com os CdU "Utilizador"e "Comerciante" a implementarem-no nas diversas vertentes. O método de acesso a esta informação varia consoante o actor que está a realizar a acção, podendo ir de um simples portal na Internet, até uma interface pré-definida de comunicação com o SP.

### 4.4.5 Pagamento Móvel

"Pagamento Móvel" é o principal CdU do SP, e representa a acção do actor principal Utilizador a efectuar um pagamento móvel no SP. Este CdU está incluído no CdU "Fazer Compras" do sistema do Comerciante, i.e. é um sub-CdU, pois é suposto o Utilizador escolher o bem que deseja comprar antes de avançar para a fase de pagamento. Assim, o Utilizador invoca este CdU através do sistema do Comerciante e não directamente no SP. O CdU "Fazer Compras" do sistema do Comerciante, não obstante a sua importância no processo de pagamento, sai fora do âmbito desta dissertação, pelo que não será detalhado.

#### 4.4.5.1 Validar Pagamento

Após o Utilizador ter expresso o seu desejo em efectuar um pagamento móvel, o Comerciante interage com o SP para validar este pagamento. Esta acção é representada pelo CdU "Validar Pagamento" incluída no CdU "Pagamento Móvel" (é um sub-CdU), e permite aos Comerciantes (actores principais) validarem os pedidos de pagamento móveis. O CdU "Validar Pagamento" inclui quatro sub-CdU, estando cada um responsável por uma tarefa especifica na acção de validar pagamentos móveis. Estes sub-CdU são:

- Autenticar intervenientes
- Verificar regras do Utilizador
- Confirmar pagamento
- Verificar saldo

O CdU "Autenticar intervenientes" tem como objectivo autenticar o Utilizador e Comerciante envolvidos na transacção e confirmar que os dados presentes no pedido de pagamento do Comerciante estão conforme os dados no pedido de compra do Utilizador. Para tal, o SP recorre a mecanismos criptográficos (ver secção 4.7) para validar o Utilizador e o Comerciante envolvidos na transacção.

O CdU "Verificar regras do Utilizador" tem como objectivo analisar as regras de autorização e restrição definidas na conta do Utilizador[2], e verificar se este tem permissões para efectuar o pagamento em questão.

O CdU "Confirmar Pagamento" tem como objectivo confirmar os detalhes do pagamento junto do Utilizador. Como neste caso é o CdU a iniciar a interacção com o Utilizador, este assume o papel de actor secundário. Após o Utilizador ter disponibilizado o seu código secreto para confirmar o pagamento, o SP valida-o e dá por concluído o CdU.

O CdU "Verificar saldo" é a última acção no processo de validar um pagamento, e tem como objectivo verificar se o Utilizador tem saldo suficiente na Carteira para realizar o pagamento. Este CdU tem duas variantes:

1. O SP tem informação disponível do saldo da Carteira que lhe permite autorizar o pagamento de imediato, agregando-o para mais tarde comunicar ao Operador responsável pela Carteira (mais detalhes na secção 4.5).

[2]A conta do Utilizador corresponde ao registo que este possui no SP.

2. O SP não tem informação disponível do saldo da Carteira que lhe permita autorizar o pagamento de imediato, e faz um pedido de autorização de pagamento ao Operador responsável pela Carteira. Neste caso, o Operador assume o papel de actor secundário, pois é o CdU a iniciar a interacção com o Operador. O pedido enviado ao Operador transmite os dados do pagamento e a informação de possíveis pagamentos passados ainda não processados. Como resposta, o Operador disponibiliza o estado do pedido de pagamento e saldo actualizado da Carteira[3].

#### 4.4.5.2 Cenários de Sucesso

De seguida é apresentado o cenário principal de sucesso do CdU "Pagamento Móvel". A sequência deste cenário é a seguinte:

1. O Utilizador indica o pagamento móvel a fazer no sistema do Comerciante.
2. O Comerciante envia o pedido de autorização de pagamento para o SP.
3. O SP autentica o Utilizador e o Comerciante envolvidos na transacção.
4. O SP verifica se as regras de autorização e restrição definidas para o Utilizador lhe permitem efectuar o pagamento em questão.
5. O SP verifica as regras de confirmação de pagamentos definidas para o Utilizador.
6. O SP pede ao Utilizador que confirme o pagamento através da introdução do seu código secreto.
7. O Utilizador verifica os dados do pagamento e insere o seu código secreto.
8. O SP compara o código secreto apresentado pelo Utilizador com o que está definido no sistema.
9. O SP verifica o saldo da Carteira do Utilizador.
10. O SP agrega o pagamento e autoriza-o de imediato.
11. O SP informa o Comerciante do sucesso do pagamento.
12. O Comerciante informa o Utilizador do sucesso do pagamento e processa a encomenda.

[3]Note-se que o saldo aqui mencionado não corresponde ao saldo real da Carteira, mas sim ao chamado montante de risco da Carteira, explicado em detalhe na secção 4.5.2.

Para além do cenário de sucesso acima apresentado, existem outros cenários que apresentam uma sequência de acções diferente, mas que no final correspondem da mesma forma a um pagamento móvel efectuado com sucesso. A estes cenários chamamos cenários alternativos de sucesso. De seguida são apresentados os cenários alternativos de sucesso do CdU "Pagamento Móvel".

**Alternativa 1** (A1): *as regras de confirmação do pagamento do Utilizador dispensam-no da introdução do seu código secreto*

A sequência A1 começa no ponto 5 do cenário principal de sucesso.

6. O SP dá o pagamento por confirmado e dispensa o Utilizador de apresentar o seu código secreto.
7. O SP verifica o saldo da Carteira do Utilizador.
8. O SP agrega o pagamento e autoriza-o de imediato.
9. O SP informa o Comerciante do sucesso do pagamento.
10. O Comerciante informa o Utilizador do sucesso do pagamento e processa a encomenda.

**Alternativa 2** (A2): *a informação do SP acerca da Carteira não permite autorizar o pagamento de imediato (saldo é inferior ao montante do pagamento)*

A sequência A2 começa no ponto 9 do cenário principal de sucesso.

10. O SP pede ao Operador responsável pela Carteira que autorize o pagamento.
11. O Operador confirma o pagamento e indica o saldo actualizado da Carteira para pagamentos no SP.
12. O SP informa o Comerciante do sucesso do pagamento.
13. O Comerciante informa o Utilizador do sucesso do pagamento e processa a encomenda.

#### 4.4.5.3 Cenários de Falha

Caso o CdU não tenha sucesso, dá-se o nome de cenário de falha à sequência de acções que levou ao insucesso do CdU. De seguida são apresentados os cenários de falha possíveis no CdU "Pagamento Móvel".

**Erro 1** (E1): *autenticação do Utilizador ou Comerciante inválidas*

A sequência E1 começa no ponto 3 do cenário principal de sucesso.

4. O SP informa o Comerciante que a autenticação do Utilizador ou Comerciante é inválida
5. O Comerciante informa o Utilizador do insucesso do pagamento; o CdU falha.

**Erro 2** (E2): *o Utilizador não tem permissões para comprar o bem em questão*

A sequência E2 começa no ponto 4 do cenário principal de sucesso.

5. O SP informa o Comerciante que o Utilizador não tem permissões para comprar o bem em questão.
6. O Comerciante informa o Utilizador do insucesso do pagamento; o CdU falha.

**Erro 3** (E3): *o Utilizador apresenta um código secreto inválido*

A sequência E3 começa no ponto 8 do cenário principal de sucesso.

9. O SP informa o Comerciante que o Utilizador não confirmou o pagamento.
10. O Comerciante informa o Utilizador do insucesso do pagamento; o CdU falha.

**Erro 4** (E4): *o Operador responsável pela Carteira não autoriza o pagamento*

A sequência E4 começa no ponto 10 do cenário alternativo A2.

11. O Operador informa SP que o pagamento não foi autorizado.
12. O SP informa o Comerciante que o pagamento não foi autorizado.
13. O Comerciante informa o Utilizador do insucesso do pagamento; o CdU falha.

#### 4.4.5.4 Diagramas

De seguida são apresentados vários diagramas do CdU "Pagamento Móvel", por forma a complementar as apresentações textuais anteriores.

A figura 4.5 apresenta o diagrama de sequência que representa o cenário de sucesso A2 do CdU "Pagamento Móvel". Um diagrama de sequência ilustra uma interacção segundo uma visão temporal.

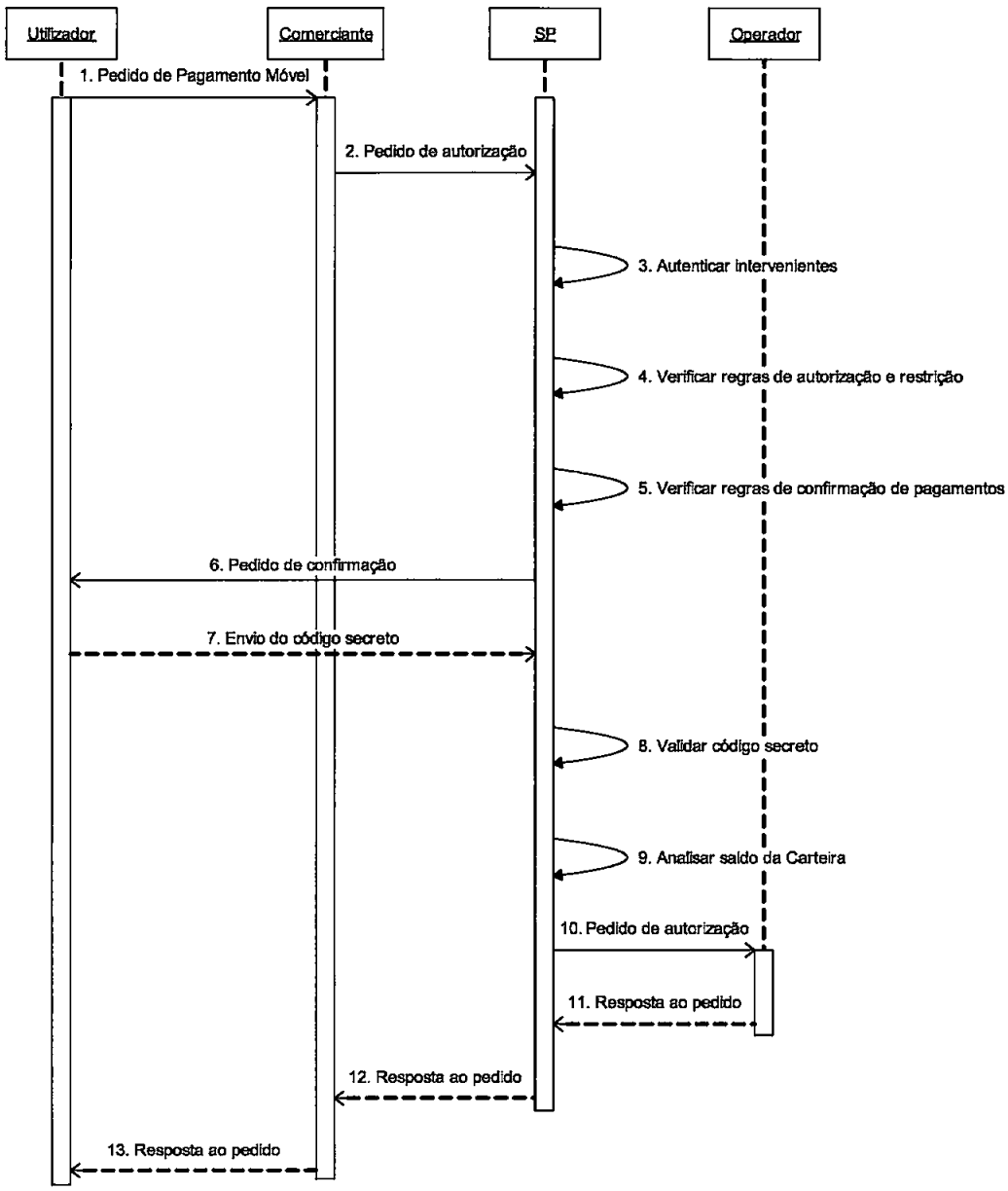


Figura 4.5: Diagrama de sequência do cenário alternativo de sucesso A2 do CdU Pagamento Móvel

A figura 4.6 apresenta o diagrama de actividades de um pagamento móvel. Este diagrama ilustra o fluxo de controle entre as várias actividades.

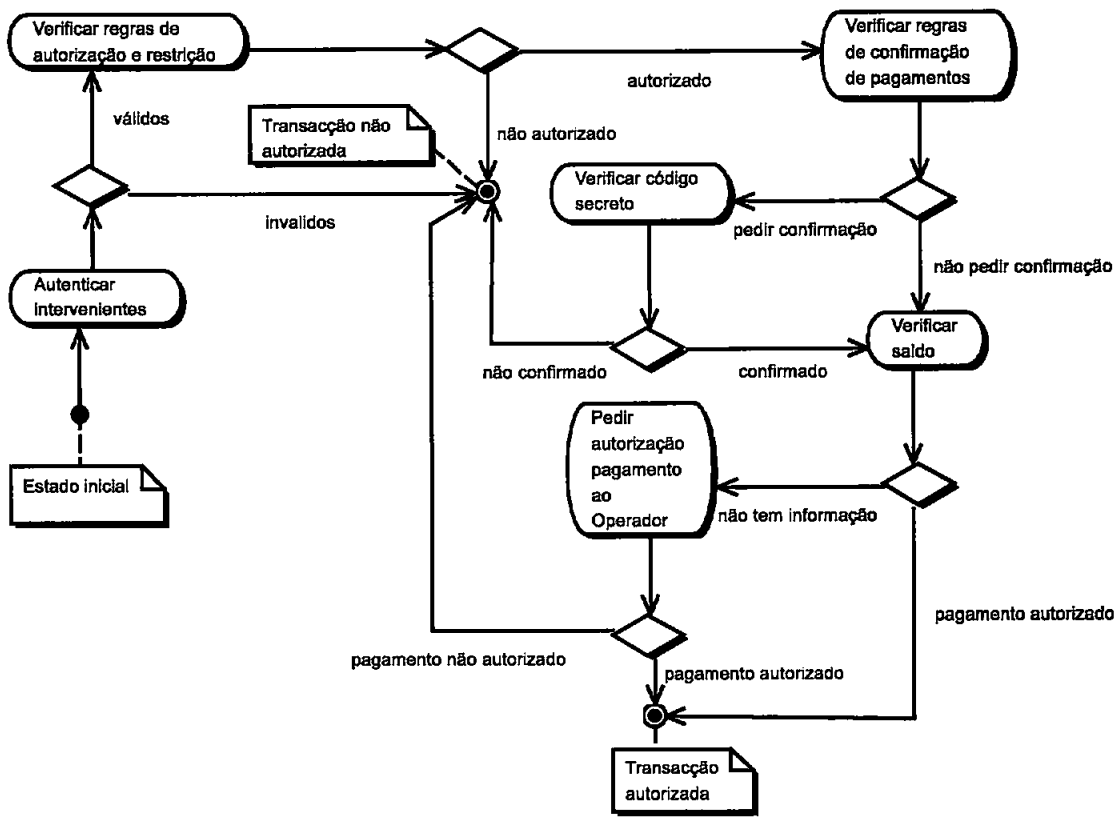


Figura 4.6: Diagrama de actividades do CdU Pagamento Móvel

A figura 4.7 ilustra o diagrama de estados de um pagamento móvel no SP, que representa os possíveis estados e transições de estados por que um pagamento pode passar ao longo do seu processamento no SP, i.e, ao longo dos CdU por onde passa.

Um diagrama de estados permite modelar o comportamento interno de um determinado objecto (neste caso, um pagamento), subsistema ou sistema global [32].

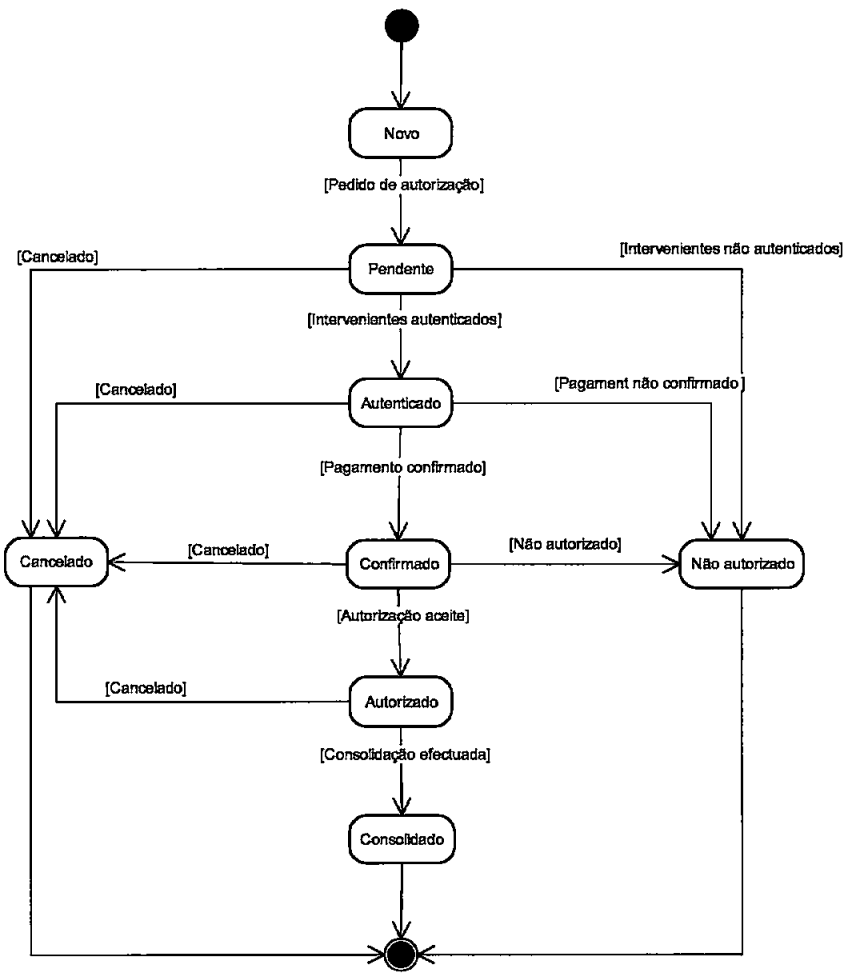


Figura 4.7: Diagrama de estados do Pagamento Móvel

Ao longo do seu ciclo de vida no SP, um pagamento pode ser cancelado caso o SP assim o entenda. O motivo para cancelar um pagamento pode, por exemplo, passar por falhas internas do SP, que o obriguem a abortar um pagamento em pleno processamento.

### 4.4.6 Cancelar Pagamento

O CdU "Cancelar Pagamento" representa a acção de cancelar um pagamento previamente autorizado. Este CdU tem como actor principal o Comerciante. Caso o pagamento já tenha sido processado, i.e., comunicado ao Operador, é requerido ao actor secundário Operador, que o cancele do seu lado.

O Comerciante poderá invocar este CdU, por exemplo, no caso de ter perdido a ligação ao Utilizador antes de conseguir entregar os bens envolvidos na transacção.

### 4.4.7 Consolidação

O CdU "Consolidação" tem como objectivo distribuir as receitas geradas pelos pagamentos móveis dos Utilizadores, pelos restantes membros da cadeia de valor. O processo de consolidação representa a última fase do pagamento, e é normalmente realizada no final um determinado período (e.g., dia, semana, mês).

Como são os Operadores que cobram os Utilizadores pelos seus pagamentos móveis, são estes que detêm o total das receitas geradas. Assim, o CdU "Consolidação" tem como actor principal o Operador, que depois de retirar a sua parte das receitas, disponibiliza o restante ao PSP[4]. Por sua vez, o PSP retém a sua parte das receitas e distribui o restante pelos Comerciantes envolvidos nos pagamentos. Note-se que os Comerciantes interagem com este CdU como actores secundários.

O facto de ser o PSP a distribuir as receitas aos Comerciantes, e não os Operadores, garante a privacidade da informação relativa ao tipo de bens adquiridos pelos Utilizadores, perante os Operadores.

## 4.5 Optimização no Processamento das Transacções

Como foi referido anteriormente, os sistemas de pagamentos electrónicos, particularmente os de micro-pagamentos, devem ter em consideração os custos associados ao processamento das transacções. Caso esse custo seja demasiado elevado, é muito provável que o sistema esteja condenado ao insucesso.

[4]O modelo de negócio utilizado para a distribuição das receitas sai fora do âmbito desta dissertação, pelo que não será detalhado.

Em cenários de micro-pagamentos, este custo torna-se ainda mais relevante, já que as margens de lucro são muito baixas, e o negócio encontra-se no volume de transacções. Estando o SP vocacionado para cenários de micro-pagamentos, esta problemática torna-se especialmente importante. Assim, foram consideradas as seguintes variáveis no processo de quantificação do custo de processamento por transacção no SP:

- Tempo de processamento de um pagamento.
- Número de interacções do Utilizador com o sistema, para realizar um pagamento.
- Número de ligações entre todos as intervenientes para realizar um pagamento.

Os mecanismos abaixo descritos têm por objectivo a diminuição do custo de processamento por transacção, tendo em conta as variáveis acima mencionadas.

### 4.5.1 Mecanismo de Sessão

Uma das características desejáveis num sistema de micro-pagamentos, é que o acto de comprar seja o mais simples e agradável possível para o Utilizador. Desta forma, potencia-se o acto de compra impulsiva, rentabilizando o negócio. Tendo em conta estes factores, o SP utiliza um mecanismo de sessão que tem como objectivo diminuir o número de interacções do Utilizador com o SP.

O mecanismo de sessão consiste em criar sessões limitadas no tempo para Utilizadores que efectuem um pagamento e o confirmem com o seu código secreto. Após aberta a sua sessão, o Utilizador fica dispensado de confirmar os pagamentos seguintes que sejam efectuados dentro do tempo da sua sessão. Ao expirar o tempo para a sua sessão, o Utilizador terá que confirmar o próximo pagamento de forma a ser-lhe atribuída uma nova sessão. Desta forma, evita-se que em pagamentos efectuados num curto intervalo de tempo (usual em cenários de micro-pagamentos), o Utilizador tenha que estar sempre a confirmar os pagamentos através da introdução do seu código secreto.

Este mecanismo permite diminuir o número de interacções do Utilizador com o SP, e consequentemente o tempo médio de processamento de um pagamento. Caso o Utilizador queira usufruir das funcionalidade do mecanismo de sessão (caso contrário terá que confirmar sempre os seus pagamentos), terá que definir o(s) tempo(s) das suas sessão na sua área de cliente (definida na secção 4.6). Por exemplo, o Utilizador pode definir um tempo de sessão de trinta minutos para

pagamentos abaixo 1 euro, e de zero minutos (precisa sempre de confirmar os pagamentos) para valores superiores.

O módulo de confirmação de pagamentos, definido na secção 4.6, implementa este mecanismo.

### 4.5.2 Mecanismo de Agregação de Transacções

Outra das características desejáveis do SP é que o número de ligações entre os vários intervenientes seja o mais reduzido possível, por forma a diminuir o tempo de processamento das transacções. Para tal, foi desenvolvido um mecanismo de agregação de transacções, que tem como objectivo reduzir o número de ligações entre o SP e o Operador. Este mecanismo possibilita a autorização de pagamentos por parte do SP, sem ter que recorrer sempre ao Operador, que é a única entidade com acesso ao saldo real das Carteiras. A decisão do SP em agregar (e autorizar de imediato) ou não (passando a autorização para o Operador) um pagamento, é realizada com o auxilio da seguintes variáveis:

1. A carteira utilizada, $c$.

2. O montante dos $n$ pagamentos $P$ que foram agregados no passado e que estão por liquidar sobre a carteira $c$, $\sum_{k=1}^{n} P_k(c)$.

3. O montante do último pagamento sobre a carteira $c$, $P_{n+1}(c)$ (i.e, o pagamento que está a ser autorizado).

4. O *montante de risco* (descrito na secção 4.5.3) atribuído pelo Operador à Carteira $c$, e que corresponde ao montante máximo dos pagamentos que podem ser agregados antes de se comunicar com o Operador, $M(c)$.

Com base nestas variáveis, o SP decide agregar um pagamento e autorizá-lo de imediato caso

$\sum_{k=1}^{n} P_k(c) + P_{n+1}(c) < M(c)$

e decide passar a autorização para o Operador responsável pela Carteira caso

$\sum_{k=1}^{n} P_k(c) + P_{n+1}(c) >= M(c)$

No último caso, o SP envia a informação do pedido de pagamento e o agregado dos pagamentos por liquidar para o Operador responsável pela Carteira. Ao receber o pedido, o Operador consoante o saldo da Carteira, aceita ou rejeita o pedido de autorização e processa os pagamentos agregados. Seguidamente, calcula um novo *montante de risco* actualizado e devolve-o ao SP, juntamente com a resposta ao pedido de autorização de pagamento.

O módulo de agregação de pagamentos, definido na secção 4.6, implementa este mecanismo.

### 4.5.3 Montante de Risco

O cálculo do *montante de risco* das Carteiras, poderá ser definido da forma que os Operadores entenderem. Nomeadamente, este processo poderá recair sobre os departamentos de análise de risco (analisam o risco de fraude e de crédito a clientes) dos Operadores.

O cálculo do *montante de risco* de uma Carteira, é processado cada vez que o Operador recebe um pedido de autorização de pagamento, de forma a que o SP fica com uma informação actualizada da situação da Carteira.

Caso o Operador verifique que um *montante de risco* que enviou ao SP já não se encontra actualizada (i.e, o saldo da Carteira já não permite mais pagamentos), poderá enviar uma notificação para o SP requerendo o congelamento de mais pagamentos sobre essa Carteira. Este cenário pode ocorrer caso o Operador tenha transmitido um *montante de risco* relativo a uma Carteira, que posteriormente, por alguma razão, já não se encontra actualizado. Ainda que este tipo de situações possa ser esporádico, desta forma previne-se a utilização de uma Carteira sem fundos.

## 4.6 Arquitectura

O modelo apresentado nesta dissertação, engloba quatro sistemas distintos, que interagem entre si com a finalidade de realizar pagamentos móveis. Estes sistemas são:

- Sistema do Utilizador
- Sistema do Comerciante

- Sistema de Pagamentos (controlado por um PSP e apresentado nesta dissertação como SP)
- Sistema do Operador

A figura 4.8 apresenta o diagrama de componentes de todos os sistemas. Cada um dos módulos apresentados representa um componente de software instalado num determinado sistema, cuja função consiste em realizar uma ou mais tarefas especificas.

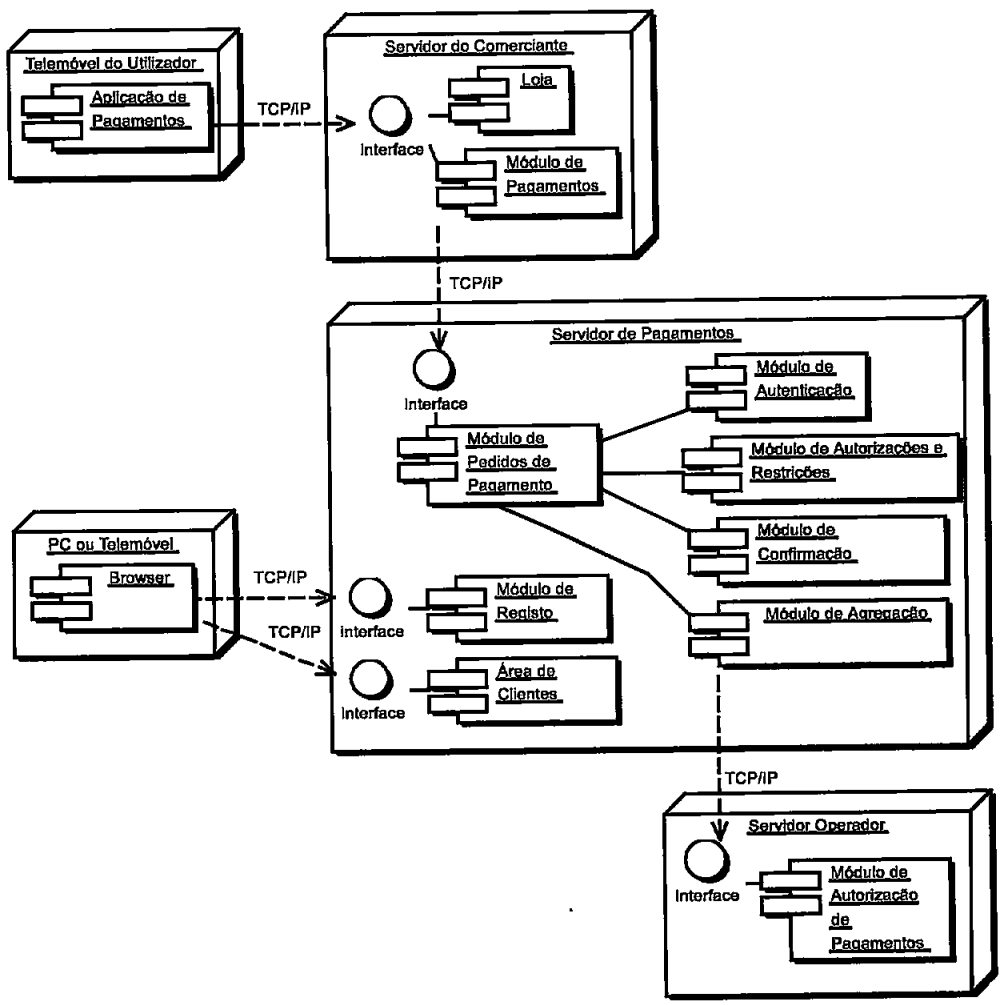


Figura 4.8: Diagrama de componentes

De seguida é descrito cada um dos módulos presentes nos vários sistemas, tal como apresentado na figura 4.8.

### Módulo de Registo

O módulo de registo (daqui por diante designado simplesmente por MR) está instalado no SP, e tem como função disponibilizar o mecanismo de registo para Utilizadores, Comerciantes e Operadores. Tipicamente, o MR consiste num portal na Internet, onde são recolhidos os dados necessários para a criação das diversas contas no SP.

### Área de Clientes

A área de clientes (daqui por diante designado simplesmente por AC), está instalada no SP, e tem como função disponibilizar uma interface para os Utilizadores, Comerciantes e Operadores poderem consultar, alterar e remover os seus dados. Tipicamente, a AC consiste num portal na Internet, onde, mediante autenticação, os clientes podem aceder à sua conta no SP. Por exemplo, um Utilizador que deseje autorizar outro Utilizador a usar a sua Carteira, deverá ir à sua área de cliente e adicioná-lo como seu sub-utilizador.

### Aplicação de Pagamentos

A aplicação de pagamentos (daqui por diante designado simplesmente por AP), é um software instalado no telemóvel do Utilizador, que lhe permite efectuar pagamentos móveis no SP. O Utilizador escolhe os bens que pretende adquirir junto do Comerciante, e no momento em que expressa a sua vontade de os comprar, o AP realiza as seguintes acções:

1. Pede ao Comerciante os detalhes dos bens que o Utilizador pretende comprar. Como resposta, o Comerciante disponibiliza dados como preço, identificador da transacção, etc.

2. Constrói o pedido de pagamento, recorrendo a mecanismos de criptografia de chave simétrica, por forma a garantir a confidencialidade dos dados a transmitir (explicado em detalhe na secção 4.7).

3. Envia o pedido de pagamento para o Comerciante e fica à espera dos bens.

### Loja

A Loja é uma aplicação instalada no sistema do Comerciante, que disponibiliza os bens a vender aos Utilizadores.

### Módulo de Pagamentos

O módulo de pagamentos (daqui por diante designado por MP) é controlado pelo Comerciante, e tem como objectivo processar os pedidos de pagamento dos Utilizadores que desejam comprar bens na sua Loja. O MP responde a pedidos de detalhes de pagamento do AP, e envia os pedidos de compra vindos do AP, juntamente com os respectivos pedidos de pagamento, para o SP.

### Módulo de Pedidos de Pagamento

Este módulo (daqui por diante designado por MPP) é a porta de entrada dos pedidos de pagamento móvel do Utilizador no SP. O MPP disponibiliza uma interface para comunicar com os Comerciantes. Ao receber um pedido, o MPP regista-o no sistema e atribui-lhe um identificador único para ser identificado em fases posteriores do processo de pagamento.

### Módulo de Autenticação

O módulo de autenticação (daqui por diante designado simplesmente por MA) está instalado no SP, e tem como função autenticar os intervenientes presentes no pedido de pagamento recebido pelo MPP. O MA verifica se o Utilizador e o Comerciante são quem dizem ser, e se os dados do pedido de compra do Utilizador são coerentes com os dados do pedido de pagamento do Comerciante. Este processo é realizado com recurso a mecanismos criptográficos, explicados em detalhe na secção 4.7.

### Módulo de Autorizações e Restrições

O módulo de autorizações e restrições (daqui por diante designado simplesmente por MAR) está instalado no SP, e tem como função decidir de acordo com as regras de autenticação e restrição definidas para o Utilizador, se este pode ou não efectuar o pagamento. Ao chegar um pedido ao MAR, este efectua as seguintes verificações:

1. O Utilizador tem permissões para utilizar a Carteira apresentada.
2. O Utilizador tem permissões para comprar o tipo de bens em questão.

3. O Utilizador tem permissões para gastar o montante em questão.

As regras de autorização e restrição são definidas pelo proprietário da Carteira envolvida na transacção.

### Módulo de Confirmação

O módulo de confirmação (daqui por diante designado simplesmente por MC) está instalado no sistema de pagamentos, e tem como função autenticar os Utilizadores envolvidos nas transacções e confirmar que estes tem conhecimento do pagamento que estão prestes a efectuar. Ao chegar um pedido ao MC, este verifica as regras do Utilizador em matéria de confirmação de pagamentos. Como foi descrito na secção 4.4.3, o Utilizador pode definir uma série de preferências relativas ao processo de confirmação dos pagamentos na sua Carteira. Consoante estas preferências, o MC pode pedir ao Utilizador que confirme o pagamento, ou ignorar esta fase e passar para a seguinte, dando assim o pagamento como confirmado. Caso se dê o primeiro caso, é pedido ao Utilizador que confirme o pagamento através da apresentação do seu código secreto, que será posteriormente validado pelo MC.

### Módulo de Agregação de Transacções

O módulo de agregação de transacções (daqui por diante designado simplesmente por MAT) está instalado no SP, e tem como função autorizar os pedidos de pagamento. Como foi descrito na secção 4.5.2, o Operador responsável pela Carteira disponibiliza ao SP um *montante de risco*, que será utilizado pelo MAT para decidir se autoriza um pedido de pagamento e o agrega, ou se pede autorização ao Operador. Este processo de decisão é explicado em detalhe na secção 4.5.2.

### Módulo de Autorização de Pagamentos

O módulo de autorização de pagamentos (daqui por diante designado simplesmente por MAP) está instalado no sistema do Operador, e tem como função autorizar pedidos de pagamentos vindos do SP (mais especificamente do MAT). Quando um pedido chega ao MAP, este verifica junto do saldo da Carteira envolvida na transacção a autorização do pagamento. Caso o pagamento seja autorizado, o MAP actualiza o saldo da Carteira e calcula um novo *montante de risco* (como definido na secção 4.5.2). O resultado do pedido de autorização é comunicado ao SP, e caso seja positivo, é também disponibilizado o novo *montante de risco* da Carteira.

## 4.7 Protocolo de Autenticação Anónimo

O protocolo de autenticação utilizado no SP foi baseado na proposta apresentada por [35], tendo sido adaptado às especificidades do SP.

### 4.7.1 Conceitos

A segurança é um elemento fundamental em qualquer sistema de pagamentos electrónicos. Se os consumidores se sentirem inseguros ao utilizar um sistema de pagamentos, muito provavelmente deixam de o utilizar, e este estará condenado ao insucesso.

Quando maior for o nível de segurança utilizado num sistema de pagamentos electrónicos, maior será a complexidade computacional envolvida (mais recursos computacionais necessários) para o implementar [34]. O facto do SP utilizar tecnologias móveis, muitas das quais com limitações significativas a vários níveis, influenciou a escolha do mecanismo de segurança. Assim sendo, o mecanismo de segurança escolhido toma em consideração as especificidades do ambiente envolvente, e o nível de segurança apropriado para o tipo de sistema em questão. De entre as limitações existentes nas tecnologias móveis, destacam-se as seguintes:

- Redes móveis com largura de banda limitada
- Dispositivos móveis com poucos recursos computacionais
- Dispositivos móveis com fracas capacidade de armazenamento

De seguida são feitas algumas considerações relativamente a mecanismos criptográficos usualmente utilizados em sistemas de pagamentos electrónicos.

#### Criptografia de Chave Simétrica

A Criptografia de chave simétrica [45] pressupõe a utilização de algoritmos onde a chave (o segredo) utilizada para decifrar um conjunto de dados pode ser calculada a partir da chave utilizada para cifrar os mesmos. Na maior parte dos algoritmos simétricos ambas as chaves são iguais. A segurança deste tipo de algoritmos reside na manutenção da privacidade da chave utilizada, uma vez que qualquer entidade com conhecimento da mesma pode cifrar e decifrar dados.

### Algoritmo de Sumário

Um algoritmo de sumário[5] [45] é uma função que, recebendo como valor de entrada dados de tamanho arbitrário, produz como resultado um valor de tamanho fixo. Para além disso, este tipo de funções tem de obedecer a um conjunto de propriedades:

- Facilidade no cálculo do resultado da função com base nos dados de entrada.
- Dificuldade no cálculo dos dados de entrada com base no resultado da função.
- Dificuldade em encontrar dois conjuntos de dados de entrada distintos que, aplicando-se-lhes o algoritmo de sumário, produzam o mesmo resultado.

Com base nas propriedades acima definidas consegue-se obter uma identificação inequívoca de qualquer conjunto de dados. Um algoritmo de sumário é publico, i.e., não existe qualquer tipo de segredo no processo. A segurança do mesmo baseia-se no conjunto de propriedades acima definido , ou seja, na sua não-invertibilidade e na independência que o sumário obtido possui dos dados de entrada. A alteração de um bit nos dados de entrada produz, com uma alta probabilidade, um resultado distinto do produzido pelos dados iniciais. Desta forma, uma entidade pode sempre verificar se um sumário corresponde a um determinado conjunto de dados.

### Criptografia de Chave Pública

A criptografia de chave pública [45] (ou assimétrica) pressupõe a existência de um par de chaves complementares, sendo uma pública e outra privada. A chave pública pode ser divulgada, enquanto que a privada se deve manter secreta. Para a criptografia de chave pública, é essencial que a chave privada seja conhecida apenas pelo seu titular.

O tempo e os requisitos computacionais de um algoritmo de chave pública são significativamente superiores a um algoritmo de chave simétrica [45]. Assim, e de acordo com as especificidades do SP, foi decidido utilizar criptografia de chave simétrica e algoritmos de sumário para autenticar os vários intervenientes e cifrar as mensagens trocadas. A criptografia de chave pública será usada para efectuar a distribuição das chaves simétricas, na altura de registo dos vários actores.

[5] Também conhecido por *hash* ou *message digest*

O protocolo de autenticação escolhido é baseado numa *Trusted Third Party*, cuja função consiste em autenticar os vários intervenientes no processo de pagamento. No modelo proposto, o papel de *Trusted Third Party* é atribuído ao PSP.

### 4.7.2 Notação

A notação utilizada para definição do protocolo de autenticação é a seguinte:

- U: Utilizador
- C: Comerciante
- O: Operador
- $K_{A-B}$: Chave secreta partilhada entre a entidade A e a entidade B
- $KA_{A-B}$: Chave de autenticação partilhada entre a entidade A e a entidade B
- $H(X)$: Algoritmo de sumário aplicado à mensagem $X$
- $N_A$: Numero aleatório gerado pela entidade A
- $E_K(X)$: Mensagem $X$ cifrada com a chave $K$ através de um algoritmo de chave simétrica
- $ID_A$: Identidade da entidade A
- $NID_A$: Pseudónimo da entidade A
- $I_z$: Item z
- $P_z$: Preço do item z
- $T_z$: Tipo do item z; este identificador serve para o SP, particularmente o seu Módulo de Autorizações e Restrições (definido na secção 4.6), verificar se o Utilizador pode comprar bens deste tipo
- $TS_A$: *Timestamp*[6]
- $A- > B$: Entidade A envia uma mensagem para a entidade B
- $O_A$: Identificador da transacção gerado pela entidade A
- $C_A$: Carteira do Utilizador A

[6]Selo Temporal.

- $PA_A$: Montante dos pagamentos acumulados na Carteira do Utilizador A
- $MR_{C_A}$: Montante de risco para a Carteira do Utilizador A
- $RP$: Resultado do pedido de autorização de pagamento

A chave de autenticação entre entidade a A e a entidade B, $KA_{A-B}$, é utilizada como chave de cifra das mensagens trocadas entre A e B, para que possam comunicar de forma segura sobre uma rede insegura (a Internet). Esta chave é gerada com recurso às seguintes variáveis:

1. Chave secreta acordada entre a entidade A e a entidade B, $K_{A-B}$
2. Número aleatório gerado pela entidade A, $N_A$

Assim, $KA_{A-B}$ é o resultado do sumário de $K_{A-B}$ e $N_A$.

Ao enviar uma mensagem para a entidade B, a entidade A inclui os seguintes dados:

- Mensagem cifrada através da chave de autenticação, $E_{KA_{A-B}}(X)$
- Número aleatório utilizado no cálculo da chave de autenticação, $N_A$

Desta forma, quando a mensagem chega à entidade B, este calcula a chave de autenticação com recurso à chave secreta que partilha com a entidade A e o número aleatório que recebeu na mensagem. Seguidamente, utiliza a chave de autenticação gerada para decifrar a $E_{KA_{A-B}}(X)$ que recebeu.

O facto de $KA_{A-B}$ ser sempre diferente (devido ao $N_A$) para cada mensagem trocada entre a entidade A e a entidade B, torna muito difícil o processo de obtenção da chave secreta, $K_{A-B}$, através da análise de informação interceptada.

Como foi referido acima, o papel de *Trusted Third Party* é atribuído ao PSP, que é suposto ser honesto e confiável pelas outras entidades. Todas as outras entidades precisam de se registar no PSP e partilhar uma chave secreta com este.

### 4.7.3 Protocolo

Nesta secção é apresentado o protocolo de autenticação anónimo, especificando o formato das mensagens trocadas entre os vários intervenientes e as operações criptográficas por estes efectuadas.

1. Pedido de Compra (entre o Utilizador e o Comerciante)

   $U->C : I_Z$

   $C->U : I_Z, P_Z, ID_C$

   $U->C : PedidoCompra, NID_U, N_U, I_Z$

   $PedidoCompra = E_{KA_{U-PSP}}(ID_U, ID_C, I_Z, P_Z, TS_U, H(I_Z, P_Z, TS_U))$

2. Pedido de Pagamento (entre o Comerciante e o PSP)

   $C->PSP : PedidoCompra, NID_U, N_U, PedidoPagamento, ID_C, N_C$

   $PedidoPagamento = E_{KA_{C-PSP}}(I_Z, P_Z, T_Z, O_C, TS_C, H(I_Z, P_Z, T_Z, TS_C))$

3. Pedido de Autorização (entre o PSP e o Operador)

   $PSP->O : PedidoAutorizacao, N_{PSP}$

   $PedidoAutorizacao = E_{KA_{PSP-O}}(O_{PSP}, P_Z, C_U, PA_U, TS_{PSP}, H(O_{PSP}, P_Z, C_U, PA_U, TS_{PSP}))$

4. Resposta ao Pedido de Autorização (entre o Operador e o PSP)

   $O->PSP : RespostaAutorizacao$

   $RespostaAutorizacao = E_{KA_{PSP-O}}(RP, MR_{C_U})$

5. Resposta ao Pedido de Pagamento (entre o PSP e o Comerciante)

   $PSP->C : RespostaU, RespostaC$

   $RespostaC = E_{KA_{F-PSP}}(O_C, RP)$

   $RespostaU = E_{KA_{U-PSP}}(I_Z, P_Z, RP)$

6. Resposta ao Pedido de Compra (entre o Comerciante e o Utilizador)

   $C- > U : RespostaU, content(I_Z)$

### 4.7.4 Conclusões

O protocolo de autenticação acima descrito garante os seguinte requisitos:

1. **Autenticação**: Todos os intervenientes partilham um chave secreta com o PSP. Desta forma, o PSP ao receber pedidos de pagamento, autentica os vários intervenientes.

2. **Confidencialidade**: Através da cifra das mensagens trocadas, garante-se a confidencialidade da informação em trânsito.

3. **Integridade**: Para proteger a informação de ser modificada em trânsito, é enviado juntamente com a mensagem, um sumário de alguns dados relevantes. Desta forma, o receptor da mensagem pode verificar se a mensagem foi ou não modificada em trânsito.

4. **Anonimato**: É importante prevenir o Comerciante de conhecer a real identidade do Utilizador. Para tal, o Utilizador ao comunicar com o Comerciante, apresenta um pseudónimo só conhecido pelo PSP. Desta forma, a privacidade do Utilizador fica salvaguardada.

5. **Imune a ataques** *key guessing*: Como a chave de autenticação é criada de forma dinâmica, o sucesso de ataques *key guessing* é quase impossível.

# Capítulo 5

# Implementação e Testes

Neste capítulo serão primeiramente definidas as tecnologias utilizadas na implementação do SP apresentado no capítulo 4. Posteriormente são descritos alguns aspectos da implementação efectuada e por fim são apresentados resultados de testes práticos realizados, tendo por base essa mesma implementação.

## 5.1 Tecnologia Utilizada

A implementação do SP foi realizada recorrendo à linguagem de programação Java. A Máquina Virtual e o compilador Java utilizados pertencem à versão *Java 2 Platform, Enterprise Edition 1.4 SDK* [10] (J2EE). Esta linguagem preenche totalmente os requisitos necessários a uma implementação deste tipo, nomeadamente:

- Múltiplas possibilidades de utilização de pacotes criptográficos;
- *Interfaces* e *drivers* com fiabilidade e desempenho amplamente testados, para as bases de dados mais comuns, como *MySQL*, *PostgreSQL* ou *Oracle*;
- Interfaces para acesso a directorias, nomeadamente para acesso a serviços de LDAP;
- Independência de sistema operativo;
- Suporte para a tecnologia *Java Message Service* (JMS) [12];
- Suporte para a tecnologia *Enterprise JavaBeans* (EJB) [5];
- Suporte para a tecnologia *Servlet* [14];
- Suporte para a tecnologia *Java Server Pages* (JSP) [13];

- Facilidade de integração com diferentes servidores aplicacionais.

O J2EE define um standard para o desenvolvimento de aplicações empresariais. Esta plataforma simplifica o seu desenvolvimento, passando-as por componentes normalizados e modulares, e disponibilizando um conjunto completo de serviços a esses componentes. Muitos dos detalhes de comportamento das aplicações são gerados automaticamente, sem a necessidade de recorrer a programação complexa.

Enquanto que para o SP foi escolhida a tecnologia J2EE, para a aplicação de pagamentos instalada no telemóvel dos Utilizadores optou-se pela tecnologia *Java 2 Micro Edition* (J2ME) [11].

O J2ME é um sub-conjunto do Java, especialmente adaptado para dispositivos móveis com capacidades limitadas em termos de processador, memória, ecrã e capacidade de introdução de dados. Entre estes dispositivos encontram-se os telemóveis, *PDAs*, e *set-top boxes* de televisão. Tal como o seu homólogo para a plataforma empresarial (J2EE), o J2ME também inclui uma Máquina Virtual, denominada de KVM, e um conjunto de interfaces Java destinadas ao desenvolvimento de aplicações móveis [48]. A escolha desta tecnologia em detrimento de outras (BREW, Symbian, etc), deveu-se às seguintes potencialidades do J2ME:

- Interfaces flexíveis;
- Modelo de segurança robusto;
- Suporte para vários protocolos de rede;
- Corre numa vasta diversidade de dispositivos móveis;
- Possibilidades de utilização de pacotes criptográficos adaptados ao ambiente móvel;
- Tecnologia suportada pelos principais fabricantes de dispositivos móveis.

A restante tecnologia utilizada foi a seguinte:

- Sistema Operativo: Linux
- Software Criptográfico: *Bouncy Castle* [3]
- Servidor LDAP: *OpenLDAP* [22]
- Base de Dados: *MySQL* [20]

- Servidor Aplicacional: *JBoss* [15]
- Servidor Web: Tomcat 5 [2]
- Simulador de telemóvel: *J2ME Wireless Toolkit 2.2* [9]
- Ferramentas para efectuar testes: *Junit* [16] e *JUnitPerf* [17]

## 5.2 Repositório

O repositório do SP armazena toda a informação relevante para o processamento de pagamentos móveis, estando repartido por várias tabelas. As tabelas do repositório são:

- *Customer*
- *Merchant*
- *Mobile_operator*
- *Wallet*
- *Product_type*
- *Authorization_rules*
- *Restriction_rules*
- *Control*
- *Customer_session*
- *Payment_order*

A figura 5.1 ilustra o diagrama de entidade-relação do repositório do SP.

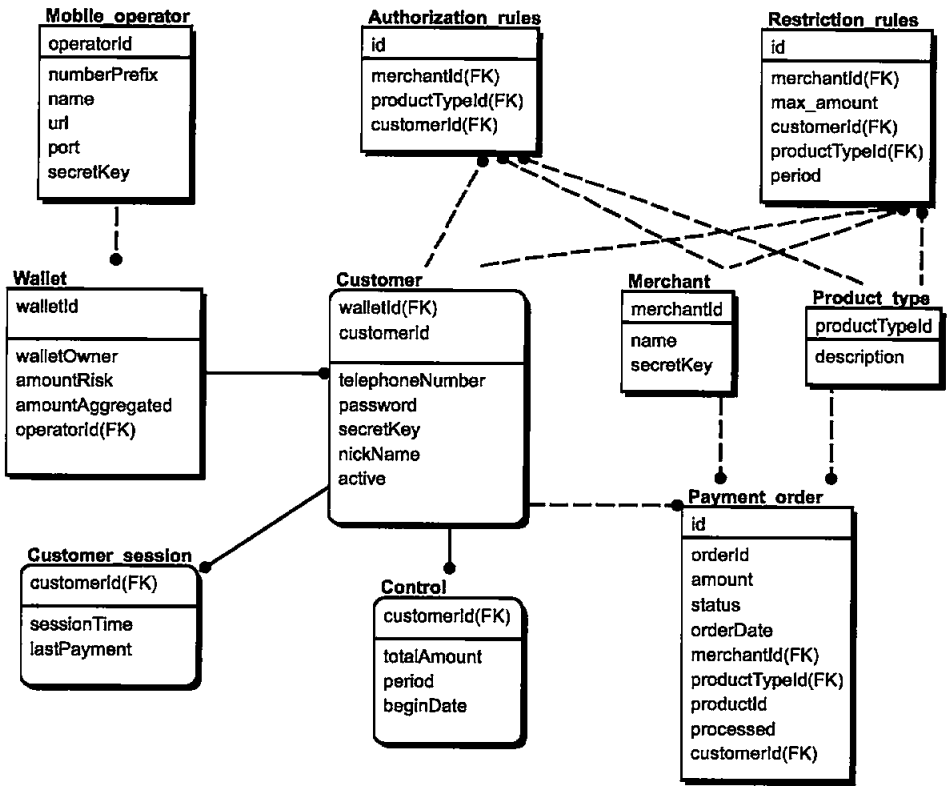


Figura 5.1: Repositório do SP

De seguida são descritas e enquadradas as tabelas do repositório e os respectivos elementos.

### Tabela *Customer*

A tabela *Customer* contém a informação dos Utilizadores do SP. Os elementos desta tabela são:

- *customerId*: Identificador interno do Utilizador.
- *nickName*: Pseudónimo do Utilizador, usado por este para se identificar perante os Comerciantes.

- *walletId*: Identificador interno da Carteira. Este elemento é chave primária da tabela *Wallet* e representa a Carteira que o Utilizador definiu para debitar os seus pagamentos.
- *telephoneNumber*: Número de telemóvel do Utilizador, utilizado para efectuar os pagamentos móveis.
- *password*: Código secreto do Utilizador, usado para confirmar os seus pagamentos móveis.
- *secretKey*: Chave secreta partilhada entre o Utilizador e o SP, usada para cifrar as mensagens trocadas entre ambos.
- *active*: Indicação se o Utilizador já se encontra activo no SP. No caso do Utilizador ter definido uma Carteira que não a sua para efectuar pagamentos, o estado do seu registo só passará a activo após o dono da Carteira o autorizar como seu sub-utilizador.

Por cada Utilizador que se regista no SP, é criado um novo registo na tabela *Customer* com os dados desse Utilizador.

### Tabela *Merchant*

A tabela *Merchant* contém a informação dos Comerciantes do SP. Os elementos desta tabela são:

- *merchantId*: Identificador interno do Comerciante.
- *name*: Nome do Comerciante.
- *secretKey*: Chave secreta partilhada entre o Comerciante e o SP, usada para cifrar as mensagens trocadas entre ambos.

Por cada Comerciante que se regista no SP, é criado um novo registo na tabela *Merchant* com os dados desse Comerciante.

### Tablela *Mobile_operator*

A tabela *Mobile_operator* contém a informação dos Operadores do SP. Os elementos desta tabela são:

- *operatorId*: Identificador interno do Operador.
- *numberPrefix*: Prefixo dos números de telefone atribuído ao Operador.
- *name*: Nome do Operador.
- *url*: Endereço do servidor do Operador para onde enviar os pedidos de autorização de pagamento.
- *port*: O porto do servidor do Operador para onde enviar os pedidos de autorização de pagamento.
- *secretKey*: Chave secreta partilhada entre o Operador e o SP, usada para cifrar as mensagens trocadas entre ambos.

Por cada Operador que se regista no SP, um novo registo é criado na tabela *Mobile_operator* com os dados desse Operador.

### Tabela *Wallet*

A tabela *Wallet* contém a informação das Carteiras (contas dos clientes nos Operadores) dos Utilizadores no SP. Os elementos desta tabela são:

- *walletId*: Identificador interno da Carteira.
- *walletOwner*: Identificador do Utilizador dono da Carteira. Este elemento é chave primária da tabela *Customer*.
- *amountRisk*: Montante de risco da Carteira (definido na secção 4.5.3), atribuído pelo Operador responsável por esta.
- *amountAggregated*: Montante de pagamentos agregados do lado do SP e ainda não comunicados ao Operador responsável pela Carteira.
- *operatorId*: Identificador do Operador responsável pela Carteira. Este elemento é chave primária da tabela *Mobile_operator*.

Por cada Utilizador que se regista no SP e indica a Carteira do seu Operador para debitar os pagamentos móveis, um novo registo é criado na tabela *Wallet*.

**Tabela *Product_type***

A tabela *Product_type* contém a informação dos tipos de bens previstos no SP. Os elementos desta tabela são:

- *productTypeId*: Identificador interno do tipo de bem.
- *description*: Descrição do tipo de bem. Por exemplo, infantil, noticias, serviços, desporto, adulto, etc.

Todos os bens que os Comerciantes vendem aos Utilizadores, devem pertencer a um dos tipos definidos na tabela *Product_type*. Nomeadamente, cada pedido de pagamento enviado pelo Comerciante para o SP, indica o tipo de bem envolvido na transacção (os dados de um pedido são descritos na secção 4.7.3).

**Tabela *Authorization_rules***

A tabela *Authorization_rules* contém a informação das regras de autorização de compras definidas para os Utilizadores do SP. Os elementos desta tabela são:

- *id*: Identificador interno da regra de autorização.
- *merchantId*: Identificador do Comerciante. Este elemento é chave primária da tabela *Merchant*. Caso a regra de autorização se destine a todos os Comerciantes em geral, este elemento apresenta o valor 0 (não atribuído a nenhum Comerciante).
- *productTypeId*: Identificador do tipo de produto envolvido na autorização em causa. Este elemento é chave primária da tabela *Product_type*. Caso a regra de autorização se destine a todos os tipos de bens em geral, este elemento apresenta o valor 0 (não atribuído a nenhum tipo de bem).
- *customerId*: Identificador do Utilizador a quem a autorização se destina. Este elemento é chave primária da tabela *Customer*.

Por cada Utilizador registado no SP, existe pelo menos um registo na tabela *Authorization_rules* associada a este. Cada vez que um super-utilizador define na sua área de cliente uma nova regra de autorização para um seu sub-utilizador, é criado um novo registo na tabela *Authorization_rules*.

**Tabela *Restriction_rules***

A tabela *Restriction_rules* contém a informação das regras de restrição de compras definidas para os Utilizadores do SP. A tabela *Control*, apresentada mais abaixo, controla a aplicação das restrições nesta tabela definidas. Os elementos desta tabela são:

- *id*: Identificador interno da regra de restrição.
- *merchantId*: Identificador do Comerciante envolvido na restrição. Este elemento é chave primária da tabela *Merchant*. Caso a regra de restrição se destine a todos os Comerciantes em geral, este elemento apresenta o valor 0 (não atribuído a nenhum Comerciante).
- *max_amount*: Restrição do montante máximo permitido para pagamentos efectuados pelo Utilizador, sobre o período definido no elemento *period* apresentado mais abaixo.
- *customerId*: Identificador do Utilizador a quem a restrição se destina. Este elemento é chave primária da tabela *Customer*.
- *productTypeId*: Identificador do tipo de produto envolvido na restrição em causa. Este elemento é chave primária da tabela *Product_type*. Caso a regra de restrição se destine a todos os tipos de bens geral, este elemento apresenta o valor 0 (não atribuído a nenhum tipo de bem).
- *period*: Período temporal associado a esta restrição. Pode ser horas, dias, semanas ou meses.

Cada vez que um super-utilizador define na sua área de cliente uma nova regra de restrição para um seu sub-utilizador, é criado um novo registo na tabela *Restriction_rules*.

### Tabela *Control*

A tabela *Control* contém a informação de controle dos pagamentos de um Utilizador. Esta tabela permite ao SP aplicar de forma correcta as regras de restrição definidas para o Utilizador. Os elementos desta tabela são:

- *customerId*: Identificador do Utilizador. Este elemento é chave primária da tabela *Customer*.
- *period*: Tempo definido para a restrição que se está a controlar. Este elemento contém o mesmo valor do elemento com o mesmo nome na tabela *Restriction_rules*.

- *beginDate*: Data e hora do primeiro pagamento do Utilizador que se está a controlar.
- *totalAmount*: Montante total dos pagamentos do Utilizador até ao momento, dentro do período (elemento *period*) definido para a restrição.

### Tabela *Customer_session*

A tabela *Customer_session* contém a informação das sessões dos Utilizadores. O mecanismo de sessão, definido na secção 4.5.1, utiliza esta tabela no seu processo de decisão. Os elementos desta tabela são:

- *customerId*: Identificador do Utilizador. Este elemento é chave primária da tabela *Customer*.
- *sessionTime*: Tempo de sessão definido para o Utilizador. Após um primeiro pagamento confirmado (apresentado o código secreto), o Utilizador fica dispensado de confirmar os pagamentos futuros durante o tempo definido neste elemento.
- *lastPayment*: Data e hora do último pagamento efectuado pelo Utilizador.

Por cada sessão aberta para um Utilizador, i.e, após um primeiro pagamento efectuado sem uma sessão aberta, é criado um novo registo na tabela *Customer_session* com os dados dessa sessão.

### Tabela *Payment_order*

A tabela *Payment_order* contém a informação dos pedidos de pagamento efectuados no SP. Os elementos desta tabela são:

- *id*: Identificador interno do pedido de pagamento.
- *orderId*: Identificador atribuído pelo Comerciante ao pedido de pagamento.
- *amount*: Montante do pagamento.
- *status*: Estado do pagamento. Este elemento vai sendo alterado, à medida que o pagamento passa pelas várias fases no processo de autorização.
- *orderDate*: Data e hora do pedido de pagamento.
- *merchantId*: Identificador do Comerciante. Este elemento é chave primária da tabela *Merchant*.

- *productTypeId*: Identificador do tipo de produto. Este elemento é chave primária da tabela *Product_type*.
- *productId*: Identificador atribuído pelo Comerciante ao bem envolvido no pagamento.
- *processed*: Indicação se o pagamento já foi processado.
- *customerId*: Identificador do Utilizador responsável pelo pagamento.
- *walletId*: Identificador da Carteira do Utilizador. Este elemento é chave primária da tabela *Wallet*.

Por cada pedido de pagamento que chega ao SP, é criado um novo registo na tabela *Payment_order* com os dados desse pedido. O elemento *status* desta tabela, vai adquirindo vários valores à medida que o pagamento passa pelos vários estados apresentados na figura 4.7.

## 5.3 Modelo do Sistema de Pagamentos

### 5.3.1 Estrutura do Sistema

Nesta secção será apresentada a estrutura de software presente nos vários módulos (descritos na secção 4.6) que compõem o SP.

A figura 5.2 ilustra a estrutura do SP dividida por pacotes. Cada um dos pacotes apresentados implementa um dos módulos do SP.

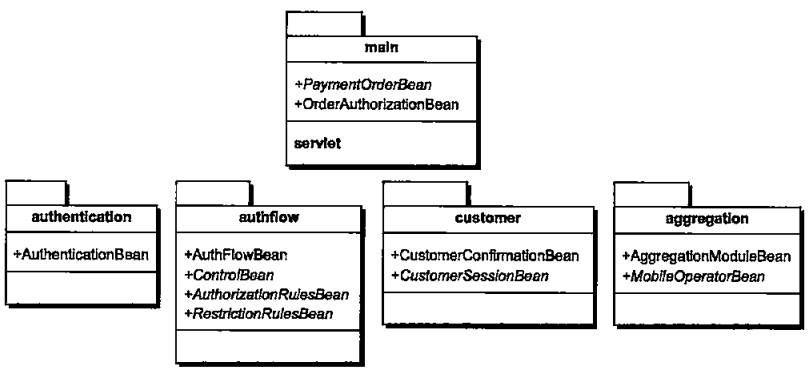


Figura 5.2: Diagrama de pacotes do SP

O pacote ***main*** implementa o Módulo de Pedidos de Pagamento (descrito na secção 4.6), que controla os pedidos de pagamentos que chegam ao SP. A figura 5.3 ilustra as classes presentes neste pacote.

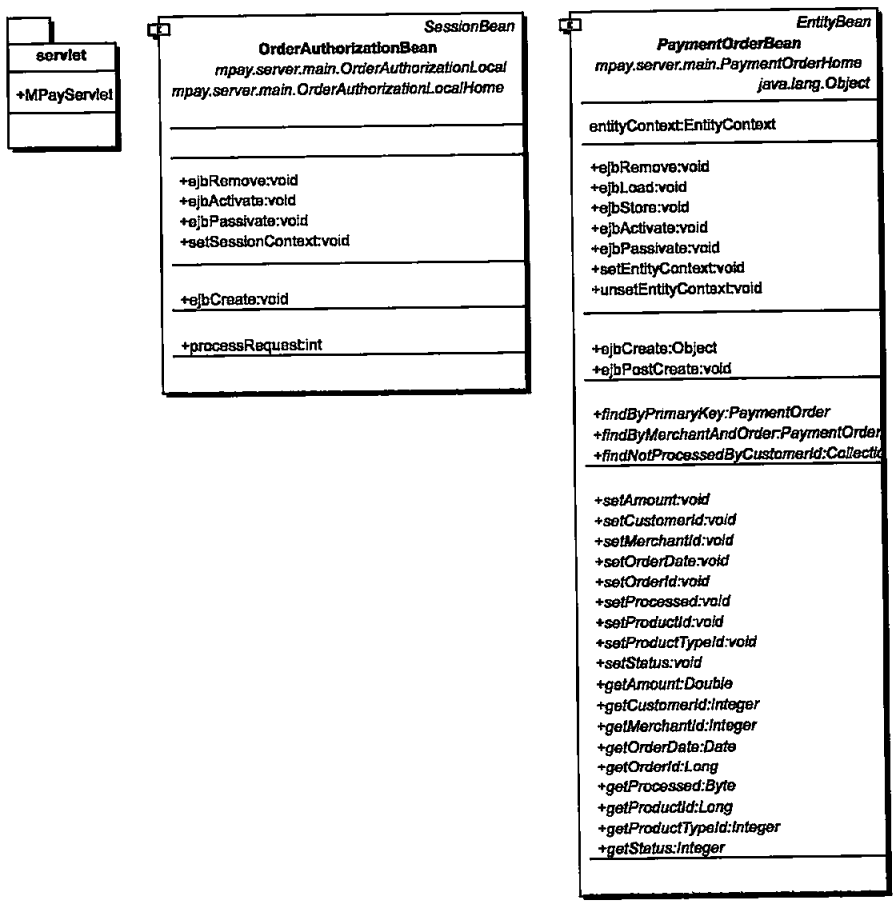


Figura 5.3: Diagrama de classes do pacote *main*

O pacote ***authentication*** implementa o Módulo de Autenticação (descrito na secção 4.6), que autentica o Utilizador e o Comerciante envolvidos numa transacção. A figura 5.4 ilustra a classe presente neste pacote.

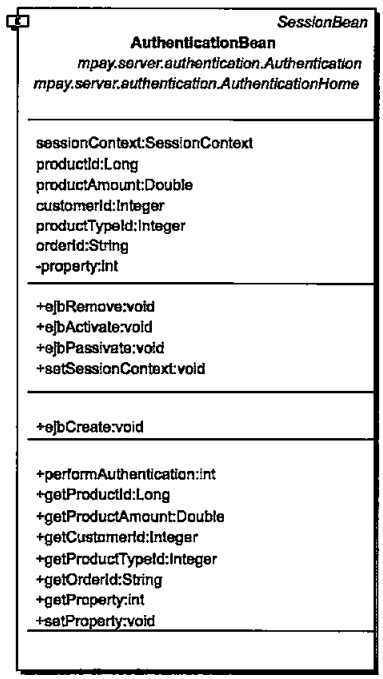


Figura 5.4: Diagrama de classes do pacote *authentication*

O pacote ***authflow*** implementa o Módulo de Autorizações e Restrições (descrito na secção 4.6), que decide, consoante as regras de autorização e restrição definidas para o Utilizador, se um pagamento é aceite e passa para a próxima fase do processo de pagamento, ou se pelo contrário, é imediatamente rejeitado. A figura 5.5 ilustra as classes presentes neste pacote.

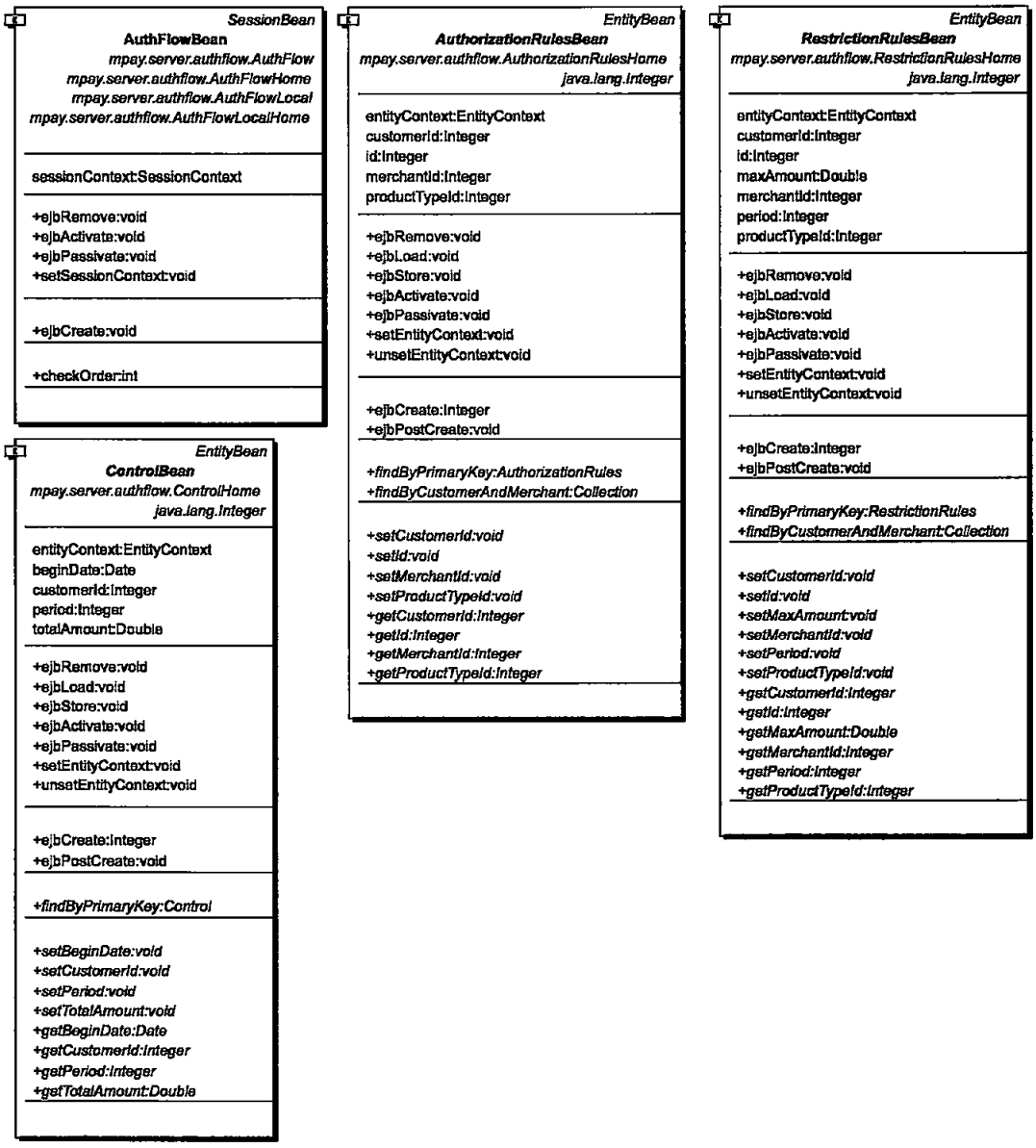


Figura 5.5: Diagrama de classes do pacote *authFlow*

O pacote ***customer*** implementa o Módulo de Confirmação (descrito na secção 4.6) que, consoante as preferências do Utilizador, confirma os detalhes do pagamento junto deste (pede-lhe o seu código secreto), ou dá o pagamento por confirmado, e passa automaticamente para a próxima fase do processo de pagamento. A figura 5.6 ilustra as classes presentes neste pacote.

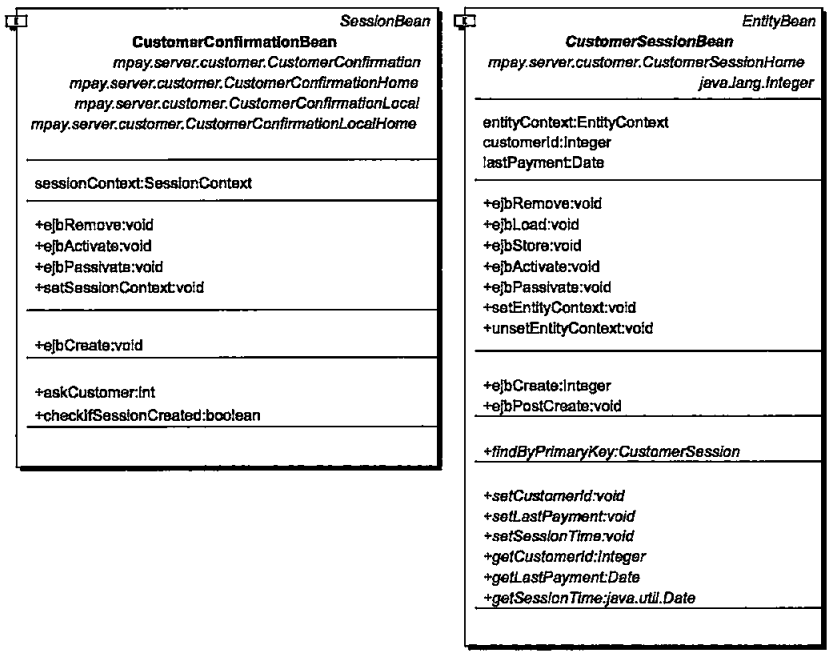


Figura 5.6: Diagrama de classes do pacote *customer*

O pacote ***aggregation*** implementa o Módulo de Agregação (descrito na secção 4.6) que, consoante a informação do *montante de risco* (descrito na secção 4.5.3) e dos pagamentos agregados, decide se agrega o pagamento e o autoriza de imediato, ou se pede autorização ao Operador responsável pela Carteira. A figura 5.7 ilustra as classes presentes neste pacote.

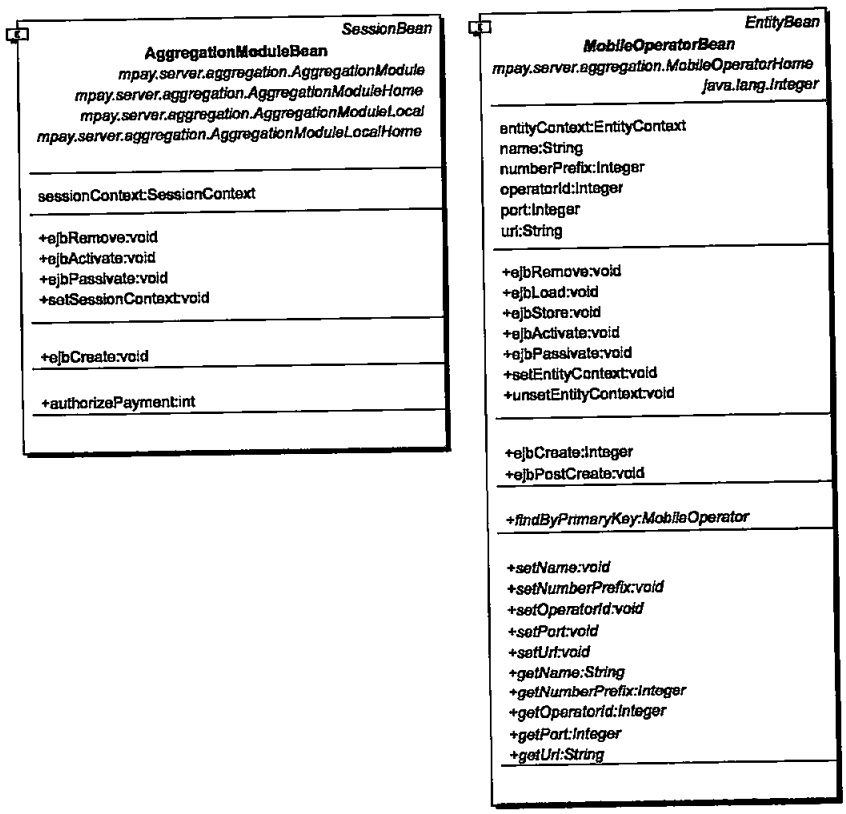


Figura 5.7: Diagrama de classes do pacote *aggregation*

### 5.3.2 *Workflow*

Os pedidos de pagamento chegam ao SP através da classe *MPayServlet* que se encontra no pacote *main* (pertencente ao Módulo de Pedidos de Pagamento). Esta classe disponibiliza uma interface HTTP para o exterior, com a finalidade de receber pedidos POST com a informação dos pagamentos a autorizar. É portanto a camada de apresentação do SP. Ao receber um pedido, a *MPayServlet* invoca o método *processRequest* da classe *OrderAuthorizationBean*, que irá processar toda a lógica de negócio. O método *processRequest* é o responsável pela coordenação do processo de pagamento, interagindo com os vários módulos do SP.

A figura 5.8 apresenta o diagrama de sequência[1] do método *processRequest* da classe *OrderAuthorizationBean*, ilustrando as várias fases por que um pedido de pagamento passa no SP.

[1] O diagrama de sequência apresentado, encontra-se simplificado, tento sido retiradas algumas especificidades do método *processRequest*.

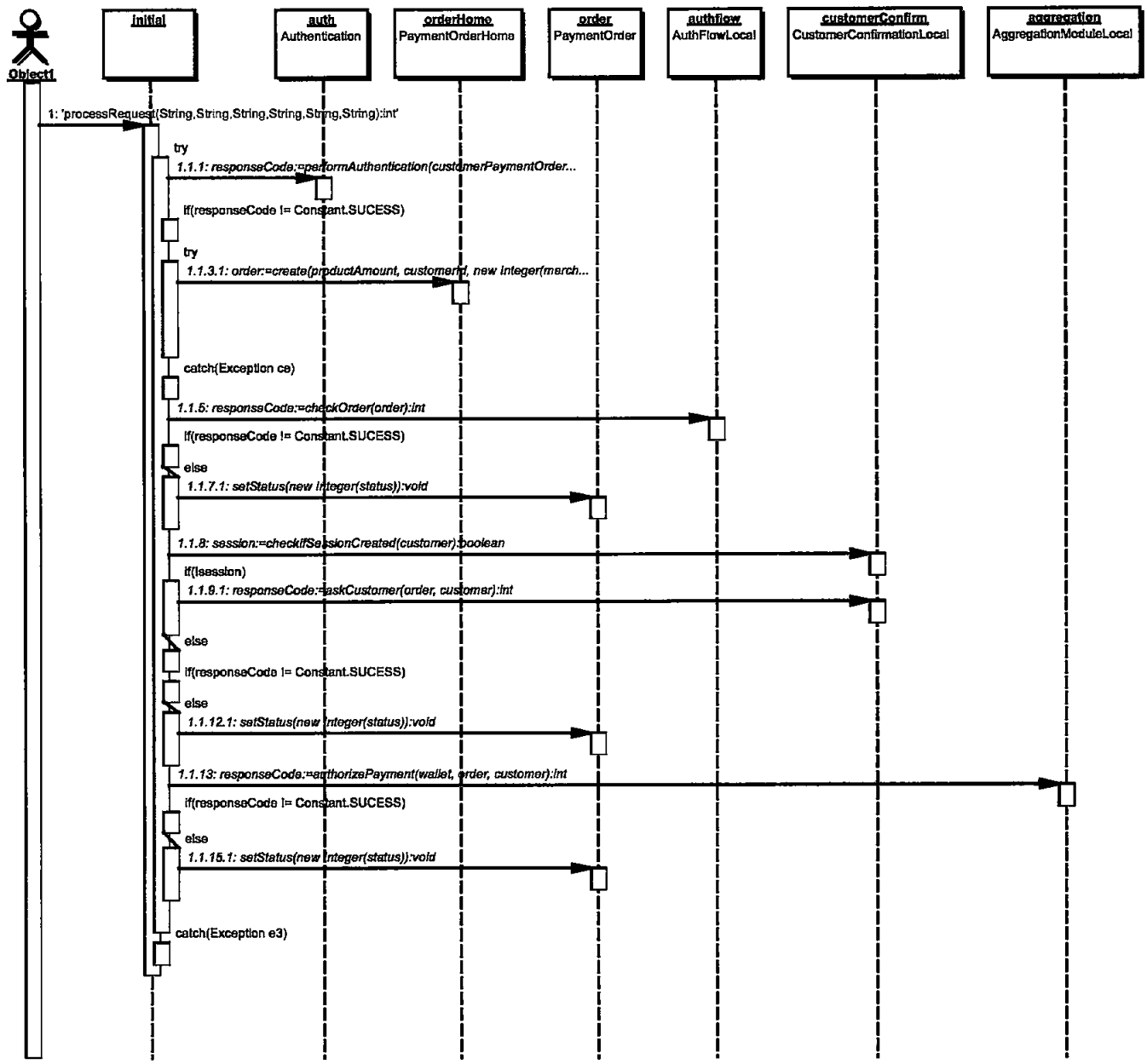


Figura 5.8: Diagrama de sequência do método *processRequest* da classe *Order-AuthorizationBean*

## 5.4 Códigos de Erro

Caso um pagamento não seja autorizado, é devolvido na resposta ao pedido de autorização do Comerciante um código de erro e respectiva descrição. A tabela 5.1 apresenta os códigos de erro e correspondentes descrições presentes no SP.

| Código de erro | Descrição do erro |
|---|---|
| 2 | *invalid merchant* |
| 3 | *invalid product type* |
| 4 | *invalid wallet* |
| 5 | *invalid customer* |
| 6 | *customer not allowed to use wallet* |
| 7 | *duplicate order id* |
| 8 | *customer not allowed to view this product* |
| 9 | *customer restriction to this product* |
| 10 | *customer authentication failed* |
| 11 | *merchant authentication failed* |
| 12 | *not authorized* |
| 27 | *internal error* |

Tabela 5.1: Códigos de erro e respectivas descrições

Em caso de sucesso do pagamento, o SP devolve o código com o valor 1.

## 5.5 Testes

Nesta secção são descritos os testes efectuados no SP e os resultados obtidos.

### 5.5.1 Ambiente de Testes

Para efectuar os testes pretendidos, foram envolvidos os seguintes sistemas:

- Aplicação de Pagamentos
- Sistema do Comerciante
- Sistema de Pagamentos (SP)
- Sistema do Operador

Devido à impossibilidade de ter um número significativo de telemóveis a gerarem pedidos de pagamentos móveis no SP (através do Sistema do Comerciante), foi desenvolvida uma aplicação que, de forma automática, simula estes pedidos (para tal foram utilizadas as ferramentas de testes *JUnit*[16] e *JUnitPerf*[17]). O tipo de carga que se pretendia submeter o SP não poderia ser alcançado através de processos manuais (com telemóveis). Esta aplicação de pagamentos gera POSTs HTTP com pedidos de compra para o Sistema do Comerciante. Os dados dos pedidos de compra foram previamente definidos, e a aplicação foi instalada num computador pessoal com o sistema operativo Windows.

O Sistema do Comerciante foi simulado para permitir que os pedidos de compra gerados pela aplicação anterior chegassem ao SP. Para tal, foi desenvolvido o Módulo de Pagamentos (descrito na secção 4.6) que recebe pedidos de detalhes de pagamento e de compra, e envia pedidos de pagamento para o SP (como definido na secção 4.7.3).

O Sistema do Operador foi simulado para permitir que o SP possa fazer pedidos de autorização de pagamentos junto deste, quando necessário. Para tal, foi desenvolvido o Módulo de Autorização de Pagamentos (descrito na secção 4.6).

Em ambos os sistemas (Comerciante e do Operador), os respectivos módulos consistem numa *Servlet* instalada num servidor *Web*, o Tomcat, que processa os pedidos HTTP que recebe. Os sistemas foram instalados em servidores (separados) com o sistema operativo Linux.

O Sistema de Pagamentos (SP) foi implementado na sua totalidade, e suporta todas as funcionalidades descritas no capítulo 4. Este sistema foi instalado num servidor com o sistema operativo Linux.

Todos os sistemas foram colocados em máquinas separadas, por forma a tornar o ambiente de testes o mais equivalente possível ao ambiente de produção. As ligações TCP/IP entre os vários sistemas foram conduzidas numa *Local Area Network* (LAN), visto ser um ambiente laboratorial. No entanto, quando em produção, as ligações TCP/IP entre os vários sistemas serão conduzidas via a Internet.

A figura 5.9 ilustra o ambiente de testes utilizado.

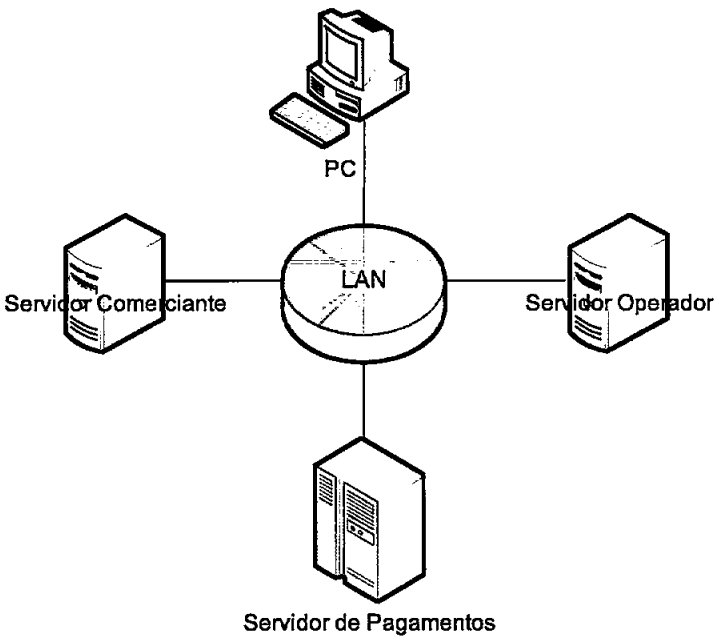


Figura 5.9: Ambiente de testes

Durante os testes efectuados, que consistiram na geração de pagamentos móveis, o processo de confirmação de pagamentos por parte dos Utilizadores (descrito na secção 4.4.5.1) foi retirado. Tal deveu-se ao facto de não estarem a ser utilizados telemóveis para gerar os pagamentos, mas sim uma aplicação que os gera automaticamente. Por outro lado, o tempo dispendido nesta acção é bastante variável, pois depende de uma acção manual directa do Utilizador, e não seria lógico contabiliza-lo para os resultados pretendidos.

No entanto, o Módulo de Confirmação (descrito na secção 4.6) foi incluído na implementação do SP, e o processo de verificação se um Utilizador precisa de confirmar um pagamento é sempre invocado (para o efeito decide sempre por não pedir confirmação ao Utilizador). Desta forma o tempo dispendido pela acção deste módulo é sempre contabilizado, tornando os resultados mais fiáveis.

### 5.5.2 Distribuição de Poisson

De acordo com as características do modelo em que o SP se insere, foi considerado que os pagamentos entram no sistema segundo uma distribuição de Poisson,

com uma taxa de $x$ pagamentos por unidade de tempo. Esta distribuição é amplamente utilizada quando se pretende simular o número de chegadas de eventos num dado período de tempo, sendo aplicável quando:

- O número de eventos que ocorrem em intervalos não sobrepostos é independente;
- A probabilidade de um evento ocorrer num pequeno intervalo de tempo é aproximadamente proporcional à amplitude desse intervalo;
- A probabilidade de mais que um evento ocorrer num pequeno intervalo de tempo é muito pequena, em comparação com a da ocorrência de um evento nesse mesmo intervalo, i.e., a probabilidade de ocorrerem chegadas simultâneas é desprezável.

A probabilidade de Poisson é dada por

$$P_n(x) = \frac{\lambda^x * e^{-\lambda}}{x!}$$

em que $x$ é o número de ocorrências do acontecimento em $n$ provas independentes, $p$ a probabilidade de um elemento dos $n$ ter uma dada propriedade, e onde $\lambda = np$ é o número médio de ocorrências deste acontecimento em $n$ provas [50].

### 5.5.3 Análise dos Testes

Os testes efectuados no SP tiveram como objectivos:

- Verificar o desempenho do SP, analisando o tempo médio de processamento por pagamento em situações de cargas distintas.
- Comprovar estatisticamente que a inclusão do MAT (descrito na secção 4.6) no SP permite obter melhores resultados em termos de tempo médio de processamento por pagamento. O MAT foi apresentado como uma optimização ao SP e será aqui comprovado.

De seguida serão apresentadas as variáveis utilizadas na geração dos pedidos de pagamentos móveis testados.

Como foi referido na secção anterior, os pagamentos chegam ao SP seguindo uma distribuição de Poisson com uma taxa de $x$ pagamentos por unidade tempo (daqui por diante designado por $\lambda$). Para os testes efectuados, foram considerados três valores $\lambda$ distintos, que representam três níveis de carga no sistema. Os $\lambda$ escolhidos foram:

1. 50 pagamentos por minuto (situação normal)
2. 100 pagamentos por minuto (situação de pico)
3. 200 pagamentos por minuto (situação de pico anormal)

Note-se que o primeiro valor do $\lambda$ corresponde a 72 mil pagamentos por dia, o segundo a 144 mil pagamentos por dia, e finalmente o terceiro a 288 mil pagamentos por dia.

Para cada bateria de testes efectuada foram incluídos três quantidades distintas de pedidos de pagamento consecutivos no SP:

1. 10 pagamentos
2. 50 pagamentos
3. 100 pagamentos

O tempo de entrada destes pagamentos consecutivos no SP, segue uma distribuição de Poisson com os valores do $\lambda$ tal como definidos acima. Assim, as várias quantidades de pagamentos consecutivos foram testadas com os vários $\lambda$.

Para cada um dos pagamentos testados foi calculado o tempo de processamento, desde o momento em que o pedido é feito, até ao momento em que é recebida a resposta. Depois de retirados os tempos dos vários pagamentos nas baterias de testes, foi feita a média ponderada dos tempos em cada uma das baterias.

O processo anterior foi repetido 30 vezes, com novos tempos de entrada dos pagamentos consecutivos no SP. Desta forma obteve-se observações diferentes em cada repetição.

Finalmente, foi calculada a média ponderada das médias resultantes de cada uma das 30 iterações.

Posteriormente, o SP foi modificado, tendo-lhe sido retirado o MAT. Desta forma o SP deixou de ter a possibilidade de agregar pagamentos do seu lado, tendo sempre que pedir a autorização do pagamento junto do Operador Móvel correspondente.

De forma a analisar os ganhos do SP com o MAT, foram efectuados testes utilizando o SP modificado sem o MAT, por forma a comparar resultados. Os testes a que o SP sem o MAT foi submetido foram exactamente os mesmos feitos ao SP com o MAT (descritos anteriormente), nomeadamente:

- O mesmo ambiente de testes, como definido na secção 5.5.1.
- As mesmas taxas de entrada de pagamentos por unidade de tempo ($\lambda$), nomeadamente os mesmos tempos de entrada dos pagamentos calculados para o SP com o MAT.
- A mesma quantidade de pedidos de pagamento consecutivos.
- Os mesmos dados de pagamento em cada um dos pedidos.

Resumidamente, os testes efectuados sobre o SP com e sem o MAT foram:

- Para os valores de $\lambda$ a 50, 100 e 200 pagamentos por minuto, foram calculadas os tempos de entrada no SP para 10, 50 e 100 pagamentos consecutivos.
- De seguida injectaram-se esses 10, 50 e 100 pagamentos no SP (em processo separados), de acordo com os tempos de entrada obtidos na operação anterior, e calculou-se o tempo médio de processamento por pagamento para cada uma das bateria de teste.
- A operação anterior foi repetida 30 vezes com os mesmos dados de pagamentos, mas com novos tempos de entrada no SP (para ter observações independentes).
- Finalmente foi calculada a média ponderada das médias de cada uma das baterias de testes, divididas pelas variáveis acima definidas, nomeadamente o $\lambda$ e o número de pagamentos consecutivos no SP.

Ao todo foram gerados 14400 pagamentos, tendo sido injectados nas mesmas condições no SP com o MAT e sem o MAT (totalizando 28800 pagamentos testados).

As tabelas a seguir apresentadas, indicam os resultados obtidos nos testes acima descritos, nomeadamente os tempos da média ponderada das médias (em milisegundos) anteriormente explicados. A secção A.1 do Apêndice, apresenta as tabelas com os resultados divididos por cada uma das 30 repetições nas várias situações distintas (vários $\lambda$ e quantidades de pagamentos consecutivos). Também no Apêndice, mas na secção A.2 são apresentados gráficos gerados a partir dos resultados obtidos nas várias situações.

A tabela 5.2 apresenta os resultados para 10 pagamentos consecutivos no SP com e sem o MAT, divididos pelos vários $\lambda$ definidos.

| 10 pagamentos consecutivos | | | | | | |
|---|---|---|---|---|---|---|
| $\lambda$ | 50 | | 100 | | 200 | |
| Modo | Com MAT | Sem MAT | Com MAT | Sem MAT | Com MAT | Sem MAT |
| Média (ms) | 705,83 | 3323,82 | 969,04 | 4596,30 | 1684,14 | 6328,00 |

Tabela 5.2: Resultado dos testes com 10 pagamentos consecutivos

A tabela 5.3 apresenta os resultados para 50 pagamentos consecutivos no SP com e sem o MAT, divididos pelos vários $\lambda$ definidos.

| 50 pagamentos consecutivos | | | | | | |
|---|---|---|---|---|---|---|
| $\lambda$ | 50 | | 100 | | 200 | |
| Modo | Com MAT | Sem MAT | Com MAT | Sem MAT | Com MAT | Sem MAT |
| Média (ms) | 775,94 | 6175,90 | 1038,53 | 14674,34 | 3273,15 | 14787,92 |

Tabela 5.3: Resultado dos testes com 50 pagamentos consecutivos

A tabela 5.4 apresenta os resultados para 100 pagamentos consecutivos no SP com e sem o MAT, divididos pelos vários $\lambda$ definidos.

| 100 pagamentos consecutivos | | | | | | |
|---|---|---|---|---|---|---|
| $\lambda$ | 50 | | 100 | | 200 | |
| Modo | Com MAT | Sem MAT | Com MAT | Sem MAT | Com MAT | Sem MAT |
| Média (ms) | 749,56 | 7089,40 | 1127,00 | 16457,52 | 6071,32 | 13516,40 |

Tabela 5.4: Resultado dos testes com 100 pagamentos consecutivos

### 5.5.4 Análise dos Resultados

Como se pode observar pelas tabelas 5.2, 5.3 e 5.4, os resultados obtidos, que equivalem ao tempo médio de processamento por pagamento, mostram que os

ganhos com a inclusão do MAT no SP são muito significativos. Em certos casos, os resultados obtidos com o MAT chegam a ser 14 vezes mais rápidos do que sem ele.

Analisando os resultados com o mesmo número de pagamentos consecutivos, mas com valores de $\lambda$ diferentes, conclui-se, como seria de esperar, que os tempos de processamento por pagamento vão aumentando à medida que o valor de $\lambda$ aumenta. O facto dos tempos de entrada entre os pagamentos irem diminuindo à medida que o valor do $\lambda$ aumenta, explica os resultados obtidos.

De seguida será feita a análise dos resultados separada pelas vários valores de $\lambda$.

Com o valor de $\lambda$ a 50, i.e., com uma taxa de entrada de 50 pagamentos por minuto, verifica-se o seguinte:

- No SP com o MAT, os tempos médios de processamento por pagamento mantêm-se praticamente iguais com as várias quantidades de pagamentos consecutivos (10, 50 e 100).

- No SP sem o MAT, o tempo médio de processamento por pagamento duplica quando se passa de 10 pagamentos consecutivos para 50. Entre 50 pagamentos consecutivos e 100, o tempo médio de processamento por pagamento aumenta ligeiramente. Verifica-se assim que o número de ligações entre o SP e o Operador, quando passa de 10 para 50 e 100, penaliza fortemente o desempenho do SP.

Com o valor de $\lambda$ a 100, i.e., com uma taxa de entrada de 100 pagamentos por minuto, verifica-se o seguinte:

- No SP com o MAT, os tempos médios de processamento por pagamento aumentam ligeiramente à medida que as quantidades de pagamentos consecutivos no SP vão aumentando (10, 50 e 100).

- No SP sem o MAT, o tempo médio de processamento por pagamento aumenta significativamente quando se passa de 10 pagamentos consecutivos para 50, e ligeiramente dos 50 para os 100 pagamentos.

Com o valor de $\lambda$ a 200, i.e., com uma taxa de entrada de 200 pagamentos por minuto, verifica-se o seguinte:

- No SP com o MAT, os tempos médios de processamento por pagamento duplicam à medida que as quantidades de pagamentos consecutivos no SP vão aumentando (10, 50 e 100). O facto dos tempos de entrada entre os pagamentos serem muito próximos (comparados com os valores de $\lambda$ a 50 e 100) explica esta perca de desempenho à medida que o número de pagamentos consecutivos injectados no SP vai aumentando.

- No SP sem o MAT, o tempo médio de processamento por pagamento aumenta significativamente quando se passa de 10 pagamentos consecutivos para os 50 e 100. Curiosamente o resultado obtido para 50 pagamentos consecutivos é ligeiramente inferior ao obtido para 100 pagamentos.

Concluindo, ficou provado que a utilização do MAT trouxe grandes benefícios ao SP, e que um dos objectivos do trabalho, a redução de custos por forma a viabilizar o negócio dos micro-pagamentos, foi concretizado com as optimizações realizadas ao SP.

# Capítulo 6

# Conclusões

Este capítulo faz um balanço sobre o trabalho apresentado ao longo da dissertação. Mais concretamente, na secção 6.1 são enumerados os objectivos alcançados, na secção 6.2 é realizada uma análise comparativa com trabalhos relacionados e na secção 6.3 são apresentadas limitações conhecidas ao sistema proposto e possíveis futuros melhoramentos.

## 6.1 Objectivos Alcançados

No inicio desta dissertação, foi traçado como principal objectivo o desenvolvimento de um sistema de pagamentos móveis para serviços e conteúdos de baixo valor, com as seguintes características: 1) ser independente do operador móvel como meio de acesso; 2) cobrar os serviços e conteúdos móveis adquiridos pelos consumidores através das contas dos respectivos operadores e 3) permitir a partilha da mesma conta por vários Utilizadores, independentemente do operador móvel que utilizam.

O sistema apresentado no capítulo 4 vai ao encontro dos objectivos traçados, nomeadamente as fortes garantias de acessibilidade, i.e., independência do Operador que suporta a comunicação e independência da Carteira usada pelo Utilizador[1]. Por outro lado, foi aproveitada a relação de confiança existente entre os Operadores e os seus clientes, particularmente na utilização dos seus mecanismos de facturação na cobrança dos pagamentos móveis.

O facto do SP ser direccionado para pagamentos móveis de baixo valor, tornou o factor custo de processamento por transacção extremamente importante e um dos

[1]Isto é, possibilidade de um Utilizador usar uma Carteira que não a sua para efectuar pagamentos móveis, independentemente do Operador que utilize.

objectivos mais importante do trabalho. Consequentemente, foram criados mecanismos que procuram reduzir estes custos (ver secção 4.5), por forma a rentabilizar um negócio cujas margens de lucro são muito baixas. Nomeadamente, foi criado um mecanismo de agregação de transacções (ver secção 4.5.2), que ficou provado através de simulações (ver secção 5.5.3) trazer importantes ganhos para o desempenho do SP.

Por outro lado, o facto do tipo de bens vendidos pelos Comerciantes serem de compra impulsiva (música, jogos, toques, etc), levou a que se procurasse tornar o acto de compra o mais agradável possível para os Utilizadores. Para tal, foi criado um mecanismo de sessão que procura minimizar as interacções dos Utilizadores com o sistema (ver secção 4.5.1).

Uma vez que o SP envolve dinheiro de pessoas, era fundamental que este fosse o mais seguro possível. Assim, foi desenvolvido um modelo de segurança (ver secção 4.7) que oferece garantias como a autenticação, confidencialidade e integridade dos dados. Devido às limitações inerentes ao ambiente móvel e aos níveis de desempenho impostos ao sistema, procurou-se adaptar o protocolo de segurança aos requisitos do SP.

Globalmente, o SP vai ao encontro dos objectivos traçados, apresentando-se apropriado para o pagamento de serviços e conteúdos de baixo valor num ambiente móvel.

## 6.2 Discussão e Comparação com Trabalhos Relacionados

Após um levantamento dos sistemas de pagamentos móveis existentes actualmente (ver secção 3), chegou-se à conclusão que existem dois modelos:

- Sistemas controlados por Operadores Móveis
- Sistemas controlados por PSPs

Uma das motivações deste trabalho prendeu-se com a percepção das limitações que os sistemas acima referidos apresentam. Ao analisar as vantagens e desvantagens destes sistemas, procurou-se conceber um novo sistema de pagamentos móveis que tirasse partido do que de melhor cada um disponibiliza, nomeadamente:

- Os mecanismos de facturação dos sistemas controlados por Operadores Móveis
- A independência do meio de acesso dos sistemas controlados por PSPs

Assim, comparando o SP no capítulo 4 com os sistemas analisados, verifica-se que este incorpora as vantagens analisadas nos outros, não partilhando no entanto as suas principais desvantagens, e.g., a dependência do meio de acesso do sistema Vodafone m-pay (apresentado na secção 3.2.2), ou a obrigatoriedade de possuir uma conta num PSP, como no sistema Paybox (apresentado na secção 3.2.1).

Por outro lado, a inclusão do MAT no SP vai ao encontro de um dos grandes pontos de referência do sistema de micro-pagamentos PepperCoin (apresentado na secção 3.1.1), o mecanismo de agregação de transacções.

Finalmente, o SP distingue-se de todos os outros pela funcionalidade que dá parte do nome ao título desta dissertação: garantias forte de acessibilidade, i.e, possibilita que vários Utilizadores, independentemente do Operador que utilizem, possam partilhar uma mesma Carteira para realizar pagamentos móveis.

## 6.3 Extensibilidade e Trabalho Futuro

O SP foi idealizado tendo em vista um cenário muito especifico: pagamentos on-line de baixo valor entre um Utilizador e um Comerciante, efectuados a partir de um telemóvel. Assim, são vários os cenários de pagamentos móveis em que o SP não pode ser utilizado.

O telemóvel é utilizada no SP como dispositivo de pagamento que permite aos Utilizadores efectuarem pagamento móveis. No entanto, a utilização do sistema em cenários de Comércio Electrónico tradicional, a partir de um computador pessoal, pode ser igualmente interessante. Neste caso, o Utilizador utilizaria o telemóvel para confirmar os pagamentos (fase de confirmação). O SP poderá ser adaptado para suportar esta funcionalidade.

A utilização do SP apenas se enquadra em cenários de pagamentos remotos, i.e., cenários onde o Utilizador e o Comerciante não se encontram fisicamente juntos. O SP poderá ser extendido para cenários de pagamentos locais, e.g, parquímetros, cafés e bilhetes de metro.

Por outro lado, o SP foi optimizado para processar pagamentos de baixo valor, ignorando as potencialidades do mercado dos macro-pagamentos. O SP poderá ser adaptado para que possa igualmente processar macro-pagamentos.

Outras das funcionalidades interessantes que o SP poderá suportar, é o pagamento entre Utilizadores, P2P. Inclusivamente, poderia-se ter pagamentos entre Utilizadores de Operadores diferentes, o que tornaria o sistema verdadeiramente global.

# Apêndice A

# Tabelas e Gráficos de Resultados

## A.1 Tabelas com Resultados dos Testes

| 10 pagamentos consecutivos | | | | | | |
|---|---|---|---|---|---|---|
| $\lambda$ | 50 | | 100 | | 200 | |
| Modo | Com MAT | Sem MAT | Com MAT | Sem MAT | Com MAT | Sem MAT |
| 1 | 668,10 | 4807,00 | 6353,90 | 8523,20 | 1594,30 | 6129,90 |
| 2 | 563,90 | 3299,70 | 729,80 | 5126,30 | 1386,00 | 5451,70 |
| 3 | 1241,90 | 3911,50 | 1016,80 | 4854,20 | 872,30 | 5430,90 |
| 4 | 530,70 | 2866,10 | 866,40 | 4884,20 | 891,20 | 4681,90 |
| 5 | 604,70 | 4015,80 | 1267,00 | 6977,00 | 718,10 | 6628,40 |
| 6 | 547,80 | 4063,80 | 666,00 | 5026,00 | 1742,40 | 5510,80 |
| 7 | 828,10 | 4786,80 | 909,50 | 5379,60 | 1356,00 | 5796,60 |
| 8 | 528,60 | 3870,60 | 972,70 | 4224,10 | 673,90 | 6236,90 |
| 9 | 522,90 | 2421,30 | 720,90 | 4401,10 | 1222,70 | 6079,70 |
| 10 | 947,40 | 3003,20 | 636,10 | 3866,50 | 1946,90 | 7015,10 |
| 11 | 506,80 | 3274,60 | 469,80 | 3732,30 | 3208,70 | 6355,10 |
| 12 | 902,40 | 4224,30 | 433,60 | 3311,70 | 2451,50 | 6780,70 |
| 13 | 579,80 | 2985,10 | 1243,80 | 3211,70 | 42240 | 6979,10 |
| 14 | 493,50 | 3038,70 | 490,60 | 4772,90 | 2926,20 | 5546,90 |
| 15 | 583,70 | 3038,10 | 528,80 | 3870,50 | 556,70 | 6007,60 |
| 16 | 719,90 | 3537,80 | 641,80 | 4236,10 | 603,70 | 4586,44 |
| 17 | 777,80 | 2049,10 | 909,50 | 6030,70 | 1234,70 | 5617,90 |
| 18 | 895,10 | 2121,10 | 838,10 | 5701,10 | 1233,80 | 5220,60 |
| 19 | 577,80 | 2633,80 | 605,00 | 5971,50 | 1177,60 | 6033,50 |
| 20 | 604,90 | 4137,10 | 725,20 | 4764,90 | 856,10 | 6883,80 |
| 21 | 687,10 | 1967,80 | 682,10 | 3646,30 | 1522,20 | 7172,30 |
| 22 | 507,60 | 2439,60 | 505,50 | 3541,90 | 1511,10 | 6701,80 |
| 23 | 886,40 | 2636,00 | 1959,50 | 6093,90 | 1291,90 | 7989,50 |
| 24 | 986,30 | 4101,70 | 756,30 | 3979,60 | 2922,30 | 7954,50 |
| 25 | 703,00 | 2759,80 | 452,60 | 3934,80 | 3569,30 | 6721,70 |
| 26 | 479,90 | 3381,80 | 522,90 | 4124,90 | 3562,00 | 6134,90 |
| 27 | 684,10 | 3250,60 | 480,90 | 3046,40 | 1552,20 | 5067,40 |
| 28 | 583,80 | 3254,80 | 1042,70 | 3769,70 | 1623,40 | 7973,60 |
| 29 | 455,80 | 3493,00 | 557,80 | 2937,30 | 1221,80 | 7537,90 |
| 30 | 1575,20 | 4344,10 | 1085,50 | 3948,60 | 871,10 | 7612,80 |
| Média (ms) | 705,83 | 3323,82 | 969,04 | 4596,30 | 1684,14 | 6328,00 |

Tabela A.1: Resultados completos dos testes com 10 pagamentos consecutivos

| 50 pagamentos consecutivos | | | | | | |
|---|---|---|---|---|---|---|
| $\lambda$ | 50 | | 100 | | 200 | |
| Modo | Com MAT | Sem MAT | Com MAT | Sem MAT | Com MAT | Sem MAT |
| 1 | 855,54 | 6950,52 | 1019,76 | 15293,18 | 2401,84 | 13563,94 |
| 2 | 762,26 | 4053,68 | 1252,90 | 13433,90 | 891,26 | 15829,58 |
| 3 | 740,82 | 4614,12 | 933,58 | 14381,18 | 3058,76 | 15049,10 |
| 4 | 774,56 | 10512,04 | 850,10 | 16091,94 | 2029,94 | 14722,62 |
| 5 | 943,42 | 12351,20 | 814,78 | 15563,10 | 5855,62 | 14793,54 |
| 6 | 616,80 | 4422,32 | 1003,56 | 13274,00 | 5637,50 | 15704,13 |
| 7 | 708,82 | 3866,96 | 1414,48 | 14207,24 | 1908,18 | 14445,54 |
| 8 | 1005,44 | 4191,82 | 1675,92 | 15431,40 | 1843,58 | 13735,18 |
| 9 | 722,40 | 10262,08 | 912,76 | 15048,76 | 2360,40 | 15501,04 |
| 10 | 617,00 | 2926,56 | 1556,30 | 12452,46 | 1339,56 | 14090,58 |
| 11 | 895,40 | 6176,46 | 905,92 | 14233,28 | 3387,40 | 13533,82 |
| 12 | 796,94 | 13490,78 | 1406,60 | 14676,50 | 5428,68 | 13874,08 |
| 13 | 732,42 | 7045,22 | 1099,94 | 15651,62 | 2443,48 | 16797,29 |
| 14 | 771,72 | 13732,96 | 844,54 | 15121,72 | 2787,34 | 14153,88 |
| 15 | 932,14 | 6979,78 | 954,40 | 15588,24 | 3474,58 | 16231,52 |
| 16 | 787,68 | 3798,28 | 1132,50 | 14688,75 | 1011,48 | 14851,08 |
| 17 | 630,94 | 3289,20 | 714,88 | 13781,26 | 2570,24 | 14569,92 |
| 18 | 897,18 | 4505,28 | 1062,14 | 13635,74 | 1818,02 | 14122,02 |
| 19 | 605,24 | 5953,76 | 823,36 | 15148,98 | 4873,52 | 13551,78 |
| 20 | 736,60 | 4027,60 | 753,52 | 13192,94 | 1444,32 | 14612,64 |
| 21 | 606,10 | 5533,18 | 970,84 | 11836,98 | 8362,88 | 15316,44 |
| 22 | 951,84 | 7689,30 | 1627,36 | 15347,66 | 4120,54 | 13786,82 |
| 23 | 655,30 | 7007,42 | 935,74 | 17480,16 | 5040,72 | 14250,06 |
| 24 | 1027,86 | 6592,48 | 1012,28 | 13857,55 | 3620,82 | 15609,82 |
| 25 | 821,40 | 3524,24 | 993,86 | 16174,29 | 1803,40 | 13720,10 |
| 26 | 605,30 | 3709,74 | 731,18 | 16930,48 | 7304,06 | 15016,54 |
| 27 | 872,48 | 7330,02 | 953,48 | 12834,48 | 2631,34 | 14639,62 |
| 28 | 734,72 | 3574,32 | 860,10 | 13269,72 | 3097,10 | 15675,36 |
| 29 | 714,92 | 4184,64 | 957,50 | 15234,08 | 3023,76 | 16405,04 |
| 30 | 754,92 | 2981,00 | 981,58 | 16368,48 | 2624,12 | 15484,64 |
| Média (ms) | 775,94 | 6175,90 | 1038,53 | 14674,34 | 3273,15 | 14787,92 |

Tabela A.2: Resultados completos dos testes com 50 pagamentos consecutivos

| 100 pagamentos consecutivos | | | | | | |
|---|---|---|---|---|---|---|
| $\lambda$ | 50 | | 100 | | 200 | |
| Modo | Com MAT | Sem MAT | Com MAT | Sem MAT | Com MAT | Sem MAT |
| 1 | 838,34 | 6267,88 | 915,02 | 15697,50 | 6954,57 | 12972,23 |
| 2 | 822,82 | 11394,35 | 1218,25 | 16495,16 | 8913,16 | 13131,34 |
| 3 | 575,48 | 6418,69 | 946,95 | 16910,53 | 9642,81 | 12589,32 |
| 4 | 820,49 | 6745,69 | 867,34 | 17737,75 | 5605,39 | 14394,54 |
| 5 | 596,03 | 4447,60 | 862,44 | 16966,29 | 7790,10 | 13311,97 |
| 6 | 804,62 | 6201,65 | 1250,22 | 15552,86 | 7998,68 | 13349,99 |
| 7 | 649,64 | 4660,60 | 946,02 | 18292,75 | 4814,41 | 13551,22 |
| 8 | 779,76 | 9423,96 | 883,92 | 16631,36 | 4863,56 | 13159,02 |
| 9 | 645,25 | 5122,97 | 994,43 | 17072,81 | 5542,17 | 13447,04 |
| 10 | 778,70 | 5854,74 | 1115,22 | 14180,06 | 5083,57 | 13427,90 |
| 11 | 795,72 | 4315,12 | 939,90 | 18334,59 | 4119,87 | 12426,74 |
| 12 | 671,71 | 6493,31 | 1028,02 | 14972,31 | 2788,11 | 13791,86 |
| 13 | 751,53 | 7095,54 | 994,56 | 16692,64 | 2198,31 | 13752,90 |
| 14 | 728,17 | 8264,55 | 912,53 | 17137,65 | 3561,60 | 13948,62 |
| 15 | 706,55 | 7362,18 | 1684,80 | 15954,41 | 8113,21 | 13491,69 |
| 16 | 684,61 | 3013,92 | 1039,68 | 16067,50 | 5789,03 | 13496,94 |
| 17 | 701,89 | 5302,11 | 1035,19 | 16528,54 | 5602,11 | 13790,65 |
| 18 | 780,65 | 4446,98 | 1161,34 | 17306,36 | 7566,37 | 12848,25 |
| 19 | 769,10 | 8250,68 | 1656,86 | 16132,89 | 3662,09 | 15082,65 |
| 20 | 806,57 | 6266,85 | 1006,77 | 14869,46 | 2695,80 | 14004,34 |
| 21 | 807,97 | 6114,97 | 1231,09 | 15680,23 | 9631,81 | 13817,97 |
| 22 | 1035,20 | 15773,67 | 1175,70 | 16460,60 | 4087,31 | 13175,36 |
| 23 | 671,91 | 7314,85 | 1193,97 | 13900,00 | 2953,56 | 14397,67 |
| 24 | 659,37 | 5777,28 | 1711,03 | 17801,20 | 3704,66 | 13674,84 |
| 25 | 754,15 | 6892,55 | 1225,65 | 15467,49 | 4109,12 | 13219,06 |
| 26 | 749,54 | 5580,72 | 966,98 | 16370,62 | 8113,65 | 13974,31 |
| 27 | 820,35 | 9589,00 | 1537,68 | 16661,36 | 9090,42 | 14584,71 |
| 28 | 800,02 | 5945,24 | 999,73 | 18786,33 | 9171,40 | 12948,34 |
| 29 | 653,29 | 8424,65 | 892,76 | 15930,38 | 8038,19 | 12893,05 |
| 30 | 827,29 | 13919,73 | 1415,95 | 17133,96 | 9934,43 | 12837,48 |
| Média (ms) | 749,56 | 7089,40 | 1127,00 | 16457,52 | 6071,32 | 13516,40 |

Tabela A.3: Resultados completos dos testes com 100 pagamentos consecutivos

## A.2 Gráficos com Resultados dos Testes

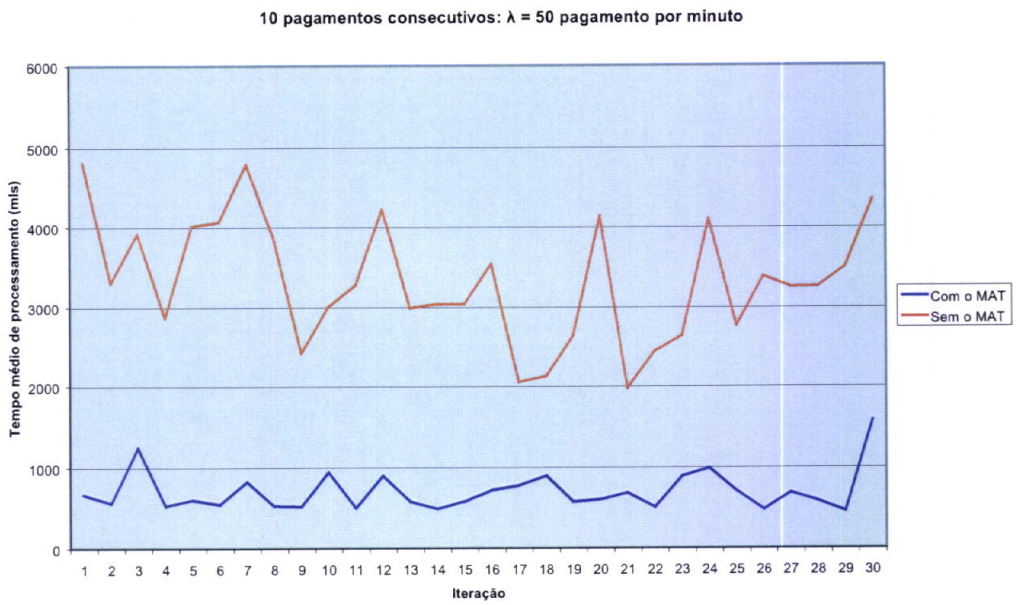


Figura A.1: Gráfico de 10 pagamentos consecutivos com $\lambda = 50$

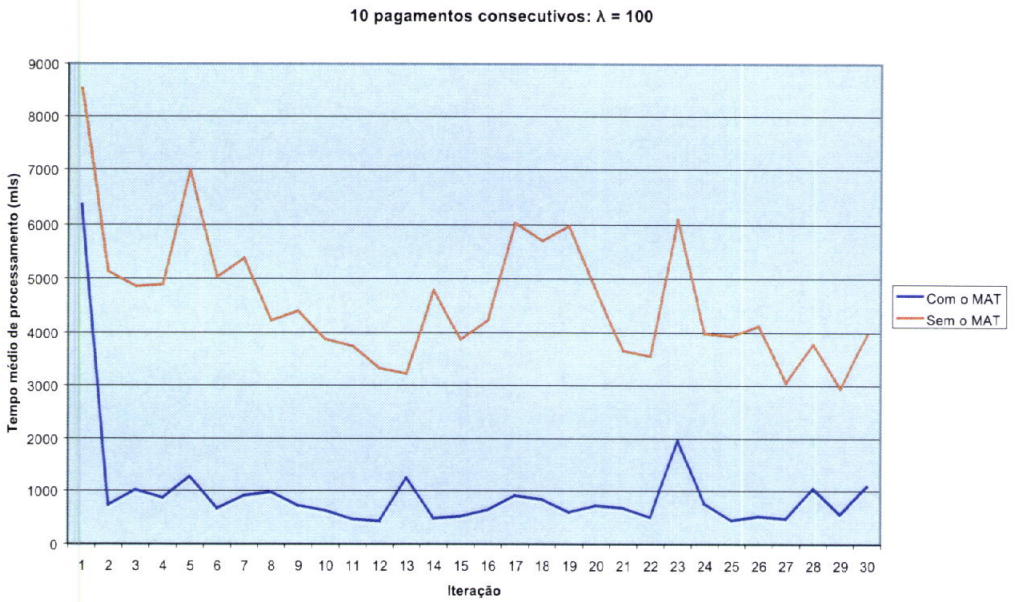


Figura A.2: Gráfico de 10 pagamentos consecutivos com $\lambda = 100$

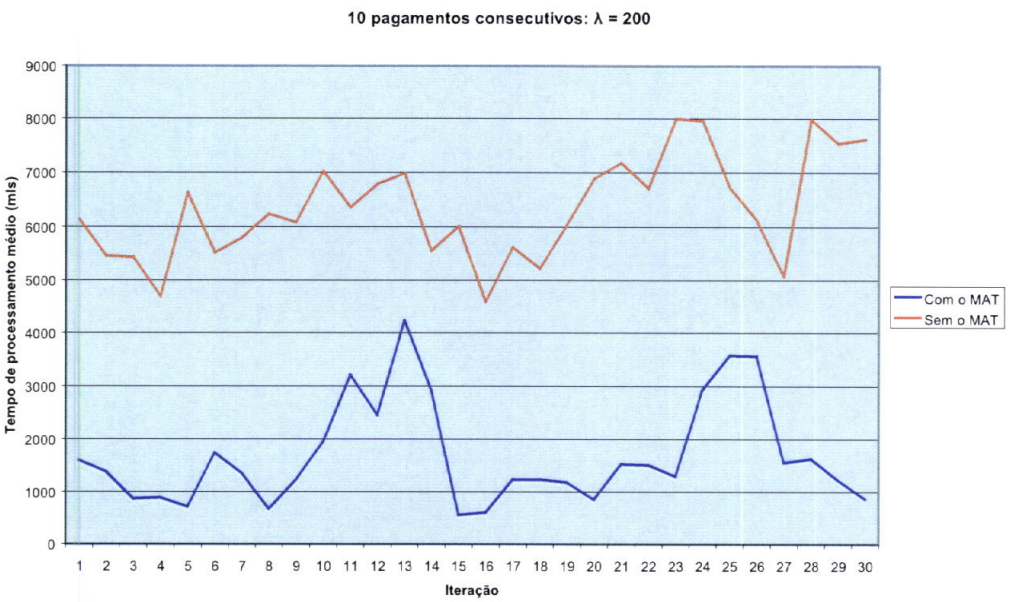


Figura A.3: Gráfico de 10 pagamentos consecutivos com $\lambda = 200$

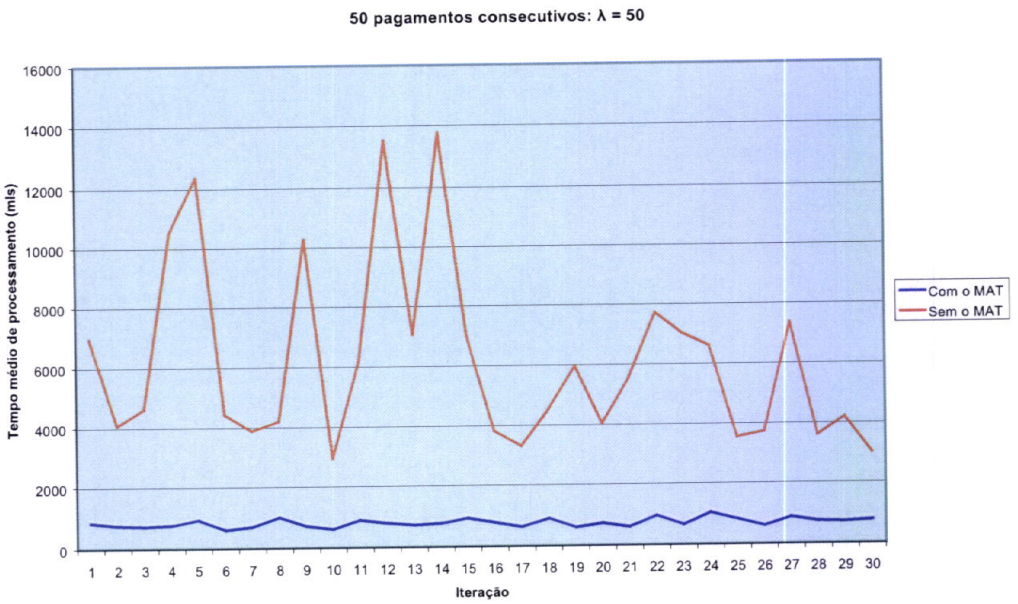


Figura A.4: Gráfico de 50 pagamentos consecutivos com $\lambda = 50$

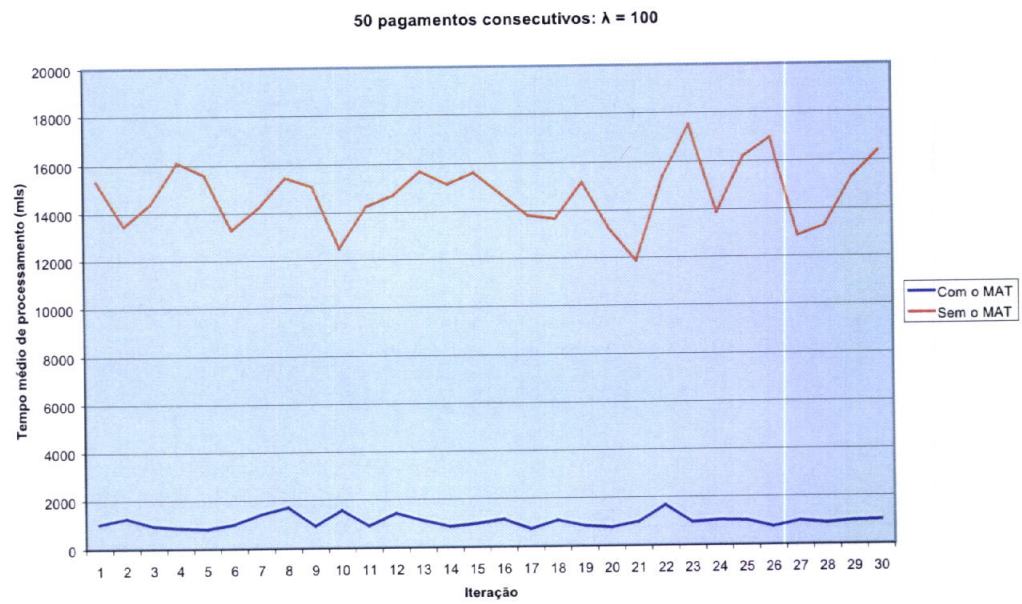


Figura A.5: Gráfico de 50 pagamentos consecutivos com $\lambda = 100$

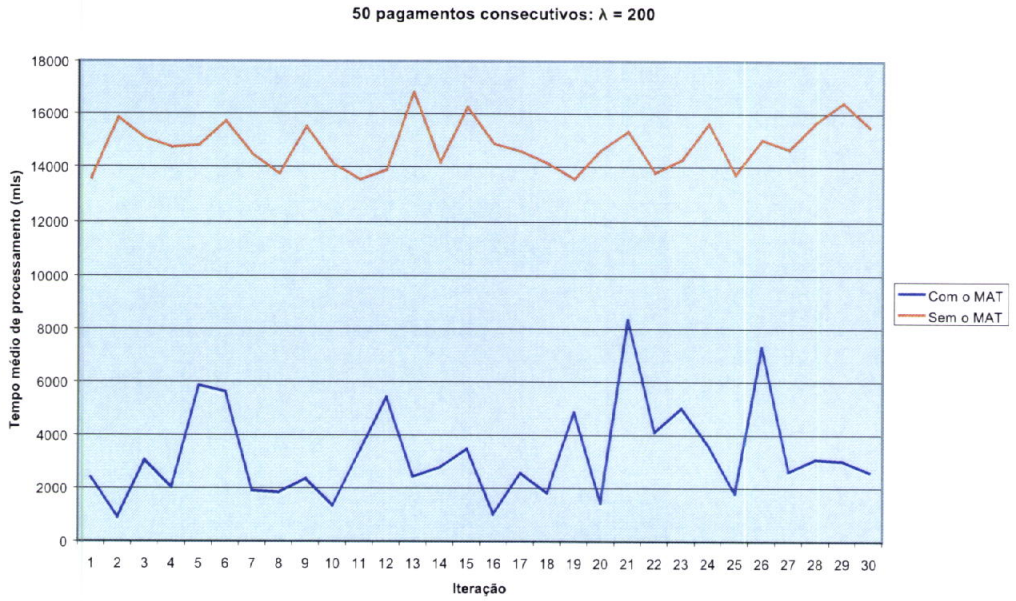


Figura A.6: Gráfico de 50 pagamentos consecutivos com $\lambda = 200$

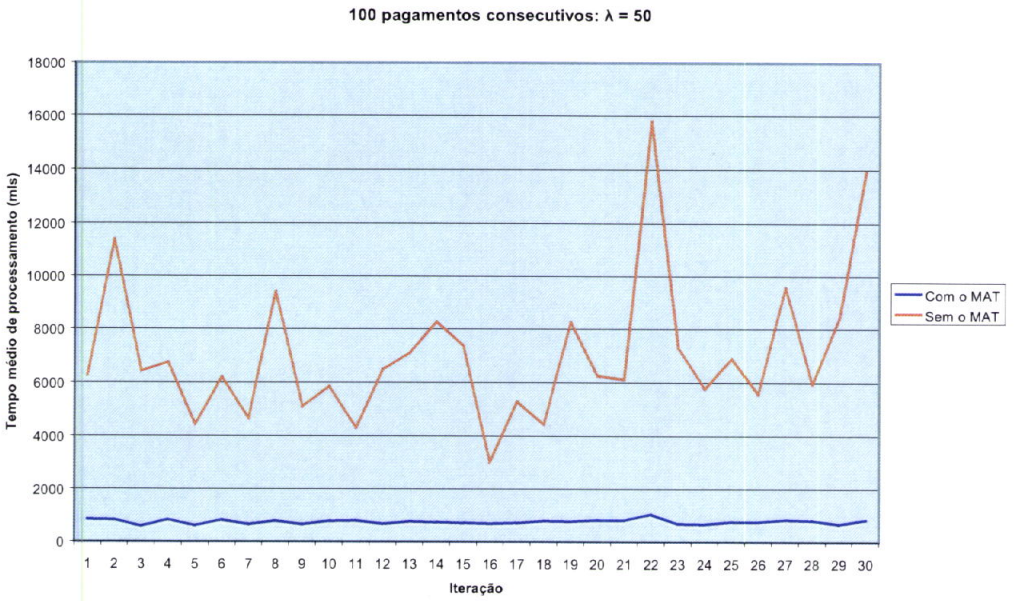


Figura A.7: Gráfico de 100 pagamentos consecutivos com $\lambda = 50$

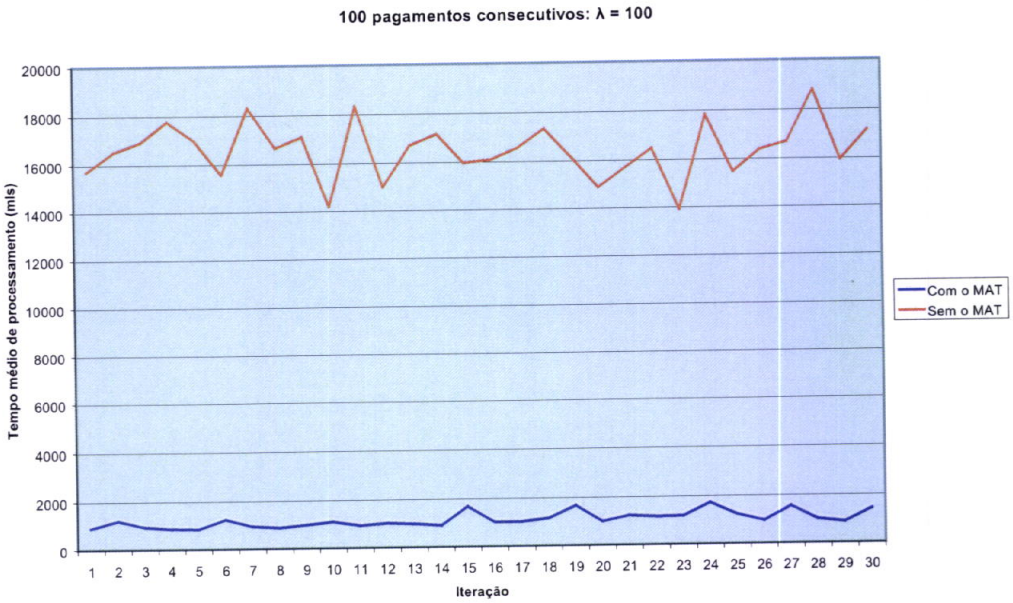


Figura A.8: Gráfico de 100 pagamentos consecutivos com $\lambda = 100$

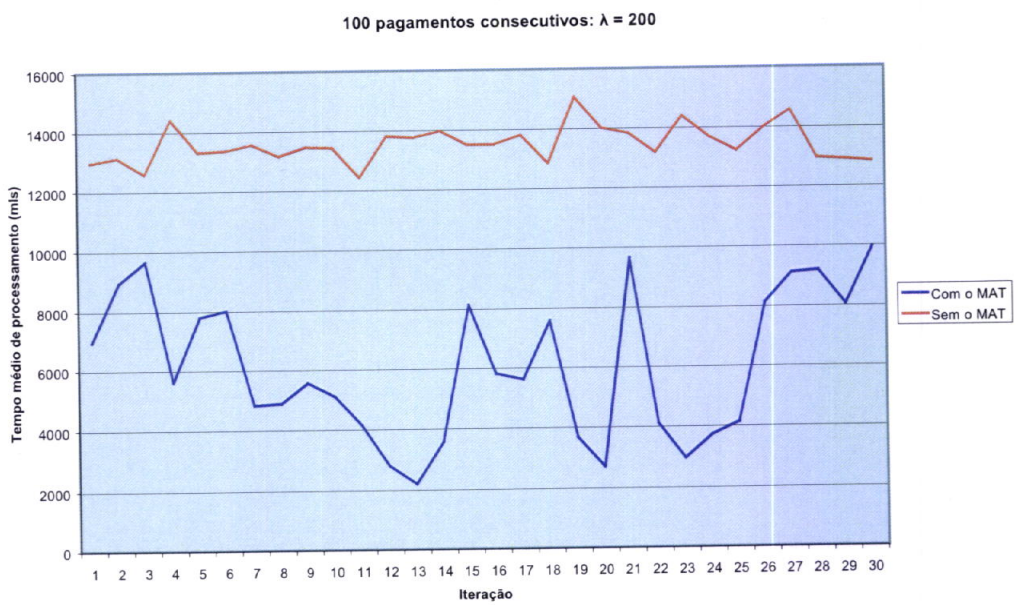


Figura A.9: Gráfico de 100 pagamentos consecutivos com $\lambda = 200$

# Referências


[1] American Express ExpressPay. http://www.americanexpress.com/expresspay.

[2] *Apache Jakarta Tomcat*. http://jakarta.apache.org/tomcat/.

[3] *Bouncy Castle*. http://www.bouncycastle.org/.

[4] Consórcios de Pagamentos Móveis. http://www.mobilepaymentsworld.com.

[5] *Enterprise JavaBeans*. http://java.sun.com/products/ejb/.

[6] ExxonMobil SpeedPass. http://www.speedpass.com.

[7] FirstGate click&pay. http://www.firstgate.com/.

[8] iMode. http://www.nttdocomo.com/corebiz/imode/index.html.

[9] *J2ME Wireless Toolkit*. http://java.sun.com/products/j2mewtoolkit/.

[10] *Java 2 Platform, Enterprise Edition*. http://java.sun.com/j2ee/.

[11] *Java 2 Platform, Micro Edition*. http://java.sun.com/j2me/.

[12] *Java Message Service*. http://java.sun.com/products/jms/.

[13] *Java Server Pages*. http://java.sun.com/products/jsp/.

[14] *Java Servlet*. http://java.sun.com/products/servlet/.

[15] *JBoss Application Server*. http://www.jboss.org/.

[16] Junit. http://www.junit.org.

[17] *JUnitPerf*. http://www.clarkware.com/software/JUnitPerf.html.

[18] MasterCard PayPass. http://www.paypass.com/.

[19] MBNet. http://www.mbnet.pt.

[20] *MySql*. http://www.mysql.com/.

[21] Obstacles Preventing Consumers From Adopting mCommerce. Internet. http://www.epaynews.com/statistics/mcommstats.html#36.

[22] *OpenLDAP*. http://www.openldap.org/.

[23] PepperCoin. http://www.peppercoin.com/.

[24] PepperCoin Tecnology. http://www.peppercoin.com/solution /technology.shtml.

[25] VISA 3D Secure. http://www.visa.com.

[26] PayCircle User Scenarios. Technical report, PayCircle, Fevreiro 2002. http://www.paycircle.org.

[27] David Araújo, Artur Romão, and Eduardo Dias. Um Modelo de Pagamentos Electrónicos para Serviços e Conteúdos Móveis com Garantias Fortes de Acessibilidade. In *Conferência Nacional de Redes de Computadores 2004*, Outubro 2004.

[28] Navneet Bhushan and Venugopal Subbarao. Mobile Commerce: Killer Applications. Technical report, ComFactory.

[29] Miguel Mira da Silva, Alberto Silva, Artur Romão, and Nuno Conde. *Comércio Electrónico na Internet.* Lidel, 2003.

[30] Ee-Peng and Keng Siau. *Advances in Mobile Commerce Technologies.* Idea Group Publishing, 2003.

[31] Mobile Payment Forum. Enabling Secure, Interoperable, and User-friendly Mobile Payments. Internet, Dezembro 2002. Mobile Payment Forum White Paper.

[32] Martin Fowler and Kendall Scott. *UML Distilled - A brief guide to the standard Object Modeling Language.* Addison-Wesley, 2000.

[33] Nick Holland. Mobile payment initiatives: Rethinking the strategy. Technical report, Mercator Advisory Group, Dezembro 2003.

[34] Gunther Horn, Keith M. Martin, and Chris J.Mitchell. Authentication Protocols for Mobile Network Environment Value-added Services. Technical report, IEEE.

[35] Zhi-Yuan Hu, Yao-Wei Liu, Xiao Hu, and Jian-Hua Li. Anonymous Micropayments Authentication (AMA) in Mobile Data Network. *IEEE INFOCOM 2004*, 2004.

[36] Malte Krueger. The Future of M-Payments. Technical report, Institute for Prospective Technological Studies, Agosto 2001.

[37] David McKitterick and Jim Dowling. State of the Art Review of Mobile Payment Technology. Technical report, Trinity College Dublin, 2003.

[38] Brian E. Mennecke and Troy J. Strader. *Mobile Commerce - Technology, Theory and Applications*, chapter 1: NTT DoCoMo's i-mode: Developing Win-Win Relationships for Mobile Commerce. Idea Group Publishing, 2003.

[39] Paul Merry. Mobile Transactions Evolving Models of Payment in the Mobile Content, Commerce and Retail Marketplaces. Technical report, ARC Group, Dezembro 2004.

[40] Elizabeth Millard. The Death of Micropayments? Technical report, E-Commerce Times, Dezembro 2004.

[41] Donal O´Mahony, Michael Peirce, and Hitesh Tewari. *Eletronic Payment Systems*. Artech House, 1997.

[42] OMG. OMG Unified Modeling Language Specification. Specification 1.5, Object Management Group - OMG, Março 2003.

[43] Jan Ondrus. A Tool Kit For A Better Understanding Of The Market. 2000.

[44] Paybox. Mobile payment delivery made simple. Internet, Julho 2004. http://www.paybox.net.

[45] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley and Sons, second edition, 1996.

[46] Seah and Pilakkat. The Future Mobile Payments Infra-structure - A Common Platform for Secure M-Payments. Technical report, Institute for Communications Research, Dezembro 2001.

[47] Alberto Silva and Carlos Videira. *UML Metodologias e Ferramentas CASE*. Centro Atlântico, 2001.

[48] Kim Topley. *J2ME in a Nutshell*. O´Reilly, 2002.

[49] Mobile Electronic Transactions. MeT White Paper on Mobile Transactions. Internet, Janeiro 2003. http://www.mobiletransaction.org.

[50] V.E.Gmurman. *Problemas em probabilidades e estatística.* Editora Mir, 1984.

[51] Vodafone. Vodafone m-pay shopping. Internet, Julho 2004. http://www.vodafone.co.uk.