IPC - Instituto Politécnico de Coimbra

ISEC - Instituto Superior de Engenharia de Coimbra

Departamento de Engenharia Informática e de Sistemas

Mestrado em Informática e Sistemas

Sistema de Pagamentos Eletrónicos

Autor:

Engº Filipe Fernandes Queirós

Orientadores:

Professor Doutor Viriato Marques (ISEC)

Engº Luís Silva (AIRC)

Coimbra, Setembro de 2015

Agradecimentos

De uma forma geral, agradeço a todas as pessoas que diretamente, ou indiretamente, contribuíram para a realização do estágio.

Dirijo o meu sincero reconhecimento e agradecimento à AIRC, através dos seus funcionários e direção que me integraram, apoiaram e sempre esclareceram as minhas dúvidas.

Ao meu orientador do Departamento de Engenharia Informática e Sistemas, Doutor Viriato Marques, pelo apoio prestado.

Por último, agradeço há minha família, amigos e namorada, que merecem sempre um lugar de destaque, pela paciência e pelo apoio ao longo desta fase.

Resumo

A presente dissertação descreve o desenvolvimento de um sistema de pagamentos eletrónicos direcionado para serviços municipais. Este sistema está dividido em três áreas principais: a administração ou *backoffice*, os portais *web* ou *frontend* e as integrações com plataformas de terceiros. Relativamente à administração do sistema foram desenvolvidas funcionalidades em PowerBuilder, com o objetivo de monitorizar, configurar e gerir todos os pagamentos efetuados pelos munícipes. Os portais *web* representam a interface do sistema com o utilizador, foram desenvolvidos em Java, JavaScript, Asp e Html, e disponibilizam todos os serviços prestados pelas câmaras municipais, permitindo a consulta, emissão e pagamento através de balcão de atendimento ou serviços *online*: cartão de crédito, referências multibanco e pagamento presencial são as modalidades de pagamento implementadas. Opcionalmente, é também possível a integração com plataformas de terceiros o que vem aumentar o número de alternativas de pagamento. Estas integrações são realizadas através de serviços *web* prezando sempre a segurança, integridade e confidencialidade dos dados. O sistema de pagamentos eletrónicos veio oferecer aos munícipes uma maior comodidade e rapidez na emissão e liquidação de taxas e licenças, permitiu reduzir os custos de atendimento, a alocação de recursos humanos e realizar a desmaterialização de documentos, contribuindo assim para a modernização da administração pública. Explicam-se também as opções tomadas na implementação do projeto, as tecnologias envolvidas no tipo de pagamentos implementados e a metodologia utilizada para o desenvolvimento. Em termos de segurança foram implementados vários mecanismos com o objetivo de proteger transações e dados. Foram realizados testes de caixa branca, preta e de segurança. O sistema encontra-se na primeira versão, mas já em operação, como parte da aplicação financeira e acessível em portais *web*.

Palavras Chave (Tema): Pagamento Eletrónicos, Pagamentos Online, Referências Multibanco, Cartão de Crédito.

Palavras Chave (Tecnologias): Java, J2EE, ASP, JavaScript, Jquery, HTML, CSS, PowerBuilder, WebServices, Informix, Websphere, faturação.

Abstract

This dissertation describes the development of an electronic payment system directed to municipal services. This system is divided into three main areas: the management or backoffice, web portals or frontend and integrations with third-party platforms. In regard to the system administration area, it was developed using Power Builder, in order to monitor, configure and manage all payment systems made by residents. The web portals represent the system interface for the user, developed in Java, JavaScript, ASP and HTML that offers all the services provided by municipalities, allowing them to be consulted, issued and paid through the service desk or online services: credit card, ATM references and attendance, correspond to the types of payment arrangements implemented. Integrations with third-party platforms are an optional area, which comes to increase the number of payment alternatives. These communications are carried out through web services accomplished through tight security, integrity and confidentiality of the data. The electronic payment system comes to offer citizens greater convenience and speed of issue and settlement fees and licenses, has reduced the attendance costs, allocation of human resources and dematerialization of documents, therefore contributing to the modernization of public administration. The choices made into the project implementation are also explained, as well as the technologies involved in the types of implemented payments and the development methodology. In terms of security various mechanisms have been implemented in order to protect transactions and data. White box, black box and security tests were carried out. The system is in the first version, but already in operation as part of financial and accessible application on web portals.

Keywords (Subject): e-Commerce, References ATM, Credit Card, Online Payments.

Keywords (Technologies): Java, J2EE, ASP, JavaScript, Jquery, HTML, CSS, PowerBuilder, WebServices, Informix, Websphere, invoicing.

Índice

Índice de Figuras

Índice de Tabelas

Acrónimos e abreviaturas

ACEP: Associação do Comércio Eletrónico em Portugal

ADM: Aplicação de Administração

AIRC: Associação de Informática da Região Centro

AMA: Agência de Modernização Administrativa

APIs: Application Programming Interfaces

BPM: Business Process Management

CA: Certified Authority

CSS: Cascading Style Sheets

CVV: Card Verification Value

DR: Diário da República

ERP: Enterprise Resource Planning

GUID: Identificador Único Global

Html: HyperText Markup Language

Http: Hyper Text Transfer Protocol

Https: Hyper Text Transfer Protocol Secure

IBM: International Business Machines

J2EE: Java 2 Platform Enterprise Edition

PPAP: Plataforma de Pagamentos da Administração Pública

PB: PowerBuilder

SIBS: Sociedade Interbancária de Serviços

SGA: Sistema de Gestão Águas

SGD: Sistema de Gestão Documental

SGF: Sistema de Gestão Faturação

SOA: Serviços Orientados Arquitetura

SOAP: Simple Object Access Protocol

SSL: Secure Sockets Layer

TI: Tecnologias da Informação

TIC: Tecnologias de Informação e Comunicação

TPA: Terminal de Pagamento Automático

WCF: Windows Communication Foundation

WSDL: Web Services Description Language

WSE: Web Services Enhancements

XML: eXtensible Markup Language

XSL: Extensible Stylesheet Language

1 Introdução

A evolução tecnológica mundial ocorre a uma velocidade nunca antes vista: as mudanças ocorridas nos últimos dez anos foram enormes quando comparadas com todas as já presenciadas pelo mundo. Neste contexto, o comércio eletrónico ganhou popularidade na última década, levando tanto as pequenas empresas quanto as grandes corporações a investirem neste novo conceito de negócio, que a Internet tornou possível através da conectividade que fornece a todo o mundo. Em virtude das rápidas e importantes transformações no mundo dos negócios, as empresas passaram a utilizar de forma ampla as tecnologias de informação e comunicação, processando um crescente número de transações e atendendo uma maior quantidade de clientes de forma mais rápida, eficaz e segura e, muitas vezes, personalizada (Guedes, R., 2009).

Porém, os sistemas de pagamento eletrónico são intrinsecamente complexos e requerem grandes cuidados no seu desenvolvimento a nível de segurança, integridade e confidencialidade dos dados. Aliado a estes aspetos, a interface com o utilizador deve ser simples e intuitiva, para que este sinta confiança nas ações que executa.

Assim sendo, o projeto descrito na presente dissertação visa colmatar uma necessidade das câmaras municipais que consiste em oferecer aos seus munícipes a possibilidade de poderem emitir documentos e pagar serviços sem necessidade de se deslocarem ao balcão de atendimento do município. O projeto foi dividido em três áreas principais:

- A administração, que corresponde a um módulo integrado na aplicação financeira da AIRC, onde são geridos e consultados todos os pagamentos efetuados pelos munícipes, configuração dos serviços que devem ter pagamentos eletrónicos, configuração dos modelos das faturas, sincronização com plataformas de terceiros e com o ERP da AIRC (nomeadamente a aplicação de gestão documental);
- A área dos portais, que representa a interface de comunicação com os munícipes: esta é dividida em balcão de atendimento (Intranet) e serviços *online* (Internet). Através de um portal o sistema permite configurar formulários para serviços que foram previamente criados na administração, emitir um documento relativo a taxa ou licença, efetuar o pagamento de um serviço, consultar a conta corrente de pagamentos do munícipe, consultar faturas,

consultar o estado de cada serviço e simular o montante a pagar por cada serviço;

- A terceira área refere-se às plataformas de terceiros que têm um papel opcional no sistema. A sua utilização vem aumentar o número de opções para o pagamento.

A implementação deste projeto revela-se fundamental no contexto atual, com vista à elevação do patamar de qualidade dos serviços prestados aos seus clientes, as Câmaras Municipais, dado estas procurarem sistematicamente simplificar, facilitar e modernizar a interação dos seus munícipes com os serviços municipais. Por fim, acompanha a evolução do comércio eletrónico na área da administração pública, garantindo a excelência dos serviços prestados.

1.1 Enquadramento

A presente tese enquadra-se na unidade curricular de Estágio/Projeto do segundo ano do Mestrado de Informática e Sistemas do ramo de Desenvolvimento de *Software* do Instituto Superior de Engenharia de Coimbra (ISEC) do Instituto Politécnico de Coimbra (IPC). O estágio teve a duração aproximada de um ano e foi desenvolvido na empresa AIRC – Associação de Informática da Região Centro -, no departamento de desenvolvimento de *software*.

A AIRC foi fundada em 1982 e encontra-se sedeada em Coimbra tendo como objetivo o desenvolvimento de soluções informáticas e a prestação de serviços de Tecnologias de Informação a trinta municípios da Região Centro do país tendo, no entanto, vindo sucessivamente a alargar o seu domínio de atuação para fora do universo dos seus fundadores e da própria Administração Pública e Local. A AIRC concentra-se na melhoria contínua das suas soluções, aplicando vastos recursos em investigação e desenvolvimento, tornando a inovação um dos objetivos permanentes no desenvolvimento de soluções tecnologicamente avançadas em diversas áreas, designadamente soluções de *e-Government*, ERP´s Autárquicos, Portais Internet e Intranet, Soluções de Mobilidade, *Business Intelligence*, *Enterprise Content Management* e BPM (*Business Process Management*). O projeto enquadra-se nas áreas de ERP Autárquicos, Portais Internet e Intranet, BPM e e-Government.

A opção por este projeto deveu-se ao facto de este tema possibilitar o aprofundamento de conteúdos relacionados com pagamentos, comércio eletrónico e segurança, o que o

torna um tema bastante atual e com um grande espaço de progressão futuro. O foco do trabalho consiste no desenvolvimento de um sistema de pagamentos eletrónicos para a Internet e Intranet dos municípios, tendo como objetivos implementar pagamentos presenciais, com multibanco e cartão de crédito.

1.2 Objetivos

Os objetivos principais deste projeto são (proposta de estágio, anexo E):

- Investigação sobre a área de negócio (pagamentos eletrónicos);
- Definição e controlo dos intervenientes de cada etapa dos pagamentos;
- Implementação da área de administração de pagamentos eletrónicos;
- Implementação de diversos tipos de pagamentos para Internet e Intranet;
- Implementação de processo de pagamento eletrónico genérico para todos os tipos de formulários;
- Definição de *layouts* de alta usabilidade para a realização de pagamentos eletrónicos;
- Implementação da área de conta corrente do munícipe.

1.3 Principais contributos deste trabalho

Os principais contributos deste trabalho são os seguintes:

- Apresentar o planeamento do sistema de pagamentos eletrónicos da AIRC;
- Apresentar uma perspetiva sobre trabalhos realizados na área de comércio eletrónico;
- Descrever os mecanismos de segurança e testes aplicados ao sistema;
- Descrever o trabalho realizado no projeto e implementação do sistema;
- Apresentar uma visão abrangente sobre o seu modo de utilização, na ótica do utilizador e do administrador;
- Apresentar os contributos que o desenvolvimento do sistema trouxera à AIRC e aos seus clientes.

1.4 Organização do relatório

O relatório está organizado em seis capítulos:

- O primeiro capítulo é composto por uma introdução ao projeto, apresentação da AIRC, contextualização do trabalho realizado e a sua motivação;
- O capítulo dois consiste no estado da arte, no qual é apresentada a investigação que foi realizada sobre o estado dos pagamentos eletrónicos em Portugal, na administração pública portuguesa e o grau de utilização dos diferentes tipos de pagamentos eletrónicos em Portugal e no mundo. Apresenta-se também uma visão geral sobre as tecnologias de suporte de segurança utilizadas em processos de pagamento eletrónico;
- O capítulo três consiste no desenho do projeto: aqui vão ser descritas as fases de planeamento, levantamento de requisitos, arquitetura e metodologia de desenvolvimento;
- O capítulo quatro descreve os aspetos de implementação do sistema, os requisitos implementados e alguns casos reais relativos ao sistema de pagamento eletrónico;
- O capítulo cinco apresenta os testes efetuados antes da entrada em produção;
- O capítulo seis apresenta as conclusões, faz um balanço sobre o trabalho desenvolvido e aponta possíveis melhorias futuras.

Incluem-se também alguns anexos com extratos de código e testes realizados.

2 Estado da arte

2.1 O Comércio Eletrónico em Portugal e no Mundo

Em muitos países europeus, as estratégias de conceção e de implementação do conceito de *e-Government* refletem uma perspetiva de reforma e de modernização para todo o sector público. Este conceito é visto como um instrumento facilitador para uma melhor governação, colocando-o no centro da reforma e da modernização da gestão pública, no qual as TI (Tecnologias de Informação) são usadas como uma ferramenta estratégica para a modernização das estruturas organizativas, dos processos, do quadro regulamentar, dos recursos humanos e da própria cultura da administração pública (Baptista, 2005). A (Comissão Europeia, 2003), define *e-Government* como a "*utilização das tecnologias de informação na administração pública combinadas com a realização de um conjunto de mudanças organizativas, com o objetivo de melhorar os serviços públicos e de reforçar a democracia e o apoio às políticas públicas*".

O ambiente empresarial, tanto a nível mundial como nacional, tem passado por profundas mudanças nos últimos anos, as quais têm sido consideradas diretamente relacionadas com as TI. Estas relações englobam desde o surgimento de novas tecnologias, ou novas aplicações - para atender as necessidades do ambiente (comércio eletrónico) -, até ao aparecimento de novas oportunidades empresariais criadas pelas novas tecnologias ou novas formas da sua aplicação. O comércio eletrónico, com as suas aplicações inovadoras e revolucionárias é tido como uma das tendências emergentes com maior poder potencial de inovação nos processos de negócio nos vários setores económicos (Albertin,A., 2000). Contudo, o comércio eletrónico é regido por mecanismos de segurança da mais alta importância, como salientado no artigo *Privacy Protection in Electronic Commerce* (Head e Yuan, 2011). Este artigo aprofunda os conceitos e interações chave para que possa ser desenvolvido um sistema com privacidade e segurança, propondo a implementação teórica de uma plataforma / modelo para a proteção da privacidade em sistemas de comércio eletrónico, aponta meios de proteção de privacidade, violação da privacidade e as responsabilidades de cada pessoa num sistema de comércio eletrónico. A ética é fundamental para todos os engenheiros de software e a construção de um sistema de pagamentos eletrónicos deve ser feita com base em comportamentos éticos. (Leitch,S. e Warren,M., 2011) descrevem comportamentos não éticos que devem ser evitados no âmbito do comércio

eletrónico tais como recolha e divulgação de dados, a sua utilização para efeitos de *marketing* e tecnologias intrusivas.

O respeito pela ética reforça também a confiança dos utilizadores, constituindo assim um pilar muito importante no desenvolvimento de um sistema de pagamentos eletrónicos. A conjugação entre ambiente, personalidade e risco formam o conceito de *confiança* para cada utilizador (Choobineh e Kini, 1998). (Dennis,A., 2001) demonstra que a facilidade de uso, a segurança e a confiança são as características mais importantes para um sistema de pagamentos. Este estudo foi realizado através de inquéritos ao utilizador com uma amostra de 1328 pessoas, das quais 94,1% são utilizadoras de sistemas de pagamentos eletrónicos (Abrazhevich, 2001).

Mais especificamente, em Portugal e nos últimos anos, o *e-commerce* tem assumido um papel de importância crescente no desenvolvimento das empresas, possibilitando-lhes uma maior comunicação global das suas marcas e serviços, ao permitir que os consumidores tenham acesso aos seus produtos, serviços e / ou informação de uma forma rápida, simples, cómoda e eficaz, em qualquer parte do mundo e a qualquer hora (Ferreira, 2014). A modernização administrativa foi considerada como um dos instrumentos essenciais na estratégia de desenvolvimento do País, tendo sido atribuído um particular relevo aos domínios da administração eletrónica (desmaterialização) e da simplificação administrativa, como áreas decisivas para elevar os padrões de competitividade e de qualidade de vida dos cidadãos (DR, 2009, I Série - N.º 192, 2 de Outubro de 2009).

Assim, no âmbito do desenvolvimento da administração eletrónica e da simplificação administrativa foi instituída, em 2007, a Agência de Modernização Administrativa (AMA) como um Instituto Público, integrado na administração indireta do Estado, que tem por missão desenvolver, coordenar e avaliar medidas, programas e projetos nas áreas da modernização e da simplificação administrativa e regulatória, da administração eletrónica e da distribuição de serviços públicos. Na área da administração eletrónica a AMA tem a responsabilidade, para além de outras, de promover a utilização de pagamentos eletrónicos enquanto meio de pagamento de serviços, através da disponibilização de serviços integrados de pagamentos eletrónicos nas plataformas da Administração Pública, permitindo uma articulação mais eficaz com os vários agentes sociais (públicos e privados), potenciando a existência e a interoperabilidade de serviços de partilha e centrando-os cada vez mais nas

necessidades dos cidadãos e das empresas. Criando a Plataforma de Pagamentos da Administração Pública (PPAP) na lógica de serviços partilhados de tecnologias de informação e comunicação (TIC), a PPAP é o sistema que permite aos organismos disponibilizar múltiplos métodos de pagamentos para os diferentes canais de atendimento (sites / portais e balcões de atendimento), despoletados a partir dos seus sistemas operacionais, garantindo a sua gestão, controlo e monitorização integrada. Esta aposta no comércio eletrónico é claramente visível em Portugal, como mostra o relatório da SIBS (SIBS Market Report 2012): embora do total de compras pagas com recurso a cartão bancário apenas 1,2% ssejam referentes a transações realizadas através da Internet, este valor mostra uma evolução notória do *e-Commerce* em Portugal nos últimos cinco anos, dado que estes 1,2% se traduzem em cerca de 8,4 milhões de transações, correspondentes a 678 milhões de euros, quando em 2007 o valor se situava em apenas 0,7%, totalizando apenas cerca de 3,9 milhões de operações. Num relatório que traça o perfil do país nos pagamentos *online*, a SIBS nota ainda que o comércio eletrónico em Portugal apresenta uma percentagem superior à média europeia, com 19% das empresas a declararem ter o seu comércio eletrónico ativo, contra 15% a nível Europeu.

Um estudo da Associação do Comércio Eletrónico em Portugal (ACEP) / Netsonda (Comprar na Internet) revelou que cerca de 78% dos utilizadores da Internet já fizeram compras *online* e compram principalmente produtos informáticos, eletrónicos, bilhetes para desporto e espetáculos. No primeiro trimestre de 2014 os meios de pagamento mais utilizados foram o cartão de crédito e as referências multibanco, como podemos ver pelos gráficos seguintes (figura 1).

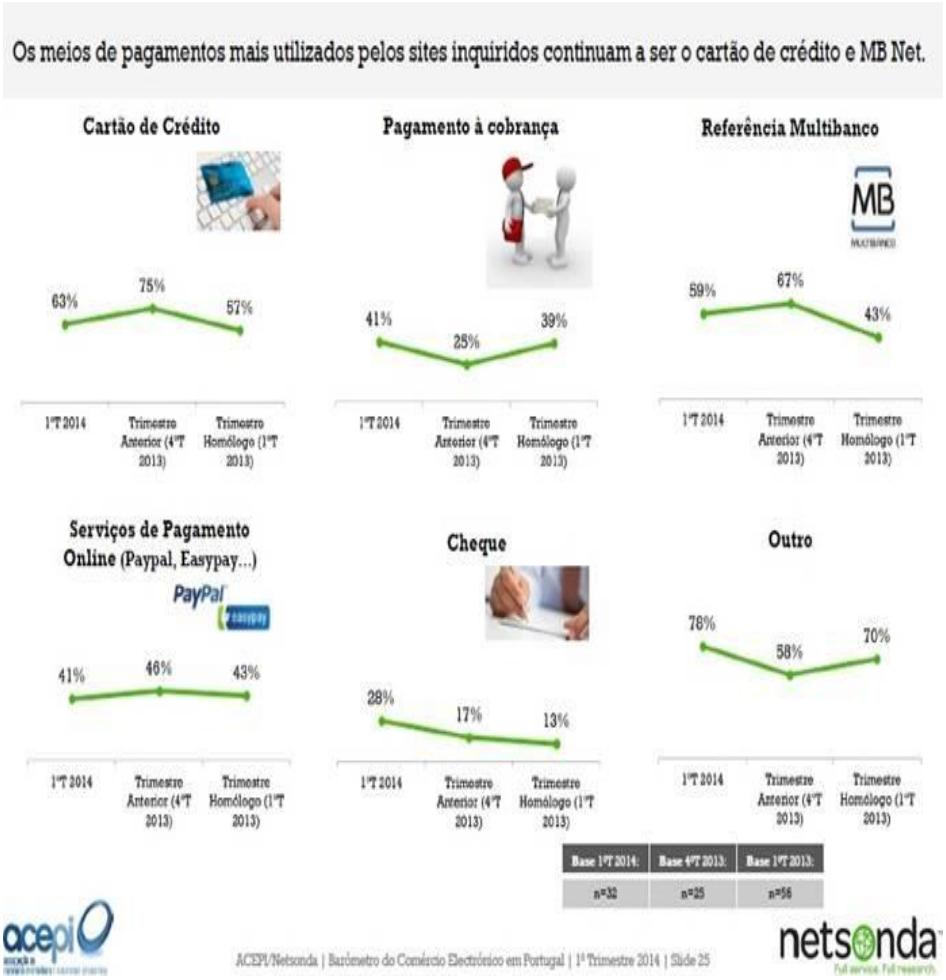


Figura 1- Utilização dos métodos de pagamentos em Portugal [fonte: ACEP / Netsonda, 2012].

As referências multibanco são consideradas como um método de pagamento seguro e de confiança, principalmente junto de cibernautas avessos a revelar os seus dados bancários *online* por receio de uso fraudulento ou risco de exposição. Através deste método, as encomendas pagas são automaticamente processadas e a confirmação do pagamento prontamente enviada às entidades comerciais, minorando os riscos.

Atualmente, um cliente que deseje pagar por referências multibanco tem várias alternativas ao seu dispor: pode pagar através de um terminal Multibanco, Home-Banking, MB Spot, Telemóvel ou TPA, bastando para isso ter apenas os dados disponibilizados pela entidade comercial no momento da sua encomenda. Um estudo da Basef Banca de Marktest, revela que as caixas multibanco são o canal bancário preferido dos Portugueses, seguido do contacto direto e do Home-banking que triplicou o seu crescimento desde 2002, contando em 2011 com 2,2 milhões de utilizadores (Patrícia,C., 2012). Claramente o comércio eletrónico é uma aposta segura para o

futuro. Com o crescimento da Internet são cada vez mais as empresas que vêem esta alternativa como forma de dinamizar o seu negócio. Só no primeiro trimestre de 2014, verificou-se um aumento de 80% do número de pessoas que compra pela Internet (Relatório Basef Banca de Marktest, 2011).

Contudo, as características dos mercados virtuais, que resultam numa redução das barreiras à entrada de novos concorrentes e conduzem a uma hiper-competição, justificam, ainda mais, a necessidade de um posicionamento estratégico. De facto, com a Internet a informação é rapidamente acessível, o que reduz os custos de mudança e obriga as empresas a serem ainda mais criativas para se diferenciarem (Torres,P., 2012).

Atualmente, a evolução do *e-commerce*, em especial no que toca aos pagamentos *online*, não está refletida nos serviços prestados pelos municípios. Por exemplo, um munícipe para pagar uma taxa ou licença emitida tem de se deslocar ao balcão de atendimento da câmara municipal, o que hoje em dia, no contexto acima descrito, requer urgente inovação e evolução. A AIRC, como empresa atenta à evolução do mercado e às necessidades dos seus clientes, aposta nos pagamentos eletrónicos como uma nova área estratégica, contribuindo assim para a modernização dos serviços da administração pública.

2.2 Segurança

2.2.1 Encriptação de dados

A encriptação de dados está diretamente relacionada com a segurança e merece destaque no sistema de pagamentos. A palavra Criptografia vem das palavras gregas que significam escrita secreta (Tanenbaum,A., 2003). É uma técnica utilizada para cifrar uma informação, tornando-a incompreensível, exceto para os destinatários e o transmissor, que sabem como decifrá-las (Kurose,J., 2003) e é necessária em operações com dados bancários ou dados confidenciais dos utilizadores. A criptografia de dados é uma matéria que vem sendo aperfeiçoada desde a Segunda Guerra mundial, exercendo um papel importantíssimo na mesma. O matemático Allan Turing foi o principal elemento da equipa de criptoanalistas que descodificaram as mensagens

trocadas pelos Alemães através da máquina Enigma[1] (Crato,N., 2010). Com a evolução das tecnologias a criptografia também evoluiu deixando para trás as máquinas rudimentares que criptografavam com limitações físicas e de processamento, e evoluindo até às máquinas baseadas em algoritmos complexos com as capacidades de hardware por eles implicadas. Existem fundamentalmente dois tipos diferentes de criptografia: a simétrica e a assimétrica (Fitzgerald,J. e Dennis,A., 2005):

- A criptografia simétrica ou criptografia de chave única, utiliza uma única chave para encriptar e decifrar os dados. A chave é partilhada entre os envolvidos na comunicação, o que torna esse sistema suscetível a falhas de segurança. Caso a chave seja intercetada por agentes externos, as mensagens podem ser lidas e modificadas pelo novo agente da conversa. Não é possível garantir a identidade da pessoa que enviou a mensagem porque a chave pode estar a ser usada por mais pessoas (Jie e Hong, 2010). A principal vantagem da criptografia simétrica é a rapidez na criptografia e decifração das informações, e a necessidade de um menor número de portas lógicas para implementação em hardware (Sarma et al, 2003). Como desvantagem aponta--se o sistema de gestão das chaves, dado que a chave secreta é pública, devendo por isso ser transmitida ao recetor, e tornando-se assim vulnerável a interseção.
- A criptografia assimétrica, conhecida também como criptografia de chave pública (Stallings,W., 1999), veio para resolver o problema de a chave ser partilhada e assim evitar que os agentes externos consigam aceder-lhe. Esta criptografia utiliza duas chaves diferentes, uma pública e outra privada, de modo que é computacionalmente complexo e normalmente impraticável a dedução da chave privada através da chave pública (Schneier,B., 1996). Qualquer pessoa pode cifrar a mensagem com a chave pública, mas não pode decifrá-la com a mesma chave, sendo necessária a chave privada para decifrá-la, que, teoricamente, só a pessoa autorizada, dona da chave pública informada e utilizada para cifrar a mensagem, tem. As duas chaves (pública e privada) detêm uma relação matemática entre elas. Segundo (Schneier,B., 1996) a técnica de criptografia de chave pública pode ser observada na Figura 2. Alice

[1] "Enigma" era o nome de uma máquina de codificação automática de mensagens, utilizadana Segunda Guerra Mundial

deseja enviar uma mensagem de forma segura para Bob; Alice e Bob concordam com um sistema de criptografia de chave pública em comum; Bob envia para a Alice a sua chave pública, podendo enviá-la ou disponibilizá-la por qualquer meio de comunicação, não sendo necessário um meio seguro; Alice cifra a mensagem que ela deseja enviar com a chave pública de Bob e envia a mensagem assim cifrada para Bob; este, ao receber a mensagem de Alice, vai decifrá-la utilizando a sua chave privada e obtém a mensagem original enviada por Alice. O procedimento é seguro porque se aplicarmos a chave pública de Bob sobre o texto criptografado por Alice, não teremos a mensagem original: apenas a chave privada de Bob permite reconstruí-la.

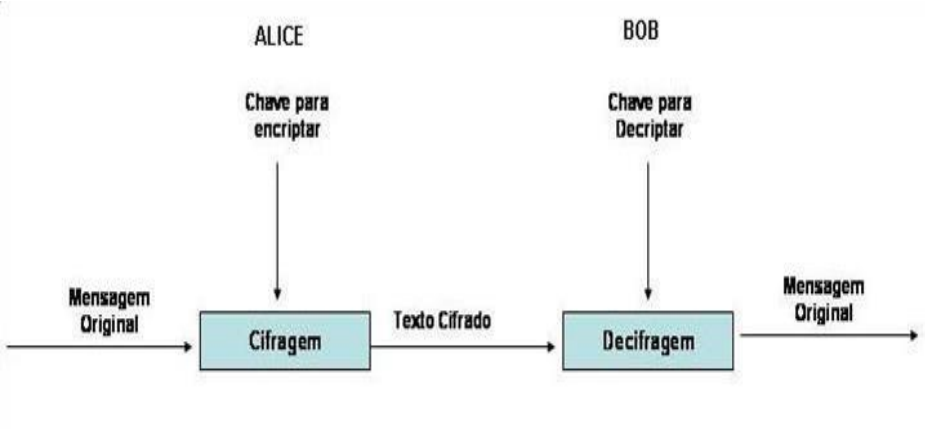


Figura 2 – Criptografia Assimétrica [fonte: Schneier, 1996]

Atualmente o único obstáculo existente para deduzir a chave privada através da chave pública é a capacidade computacional em tempo útil. Ora vejamos, o RSA (sigla derivada dos nomes dos seus autores Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman) baseia-se no facto de que, embora seja fácil encontrar dois números primos de grandes dimensões (ex. 100 dígitos), conseguir fatorizar o produto de tais dois números é considerado computacionalmente complexo (o tempo estimado para o conseguir ronda os milhares de anos). Este algoritmo mostra-se computacionalmente inquebrável com números de tais dimensões, e a sua força é quantificada através do número de bits utilizados para representar tais números. Para um número de 100 dígitos são necessários 330 bits e as implementações atuais superam os 1024 e mesmo os 2048 bits. A discussão prende-se em saber qual é o tamanho seguro para o módulo usado no RSA: de acordo com Christof Paar muitas aplicações utilizam módulos de 1024 bits. Porém, hoje em dia é possível fatorizar números desta magnitude em 10 a 15

> anos e as agências de inteligência podem ser capazes de fazê-lo ainda de forma mais rápida, já que tipicamente empregam as maiores autoridades em criptografia do mundo. Portanto, já é aconselhado utilizar parâmetros de RSA na ordem de 2048 a 4096 bits para garantir maior segurança (Paar,C., 2009).

Os autores (Hu,X. e Ma,L., 2010) descrevem a criptografia híbrida, que integra quatro tipos de tecnologia: a tecnologia de criptografia, síntese digital, autenticação digital e assinatura digital. Os autores apontam que a criptografia híbrida não pode garantir a verdade e integridade dos dados, e que por isso é necessário combinar outros mecanismos de integridade com base na criptografia, ou seja, a utilização de uma função de Hash. É uma função matemática aplicada à encriptação do resumo com a chave privada para criação de um código chamado message digest (Stallings,W., 1999). Dessa forma o receptor pode verificar a assinatura computando o hash da mensagem, decrifando a assinatura com a chave pública do remetente, e comparando o resumo computado com o resumo decrifado. Igualidade entre os resumos confirma que a mensagem não foi modificada, visto que ela foi assinada por o remetente — presumindo que o remetente manteve a chave privada secreta.

2.2.2 Certificação digital

A certificação digital baseia-se na criptografia de chave pública. Tecnicamente, um certificado digital é um conjunto de dados assinado digitalmente pela autoridade certificadora, que têm a função de criar, manter e controlar todos os certificados por elas emitidos, incluindo a invalidação de certificados comprometidos ou expirados (Leavitt,N., 2011). Os certificados digitais são compostos pelas seguintes informações, entre outras: nome e endereço da empresa, chave pública, validade do certificado, nome e endereço da Autoridade Certificadora e política de utilização. As políticas de utilização são as técnicas e procedimentos para que a certificação digital seja legal, cada país têm entidades específicas que emitem certificados com cadeias de certificação legais.

2.2.3 Assinatura digital

A assinatura digital baseia-se num código utilizado para verificar a integridade de uma informação ou mensagem, podendo ser utilizada para verificar a validade do remetente, através de criptografia assimétrica (Fitzgerald,J. e Dennis,A., 2005). No processo de

assinatura digital, com o qual se pretende garantir a autenticidade do remetente, este usa a sua chave privada para assinar a mensagem. Por outro lado, o destinatário usa a chave pública do remetente para confirmar que ela foi enviada por aquela pessoa. Com a assinatura digital pode garantir-se (Stewart et al, 2008):

- Autenticidade: o facto de a assinatura ter sido realizada pela chave privada do remetente e confirmada pela chave pública, garante que foi realmente aquele utilizador que a enviou;
- Integridade: como a assinatura digital usa uma função de Hash, é possível garantir que a mensagem não foi alterada no seu caminho até ao destino;
- Negação do envio: o utilizador não pode negar a autoria daquela mensagem.

2.2.4 SSL

SSL (*Secure Sockets Layer*) é um *standard* para uma tecnologia de segurança, para estabelecer e encriptar a conexão entre o servidor e o cliente. SSL permite que informações sensíveis, como números de cartões de crédito, números de segurança social e credenciais de *login* sejam transmitidas de forma segura. Normalmente, os dados processados entre os navegadores e servidores *web* são enviados em texto simples, tornando-os vulneráveis a espionagem. O SSL é um protocolo de segurança. Os protocolos descrevem como os algoritmos devem ser utilizados, e neste caso o protocolo SSL determina variáveis da criptografia, tanto para a ligação como para os dados a serem transmitidos.

2.2.5 HTTPS

HTTPS (*Hyper Text Transfer Protocol Secure*) é uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS. Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que verifique a autenticidade do servidor e do cliente por meio de certificados digitais, utilizando as tecnologias que foram descritas anteriormente. O protocolo HTTPS é utilizado, em regra, quando se deseja evitar que a informação transmitida entre o cliente e o servidor seja visualizada por terceiros, como por exemplo no caso de pagamentos *online*.

2.2.6 O futuro: criptografia quântica

A segurança das transações bancárias, comércio eletrónico e das mensagens militares assenta em sistemas de criptografia muito seguros. Mas muito seguros não é o mesmo

que absolutamente seguros. A segurança do mais fiável dos sistemas modernos de criptografia, o RSA, baseia-se na dificuldade em encontrar os fatores primos de números muito grandes. Os algoritmos até hoje conhecidos não conseguem fazer essa factorização em tempo útil (explicado na sub secção encriptação de dados – chaves assimétricas), mesmo com recursos aos computadores mais poderosos que existem**.** Com o avanço tecnológico isto poderá vir a ser exequível originando o colapso das transações seguras como as conhecemos atualmente. Por isso, os esforços no presente e futuro estão voltados para a criptografia quântica de modo a construir um sistema que seja completamente inviolável. A criptografia quântica destaca-se face aos outros métodos criptográficos por não necessitar previamente de comunicações de chaves secretas, permitir a deteção de intrusos e ser segura mesmo que o intruso possua tecnologia computacional ilimitada. Assim, esta técnica criptográfica será mais segura que as utilizadas atualmente, pois está baseada em leis da física, enquanto as atuais estão baseadas em funções matemáticas que são secretas somente porque o poder computacional é limitado. A incerteza do mundo quântico dá-nos a certeza que não somos escutados (Crato,N., 2010).

2.3 Pagamentos Eletrónicos

(N. Asokan et al, 2012) investigadores da IBM (*International Business Machines Corporation*) explicam no artigo *Electronic Payment Systems* os conceitos chave para o desenvolvimento de um sistema de pagamentos eletrónicos. Os autores referem todas as características acima descritas e introduzem modelos de arquitetura, segurança, fiabilidade, encriptação de dados e técnicas de pagamento. Classificam os sistemas de pagamentos em dois modelos de arquitetura, os "*Cash-like*" e "*Cheque-like*": o modelo "*Cash-like*" representa um sistema de pagamentos em que o dinheiro é retirado em tempo real da conta do pagador quando este efetua o pagamento; no modelo "*Cheque-like*" a transação referente ao pagamento não é executada em tempo real. Para o desenvolvimento do sistema de pagamentos o artigo enumera três áreas chave; 1) a integridade e autorização; 2) a confidencialidade; 3) a disponibilidade e confiabilidade. A integridade do sistema de pagamentos significa que "nenhum dinheiro é retirado ao utilizador a menos que seja autorizado por ele", existindo várias formas de obter autorização do utilizador. As aconselhadas são: "autorização *out-band*" que corresponde à utilização de canais externos como o correio eletrónico ou telefone; "autorização por palavra-chave", em que todo o processo de trocas de mensagens é

encriptado e autenticado com uma palavra-chave combinada entre ambas as partes; "autorização por assinatura" em que existe uma troca de certificados em que só o dono do certificado privado consegue assinar as mensagens. A autorização é o relacionamento mais importante no sistema de pagamentos, e a utilização de vários mecanismos de autorização em simultâneo é viável e aconselhável de forma a complementarem-se e a melhorarem a segurança global do sistema. A confidencialidade está relacionada com a restrição de dados nas transações, que só devem ser divulgadas aos intervenientes nas mesmas. A disponibilidade e confiabilidade representam a fiabilidade do sistema, as transações devem ser atómicas, existindo dois estados possíveis nomeadamente ocorrerem com sucesso ou canceladas por completo.

Contudo, este artigo apresenta conceitos base e imprescindíveis para a criação de um sistema de pagamentos, mas não refere casos práticos de implementação.

(Hun, P., 2008) Design and Implementation of Secure Electronic Payment System (Client) apresenta padrões de arquiteturas de desenvolvimento a serem utilizados num sistema de pagamentos eletrónicos. A utilização de esquemas visuais e casos práticos (exemplo de implementação de um banco) facilitam a aprendizagem e tornam o seu conteúdo claro e objetivo. Todas as modalidades de pagamentos têm as suas vantagens e desvantagens, e por isso a sua análise e avaliação são uma preocupação constante. Existe a necessidade de perceber as vantagens e desvantagens de modalidades de pagamento como as referências multibanco, os cartões de crédito, paypal, MBNet e outras.

O artigo "Analysis of Security Issues in Electronic Payment Systems" divide as modalidades de pagamentos em quatro categorias: sistema de dinheiro eletrónico, sistemas de cheque eletrónico, sistema de pagamento eletrónico com cartão inteligente e sistema de pagamento de cartão de crédito *online* (Aigbe,P. e Akpojaro,J., 2014). Para cada modalidade são identificados e explicados os mecanismos de fraude, mecanismos de autenticação segura, as vantagens e desvantagens da sua implementação no sistema de pagamentos eletrónicos.

- O sistema de dinheiro eletrónico providencia um meio de pagamento seguro, rápido e de poucos custos para pagamentos na Internet. Estes sistemas são criados por as mais variadas redes (Ex: PayPal, MBNet) e não usam diretamente

o sistema bancário corrente, são adequados para micropagamentos (Au, M., at al, 2011). Estas transações necessitam que o utilizador tenha conta criada nos sistemas que as processam;

- O sistema de cheque eletrónico também denominado eCheque, é um método que permite ao utilizador efetuar compras através de serviços como o PayPal sem ter crédito suficiente na sua conta. Este método é normalmente utilizado quando o utilizador não possui cartão de crédito. A plataforma onde este está a efetuar a compra ou pagamento realiza um pedido à conta bancária do utilizador debitando o valor necessário para o pagamento. A desvantagem deste meio de pagamento é que a transferência do montante em causa, do banco para a conta do serviço de pagamento, não é imediata, porque existe a necessidade de cumprir várias verificações de segurança por parte do banco;
- O sistema de pagamento eletrónico com cartão inteligente é implementado por um cartão com um chip que guarda informação pessoal sobre o utilizador (*smart card*). A utilização do cartão inteligente como instrumento de pagamento tem um poder de processamento que permite ao sistema de cartões inteligentes ser usado para múltiplas funções e/ou aplicações, aumentando a mobilidade e portabilidade dos dados (Batina,L., et al, 2010). A grande desvantagem descrita para este sistema é a perda ou roubo do cartão que leva à perda completa dos dados, o que pode originar uma fraude. Estes cartões utilizam três mecanismos de verificação e autenticação nomeadamente um número de identificação pessoal como o PIN, assinatura digital e impressão digital (Aigbe,P e Akpojaro,J., 2014). Estes mecanismos aumentam o nível de segurança deste sistema de pagamentos;
- O sistema de pagamento por cartão de crédito consiste na utilização de um cartão de crédito para efetuar os pagamentos. Um cartão de crédito está associado a uma conta bancária que tem a possibilidade de emprestar dinheiro ao utilizador, ou seja, os consumidores estão autorizados a adquirir bens ou serviços a crédito. O cartão de crédito é um sinal de confiança, transfere o risco de concessão de crédito do comerciante para o banco emissor do cartão.

3 Desenho do projeto

3.1 Planeamento e Metodologia

O projeto foi desenvolvido / dividido em sete metas principais. Neste contexto, uma meta é um marco temporal em que existe uma apresentação do projeto à equipa e diretor de desenvolvimento. Cada meta tem objetivos previamente traçados. Qualquer atraso, com a consequente não entrega dos requisitos planeados para cada meta, pode comprometer o planeamento geral do projeto. As principais metas definidas foram as seguintes:

1. Análise do problema, do mercado e levantamento de requisitos;
2. Implementação de pagamentos presenciais;
3. Implementação de pagamentos multibanco;
4. Implementação de pagamentos multibanco integrados com a plataforma PPAP;
5. Implementação de pagamentos com cartão de crédito;
6. Testes ao sistema de pagamentos;
7. Entrada em produção da primeira versão (disponibilização aos clientes)

O projeto teve um acompanhamento constante ao longo da sua implementação, dado que foi utilizada uma metodologia ágil para a sua elaboração, denominada SCRUM: através de reuniões diárias (onde são expostos os problemas e o trabalho feito no dia anterior) e de reuniões de *sprint review* (apresentação do trabalho elaborado durante cada *sprint*, que no caso da AIRC tem a duração de um mês) o andamento do projeto foi constantemente controlado e avaliado. Desta forma existiu sempre uma grande capacidade de adaptação à mudança sem causar desvios significativos no planeamento global inicial.

3.1.1 Tipos de pagamento

Inicialmente a AIRC não tinha nenhum sistema de pagamentos eletrónicos *online* e por isso existia a necessidade de perceber quais os métodos de pagamentos que deveriam ser desenvolvidos para uma primeira versão do sistema. Após uma análise inicial, percebeu-se que os necessários meios de pagamento para uma primeira versão da aplicação seriam o presencial, o pagamento multibanco e o pagamento por cartão de crédito. Como se pode constatar através do estado da arte apresentado no capítulo 2, estes tipos de pagamentos são aqueles em que os portugueses mais confiam e que mais utilizam. Os pagamentos presenciais estão inseridos no sistema com o objetivo de

manter a compatibilidade com os pagamentos presenciais existentes nas aplicações da AIRC, ou seja, manter um único sistema de pagamentos e para isso acontecer é necessário englobar a opção de atendimento presencial no sistema de pagamentos eletrónicos. O tipo de pagamento presencial é o meio mais utilizado em Portugal. Neste sistema o utilizador encontra-se fisicamente no local de pagamento, existindo assim um atendimento personalizado e de confiança. As desvantagens são a necessidade de deslocamento, e a frequente necessidade de espera para ser atendido. Como forma de colmatar estas problemas oferecendo ao cliente várias opções, decidiu implementar-se também o pagamento por referências multibanco e cartões de crédito.

O pagamento através de referências multibanco[2] tem várias vantagens para os utilizadores de comércio eletrónico, nomeadamente:

- Pagamento fácil e simples;
- Método de pagamento seguro e de confiança, com que o utilizador está familiarizado;
- O pagamento pode ser realizado em qualquer terminal Multibanco, telemóvel ou terminal de pagamento automático (TPA), Home-Banking[3] ou MB Spot[4];
- O pagamento pode ser realizado 24 horas por dia;
- O pagamento é efetuado diretamente a partir da conta bancária do utilizador;
- O vendedor recebe notificações dos pagamentos, em tempo real;
- Os dados do utilizador estão protegidos e não há necessidade de introduzir dados bancários *online*;
- Os custos para o vendedor não sofrem alterações, independentemente da escolha do canal / forma de pagamento;
- Os prazos de pagamento são mais reduzidos e as cobranças mais eficazes, com menos custos e burocracia associada;
- O *check out* nas lojas *online* é processado no site do vendedor, sem necessidade de recorrer a outros sites.

[2] Uma referência multibanco consiste numa cadeia de números até nove dígitos que é emitida por a entidade responsável pelo serviço.
[3] Home-Banking é o acto de realizar operações bancárias através da Internet, podendo recorrer ao site do seu banco.
[4] MB Spot é um serviço que permite a realização de operações como o carregamento do telemóvel ou o pagamento de facturas através de terminais de pagamento automático e as lojas que as admitem encontram-se identificadas com o símbolo do serviço.

Todas estas vantagens têm contribuído para a confiança e a crescente utilização das referências multibanco como meio de pagamento *online*. O método de pagamento por referência multibanco é bastante simples, o utilizador ao comprar um produto é atribuida uma referencia multibanco com o montante a pagar. Em seguida, o utilizador deve aceder a um terminal multibanco ou através de outros serviços como o Home-Banking, aceder à área de pagamento por referências e digitar a referência e o montante a pagar.

O pagamento por cartão de crédito complementa a opção de pagamento por referências multibanco, oferecendo o mesmo tipo de vantagens que este último, com exceção para a forma de efetuar o pagamento que neste caso é processado imediatamente no site ou portal do vendedor. Além disso, o pagamento por cartão de crédito oferece a possibilidade de pagar recorrendo a crédito bancário.

A integração com a plataforma desenvolvida pela AMA e denominada por PPAP, é outra opção que a AIRC pretende incluir no seu sistema de pagamentos, na vertente de integrações com aplicações de terceiros. Esta integração afeta o tipo de pagamento por multibanco, porque determina as referências multibanco geradas, bem como o registo dos pagamentos efetuados, que passarão aser exclusivamente da responsabilidade da PPAP: esta comunicará todas as transações ao sistema da AIRC, de forma a manter sempre a integridade e a atualização dos dados em tempo real. Esta opção de pagamentos será vantajosa para clientes que já possuam contratos com a AMA e assim será possível rentabilizar esses contratos através dos portais ou serviços disponibilizados pela AIRC.

3.2 Análise de requisitos

O levantamento de grande parte dos requisitos foi feito na fase inicial do projeto através de várias reuniões com a participação do coordenador do projeto, um elemento da equipa do Sistema de Gestão de Faturação (SGF) e o elemento responsável pelo desenvolvimento do projeto. Estas reuniões foram realizadas com o objetivo de discutir e analisar as necessidades dos clientes na área de pagamentos eletrónicos e posteriormente fazer o levantamento dos requisitos a serem implementados.

Devido ao facto de o projeto estar a ser desenvolvido através de uma metodologia de desenvolvimento ágil, houve a necessidade de alterar ou até mesmo acrescentar requisitos ao projeto durante o seu desenvolvimento. Não foi elaborado documento de

levantamentos de requisitos, mas foram registados e descritos através da plataforma de gestão e controlo de projetos Jazz[5]. Uma das vantagens da utilização de metodologias ágeis é simplificar as fases de desenvolvimento de software e o controlo do cumprimento de requisitos ao longo da evolução do projeto. Cada requisito funcional representa uma história na plataforma Jazz, que é descrita através do seu valor para o negócio e critérios de aceitação, ou seja cada história é analisada e verificada se acrescenta funcionalidade ou valor para o cliente. Todas as histórias são compostas por tarefas e defeitos, e uma história só está implementada após a realização de todas as tarefas a ela associadas e dos respetivos testes, quando efetuados com sucesso.

Enumeram-se em seguida todos os requisitos funcionais e não funcionais que foram identificados. Todos estes requisitos estão registados na plataforma de gestão e controlo de equipas / projetos, o Jazz.

3.2.1 Requisitos funcionais

O sistema de pagamentos deve:

- Permitir simular o valor de uma taxa / licença;
- Permitir configurar o tipo de serviço para cada formulário;
- Permitir configurar os tipos de pagamentos ativos (multibanco e cartão de crédito);
- Permitir configurar a ligação com a PPAP;
- Permitir submeter tipos de formulários genéricos com pagamentos;
- Permitir submeter tipos de formulários de urbanismo com pagamentos;
- Permitir submeter tipos de formulários do sistema de gestão de águas (SGA) com pagamentos;
- Registar cada transação no sistema de gestão documental (SGD);
- Permitir configurar ficheiros de linguagem para os diferentes tipos de pagamentos;
- Permitir emitir formulários de taxas / licenças com modalidade de pagamento presencial na Intranet;

[5] Jazz é uma ferramenta da IBM, que está optimizada para a colaboração, gestão e controlo dos ciclos de projetos.

- Permitir emitir formulários de taxas / licenças com modalidade de pagamento presencial nos serviços *online*;
- Permitir emitir formulários de taxas / licenças com modalidade de pagamento multibanco na Intranet;
- Permitir emitir formulários de taxas / licenças com modalidade de pagamento multibanco nos serviços *online*;
- Permitir emitir formulários de taxas / licenças com modalidade de pagamento cartão de crédito nos serviços *online*;
- Permitir ser ativado ou desativado;
- Permitir pagamentos por referências multibanco;
- Permitir pagamentos por referências multibanco integradas com a PPAP;
- Permitir visualizar a fatura de pagamento de uma taxa / licença emitida;
- Permitir consultar o tipo de pagamento de uma taxa / licença emitida;
- Permitir consultar o estado de uma taxa / licença emitida;
- Dar a opção de receber notificações por correio eletrónico, após efetuar o pagamento por cartão de crédito;
- Dar a opção de receber notificações por telefone, após efetuar o pagamento por cartão de crédito;
- Permitir anular o processo de pagamento por cartão de crédito;

3.2.2 Requisitos não funcionais

O sistema de pagamentos deve:

- Ser simples e intuitivo de utilizar;
- Deve ser seguro;
- Deve ser robusto;
- Deve manter o utilizador informado em todas as fases de pagamento;
- Deve ter uma área de configuração para administradores;
- Deve ser extensível aos vários tipos de formulários (licenças / taxas) disponibilizados pela AIRC;

3.3 Arquitetura

Para garantir todos estes requisitos e manter a compatibilidade com o Enterprise Resource Planning[6] (ERP) da AIRC, foi implementada a arquitetura apresentada nas figuras 3, 4 e 5.

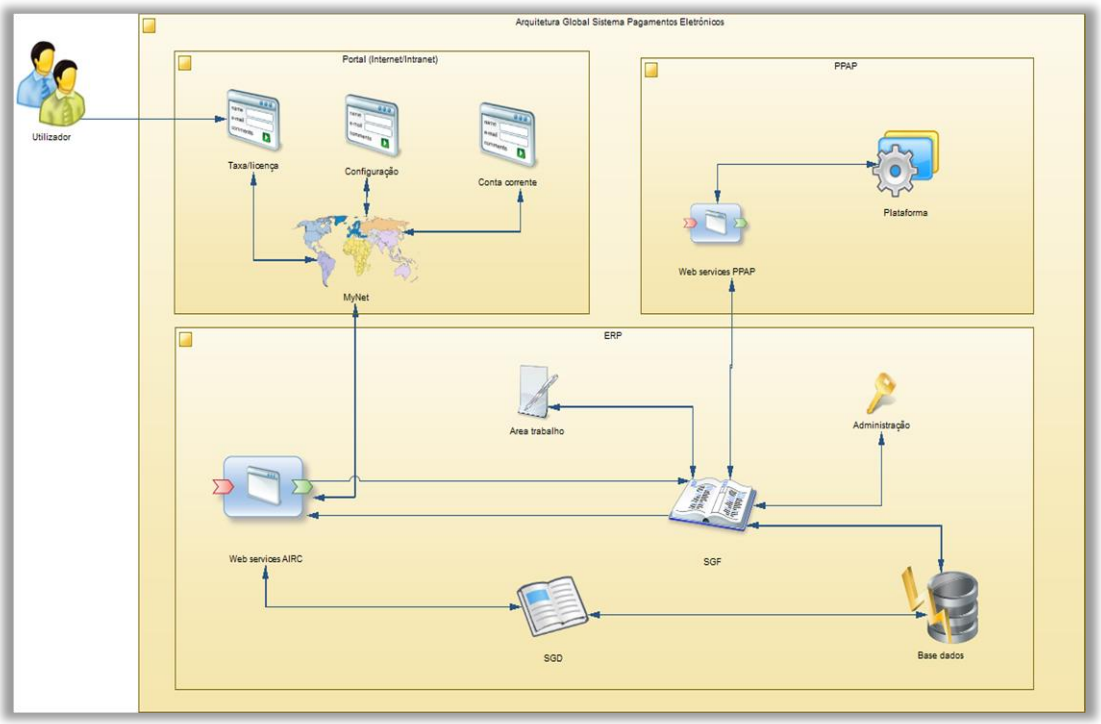


Figura 3 - Arquitetura do sistema de pagamentos eletrónicos

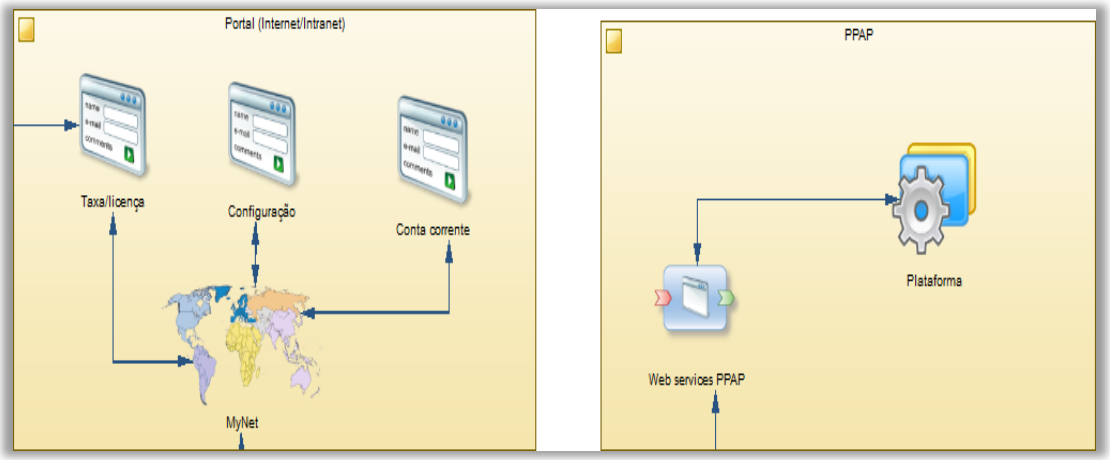


Figura 4 - Arquitetura dos sub-sistemas do MyNet e da PPAP

[6] Um ERP é um sistema de gestão empresarial. No caso da AIRC é um sistema que engloba toda a comunicação e interação entre as várias aplicações esetores municipais.

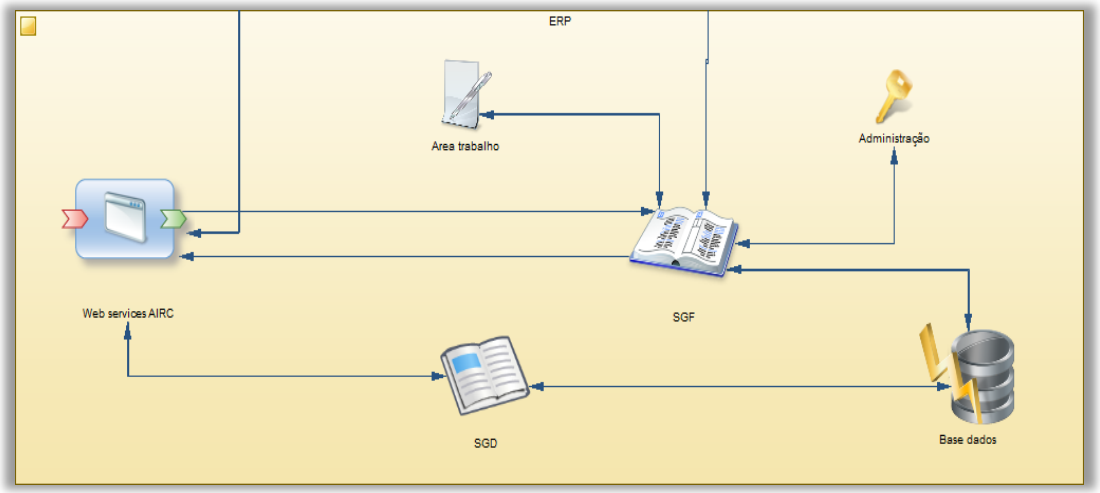


Figura 5 - Arquitetura do sub-sistema do ERP

Estas figuras são um esquema de alto nível da arquitetura implementada para o sistema de pagamentos eletrónicos. Para representação em detalhe, esta estrutura foi dividido em três áreas, sendo elas a

1. Área de portais *web* (MyNet) que funciona como a ponte de comunicação com o munícipe. O MyNet é um sistema desenvolvido pela AIRC, como uma solução de atendimento e relacionamento com o cidadão, onde se centralizam todas as capacidades de prestação de serviço, independentemente do canal de atendimento (presencial, telefónico, correio tradicional e eletrónico, e Internet), garantindo, em simultâneo, a integração de ferramentas de trabalho, e a organização e a partilha do conhecimento dentro de um Município. Na Figura 6 está representada a estrutura geral do sistema MyNet, repartida, essencialmente, por três partes:

   Intranet. Uma solução de Intranet, de exploração reservada aos colaboradores do município, que permite, em simultâneo, a difusão de informação, a partilha de conhecimento, e o acesso às soluções e ferramentas de gestão e de colaboração do Município;

   Balcão Único de Atendimento. É uma solução de atendimento e de gestão do relacionamento com os munícipes, que combina integração, automação e capacidade de monitorização e acompanhamento de qualquer pedido ou interação, garantindo eficiência nas respostas e redução dos custos de atendimento;

Serviços Online. Plataforma de serviços *online* (Internet) que disponibiliza aplicações, funcionalidades e conteúdos orientados para a interação com os munícipes, via Internet e complementando as capacidades do Balcão Único de Atendimento;

Figura 6 - Possíveis combinações no sistema MyNet

Através do MyNet o atendedor da câmara Municipal configura os formulários de forma a possibilitar pagamentos eletrónicos. Cada formulário criado pretende representar um serviço que a câmara oferece aos seus munícipes, podendo este conter pagamentos eletrónicos. Existe ainda a opção de o munícipe consultar todas a emissões de pagamentos que realizou, através da sua conta corrente de taxas ou pagamentos. As opções de pagamentos vão ser diferentes caso o utilizador aceda através dos serviços *online* ou do balcão de atendimento. Na área do MyNet, o desenvolvimento do sistema de pagamentos eletrónicos permitiu a evolução e maturação de conhecimentos em áreas como *Java 2 Platform Enterprise Edition*[7] (J2EE), *HyperText Markup Language*[8]

[7] J2EE é uma plataforma independente com ambiente de desenvolvimento Java, que contém um conjunto de serviços, APIs e protocolos que possibilita desenvolver aplicações web.
[8] HTML é uma linguagem de marcação utilizada para produzir páginas na Web. Documentos HTML podem ser interpretados por os browsers.

(Html), *Cascading Style Sheets*[9] (CSS), *Javascript*[10], *jQuery*[11], *Extensible Stylesheet Language*[12] (XSL), *eXtensible Markup Language*[13] (XML) e *Web Services*[14].;

2. A área do ERP, em que tudo o que é processado no MyNet é enviado através de W*eb Services* para as diferentes aplicações do ERP. No caso do sistema de pagamentos eletrónicos vamos interagir diretamente com o SGD e o SGF: o SGD **(Sistema de Gestão Documental)** é a aplicação que controla toda a gestão documental de um Município e o SGF **(Sistema de Gestão de Faturação)** é a aplicação que controla a faturação de um Município. A aplicação SGF é responsável pelo *backoffice* dos pagamentos eletrónicos, e aqui se concentra a lógica administrativa dos pagamentos eletrónicos. O desenvolvimento desta área de negócio permitiu adquirir conhecimentos em *PowerBuilder*[15] (PB), *Informix*[16], faturação e segurança;
3. Por último, a área PPAP (Plataforma Pagamentos da Administração Pública) que consiste na integração do sistema de pagamentos desenvolvido na AIRC com a plataforma da AMA. Esta integração é feita através de *Web Services*, sendo opcional no sistema de pagamentos eletrónicos.

[9] CSS é uma linguagem de folhas de estilo utilizada para definir a apresentação de documentos escritos em uma linguagem de marcação, como HTML ou XML. Seu principal benefício é proporcionar a separação entre o formato e o conteúdo de um documento.
[10] JavaScript é uma linguagem de script, é a principal linguagem para programação do lado cliente em aplicações web.
[11] jQuery é uma libraria de Javascript. É uma API compatível com todos os browsers, que torna a manipulção de documentos HTML, animações, eventos e Ajax muito simples de usar.
[12] XSL é usado para tranformar XML em documentos HTML que podem ser interpretados nos browsers.
[13] XML é uma definição W3C que define um conjunto de regras para codificação de documentos em formato de leitura humano e maquina.
[14] Web service é uma solução utilizada na integração de sistemas e na comunicação entre aplicações diferentes.
[15] O PowerBuilder é uma linguagem de programação orientada a objetos, mas que disponibiliza recursos bastante variados, permitindo que o programador utilize desde técnicas avançadas de programação, como orientação a objetos, até formas mais simples como programação estruturada e orientação a eventos.
[16] Informix é um sistema de bases de dados relacionais da Internacional Business Machines (IBM).

4 Implementação

Esta secção descreve os diversos aspetos da implementação do sistema de pagamentos eletrónicos. O sistema de pagamentos eletrónicos é utilizado por três tipos de personas, nomeadamente:

- **Administrador**: representa o funcionário que trabalha na aplicação SGF, esta configura os serviços e faturas que ficam disponíveis para o MyNet. Controla e gere todos os pagamentos emitidos e liquidados na câmara municipal;
- **Atendedor**: representa o funcionário que trabalha no balcão de atendimento (MyNet), este tem a tarefa de construir formulários para os serviços configurados na administração de forma a disponibilizar ao munícipe esses serviços com pagamentos eletrónicos;
- **Munícipe**: representa o utilizador que usufrui dos serviços disponibilizados pelo município. Emite e paga taxas / licenças através do balcão de atendimento ou serviços *online*.

4.1 Configurações do sistema

4.1.1 Administração do sistema

A configuração do sistema de pagamentos é uma tarefa administrativa que foi implementada através de um formulário desenvolvido em PowerBuilder. Tem por objetivo guardar na base de dados os tipos de pagamentos que determinado cliente pretende ativar, e os parâmetros de comunicação com a PPAP (figura 7). Estes parâmetros são utilizados na lógica de negócio implementada na aplicação SGF.

Do formulário constam os seguintes campos:

- **Serviço emissor.** As câmaras Municipais são representadas por estruturas orgânicas ou departamentos, pelo que este campo apresenta os serviços emissores existentes em cada câmara Municipal. A submissão de uma taxa / licença através do MyNet fica associada ao serviço emissor selecionado neste campo. Para este tipo de submissões aconselha-se a criação de um serviço emissor "virtual" (não faz parte da estrutura orgânica) denominado por "Serviços Online". Este serviço virtual serve para identificar os pagamentos que são processados através dos serviços *online*;

- **Posto Emissor:** Para cada serviço emissor existem funcionários associados. O campo do posto emissor representa o funcionário que vai estar associado ao registo de pagamentos através do MyNet;
- **PAP Ativo:** Indica se a integração com a plataforma da AMA vai estar ativa ou não;

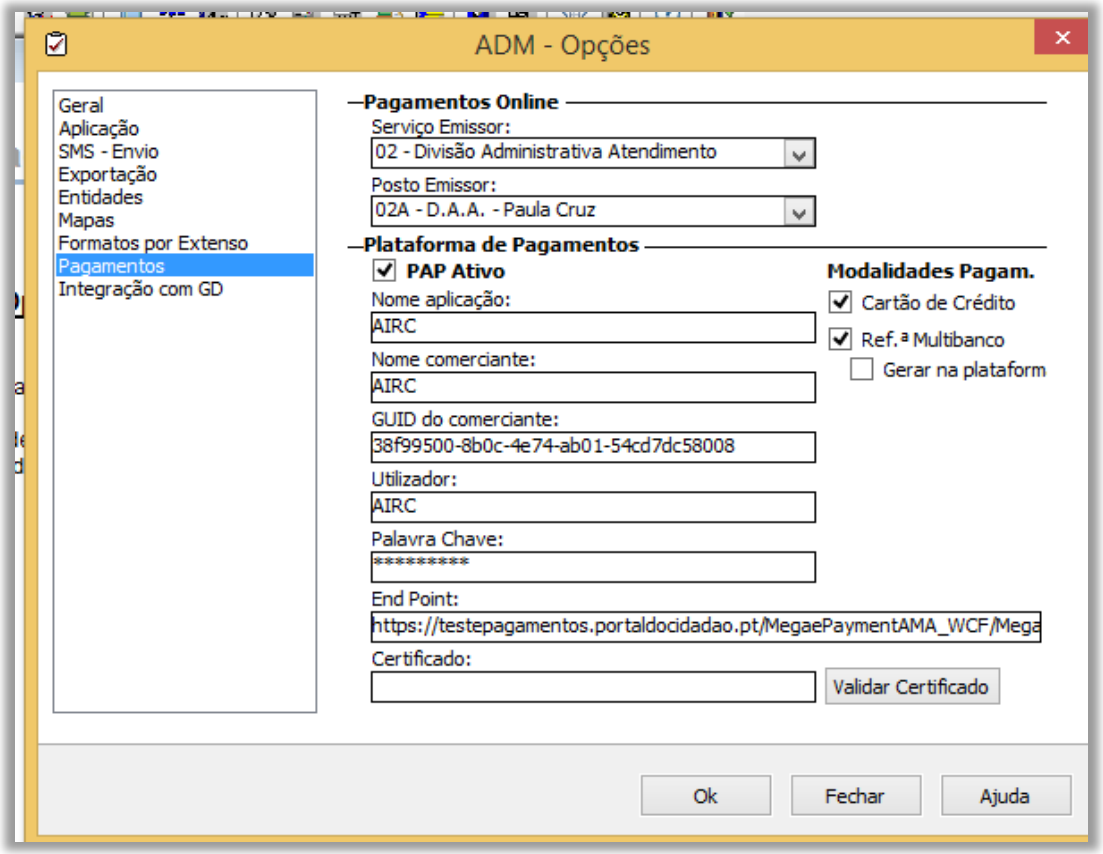


Figura 7 – Janela de configuração na administração do sistema de pagamentos

- **Nome aplicação:** regista o nome da aplicação que vai comunicar com a PPAP;
- **Nome comerciante:** regista o nome da entidade / empresa que vai comunicar com a PPAP;
- **GUID do comerciante.** Campo que regista o Identificador Único Global[17] (GUID) da entidade / empresa que vai comunicar com a PPAP.
- **Utilizador:** regista a identificação do utilizador que comunica com a PPAP. Este utilizador tem de ser comunicado à AMA;

[17] GUID é um tipo especial de identificador utilizado em aplicações de software para oferecer um número de referência que será único em qualquer contexto.

- **Palavra-chave:** representa a palavra-chave do utilizador acordado com a AMA;
- **Endpoint:** regista a *Web Services Description Language*[18] (WSDL) de comunicação com os serviços da PPAP;
- **Certificado:** verifica a validade do certificado que é usado para assinar as mensagens de comunicação com a PPAP. Para isso o certificado tem de estar instalado no servidor;
- **Modalidade de pagamento:** este campo oferece a possibilidade de desativar ou ativar os diferentes tipos de modalidades de pagamentos. A seleção da *checkbox* "cartão de crédito" ativa os pagamentos com cartão de crédito. A seleção da *checkbox* "referências multibanco" ativa os pagamentos com referências multibanco. Caso seja selecionada a *checkbox* "gerar na plataforma" e a *checkbox* "referências multibanco", fica ativa a geração de referências multibanco através da PPAP.

4.1.2 MyNet e SGF

No MyNet existem configurações que devem ser efetuadas para o correto funcionamento do sistema. Quando um funcionário cria formulários para serem disponibilizados aos munícipes deve ter em conta se quer incorporar pagamentos eletrónicos na submissão do formulário. Cada formulário representa um serviço disponibilizado pela câmara municipal. Caso o serviço seja faturado através do editor de formulários o atendedor (área no MyNet que permite aos funcionários criarem formulários, representado na figura 8) adiciona um novo campo ao formulário, chamado de "Formulário de Pagamentos Eletrónicos" (figura 9). Este campo é considerado um campo complexo e inovador no MyNet: inicialmente o editor de formulários estava programado para inserir vários tipos de campos mas sempre em formato individual. Isto quer dizer que um funcionário, para criar um formulário com pagamentos eletrónicos, tinha de colocar cinco campos individuais com nomes específicos. Isto tornava-se impraticável para o funcionário e para o sistema, porque se os nomes dos campos não fossem colocados corretamente ocorriam falhas no sistema de pagamentos. Para solucionar este problema foi criado o chamado campo complexo: esta inovação permite ao funcionário adicionar simplesmente um campo ao formulário,

[18] WSDL é o formato XML para definir ou descreber um conjunto de serviços de rede.

mas este campo tem programado todo o ambiente de pagamentos eletrónicos no MyNet retirando assim complexidade de configurações e lógica do lado do funcionário.

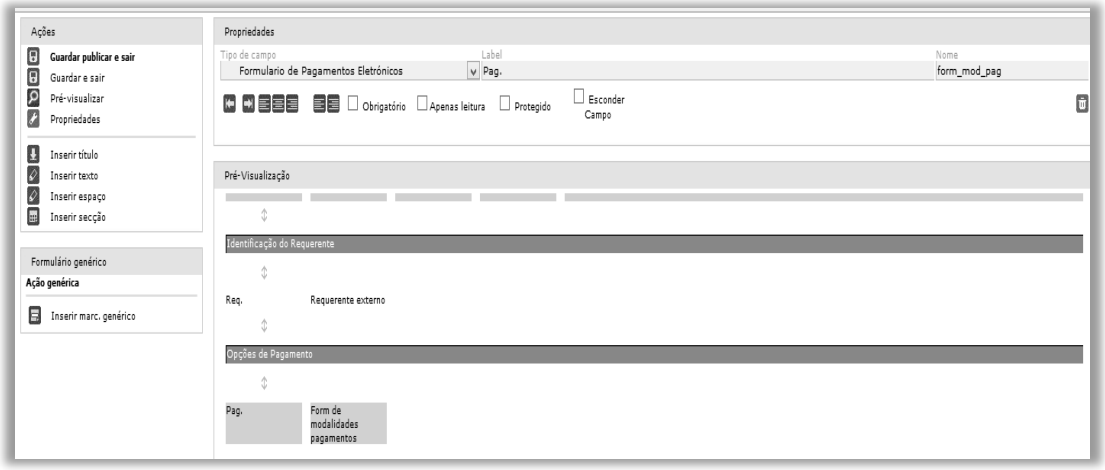


Figura 8 – Exemplo de criação de um formulário no editor de formulários

Figura 9 – Tipo de campo do formulário de pagamentos eletrónicos

Após o campo de pagamentos eletrónicos estar inserido no formulário, o funcionário deve aceder ao configurador de registo do formulário e configurar o tipo de taxa / licença que pretende associar ao formulário. O configurador de registo (figura 10) é uma área no MyNet que permite ao funcionário escolher a área onde quer registar aquele formulário na gestão documental e tipo de serviço de pagamento associado, entre outras opções.

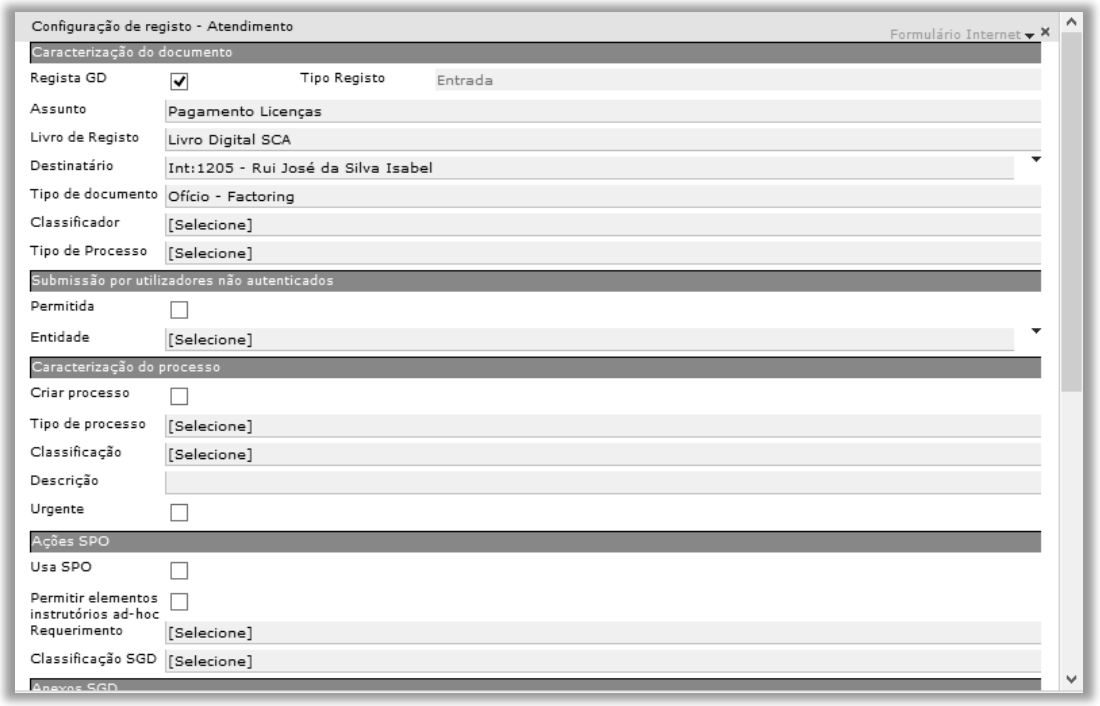


Figura 10 – Exemplo do configurador de registo de um formulário

Para associar o formulário a um tipo de serviço, basta aceder ao separador de pagamentos no configurador de registo e selecionar o campo de integração com os pagamentos e o tipo de serviço associado, como podemos ver na figura 11.

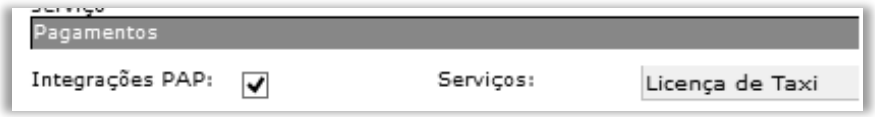


Figura 11 – Opção de configuração dos pagamentos em um formulário no Mynet

Os serviços que existem no Município devem ser previamente criados e configurados na aplicação SGF através da janela de "Tipos de documentos", como podemos ver na figura 12. Caso os serviços sejam configurados para serem utilizados no MyNet a *dropdown* de serviços (figura 11) vai listá-los. Assim o funcionário só tem de escolher o serviço de pagamento que quer associar ao formulário.

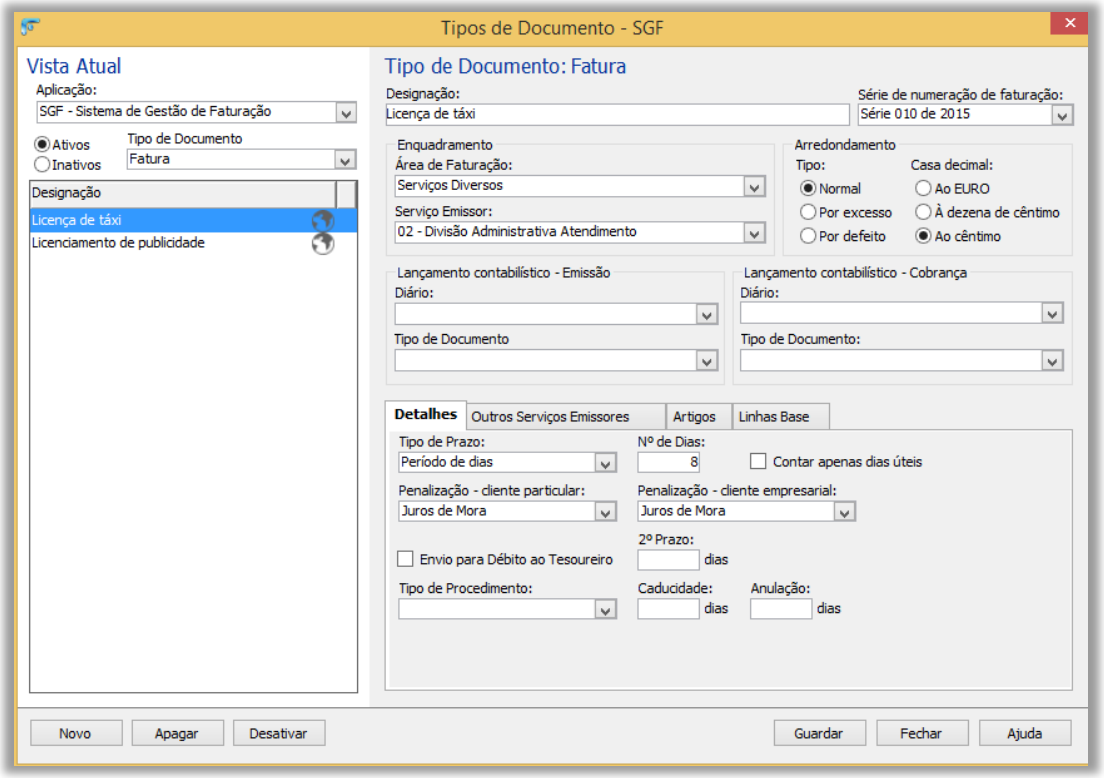


Figura 12 – Exemplo da janela de criação / configuração de um serviço no SGF

Para associar o tipo de documento criado aos serviços disponíveis do MyNet, o funcionário tem de aceder no SGF à janela de configuração dos serviços para os Serviços Online (figura 13). Essa janela disponibiliza uma área que permite ao funcionário criar um serviço para o MyNet e associá-lo ao tipo de documento criado anteriormente (figura 14).

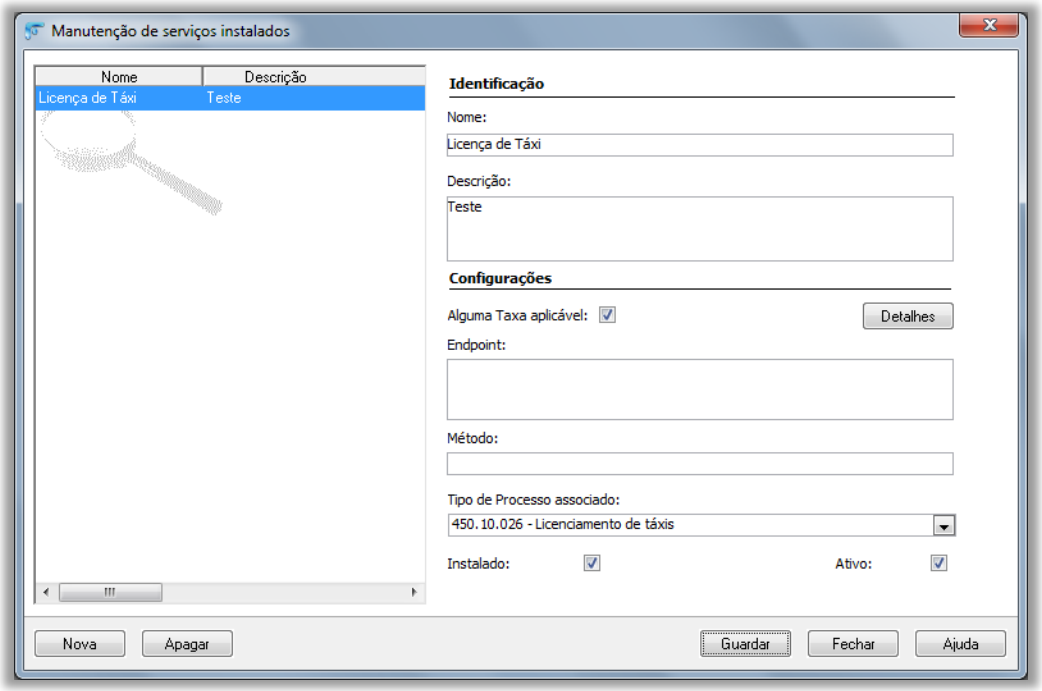


Figura 13 – Janela de criação de serviço disponível para o MyNet

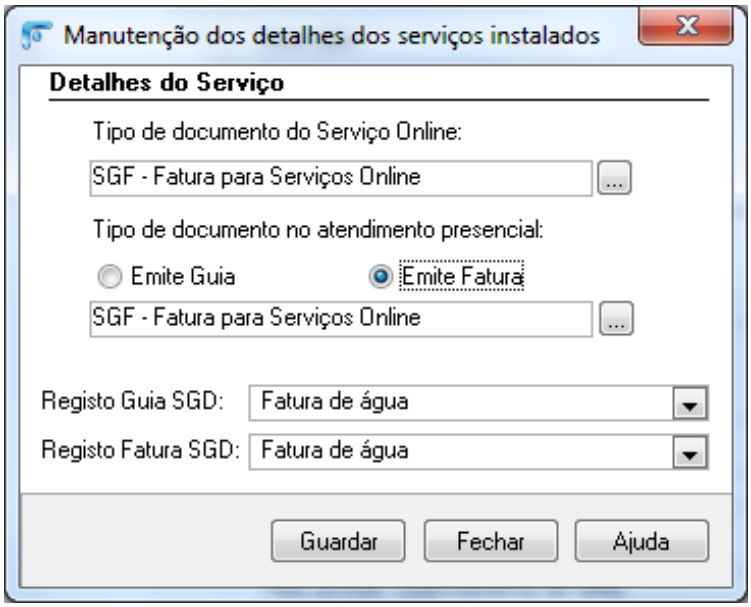


Figura 14 – Janela de detalhes que permite associar um tipo de documento ao serviço a ser criado

Após a realização das configurações, o sistema de pagamentos eletrónicos está pronto a ser utilizado por os munícipes.

Nota: As configurações do lado do ERP ou aplicações da AIRC necessitam de ser realizadas uma vez por serviço. As configurações do lado MyNet devem ser realizadas

sempre que o funcionário cria um novo formulário com o objetivo de disponibilizar pagamentos eletrónicos.

4.2 Pagamentos presenciais

4.2.1 Diagrama de sequência

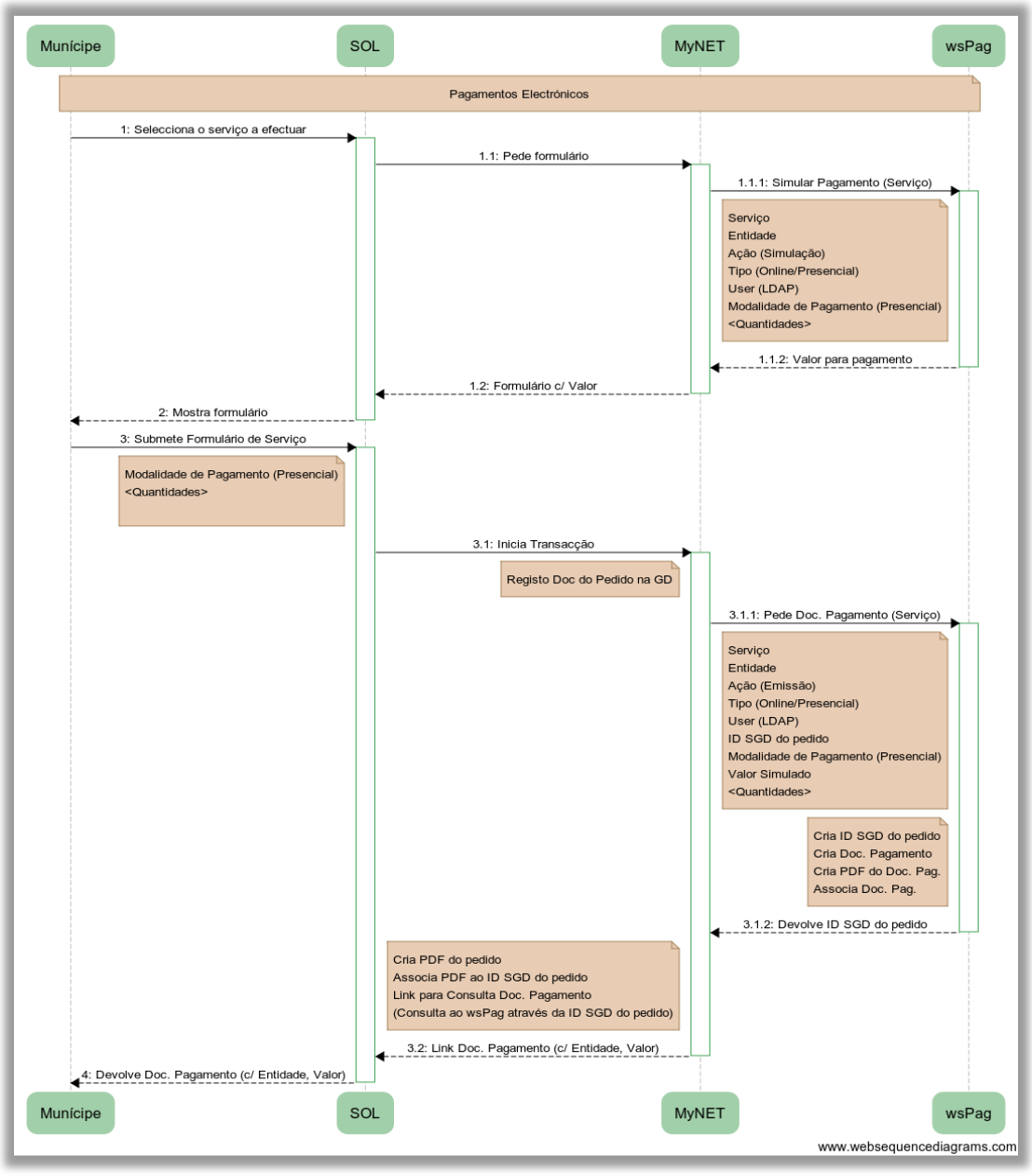


Figura 15 - Diagrama de sequência dos pagamentos presenciais

4.2.2 Descrição

Os pagamentos presenciais foram implementados no sistema recorrendo ao seguinte processo de negócio: o munícipe acede ao MyNet, seja através dos serviços *online* ou no balcão de atendimento, e escolhe a taxa / licença que pretende emitir. Ao carregar o formulário é apresentada a simulação do montante a pagar por aquele serviço. Após a submissão é criado um registo do novo processo no SGD, e caso o registo na gestão documental seja efetuado com sucesso é emitida a taxa / licença e apresentada ao munícipe a fatura com o montante a pagar. Como o pagamento escolhido foi o presencial, o munícipe tem de se deslocar ao funcionário da câmara responsável pela tesouraria. O funcionário acede à área de trabalho do SGF e tem a opção de pesquisar as taxas / licenças emitidas por munícipe, por intervalo de datas, por número de processo e assim efetuar o pagamento. O pagamento pode ser feito parcialmente, anulado ou pago por inteiro. Caso seja pago parcialmente, a taxa / licença passa do estado "emitida" para o estado "pago parcialmente", e existe sempre um prazo limite de pagamento exigido pela câmara e configurado na criação do serviço. Caso a emissão seja anulada, a taxa / licença transita para o estado de "anulada". Se o munícipe optar por pagar o montante por inteiro a taxa / licença transita para o estado "paga". Uma taxa / licença só tem valor legal quando efetuado o seu pagamento e o estado transitar para "pago". O munícipe pode acompanhar todo o seu histórico de pagamentos e os detalhes de cada submissão, através da sua conta corrente de pagamentos no MyNet.

4.2.3 Exemplo de emissão Licença Táxis

- O munícipe acede ao MyNet através dos serviços *online* ou no balcão de atendimento. Escolhe o formulário de licença de táxis que deve conter a simulação do montante a pagar pelo serviço, e preenche os dados requeridos, conforme apresentado na figura 16.

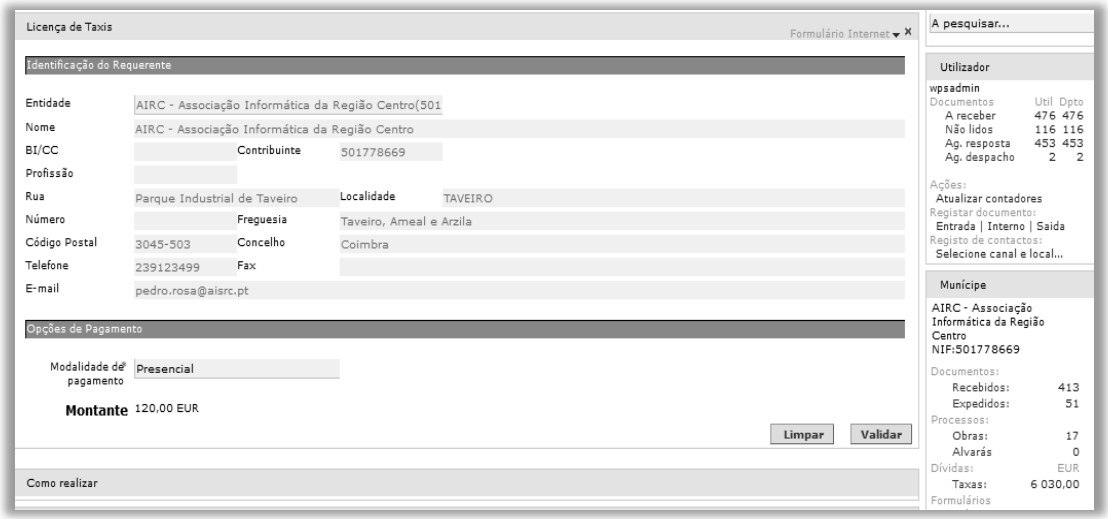


Figura 16 – Formulário de licença de táxis com pagamentos eletrónicos (modalidade presencial)

- Submete o formulário e após o processamento recebe a resposta (figura 17).

Figura 17 – Resposta a pagamentos presenciais com sucesso

- Após a emissão da licença o munícipe tem de se deslocar ao funcionário da câmara responsável pela tesouraria. O funcionário consulta a área de trabalho criada na aplicação SGF para pagar / anular a licença de táxis emitida (figura 18).

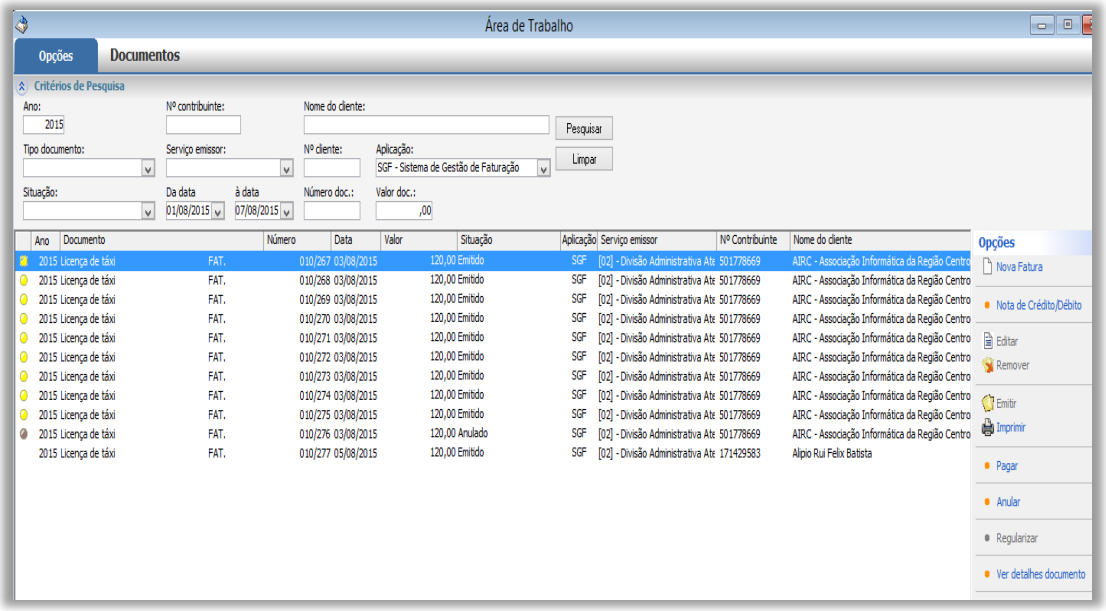


Figura 18 – Área de trabalho do SGF

- O munícipe pode acompanhar todo o seu histórico de pagamentos através da sua conta corrente de taxas (figura 19 e 20).

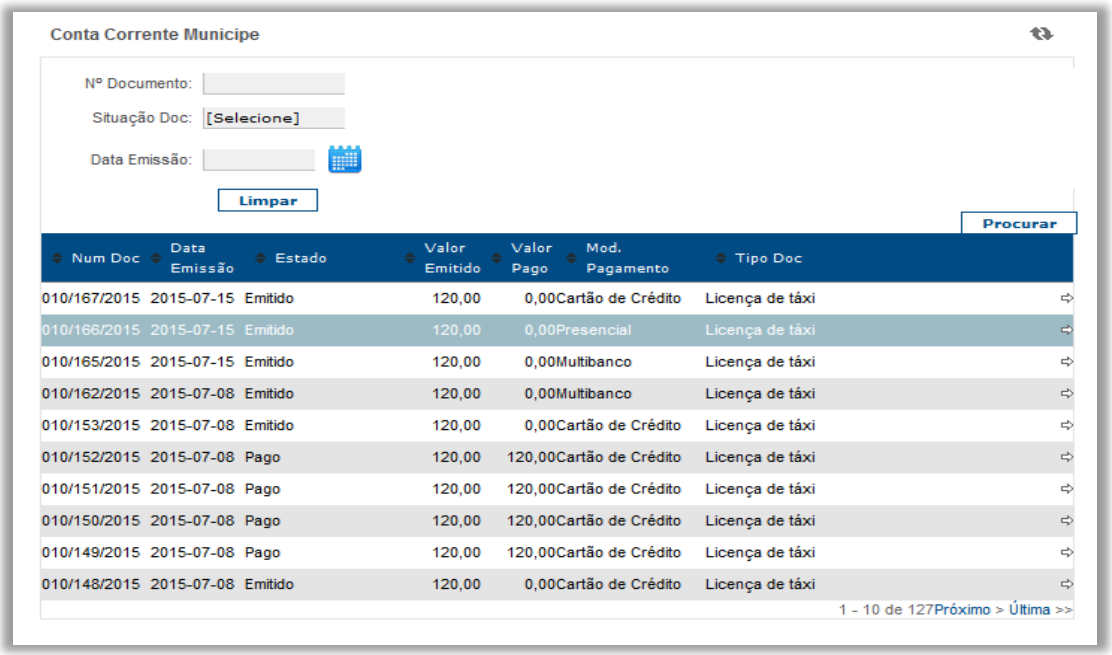


Figura 19 – Conta corrente de taxas ou pagamentos do munícipe

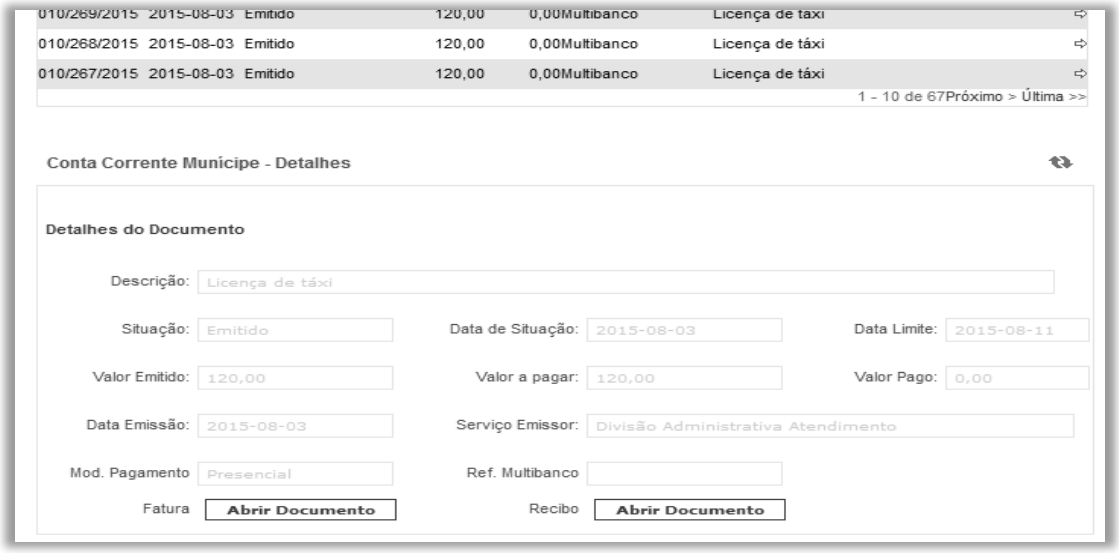


Figura 20 – Informação detalhada de uma licença de táxi

4.3 Pagamentos multibanco AIRC

4.3.1 Diagrama de sequência

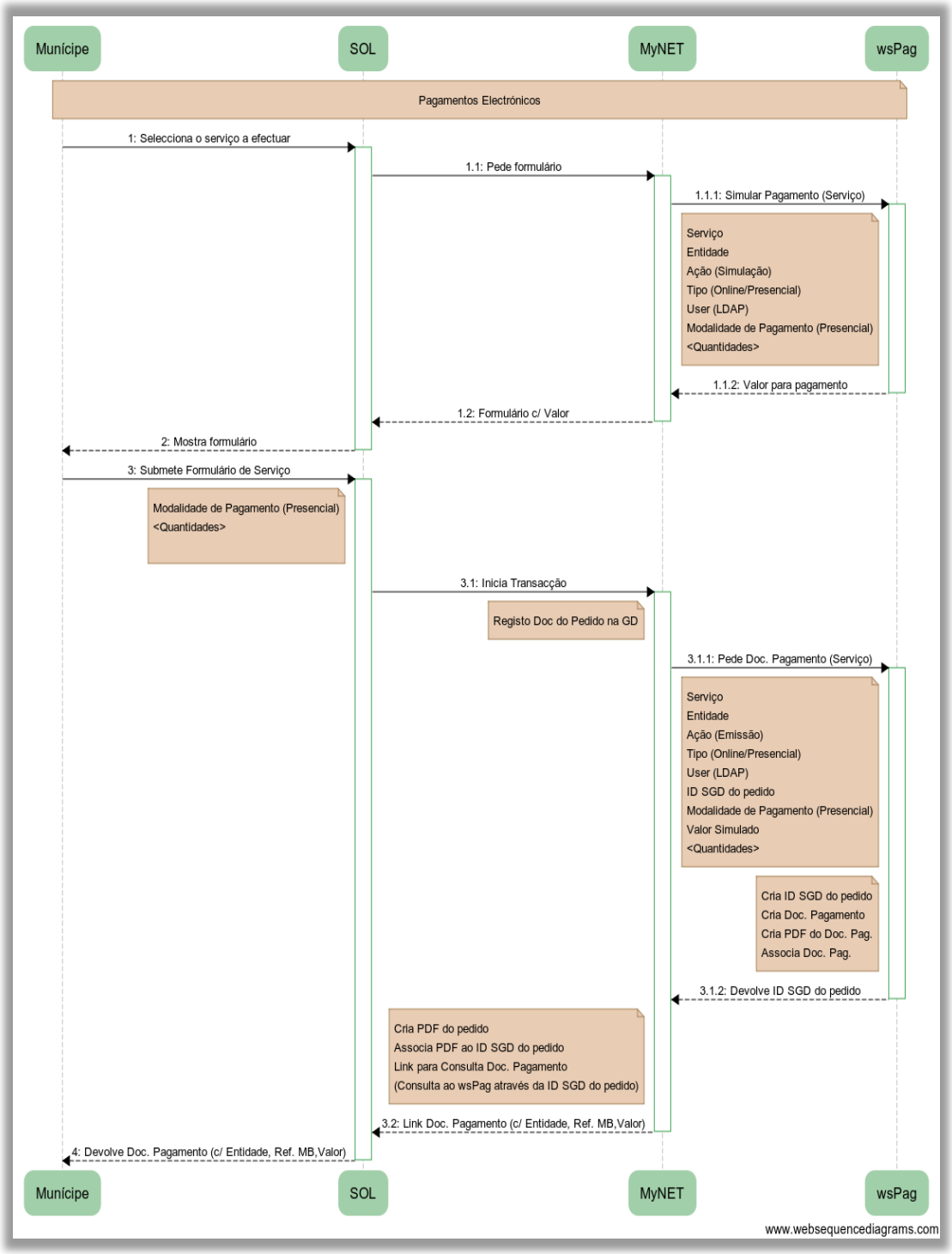


Figura 21 - Diagrama de sequência dos pagamentos multibanco AIRC

4.3.2 Descrição

Os pagamentos multibanco foram implementados no sistema recorrendo ao seguinte

processo de negócio: o munícipe acede ao MyNet, seja através dos serviços *online* ou no balcão de atendimento e escolhe a taxa / licença que pretende emitir. Ao carregar o formulário é apresentada a simulação do montante a pagar por aquele serviço. O munícipe escolhe a modalidade de pagamento multibanco e pode submeter o formulário. Após a submissão é criado um registo do novo processo no SGD, e caso o registo na gestão documental seja efetuado com sucesso é emitida a taxa / licença e apresentada a fatura ao munícipe com a entidade SIBS, referência multibanco e o montante a pagar. O munícipe pode pagar deslocando-se a um terminal multibanco, TPA, Home-Banking ou MB Spot. A Referência Multibanco é gerada na AIRC através de um algoritmo de check-digits. No sistema multibanco existem 3 conjuntos de dígitos utilizados pelo cliente para efetuar o pagamento: entidade, referência e montante, conforme apresentado na figura 22:

Figura 22 –Caixa com dados de pagamento multibanco

A caixa representada na figura 22 é impressa na fatura (usualmente no canto inferior esquerdo), e a data limite de pagamento pode ser também apresentada. Em seguida explica-se o processo implementado para gerar as referências multibanco:

- **Entidade:** a entidade tem sempre cinco dígitos e é fornecida pela SIBS, entidade reguladora, e a esta é associado o contrato de identificação da entidade AIRC;
- **Valor:** montante a pagar pelo serviço;
- **Referência:** a referência é composta sempre por 9 dígitos (em grupos de 3, o que facilita a visualização) e no sistema é gerada do seguinte modo:

Exemplo: SSSDDDDCC

  - SSS: três dígitos que identificam a sub-entidade (o vendedor). Este

código é atribuído pela SIBS;

- DDDD: ID - quatro dígitos que identificam o número da aplicação da AIRC que deu origem ao pedido da fatura. Este ID terá que ter obrigatoriamente 4 dígitos, pelo que caso o número da aplicação tenha menos de 4 dígitos são preenchidos os restantes com zeros à esquerda.
- CC: dois dígitos de controlo (check-digits): servem para o terminal validar se a informação está correta. Se o dígito de controlo só tiver um algarismo é formatado para 2 algarismos colocando um "0" à esquerda.

Após efetuar o pagamento, o munícipe tem de aguardar que os serviços do Município confirmem a entrada do pagamento e alterem o estado da taxa / licença de "emitida" para "paga". Os pagamentos através de referências multibanco só aceitam montantes integrais, isto é, o contrato realizado com a SIBS para emissão de referências não permite ao munícipe pagar mais ou menos que o montante constante da fatura. O munícipe pode acompanhar todo o seu histórico de pagamentos e os detalhes de cada submissão, através da sua conta corrente de pagamentos no MyNet.

4.3.3 Exemplo de emissão Licença Táxis

- O munícipe acede ao MyNet através dos serviços *online* ou no balcão de atendimento. Escolhe o formulário de licença de táxis que deve conter a simulação do montante a pagar por o serviço e preenche os dados requeridos (figura 23).

Figura 23 - Formulário de licença de táxis com pagamentos eletrónicos (modalidade multibanco)

- Submete o formulário e após o processamento recebe a resposta (figura 24);

Figura 24 - Resposta a pagamentos com referência multibanco com sucesso

- Após a emissão da licença, o munícipe tem de efetuar o pagamento através da referência multibanco para que a licença possa ser considerada válida. O pagamento pode ser feito através de um terminal multibanco, TPA, Home-Banking ou MB Spot;
- Efetuando o pagamento da licença o munícipe aguarda que os serviços municipais transitem o estado da sua licença para "paga". O munícipe pode acompanhar todo o seu histórico de pagamentos através da sua conta corrente de taxas (figura 25 e 26).

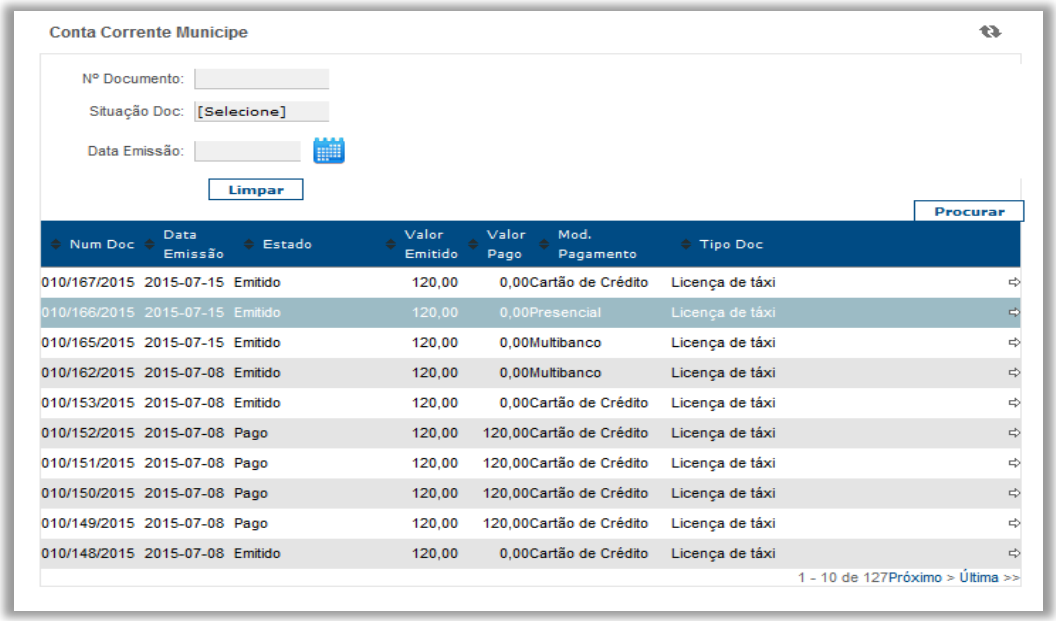


Figura 25 - Conta corrente de taxas ou pagamentos do munícipe

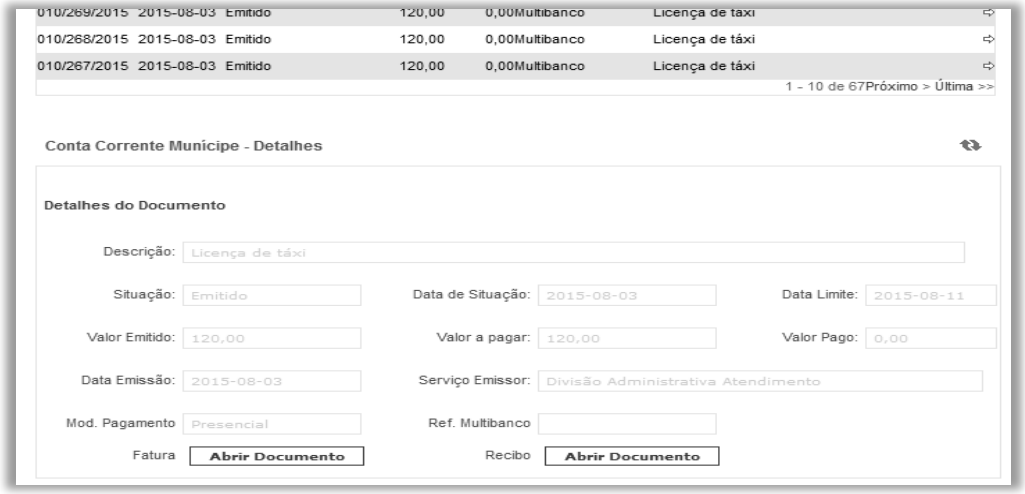


Figura 26 - Informação detalhada de uma licença de táxi

4.4 Pagamentos multibanco: integração com a PPAP

4.4.1 Diagrama de sequência

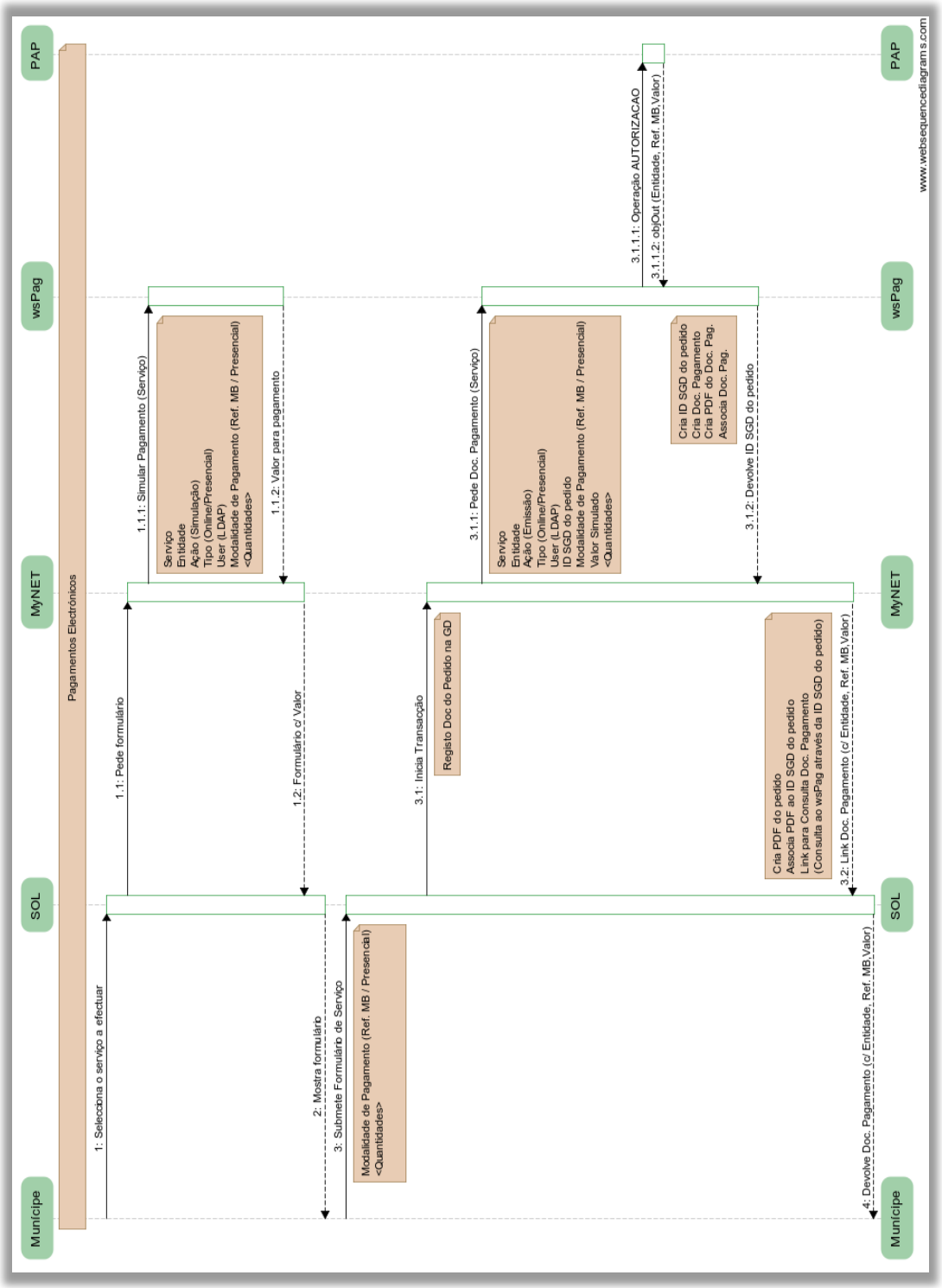


Figura 27 – Diagrama de sequência dos pagamentos com referência multibanco

4.4.2 Descrição

Os pagamentos multibanco com integração PPAP foram implementados no sistema recorrendo ao seguinte processo de negócio: o munícipe acede ao MyNet, seja através dos serviços *online* ou no balcão de atendimento e escolhe a taxa / licença que pretende emitir. Ao carregar o formulário é apresentada a simulação do montante a pagar pelo serviço. O munícipe escolhe a modalidade de pagamento multibanco que já está configurada para utilizar a PPAP e pode submeter o formulário. Após a submissão é criado um registo do novo processo no SGD. Caso o registo na gestão documental seja efetuado com sucesso é emitida a taxa / licença e apresentada a fatura ao munícipe com a entidade SIBS, referência multibanco e o montante a pagar. A referência é gerada na PPAP e fica registada a emissão da referência na plataforma da AMA. Quando o munícipe efetuar o pagamento da licença emitida a PPAP é notificada e regista a transação do pagamento. Posteriormente os dados da aplicação SGF são sincronizados com a plataforma, mantendo a integridade dos pagamentos já liquidados sobre serviços adquiridos à câmara. Toda a lógica de geração e atualização do pagamento está do lado da PPAP, sendo que à AIRC cabe apenas a responsabilidade de fazer a comunicação, o registo da emissão e a sincronização dos dados, de forma a manter a coerência entre as licenças emitidas e pagas. O munícipe pode efetuar o pagamento através de um terminal multibanco, TPA, Home-Banking ou MB Spot. Para que seja possível a sincronização de dados com a PPAP foi implementada uma área de plataformas externas no SGF (figura 28). Ao aceder a esta área, o funcionário tem a possibilidade de visualizar todas as emissões que têm interação com plataformas de terceiros, sincronizá-las e atualizar o estado das licenças emitidas de forma automática (figura 29). O munícipe pode acompanhar todo o seu histórico de pagamentos e os detalhes de cada submissão, através da sua conta corrente de pagamentos no MyNet.

As comunicações entre plataformas estão sujeitas a regras de segurança que são abordadas no subcapítulo “4.5 Mecanismos de Segurança”. A PPAP, além de implementar as normas de segurança, dispõe de *Web Services* que permitem a interação de sistemas externos, através da disponibilização de métodos para leitura dos registos efetuados por as entidades externas na plataforma, valores pagos, efetuar novos registos, gerar referências multibanco, entre outros (Barradas, J. et al, 2011).

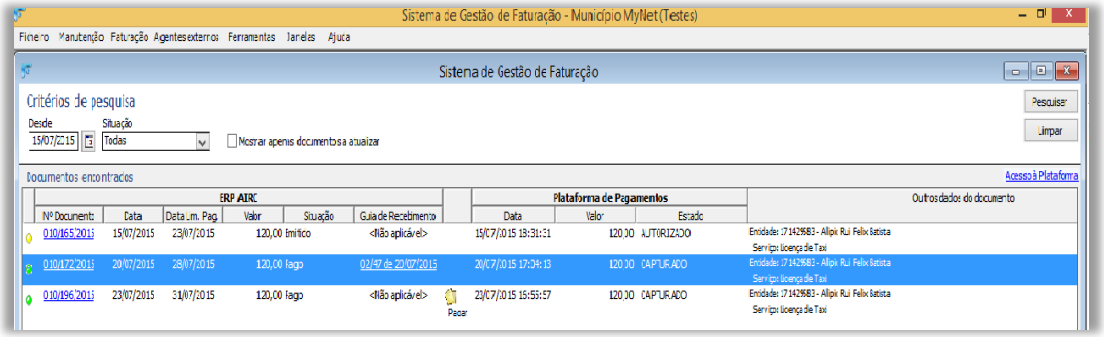


Figura 28 – Área de integração com a PPAP

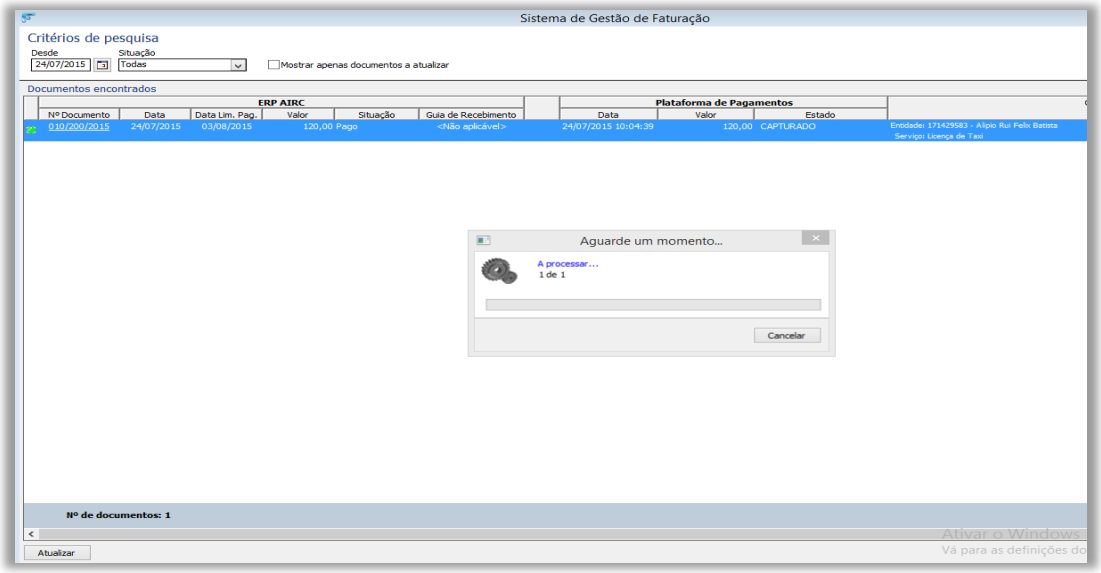


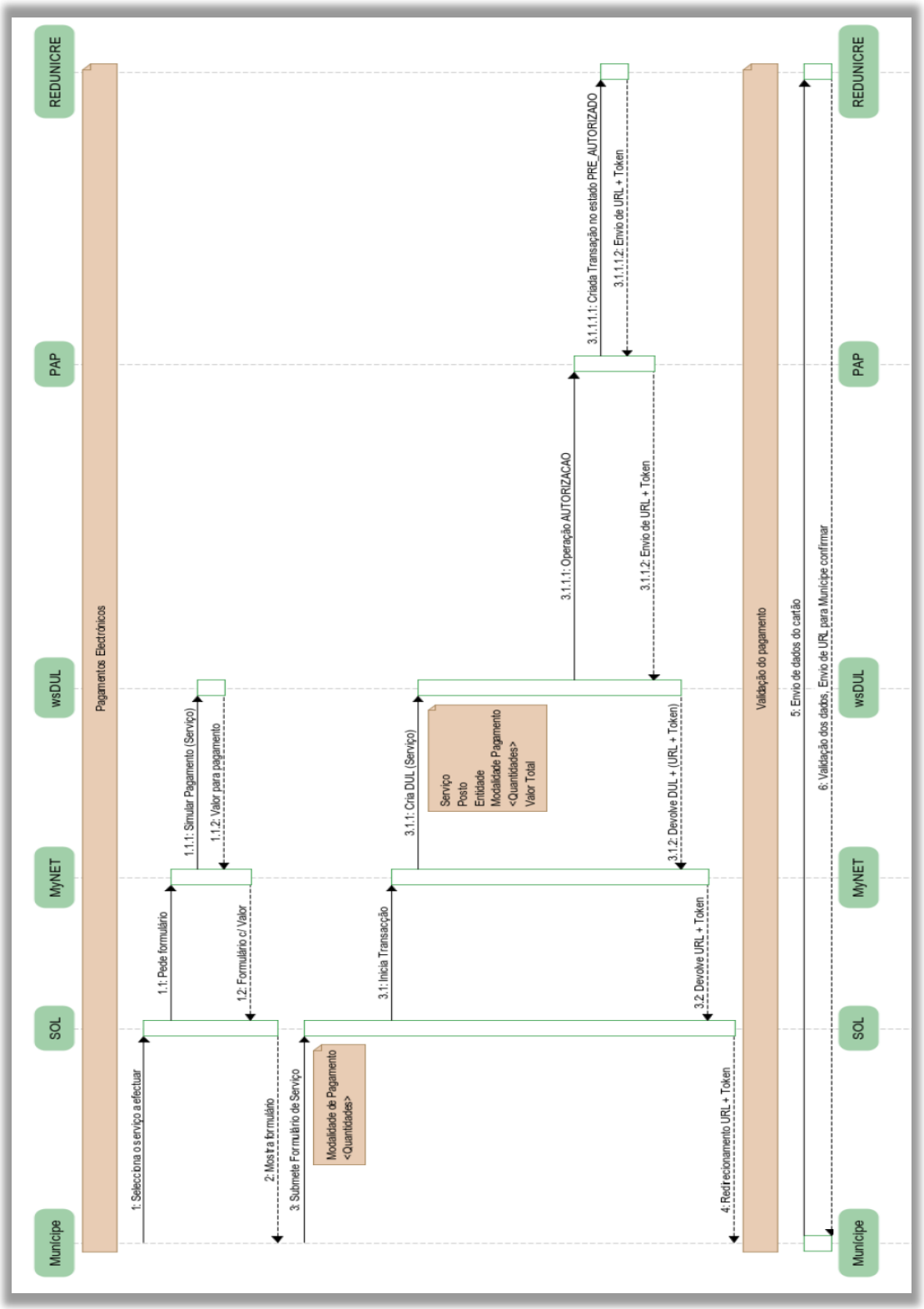
Figura 29 - Área de integração com a PPAP, processo de atualização dos pagamentos

4.4.3 Exemplo de emissão Licença Táxis

Para o munícipe o processo de emissão de uma licença de táxis com referências multibanco através do sistema da AIRC ou através da integração com a PPAP é igual, simples e intuitivo. O exemplo pode ser consultado no subcapítulo anterior "4.2 Pagamentos multibanco AIRC".

4.5 Pagamentos cartão de crédito

4.5.1 Diagrama de sequência



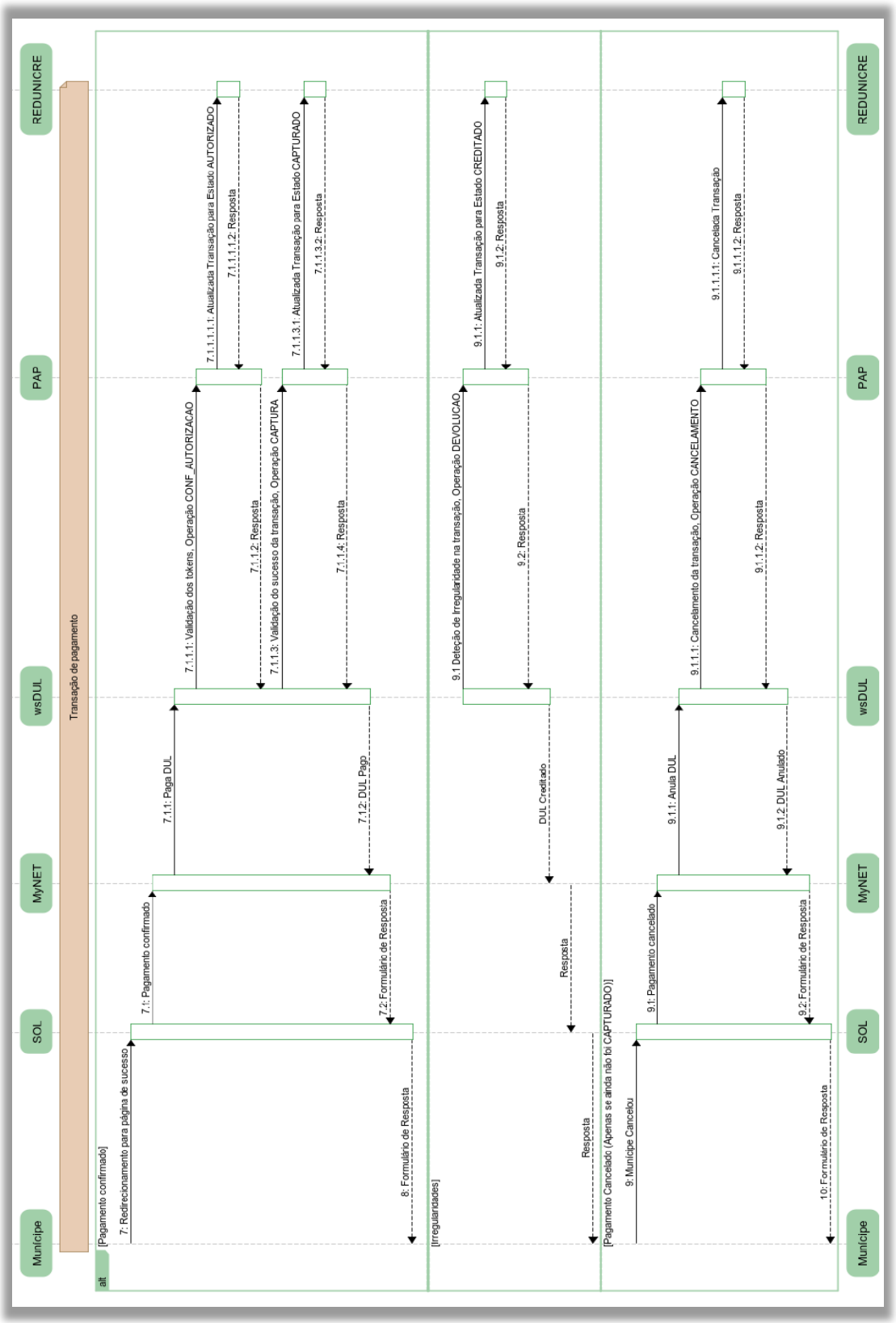


Figura 30 - Diagrama de sequência dos pagamentos com cartão de crédito

4.5.2 Descrição

Para implementar os pagamentos com a modalidade de cartão de crédito optou-se por utilizar serviços já consolidados no mercado e que garantissem pagamentos com cartões de crédito, os quais não existiam na AIRC. Por isso a parceria com a Unicre foi a opção tomada para esta implementação. A Unicre é uma empresa portuguesa especializada na gestão e emissão de cartões de pagamento há 41 anos. Possui duas marcas de negócio - Unibanco e Redunicre - e atua em três vertentes: cartões de crédito e crédito, soluções para aceitação de pagamentos e serviços de Card Management.

- **UNIBANCO:** centra a sua atuação na conceção e comercialização de soluções de pagamento (cartões) e crédito, bem como de serviços associados, sob a marca própria ou em parceria com outras marcas, destinadas a particular e empresas;
- **REDUNICRE**: realiza a conceção e comercialização de soluções para aceitação de pagamentos em estabelecimentos comerciais, presenciais e virtuais, com cartões nacionais e estrangeiros dos sistemas internacionais de pagamento Visa, MasterCard, Visa Electron, Maestro, VPay, Diners e JCB;
- **CARD MANAGEMENT**. presta serviços especializados a instituições financeiras e afins, relacionados com operações de emissão e gestão de cartões de pagamento, englobando o desenvolvimento de novos negócios, as operações com os sistemas internacionais, apoio operacional e ainda serviços técnicos de emissão de cartões e concessão de crédito, aceitação de cartões, segurança e gestão de transações.

Devido ao seu historial e provas dadas ao longo dos anos, esta foi uma das opções preferenciais. A constatação que a PPAP também utilizava a Redunicre para efetuar pagamentos com cartão de crédito veio reforçar a opção por a Redunicre. A existência de contactos com a AMA, certificados e protocolos de comunicação já estabelecidos veio ajudar a implementação dos pagamentos com cartão de crédito através da PPAP e Redunicre. A desvantagem desta opção estava relacionada com a limitação dos tipos de cartões de crédito. Apesar de a Redunicre suportar vários tipos de cartão de crédito, a PPAP está limitada ao suporte de cartões Visa e Master Card. Contudo, estes dois tipos de cartões de crédito são os mais utilizados em Portugal e no mundo (Faria, N., 2014).

De acordo com a Redunicre os cartões:

- VISA: são usados em mais de 170 países espalhados pelo Mundo. Existem cerca de 1,4 biliões de cartões VISA responsáveis por 45 biliões de transações. Estes cartões são aceites em mais de 27 milhões de comerciantes e 1 milhão de caixas multibanco. Na Europa, por cada 9€ gastos, mais de 1€ é gasto com um cartão VISA.
- MasterCard: os 817 milhões de cartões de MasterCard são usados em mais de 240 países e representaram em 2006, 16.1 biliões de transações. Estes cartões são aceites em mais de 25 milhões de comerciantes espalhados pelo Mundo.

A limitação dos dois tipos de pagamentos acaba por não ser preocupante para a primeira versão do sistema, pelo que ficou decidido implementar os pagamentos com cartão de crédito através da PPAP e Redunicre.

As transações efetuadas com a Redunicre vão estar associadas a um *timedtoken*[19] que deve ser enviado em cada transação. Caso o *timedtoken* seja inválido ou tenha expirado o processo é cancelado. A utilização dos serviços de cartão de crédito da Redunicre requer alguns dados essenciais, tais como:

- Identificação da entidade (AIRC);
- Identificação do domínio ou página onde se realizem as transações;
- Mecanismo de redireccionamento para a página que processa a transação (Redunicre);
- Identificar a página para onde são redirecionados os pagamentos com sucesso e os cancelados;
- Definir com a Redunicre o aspeto visual da página onde serão feitas as transações;
- Definir com a Redunicre o modo de redireccionamento pretendido, manual ou automático.

Para emitir uma taxa / licença com pagamento através de cartão de crédito, o munícipe deve aceder ao MyNet através dos serviços *online* e escolher a taxa / licença que pretende emitir. Ao carregar o formulário é mostrada a simulação do valor que o

[19] TimedToken identifica a sessão de pagamentos do lado da Redunicre, é representado por uma string alfanúmerica.

munícipe tem de pagar. Caso pretenda emitir a taxa / licença, seleciona a modalidade de pagamento por cartão de crédito. Existe ainda a opção de receber notificações via correio eletrónico ou via telefone: para as receber basta ativar a opção de receção de notificações no formulário, e inserir o correio eletrónico ou o telefone (dados opcionais), procedendo então à submissão do formulário. Após a submissão é criado um registo do novo processo no SGD, e caso o registo na gestão documental seja efetuado com sucesso é emitida a taxa / licença no SGF e em seguida é apresentado ao munícipe um formulário em que pode visualizar a fatura emitida e prosseguir com o pagamento. Cada transação é identificada com um *timedtoken* diferente. Após o utilizador avançar na etapa de pagamento, será redirecionado para uma página segura da Redunicre e registada a emissão do pagamento na PPAP. Neste ponto o munícipe tem duas hipóteses: ou insere os dados do cartão de crédito (número do cartão, Card Verification Value (CVV)[20] e data de validade), ou cancela a operação. Caso o munícipe opte por confirmar o pagamento após introduzir os seus dados, é registado o pagamento da taxa / licença, apresentado o recibo e redirecionado (manual ou automaticamnte) para o MyNet para finalizar o processo, registando no SGF o pagamento da taxa / licença com sucesso. O estado da taxa / licença transita para "pago", automaticamente. Caso o munícipe opte por cancelar o processo, será redirecionado para o MyNet e o registo efetuado anteriormente é anulado, no SGF e na PPAP. O estado da taxa / licença emitida transita para "anulado". O munícipe pode acompanhar todo o seu histórico de pagamentos e os detalhes de cada submissão, através da sua conta corrente de pagamentos no MyNet.

4.5.3 Exemplo de emissão Licença Táxis

- O munícipe acede ao MyNet através dos serviços *online*. Escolhe o formulário de licença de táxis que deve conter a simulação do montante a pagar por o serviço, e preenche os dados requeridos (figura 31);

[20] CVV é um código de segurança impresso nos cartões de crédito que proporciona maior proteção contra fraudes em transações feitas na Internet. A utilização do código é um procedimento de autenticação exigido pelas empresas de cartões de crédito.

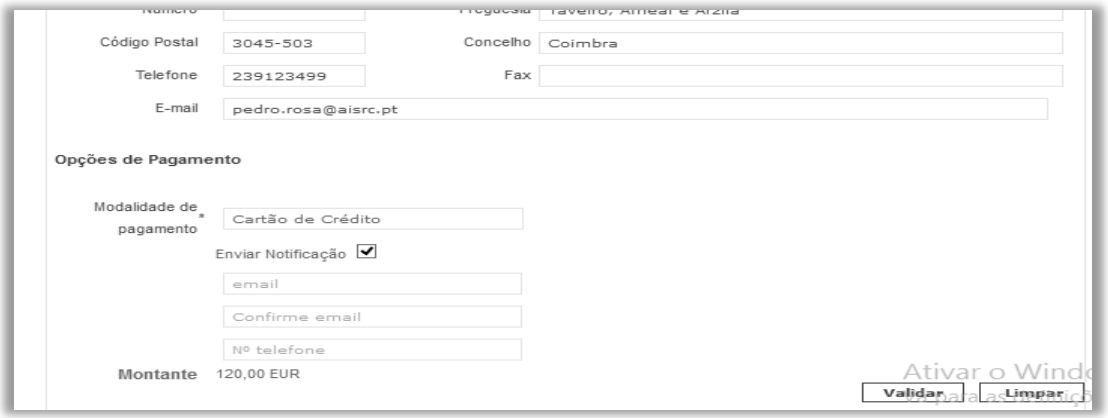


Figura 31 – Formulário de licença de táxis com pagamentos eletrónicos (modalidade cartão de crédito)

- Após selecionar a modalidade cartão de crédito o munícipe pode escolher se quer receber notificações, tais como a confirmação do pagamento e o recibo por correio eletrónico no final da transação. Caso pretenda deve preencher os campos de correio eletrónico ou telefone (figura 32);

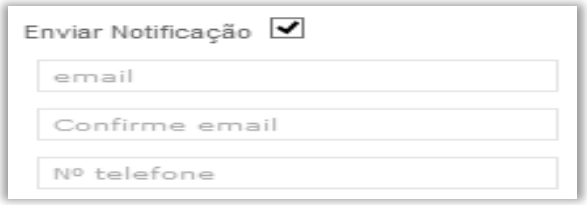


Figura 32 – Campos de enviar notificações para pagamentos com cartão de crédito

- Submete o formulário e após o processamento recebe a resposta (figura 33);

Figura 33 - Resposta intermédia a pagamentos com cartão crédito

- Clica no botão "Proceder ao pagamento" para avançar para a etapa de pagamento com cartão de crédito;
- É então redirecionado para uma página da Redunicre (figura 34);
    - Opção 1: Preenche os dados do cartão de crédito e valida o pagamento.
    - Opção 2: Cancela o pagamento e a taxa / licença emitida.

Figura 34 – Página de pagamento com cartão de crédito

- Opção 1: Completa o processo de pagamento (figura 35);

Figura 35 – Informação de validação do pagamento

- Opção 1: na figura 36 mostra-se a resposta do sistema após o munícipe finalizar o processo de pagamento com sucesso. Caso as notificações tenham sido

ativadas, é enviada uma notificação com o comprovativo de pagamento ao munícipe. A taxa / licença emitida transita de estado para "pago";

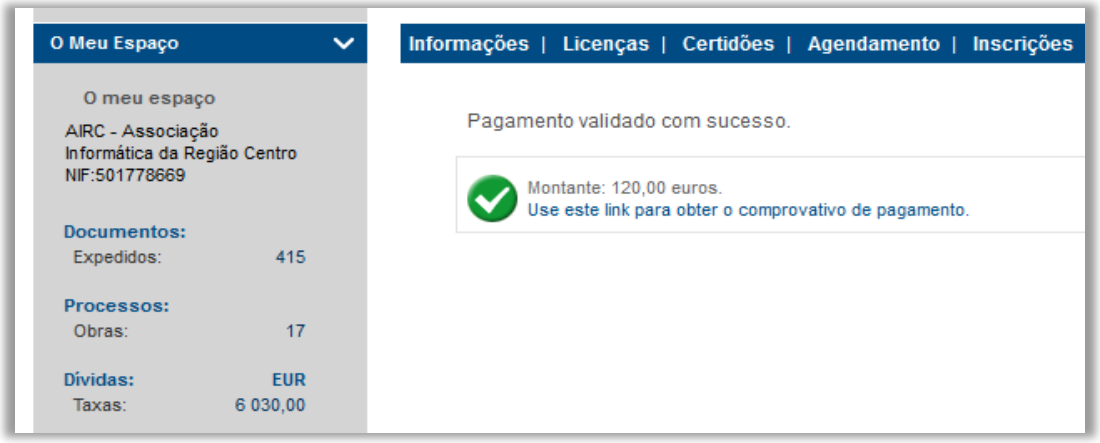


Figura 36 – Resposta de sucesso ao finalizar pagamento cartão crédito no MyNet

- Opção 2: o pagamento é cancelado e redirecionado para o MyNet, que anula a emissão da taxa / licença. A figura 37 representa a resposta do sistema quando se opta por cancelar o pagamento;

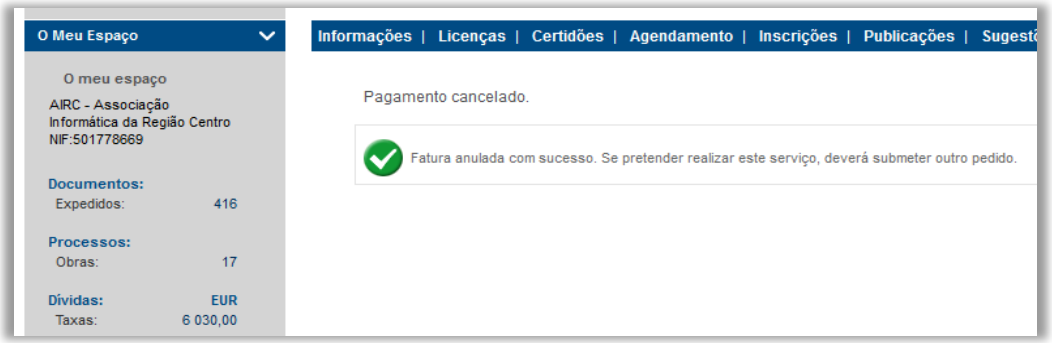


Figura 37 – Resposta ao cancelamento do pagamento por cartão de crédito

- O munícipe pode acompanhar todo o seu histórico de pagamentos através da sua conta corrente de taxas, conforme figuras 38 e 39.

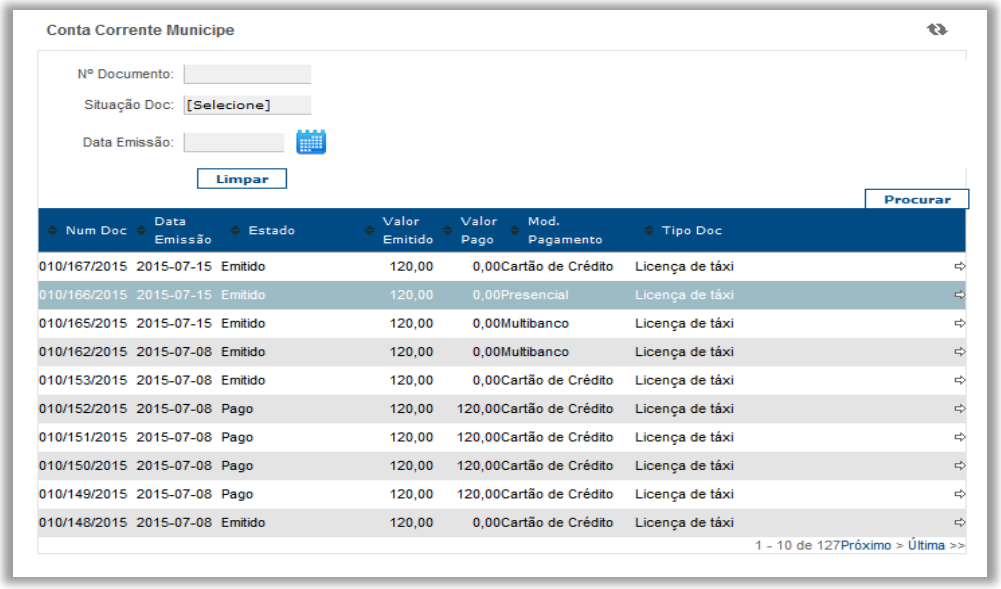


Figura 38 - Conta corrente de taxas ou pagamentos do munícipe

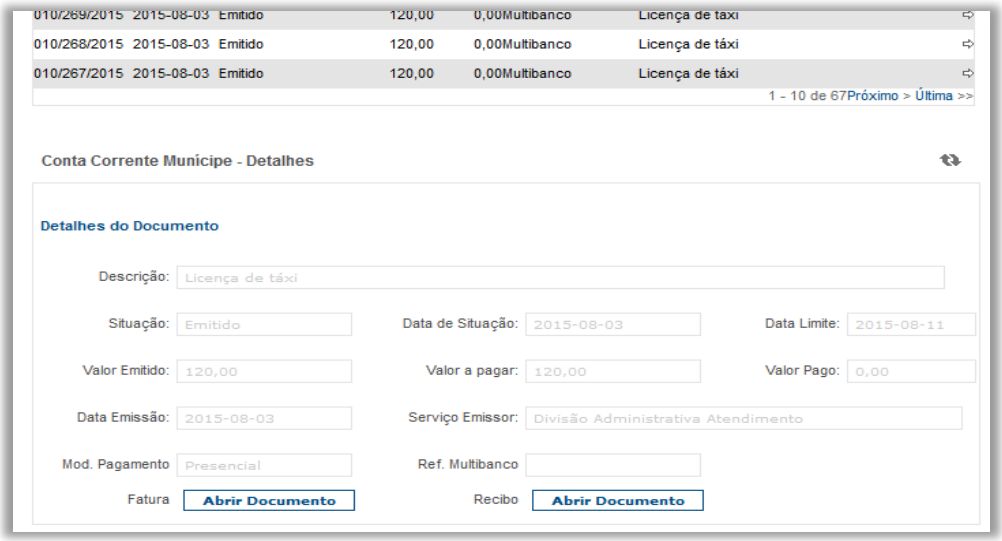


Figura 39 - Informação detalhada de uma licença de táxi

4.6 Mecanismos de segurança

A segurança é um aspeto importante no sistema de pagamentos eletrónicos porque a divulgação de dados confidenciais dos utilizadores, tais como como informações pessoais e financeiras, tem de ser protegida aquando das trocas de informação entre sistemas informáticos.

4.6.1 Web Services

Os *Web Services* estão desenvolvidos sob a tecnologia *Web Services Enhancements* (WSE) e *Windows Communication Foundation* (WCF), garantido total segurança na integração com aplicações cliente. Tanto o WSE como o WCF são um conjunto de Application Programming Interfaces[21] (APIs) construídas para conectar Serviços Orientados a Arquitetura[22] (SOA – *Service Oriented Architecture*), definindo protocolos em áreas como segurança, leitura de mensagens, anexos, comunicação e outros.

A camada de serviços em WSE assegura:

- Encriptação das comunicações, através de um certificado X.509[23];
- Autenticação através de nome e palavra-chave;
- Apenas são aceites pedidos ou mensagens assinadas;
- Cada pedido tem um tempo de expiração definido ao fim do qual é rejeitado;
- São registados os identificadores dos pedidos, e rejeitados pedidos com identificadores já utilizados;
- Todas as comunicações são realizadas em Secure Sockets Layer[24] (SSL);
- Utiliza ficheiro de *WS-Policy*[25].

Pressupostos da aplicação cliente para ligações em WSE:

- Utilizar o ficheiro de WS-Policy na máquina do cliente, fornecido pela entidade servidora;
- Se a plataforma cliente não suportar WS-Policy, é necessário que a aplicação construa as mensagens SOAP com as características de segurança requeridas: encriptação, autenticação e assinatura dos pedidos.

[21] API é um conjunto de rotinas, protocolos e ferramentas que auxiliam a construção de software, de forma a fornecer funcionalidades independentes do resto do sistema.
[22] SOA é um padrão de arquitetura de software, em que os componentes de uma aplicação providenciam serviços para outros componentes via protocolos de comunicação. Os princípios do SOA são a independência de qualquer fabricante, produto ou tecnologia.
[23] O certificado X.509 é um padrão ITU-T (International Telecommunication Union) para a infra-estrutura da chave pública do certificado.
[24] SSL é uma tecnologia de segurança standard para estabelecer e encriptar uma ligação ou comunicação entre o servidor e o cliente.
[25] WS-Policy é uma especificação que permite aos web services descreverem as suas características e os seus requisitos de segurança. As politícas (policies) são declaradas no servidor e no cliente em ficheiros XML.

- Instalação da chave pública do certificado X.509 de encriptação na máquina cliente;
- Enviar a autenticação (nome / palavra chave fornecidos pelo servidor) nas mensagens do pedido.

A camada de serviços em WCF assegura:

- Autenticação através de nome e palavra-chave;
- A comunicação com aplicações externas decorrerá exclusivamente via SSL.

Pressupostos da aplicação cliente para ligações em WCF:

- O cliente tem que ter instalado o certificado Certified Authority[26] (CA) que foi usado para emitir o certificado SSL;
- Enviar a devida autenticação (nome / palavra-chave fornecidos pela entidade servidora) nas mensagens de pedido.

A figura 40 representa como é que os vários ambientes consomem as camadas de W*eb Services*:

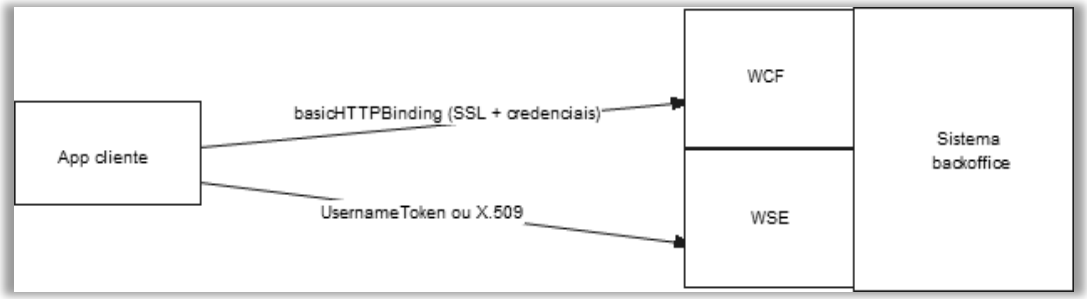


Figura 40 – Comunicação com os web services

A aplicação cliente, ou *web service client* é quem vai determinar qual o tipo de chamada a ser executada nos *web services* do servidor. Caso o *web service* cliente use tecnologias como Java, .Net 3.0 ou superior os mecanismos de comunicação e autenticação passam por WCF. Caso os serviços clientes usem tecnologias como .Net 1.1 ou 2.0 os mecanismos de comunicação são diferentes e seguem os protocolos da API WSE.

[26] CA em criptografia é a entidade que emite os certificados digitais, o dono da cadeia de certificação da chave pública. Normalmente estão identificados na cadeia de certificação de um certificado X.509.

4.6.2 Informação ao Utilizador

A informação é um aspeto que considerámos fundamental para o sistema, dado que contribui para que o utilizador veja o sistema como seguro e de confiança. Todos os passos que o utilizador tem de realizar para efetuar os seus pagamentos estão identificados e é apresentada toda a informação sobre o processo que deve ser realizado, mantendo sempre o utilizador no controlo da situação.

Assim, houve a necessidade de implementar um mecanismo chamado de "informação personalizável". O requisito surgiu porque cada cliente (município) deve informar os seus munícipes sobre o estado das ações / submissões que estes realizam nos seus portais. Contudo, numa primeira fase foi implementado um mecanismo padrão de informação ao munícipe, tendo frases não personalizáveis em cada fase dos pagamentos, o que era impraticável porque cada município queria personalizar essa informação. Para responder a essas propostas de melhorias foram criados marcadores em cada fase dos processos de pagamento. Os marcadores são identificadores que vão ser lidos a partir de um ficheiro de texto e assim, caso o cliente pretenda personalizar a informação basta alterar o marcador no ficheiro de texto. Cada marcador contém informação por omissão, caso o município não personalize essa informação. O ficheiro de texto que contém os marcadores é carregado no sistema quando este inicia e por isso a informação só pode ser modificada antes do sistema iniciar. Na figura 41 mostra-se um exemplo de uma frase por omissão, que pode ser personalizável;

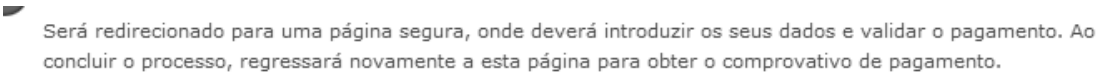


Figura 41 – Frase por omissão após emissão da licença com pagamento de cartão de crédito

4.7 Objetivos realizados

A tabela 1 apresenta o tempo percentual gasto na realização do projeto. Os objetivos enumerados na tabela encontram-se sob a forma de macro objetivos e por isso cada um deles encontra-se subdividido em mini-objetivos ou tarefas que foram realizadas ao longo do projeto;

Objetivos (Macro) Propostos	Percentagem de tempo
Investigação sobre pagamentos eletrónicos	10%
Análise de requisitos do sistema	12%
Área de configurações	5%
Pagamentos presenciais (Internet / Intranet)	10%
Pagamentos multibanco (Internet / Intranet)	13%
Pagamentos cartão de crédito (Internet)	10%
Registo da emissão no SGD	2%
Área de trabalho integrada com PPAP	5%
Ficheiros de linguagem	1%
Pagamentos em formulários de Urbanismo	1%
Pagamentos em formulários genéricos	8%
Pagamentos em formulários do SGA	2%
Criação de campo complexo de pagamentos	5%
Simulação dos montantes a pagar	3%
Introdução de marcadores de pagamentos	1%
Layout pagamentos eletrónicos	3%
Área de conta corrente do munícipe	4%
Testes ao sistema	5%

Tabela 1 – Representa a % de tempo do estágio gasto para realização dos objetivos

As percentagens de tempo referidas na tabela 1 são reais e foram retiradas da plataforma Jazz que é utilizada para gestão e controlo de projetos. Durante o desenvolvimento do projeto cada requisito ou história a ser implementada era registada na plataforma e assim foi possível obter o registo do tempo gasto em cada tarefa ou história. A utilização do Jazz é parte integral no processo de desenvolvimento de

software da empresa AIRC. A figura 42 apresenta um exemplo da plataforma, com algumas tarefas de um sprint;

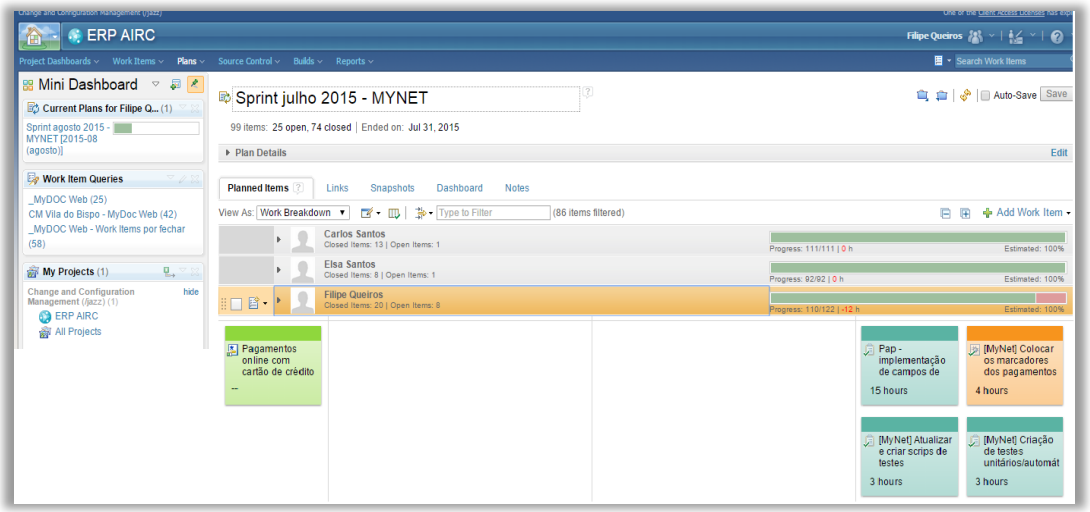


Figura 42 – Plataforma de gestão e controlo de projetos Jazz

A plataforma Jazz é utilizada com metodologias ágeis, neste caso o SCRUM. Além de registar os tempos de cada tarefa ou história, permite registar defeitos, dependências entre histórias, quem desenvolve cada tarefa ou história, atribuir tempos a cada tarefa, gerir a evolução do projeto através de ferramentas de gestão como gráficos *burndown*, registo de testes e partilha de informações relativas aos projetos, entre equipas.

5 Testes

Esta seção apresenta todos os testes que foram realizados ao sistema de pagamentos eletrónicos. Para este projeto foram realizados testes de caixa preta, testes de integração entre sistemas e testes de caixa branca.

5.1 Testes de caixa preta

Nos testes de caixa preta o analista não tem acesso ao código fonte e desconhece a estrutura interna do sistema. São também conhecidos como testes funcionais, pois são baseados nos requisitos funcionais do software. O foco, neste caso, é nos requisitos da aplicação, ou seja, nas ações que ela deve desempenhar. Para a realização dos testes de caixa preta foram desenvolvidos:

- **Scripts de teste:** os *scripts* de teste visam representar todos os requisitos funcionais do sistema, de modo a averiguar a correta implementação da funcionalidade. Estes *scripts* foram executados pela equipa de testes do MyNet. No processo de execução destes testes pela primeira vez, foram encontrados vários problemas tais como erros na submissão de formulários de urbanismo com pagamentos, símbolos errados e problemas relacionados com os diferentes tipos de navegadores *web*, entre outros. Estes erros são registados na plataforma Jazz e no script de teste como defeitos que afetam as respetivas funcionalidades. Após finalização do processo de testes, caso existam defeitos ou melhorias, estas são planeadas para resolução ou implementação no *sprint* seguinte. Trata-se de um processo cíclico de constante melhoria do software, em que a equipa de testes do MyNet participa de forma ativa. Alguns exemplos de *scripts* de teste encontram-se no anexo D;
- **Testes de sistema:** os testes de sistema são testes em que o sistema já está completamente integrado, e vai agora ser verificado quanto aos seus requisitos num ambiente de produção. Os testes de sistema não se limitam a testes de requisitos funcionais, mas também de requisitos não funcionais tais como as expetativas do cliente. Para a realização de testes de sistemas foi criado / simulado um ambiente de produção na AIRC com todo o sistema instalado e configurado, onde as equipas de testes da AIRC efetuaram os respetivos testes. Os aspetos de usabilidade que estavam menos corretos foram reportados através da ferramenta Jazz. Paralelamente realizaram-se testes de sistema em interação

com os clientes, e iniciaram-se contactos com dois municípios, Mira e Vila Real. Estes puderam assim instalar o módulo de pagamentos nos seus ambientes de teste e reportar o seu *feedback* acerca da performance do sistema.

5.2 Testes de caixa branca

Nos testes de caixa branca o analista tem acesso ao código fonte, conhece a estrutura interna do produto a ser analisado e possibilita que sejam escolhidas partes específicas de um componente para serem avaliadas. Esse tipo de teste, também conhecido como teste estrutural, é projetado em função da estrutura do componente e permite uma análise mais precisa do comportamento dessa estrutura. O acesso ao código facilita o isolamento de uma função ou ação, o que ajuda na análise comportamental das mesmas. Para a realização dos testes de caixa branca foram realizados:

- **Testes unitários ou automáticos:** os testes unitários ou automáticos visam simular o correto funcionamento de todas as ações para que o sistema está programado, bem como detetar novos problemas. Os testes automáticos foram realizados recorrendo ao jUnit[27] e apresentam-se alguns exemplos de código no anexo A. O objetivo dos testes automáticos é conseguir controlar mudanças que possam ser realizadas ao sistema em desenvolvimento e com isso criar problemas em situações que anteriormente estariam corretas. Assim, basta ao analista / programador executar os testes automáticos para obter um relatório com o resultado de cada teste, em que a cor verde simboliza que o resultado foi o esperado – ou teve sucesso - (figura 43) e a cor vermelha representa algum tipo de erro (figura 44). Em cada versão da aplicação foi executada toda a bateria de testes unitários.

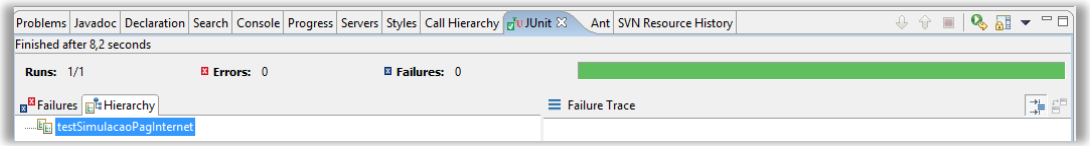


Figura 43 – Sucesso na execução de um teste unitário / automático

[27] jUnit é uma libraria ou plataforma para escrita e execução de testes automáticos ou unitários.

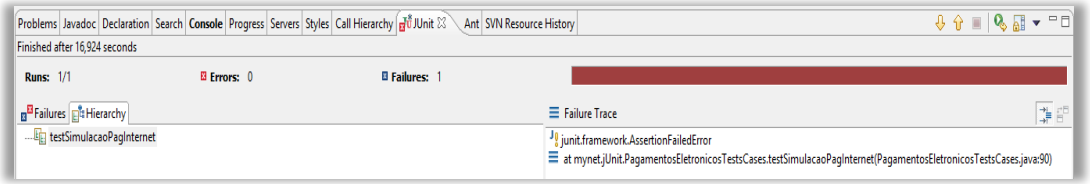


Figura 44 – Insucesso na execução de um teste unitário / automático

- **Testes de integração:** os testes de integração são um complemento aos testes unitários e visam integrar vários módulos na aplicação. No caso concreto dos pagamentos eletrónicos foram criados testes de integração entre o sistema MyNet e os serviços de forma a garantir o correto funcionamento entre os diversos subsistemas envolvidos. Este tipo de testes é importante para garantir o correto funcionamento de um sistema integrado, ao contrário dos testes unitários que testam cada módulo em separado. Para realizar este tipo de testes foram usadas duas abordagens: criação de automatismos que validassem todas as integrações ou resultados entre os sistemas; utilização da equipa de testes do MyNet para realizar todos os casos possíveis de interações entre sistemas, e cujos resultados ficaram registados num documento de testes de integração. Exemplos de código dos testes de integração podem ser consultados no anexo B e o documento relativo aos testes de integração pode ser consultado no anexo C.

5.3 Testes de segurança

Os testes de segurança permitem avaliar a vulnerabilidade do sistema contra diferentes tipos de ataques ao sistema e descobrir eventuais vulnerabilidades. As validações de segurança podem ser realizadas em duas fases: a fase estática e a fase dinâmica.

- **Fase estática.** A fase estática tem por objetivo localizar falhas inseridas durante o desenvolvimento do projeto, como um estado impossível ou erros humanos introduzidos no código. Para analisar estes erros utilizámos métodos de análise estática tis como inspeção de código. As inspeções foram realizadas por um membro sénior da equipa, sempre que foram efetuadas mudanças identificadas como críticas ao bom funcionamento do sistema. As inspeções consistem na leitura de código por alguém que não realizou aquele código, para identificar problemas que o autor não tenha identificado. As inspeções foram sempre realizadas de uma forma informal eo inspecionador, após terminar a revisão,

comunicava as situações identificadas como incorrectas sendo realizada a respetiva correção;

- **Fase dinâmica.** A fase dinâmica tem como objetivo realizar as verificações e identificar falhas durante a execução do sistema. São fornecidos dados de entrada reais ao sistema, para verificar os mecanismos de segurança. Eis alguns exemplos de testes dinâmicos realizados:
    - Tentar estabelecer ligação com os serviços através de um certificado X.509 inválido ou falso;
    - Utilizar *timedtokens* já usados em transações de pagamentos;
    - Adulterar o *timedtoken* e enviá-lo no pedido;
    - Alterar o montante a pagar que vai no pedido referente ao serviço;
    - Enviar no pedido um nome e palavra-chave não registados;
    - Tentar comunicar com os serviços sem ser via SSL;
    - Utilizar um *timedtoken* que já tenha expirado;
    - Assinar o pedido com uma chave privada diferente da correspondente chave pública.

Nota: Cada pedido criado para comunicar com os serviços é assinado com uma chave privada e é fornecido um certificado X.509 (chave pública) à entidade com que se quer comunicar. O certificado X.509 especifica, entre outras coisas, os formatos padrão para a chave pública do certificado, a lista de revogação dos certificados, os atributos do certificado e um algoritmo de validação do caminho de certificação. Esta assinatura vai permitir verificar se a mensagem é legítima, ou não.

6 Conclusões e Trabalho Futuro

6.1 Conclusões

A realização do projeto revelou-se enriquecedora para a aprendizagem ou consolidação de tecnologias e linguagens de programação como Java, PowerBuilder, Javascript, ASP, Jquery, HTML, CSS, serviços *Web* (SOAP), XSL, XML, encriptação de dados e mensagens, certificados e Informix, entre outras.

A coordenação do tempo disponível e todo o processo de acompanhamento e gestão do projeto foi um sucesso. A utilização de uma metodologia ágil (SCRUM) com entregas de reduzido volume mas periódicas veio a revelar-se uma excelente opção, dado que todas as metas foram cumpridas nos prazos determinados não havendo atraso significativo no tempo total planeado para o projeto.

O sistema de pagamentos eletrónicos foi produzido de forma modular como uma caixa isolada do exterior, isto é, pode ser integrado em aplicações diferentes de forma independente, nomeadamente em formulários de Urbanismo, Sistema de Gestão de Águas (SGA), Sistema de Gestão Documental (SGD) e Sistema de Gestão de Faturação (SGF) e outros que possam vir a existir, no futuro. Esta arquitetura permite retirar toda a lógica de negócio aos funcionários dos municípios, dado que para eles se torna muito simples configurar um formulário com pagamento eletrónico.

A introdução do sistema de pagamentos eletrónicos na panóplia de produtos da AIRC abre um novo nicho de mercado para a empresa. As necessidades dos seus clientes foram assim supridas e cada município pode prestar melhores serviços aos seus munícipes, porque a emissão e liquidação de uma taxa ou licença deixou de implicar a deslocação ao balcão de atendimento da câmara municipal, para passar a ser um processo simples, rápido e cómodo.

Os objetivos traçados para o projeto foram todos cumpridos e, após concluir com sucesso todo o processo de testes, este módulo foi disponibilizado nas aplicações AIRC.

6.2 Trabalho futuro

A margem de progressão e melhoria do sistema é grande e muitas outras funcionalidades podem ser implementadas, tais como:

- Permitir mais tipos de cartões de crédito;
- Permitir mais tipos de pagamentos, como por exmeplo MbNet e Paypal;
- Permitir emitir múltiplas taxas / licenças através de um formulário;
- Permitir simular o montante a pagar para um lote de taxas / licenças;
- Permitir pagamentos parciais por multibanco;
- Permitir efetuar pagamentos após ação desencadeada por um processo de negócio (BPM).

Referências

Abrazhevich, D. (2001) *Electronic Payment Systems: Issues of User Acceptance.* Janeiro de 2001.

Aigbe, P. & Akpojaro, J. (2014). *Analysis of Security Issues in Electronic Payment Systems.* Dezembro de 2014.

Albertin, A. L. (2000). *Comércio Eletrônico: Um Estudo no Setor Bancário.* Tese de doutoramento apresentada na Faculdade de Economia, Administração e Contabilidade (FEA) da Universidade de São Paulo (USP). São Paulo: FEA / USP.

Asokan, N., Janson, P., Steiner, M. & Waidner, M. (2012). *Electronic Payment Systems.* IBM Research Division, Zurich Research Laboratory. Novembro de 2012.

Associação do Comércio Eletrónico em Portugal & Netsonda. (2012) *Comprar na Internet.* Dezembro de 2012.

Au, M. H., Susilo, W., & Mu, Y. (2011). *Electronic cash with anonymous user suspicion.* In proceeding of the 16th Australasian Conference on Information Security and Privacy (ACISP'11). Melbourne, Australia, LNCS, Vol. 6812, 172–188.

Batina, L., Hoepman, J. H., Jacobs, B., Mostowski, W. & VullersP. (2010). *Developing Efficient Blinded Attribute Certificates onSmart Cards via Pairings.* CARDIS, Vol. 6035, 209–222.

Baptista, M. (2005). *e-Government and State Reform: Policy Dilemmas for Europe.* The Electronic Journal of e-Government, Vol. 3, No. 4.

Barradas, J., Lopes, P., Lourenço, J., Fernandes, B., Matos, L. & Caetano, P. (2011). *Mega ePayment - Plataforma de Pagamentos.*

Choobineh, J. & Kini, A. (1998). *Trust in Electronic Commerce: Definition and Theoretical Considerations.*

Comissão Europeia (2003). *The Role of e-Government for Europe's Future. Communication from the Commission to the Council, the European Parliament, the*

European Economic and Social Committee and the Committee of the Regions, Brussels.

Crato, N. (2010). *A Matemática das Coisas*. Gradiva. Fevereiro de 2010.

Crédito ou débito (2015). *Visa ou Mastercard? Qual escolher?*. http://www.creditooudebito.com.br/visa-ou-mastercard-qual-escolher/. Data de acesso: 29 de Novembro de 2015.

Diário da República (2009). Resolução do Conselho de Ministros nº 109. In Diário da República, I Série - N.º 192 — 2 de Outubro de 2009.

Faria, N. (2014). *Batalha dos cartões: marca da Visa é a mais forte, mas Mastercard ganha espaço.* InfoMoney. http://www.infomoney.com.br/minhas-financas/cartoes/noticia/3439151/batalha-dos-cartoes-marca-visa-mais-forte-mas-mastercard-ganha. Data de acesso: 29 de Novembro de 2015.

Ferreira, H. M. C. (2014). *O Estado do E-Commerce nas Pequenas Empresas Portuguesas.* Tese de Mestrado em Gestão de Serviços apresentada na Faculdade de Economia, da Universidade do Porto.

Fitzgerald, J. & Dennis, A. (2005) *Comunicação de Dados Empresariais e Redes*. RJ: LTC.

Guedes, R. E. F. F. (2009). *Comércio Eletrônico: uma realidade ou uma utopia?*. 42f. Trabalho de Conclusão de Curso (Graduação em Administração de Empresas). Universidade São Miguel, Recife, 2009.

Head, M. & Yuan, Y. (2011). *Privacy Protection in Electronic Commerce – A Theoretical Framework.*

Hu, X. e Ma, L. (2010). *A Study on the Hybrid Encryption Technology in the Security Transmission of Electronic Documents*. Isme, vol. 1, pp.60-63. International Conference of Information Science and Management Engineering.

Hun, P. (2008). *Design and Implementation of Secure Electronic Payment System (Client).*

Jie, Z. & Hong, X. (2010), *E-Commerce Security Policy Analysis*. Icece, pp.2764-2766. International Conference on Electrical and Control Engineering. China.

Leavitt, N. (2011). *Internet Security under Attack: The Undermining of Digital Certificates*. Computer, vol. 44, no. 12, pp. 17-20, doi:10.1109/MC.2011.367.

Leitch, S. & Warren, M. (2011). *Ethics and Electronic Commerce.*

Lewis, M. (2014, junho 05). *Ethical Issues Relating to E-commerce.* Linkedin. https://www.linkedin.com/pulse/20140605220127-3101310-ethical-issues-relating-to-e-commerce.

Mega ePayment (2011). *Upgrade de uma loja online.* Fevereiro de 2011.

Neto, A. C. D. (2014). *Engenharia de Software - Introdução a Teste de Software.*

Neto, J. R. & Santos, M. C. N. (2011) *Teste de Software – Uma Introdução e Exemplos.* Outubro de 2011.

Nuernberg, J. C. (2010). *O futuro do comércio eletrónico.* Dezembro de 2010.

Paar, C. (2009). *Understanding cryptography a textbook for students and practitioners*. Berlin London: Springer, 2009.

Patrícia, C. (2012). *Milhões de portugueses adeptos do homebanking*. SapoTek. http://tek.sapo.pt/noticias/internet/artigo/2_2_milhoes_de_portugueses_adeptos_do_i_homebanking_i-1211975tek.html. Data de acesso: 29 de Novembro de 2015.

Redunicre E-Commerce (2014). *Documento de integração de pagamentos com cartão de crédito.* Integration Guide Redunicre E-Commerce.

Relatório SIBS (2012). *SIBS Market Report – Pagamentos Online.* Dezembro de 2012.

Relatório Basef Banca da Marktest. (2011). *Utilização do homebanking triplica em Portugal nos últimos anos*. SapoTek. http://tek.sapo.pt/noticias/internet/artigo/utilizacao_do_i_homebanking_i_triplica_em_portugal_nos_ultimos_anos-1132017tek.html. Data de acesso: 29 de Novembro de 2015.

Sarma, S. E., Weis, S. A. & Engels, D. W. (2003). *Radio Frequency Identification: Security Risks and Challenges*. Cryptobytes, RSALaboratories, Volume 6, No 1, página 2

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms and Source*. Code in C. 2. ed. New York: John Wiley & Sons

Silva, M., Silva, A., Romão, A. & Conde, N. (2003). *Comércio Electrónico na Internet.* Lidel. Lisboa.

Stallings, W. (2003) *Cryptography and Network Security: Principles and Practice*. Third Edition. Prentice-Hall.

Stewart, J., Michael, T. & Chapple, M. (2008). *Certified Information Systems Security Professional Study Guide*. New Jersey, USA: John Wiley & Sons Publication.

Tanenbaum, A. S. (2003). *Redes de Computadores*. 4 ed. Rio de Janeiro – Elsiever.

Torres, P. M. A. G. R. (2012). *Estratégias de e-commerce e o seu impacto na performance empresarial: uma abordagem pelo progresso de criação de valor.* Tese de Doutoramento em Gestão de Empresas apresentada na Faculdade de Economia, da Universidade de Coimbra.

Kurose, J. F. K. W. (2003). *Redes de computadores e a Internet*. São Paulo. AddilsonWeslwy.

Unicre (2012). *Especialistas em cartões de pagamento.* http://www.unicre.pt/site/. Data de acesso: 29 de Novembro de 2015.

Anexo A - Exemplo de código dos testes automáticos ou unitários

```
public void testSimulacaoPagIntranet() throws MyNetErroWsPagamentosEletronicos {
    crtlPagamentosPap.enviarPedidoPap(sessao,formToken,"S",null);//pedido de simulação
    objRespostaServicoPag = crtlPagamentosPap.getObjPap();

    assertTrue(objRespostaServicoPag.getValor().length()>0);
}

/**
 * Metodo que testa a simulação do pagamento para a internet
 * @throws MyNetErroWsPagamentosEletronicos
 */
public void testSimulacaoPagInternet() throws MyNetErroWsPagamentosEletronicos {
    sessao.getToSessao().setSessaoId("internet_"+sessao.getToSessao().getSessaoId());
    crtlPagamentosPap.enviarPedidoPap(sessao,formToken,"S",null);//pedido de simulação
    objRespostaServicoPag = crtlPagamentosPap.getObjPap();

    assertTrue(objRespostaServicoPag.getValor().length()>0);
}

/**
 * Metodo que testa a emissao de pagamentos do tipo presenciais na intranet
 * @throws MyNetErroWsPagamentosEletronicos
 */
public void testEmissaoPagPresencialIntranet() throws MyNetErroWsPagamentosEletronicos{
    TODocumentoSgd doc = preRequisitosDocEmissao();
    sessao.setParametro(CtrlPagamentosPap.ID_DROPDOWN_MODALIDADES,formToken,TIPO_MODALIDADE_PRESENCIAL);//tipo modalidade presencial

    String respostaWebService = crtlPagamentosPap.enviarPedidoPap(sessao,formToken,"E",doc);//pedido de emissao
    RespostaPapDocOnline objRespostaServicoPag = crtlPagamentosPap.getObjPap();

    assertTrue(objRespostaServicoPag.getValor().length()>0 && objRespostaServicoPag.getChave().length()>0 &&
            objRespostaServicoPag.getPathDoc().length()>0);
}
```

Figura 45 – Exemplo de código dos testes unitários / automáticos

Anexo B - Exemplo de código dos testes de integração

```
        String respostaWebService = crtlPagamentosPap.enviarPedidoPap(sessao,formToken,"E",doc);//pedido de emissao
        RespostaPapDocOnline objRespostaServicoPag = crtlPagamentosPap.getObjPap();

        assertTrue(objRespostaServicoPag.getValor().length()>0 && objRespostaServicoPag.getChave().length()>0 &&
                objRespostaServicoPag.getPathDoc().length()>0);
    }

    /**
     * Metodo que testa  a integração emissao de pagamentos do tipo multibanco na internet
     * @throws MyNetErroWsPagamentosEletronicos
     */
    public void testEmissaoPagMultibancoInternet() throws MyNetErroWsPagamentosEletronicos{
        sessao.getToSessao().setSessaoId("internet_"+sessao.getToSessao().getSessaoId());//simula internet
        TODocumentoSgd doc = preRequisitosDocEmissao();
        sessao.setParametro(CtrlPagamentosPap.ID_DROPDOWN_MODALIDADES,formToken,TIPO_MODALIDADE_MULTIBANCO);//tipo modalidade multibanco

        String respostaWebService = crtlPagamentosPap.enviarPedidoPap(sessao,formToken,"E",doc);//pedido de emissao
        RespostaPapDocOnline objRespostaServicoPag = crtlPagamentosPap.getObjPap();

        assertTrue(objRespostaServicoPag.getValor().length()>0 && objRespostaServicoPag.getChave().length()>0 &&
                objRespostaServicoPag.getPathDoc().length()>0 && objRespostaServicoPag.getEntidadeSibs().length()>0
                && objRespostaServicoPag.getRefSibs().length()>0);
    }

    /**
     * Metodo que testa a integração emissao de pagamentos do tipo cartao de credito na internet
     * @throws MyNetErroWsPagamentosEletronicos
     */
    public void testEmissaoPagCartaoCreditoInternet() throws MyNetErroWsPagamentosEletronicos{
        sessao.getToSessao().setSessaoId("internet_"+sessao.getToSessao().getSessaoId());//simula internet
        TODocumentoSgd doc = preRequisitosDocEmissao();
        sessao.setParametro(CtrlPagamentosPap.ID_DROPDOWN_MODALIDADES,formToken,TIPO_MODALIDADE_CARTAO_CREDITO);//tipo modalidade cartão de credito

        String respostaWebService = crtlPagamentosPap.enviarPedidoPap(sessao,formToken,"E",doc);//pedido de emissao
        RespostaPapDocOnline objRespostaServicoPag = crtlPagamentosPap.getObjPap();

        assertTrue(objRespostaServicoPag.getValor().length()>0 && objRespostaServicoPag.getChave().length()>0 &&
                objRespostaServicoPag.getPathDoc().length()>0 && objRespostaServicoPag.getTokenCC().length()>0
                && objRespostaServicoPag.getUrlCC().length()>0);
    }
```


Figura 46 – Exemplo de código dos testes de integração automatizados

Anexo C - Documento relativos aos testes de integração do MyNet com a aplicação SGF

Pagamentos – Integração MyNet/SGF

Testes de integração com as equipas intervenientes

Apresentado por: AIRC

Revisão histórica

Data	Versão	Descrição	Autor
28/07/2015	1.0	Realização do Documento	João Francisco

Índice

1. Introdução

Este documento foi realizado para reportar os testes que foram realizados em conjunto com a equipa MyNet e Financeira. Foram testados casos de possíveis de tratamentos que os documentos submetidos podem sofrer.

2. Dados relevantes para a realização dos testes

Base de dados Informix - bd25_mynettestes;

Versão MyNet - MyNetPortal7_25.06_129.war

Endereço MyNet - http://srvwapp07.mynet.com.pt:10039/wps/myportal/

Endereço Serviços Online - http://easerver.airc.pt/servicosonlineAPP07

Aplicações Utilizadas – MyNet; ADM; SGF; SGT; SCA; TAX

Intervenientes nos testes – Luís Rodrigues; Patrícia Costa; João Francisco; Filipe Queirós

3. Pagamentos – Integração MyNet/SGF

3.1 Caso 1

Submissão via MyNet com tipo de pagamento presencial.

Fatura anulada no SGF.

3.1.1 RESULTADO

Comportamento correto.

3.2 Caso 2

Submissão via MyNet com tipo de pagamento presencial.

No SGF, anulada na totalidade emitindo uma nota de crédito e regularizando os documentos.

3.2.1 RESULTADO

No momento da emissão da nota de crédito o valor a pagar passa a zero e o estado contínua em emitido.

Após regularizar o estado passa ao estado regularizado.

Será necessário aparecer a nota de crédito, na conta corrente? (conforme o que aparece na conta corrente da aplicação)

3.3 Caso 3

Submissão via MyNet com tipo de pagamento presencial.

No SGF, emitida uma nota de débito.

3.3.1 RESULTADO

Adiciona ao valor a pagar o valor da nota de débito. (ex: valor emitido 120, nota de débito de 80 o valor emitido passa a 200)

Será necessário aparecer a nota de débito, na conta corrente? (conforme o que aparece na conta corrente da aplicação)

3.4 Caso 4

Submissão via MyNet com tipo de pagamento presencial.

No SGF, emitida uma nota de débito. E emitida uma nota de crédito na mesma fatura.

3.4.1 RESULTADO

A atualização do valor a pagar fica correto.

Será necessário aparecer a nota de débito, na conta corrente? (conforme o que aparece na conta corrente da aplicação)

3.5 Caso 5

Submissão via MyNet com tipo de pagamento presencial.

SGF efetuado pagamentos parciais à fatura emitida.

3.5.1 RESULTADO

São devolvidos do serviço tantos registos como o número de pagamentos parciais efetuados. O que causa registo repetidos na conta corrente no MyNet.

3.6 Caso 6

Tratamento no SGF de uma fatura com juros de mora

3.6.1 RESULTADO

No detalhe do documento o valor a pagar aparece negativo no montante do valor do juro de mora.

3.7 Caso 7

TAX anular uma guia paga parcial já emitida/regularizada.

3.7.1 RESULTADO

Comportamento correto

3.8 Caso 8

Submissão via MyNet com tipo de pagamento presencial.

TAX anular uma guia que já tinha sido paga.

3.8.1 RESULTADO

Comportamento correto, volta a colocar a guia em estado emitido.

3.9 Caso 9

Submissão via MyNet com tipo de pagamento multibanco, plataforma AMA.

Foi efetuada a emissão da guia.

3.9.1 RESULTADO

Comportamento correto.

Só é possível efetuar pagamentos de valor igual ao emitido.

3.10 Caso 10

Submissão via MyNet com tipo de pagamento cartão de crédito.

Foi efetuado pagamento presencialmente, porque nos serviços online o token de pagamento expirou.

3.10.1 RESULTADO

Comportamento correto.

3.11 Caso 11

Submissão via MyNet com tipo de pagamento cartão de crédito. E anulada nos serviços online.

3.11.1 RESULTADO

Comportamento correto. A fatura alterou o estado no SGF para anulado.

3.12 Caso 12

Submissão via MyNet com tipo de pagamento cartão de crédito.

Foi efetuado pagamento através do simulador de pagamentos da rede unicre.

SGF foi processado na totalidade.

3.12.1 RESULTADO

Comportamento correto.

3.13 Caso 13

Submissão via MyNet com tipo de pagamento multibanco, referência AIRC.

Foi efetuada a emissão da guia.

3.13.1 RESULTADO

Comportamento correto.

Só é possível efetuar pagamentos de valor igual ao emitido.

Anexo D - Scripts de testes dos pagamentos eletrónicos

mynet soluções web

MyNet: Sistema de Pagamentos Eletrónicos

Script de Teste

Apresentado por: AIRC

Revisão histórica do documento

12-03-2015	V0.1	Criação de documento	Filipe Queirós
20-07-2015	V0.2	Atualização do documento	Filipe Queirós

1. Introdução

1.1 Objetivo

O objetivo deste caso de teste é garantir o correto funcionamento do sistema de pagamentos eletrónicos

1.2 Definições, Acrónimos e Abreviaturas

Release – Na aplicação corresponde à versão (obtida na instalação/atualização da aplicação; na aplicação em Ajuda> Acerca).

ERP – Refere-se à sigla da aplicação da AIRC, que é representada por 3 carateres (SIC, SCA, SCE, SGD, SGP, etc.).

N/A – Significa Não Aplicável e deve ser usado nos resultados, sempre que não for possível efetuar uma determinada verificação (por exemplo quando não há atualização/conversão de base de dados).

ERROn – Pode ser utilizado para numerar os erros encontrados nas verificações correspondentes à sequência de instruções do teste, correspondendo o n ao Nº do ERRO (ERRO1, ERRO2);

Resultado Teste – O resultado de um teste corresponde à execução do script de teste e deverá ser apresentado segunda a seguinte nomenclatura NErros_NomeScriptTeste_NomeTestador.

2. Execução do teste

Responsável	
Base de dados / Servidor	
	XX.XX.XXX

3. Script de teste

3.1 Descrição

Para correta execução deste scipt de testes é necessário verificar a configuração de parâmetros no SGF, ADM e MyNet. A configuração destes parâmetros encontra-se explicada no documento "Manual de configuração pagamentos.doc" (D:\SVNRep\Mynet\Testes\Artefactos\MyNet\Pagamentos\ Manual de Configuração Pagamentos.doc).

3.2 Sequência de instruções

Pagamentos presenciais Intranet

P	V	Descrição	Resultado
1		Aceder ao editor de formulários referente a uma taxa/licença e verificar se existe o campo de nome "**Formulário Modalidades Pagamento**"	
2		Adicionar o campo anterior ao formulário	
3		Verificar se o campo inserido contem os campos de **modalidades de pagamento** e o campo de **simulação do montante**	
4		Selecionar o campo de modalidades de pagamento	
	4.1	Escolher o tipo de modalidade de pagamento presencial	
5		Selecionar uma entidade	
	5.1	Verificar se o montante simulado da taxa/licença é mostrado no campo de "**Montante**"	
6		Submeter o formulário	
7		Verificar se foi gerado o documento do pagamento (guia)	
	7.1	Verificar se os dados apresentados no documento são referentes à entidade e valor submetido	
	7.2	Verificar se os marcadores de pagamentos foram colocados no ficheiro gerado	

8		Atualizar a visão 360 da entidade selecionada e verificar se o valor das taxas em divida aumentou de acordo com o valor simulado/emitido	

Pagamentos multibanco via PPAP Intranet

P	V	Descrição	Resultado
1		Aceder a ADM e verificar se a checkbox que indica se os pagamentos integrados com a PPAP (plataforma da AMA) estão ativos	
	1.1	Caso esteja inativa devemos ativar a checkbox	
	1.2	Verificar se as credenciais de comunicação com a plataforma da AMA estão prrenchidas (user, password, endpoint de comunicação, certificado digital de comunicação)	
2		Aceder ao editor de formulários referente a uma taxa/licença e verificar se existe o campo de nome "**Formulário Modalidades Pagamento**"	
3		Adicionar o campo anterior ao formulário	
4		Verificar se o campo inserido contém os campos de **modalidades de pagamento** e o campo de **simulação do montante**	
5		Selecionar o campo de modalidades de pagamento	
	5.1	Escolher o tipo de modalidade de pagamento Multibanco	
6		Selecionar uma entidade	
	6.1	Verificar se o montante simulado da taxa/licença é mostrado no campo de "**Montante**"	
7		Submeter o formulário	
8		Verificar se foi gerado o documento do pagamento (fatura)	
	8.1	Verificar se os dados apresentados no documento são referentes à entidade e valor submetido	
	8.2	Verificar se o valor a pagar, referência e entidade SIBS são apresentados ao utilizador após submissão do formulário	

	8.3	Verificar se os marcadores de pagamentos foram colocados no ficheiro gerado	
9		Atualizar a visão 360 da entidade selecionada e verificar se o valor das taxas em divida aumentou de acordo com o valor simulado/emitido	

Pagamentos multibanco (AIRC) Intranet

P	V	Descrição	Resultado
1		Aceder a ADM (opções -> pagamentos) e verificar se a checkbox que indica se os pagamentos com integração AMA (PPAP) estão ativos	
	1.1	Caso esteja ativo, devemos **desativar** a checkbox	
2		Aceder ao editor de formulários referente a uma taxa/licença e verificar se existe o campo de nome "**Formulário Modalidades Pagamento**"	
3		Adicionar o campo anterior ao formulário	
4		Verificar se o campo inserido contém os campos de **modalidades de pagamento** e o campo de **simulação do montante**	
5		Selecionar uma entidade	
	5.1	Aceder ao formulário configurado	
	5.2	Verificar se os campos inseridos estão presentes no formulário	
6		Selecionar o campo de modalidades de pagamento	
	6.1	Escolher o tipo de modalidade de pagamento Multibanco	
7		Verificar se o montante simulado da taxa/licença é mostrado no campo "**Montante**"	
8		Submeter o formulário	
9		Verificar se foi gerado o documento do pagamento (fatura)	
	9.1	Verificar se os dados apresentados no documento são referentes à entidade e valor submetido	

	9.2	Verificar se o valor a pagar, referência e entidade SIBS são apresentados ao utilizador após submissão do formulário	
	9.3	Verificar se os marcadores de pagamentos foram colocados no ficheiro gerado	
10		Atualizar a visão 360 da entidade autenticada e verificar se o valor das taxas em divida aumentou de acordo com o valor simulado/emitido	

Pagamentos multibanco via PPAP Internet

P	V	Descrição	Resultado
1		Aceder a ADM e verificar se a checkbox que indica se os pagamentos com integração AMA (PPAP) estão ativos	
	1.1	Caso esteja inativa devemos ativar a checkbox	
	1.2	Verificar se as credenciais de comunicação com a plataforma da AMA estão preenchidas (user, password, endpoint de comunicação, certificado digital de comunicação)	
2		Aceder ao editor de formulários referente a uma taxa/licença e verificar se existe o campo de nome "**Formulário Modalidades Pagamento**"	
3		Adicionar o campo anterior ao formulário	
4		Verificar se o campo inserido contém os campos de **modalidades de pagamento** e o campo de **simulação do montante**	
5		Aceder aos serviços online	
	5.1	Fazer login com um utilizador e aceder ao formulário configurado anteriormente	
	5.2	Verificar se os campos inseridos estão presentes no formulário	
6		Selecionar o campo de modalidades de pagamento	
	6.1	Escolher o tipo de modalidade de pagamento Multibanco	

7		Verificar se o montante simulado da taxa/licença é mostrado no campo "**Montante**"	
8		Submeter o formulário	
9		Verificar se foi gerado o documento do pagamento (fatura)	
	9.1	Verificar se os dados apresentados no documento são referentes à entidade e valor submetido	
	9.2	Verificar se o valor a pagar, referência e entidade SIBS são apresentados ao utilizador após submissão do formulário	
	9.3	Verificar se os marcadores de pagamentos foram colocados no ficheiro gerado	
10		Atualizar a visão 360 da entidade autenticada e verificar se o valor das taxas em divida aumentou de acordo com o valor simulado/emitido	

Pagamentos multibanco (AIRC) Internet

P	V	Descrição	Resultado
1		Aceder a ADM (opções -> pagamentos) e verificar se a checkbox que indica se os pagamentos com integração AMA (PPAP) estão ativos	
	1.1	Caso esteja ativo, devemos **desativar** a checkbox	
2		Aceder ao editor de formulários referente a uma taxa/licença e verificar se existe o campo de nome "**Formulário Modalidades Pagamento**"	
3		Adicionar o campo anterior ao formulário	
4		Verificar se o campo inserido contém os campos de **modalidades de pagamento** e o campo de **simulação do montante**	
5		Aceder aos serviços online	
	5.1	Fazer login com um utilizador e aceder ao formulário configurado anteriormente	

	5.2	Verificar se os campos inseridos estão presentes no formulário	
6		Selecionar o campo de modalidades de pagamento	
	6.1	Escolher o tipo de modalidade de pagamento Multibanco	
7		Verificar se o montante simulado da taxa/licença é mostrado no campo "**Montante**"	
8		Submeter o formulário	
9		Verificar se foi gerado o documento do pagamento (fatura)	
	9.1	Verificar se os dados apresentados no documento são referentes à entidade e valor submetido	
	9.2	Verificar se o valor a pagar, referência e entidade SIBS são apresentados ao utilizador após submissão do formulário	
	9.3	Verificar se os marcadores de pagamentos foram colocados no ficheiro gerado	
10		Atualizar a visão 360 da entidade autenticada e verificar se o valor das taxas em divida aumentou de acordo com o valor simulado/emitido	

Pagamentos cartão de crédito

P	V	Descrição	Resultado
1		Aceder a ADM (opções -> pagamentos) e verificar se a checkbox que indica se os pagamentos com integração AMA (PPAP) estão ativos	
	1.1	Caso esteja inativa devemos ativar a checkbox	
	1.2	Verificar se as credenciais de comunicação com a plataforma da AMA estão preenchidas (user, password, endpoint de comunicação, certificado digital de comunicação)	

2		Aceder ao editor de formulários referente a uma taxa/licença e verificar se existe o campo de nome "**Formulário Modalidades Pagamento**"	
3		Adicionar o campo anterior ao formulário	
4		Verificar se o campo inserido contém os campos de **modalidades de pagamento** e o campo de **simulação do montante**	
5		Aceder aos serviços online	
	5.1	Fazer login com um utilizador e aceder ao formulário configurado anteriormente	
	5.2	Verificar se os campos inseridos estão presentes no formulário	
6		Selecionar o campo de modalidades de pagamento	
	6.1	Escolher o tipo de modalidade de pagamento cartão de crédito	
7		Verificar se apareceram no formulários os campos de "**Email**" e "**Telefone**"	
	7.1	Inserir um correio eletrónico válido	
	7.2	Inserir um número de telefone válido	
8		Verificar se o montante simulado da taxa/licença é mostrado no campo "**Montante**"	
9		Submeter o formulário	
10		Verificar se foi gerado o documento do pagamento (fatura)	
	10.1	Verificar se os dados apresentados no documento são referentes à entidade e valor submetido	
	10.2	Verificar se o valor a pagar é apresentado ao utilizador após submissão do formulário	
	10.3	Verificar se os marcadores de pagamentos foram colocados no ficheiro gerado	
11		Carregar no botão para proceder ao pagamento via rede unicre	

	11.1	Verificar se somos redirecionados para a página da rede unicre	
12		Caso cancelemos o pagamento	
	12.1	Somos redirecionados para os serviços online	
	12.2	Verificar se é mostrado a informação sobre o cancelamento do pagamento	
13		Caso efetuarmos o pagamento	
	13.1	Inserir os dados do cartão de crédito no formulário apresentado (CSV, numero de identificação e validade do cartão)	
	13.2	Submeter os dados de pagamento	
	13.3	Verificar os dados apresentados depois de efetuar o pagamento	
	13.4	Completar o processo de pagamento para voltar aos serviços online	
	13.5	Verificar se são disponibilizados informação de sucesso sobre o pagamento efetuado	
14		Após finalizar o processo de pagamento, deve verificar se recebeu um email com o estado do mesmo	

Conta corrente de pagamentos

P	V	Descrição	Resultado
1		Identificar uma entidade	
2		Emitir uma taxa/licença através da modalidade de pagamento multibanco integrado com a PPAP	
	2.1	Aceder à conta corrente e verificar se aparece a licença emitida	
	2.2	Verificar se a taxa/licença emitida está no estado “Emitido”	
	2.3	Verificar se os dados da linha da tabela e detalhes estão corretos	
	2.4	Aceder à plataforma de testes da AMA (https://testepagamentos.portaldocidadao.pt/BackOfficeAMA/transactions/search.aspx) e efetuar a simulação do pagamento	

	2.5	Aceder ao SGF (separador Agentes Externos -> serviços online -> plataforma de pagamentos) e proceder a atualização dos dados e verificar se a taxa/licença que foi paga e passou ao estado “Pago”	
	2.6	Verificar na conta corrente se o estado da taxa/licença passou a pago	
3		Emitir uma taxa/licença através da modalidade de pagamento presencial	
	3.1	Aceder à conta corrente e verificar se aparece a licença emitida	
	3.2	Verificar se a taxa/licença emitida está no estado “Emitido”	
	3.3	Verificar se os dados da linha da tabela e detalhes estão corretos	
	3.4	Aceder ao SGF (área de trabalho) e procurar a taxa/licença emitida	
	3.5	Efetuar o pagamento da taxa/licença	
	3.6	Verificar na conta corrente se a taxa/licença passou ao estado “Pago”	
4		Emitir uma taxa/licença através da modalidade de pagamento cartão de crédito	
	4.1	Aceder à conta corrente e verificar se aparece a licença emitida	
	4.2	Proceder ao pagamento da taxa/licença emitida	
	4.2.1	Verificar se o estado da taxa/licença passou a “Pago”	
	4.2.2	Verificar nos detalhes se temos disponível a guia de pagamento	
	4.3	Proceder ao cancelamento da taxa/licença emitida	
	4.3.1	Verificar se o estado da taxa/licença passou a “Anulado”	
	4.4	Verificar se os dados da linha da tabela e detalhes estão corretos	

5		Comparar os dados do formulário de detalhes com a mesma taxa/licença na aplicação SGF	
6		Comparar a integridade dos dados da conta corrente, com os dados no SGF	

Anexo E - Proposta de estágio

PROPOSTA DE ESTÁGIO

Mestrado em Informática e Sistemas

Ano Letivo de 2014/2015

TEMA

Sistema de Pagamentos Eletrónicos

SUMÁRIO

Desenvolver um sistema de pagamentos eletrónicos integrado com a aplicação de taxas da AIRC e a plataforma de pagamentos da AMA de forma a oferecer a uma câmara municipal a possibilidade de os munícipes emitirem e pagarem os seus serviços, tendo opção por vários tipos de pagamentos, tanto na Intranet e Internet.

1. Âmbito

Os sistemas de pagamentos são complexos, regidos por legislação e regras de segurança que assumem uma grande importância. As câmaras municipais necessitam de uma solução que lhes permita oferecer a possibilidade de os seus munícipes pagarem os serviços sem haver a necessidade de deslocamento, uma solução prática, desmaterializada e segura. Pretende-se que todos os trâmites do processo de pagamentos sejam claros e transparentes, tanto para os gestores como para o munícipe.

2. Objetivos

Os objetivos do estágio passam por cumprir um determinado conjunto de tarefas que se consideram necessárias para uma boa integração na equipa de desenvolvimento de *software* da AIRC. Estabelecem-se os seguintes objetivos:

- Investigação sobre a área de negócio (pagamentos eletrónicos);
- Definição e controlo dos intervenientes de cada etapa dos pagamentos;
- Implementar área de administração de pagamentos eletrónicos;
- Implementar tipos de pagamentos para Internet e Intranet;
- Implementar processo de pagamentos eletrónicos genérico a todos os formulários;
- Definir layout dos pagamentos eletrónicos;
- Implementar área de conta corrente do munícipe;

3. Programa de trabalhos

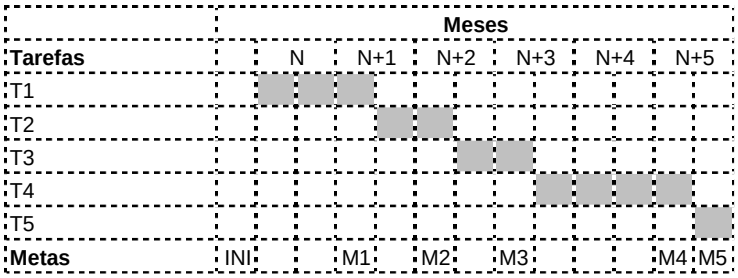
Para além das actividades ocasionais, deverá ser cumprido o seguinte plano de actividades para o desenvolvimento da camada de software de integração:

- ***T1*** – Formação e Análise – Aquisição de conhecimentos nas ferramentas de desenvolvimento identificadas para a elaboração do projecto e identificação das funcionalidades a implementar.

- ***T2*** – Desenho – Apresentação de soluções de acordo com as necessidades recolhidas.
- ***T3*** – Implementação – Construção dos âmbitos identificados, considerando a definição e criação das diferentes fases de produção.
- ***T4*** – Testes e Validação – Execução de testes para validação das tarefas desenvolvidas.
- ***T5*** – *Deployment* – Disponibilização dos resultados.

4. Calendarização das tarefas

As Tarefas acima descritas, incluindo os testes de validação de cada módulo, serão executadas de acordo com a seguinte calendarização:
O plano de escalonamento dos trabalhos é apresentado em seguida:



INI		Início dos trabalhos
M1	(INI + 6 Semanas)	Tarefa T1 terminada
M2	(INI + 10 Semanas)	Tarefa T2 terminada
M3	(INI + 14 Semanas)	Tarefa T3 terminada
M4	(INI + 22 Semanas)	Tarefa T4 terminada
M5	(INI + 24 Semanas)	Tarefa T5 terminada

5. Horário e Local de trabalho

AIRC
Parque Industrial de Taveiro, Lote 48, Apartado 2
3045-503 Coimbra

Horário: Segunda a Sexta das 09:00 às 13:00 e das 14h00 às 18:00

6. Metodologia

Deverá, atempadamente, ser elaborado um dossier de projecto onde constarão os diversos artefactos e tarefas executados na elaboração do trabalho, bem como das decisões tomadas nas diversas reuniões de acompanhamento.

7. Orientação

ISEC:

Nome:
Categoria:

Entidade de Acolhimento:

Nome: Jorge Manuel Dias Coimbra (jorge.coimbra@airc.pt)
Cargo: Diretor de Desenvolvimento