INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA INFORMÁTICA




Fleet Management

PEDRO ALEXANDRE FERREIRA MIRRA
Outubro de 2016

POLITÉCNICO
DO PORTO

INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA INFORMÁTICA




Fleet Management

PEDRO ALEXANDRE FERREIRA MIRRA
Outubro de 2016

POLITÉCNICO
DO PORTO

Instituto Superior de Engenharia do Porto

Fleet Management

Pedro Alexandre Ferreira Mirra

Dissertação para obtenção do Grau de Mestre em Engenharia Informática, Área de Especialização em Sistemas Computacionais

Orientador: Paulo Baltarejo Sousa

Co-orientador: Hugo Anstett

Porto, Outubro 2016

Dedicatória

À minha esposa, aos meus pais e à minha irmã que sempre estiveram ao meu lado neste percurso, por fim, a mim próprio, que nunca desisti mesmo com várias pedras no sapato.

Resumo

O mercado de sistemas de gestão de veículos automóveis tem vindo a crescer substancialmente, bem como a implementação e diversificação das suas funcionalidades. O mercado começa cada vez mais a evoluir para as pequenas e médias empresas, que a cada dia que passa sentem mais a necessidade de controlar os custos com a sua frota.

Os custos são de fato importantes para qualquer empresa e seu respetivo gestor de frota, no entanto vários outros aspetos entram em conta. A segurança e responsabilidade civil por eventuais danos causados são também fatores importantes na balança, assim cada vez mais as empresas deverão efetuar o controlo de acesso aos seus veículos, nomeadamente, o controlo da sua licença de condução ou até o controlo de alcoolemia.

O sistema proposto neste trabalho baseia-se não somente na parte administrativa da gestão da frota, mas também na parte de cumprimento da lei por parte da empresa, ou seja, a empresa deve garantir que o colaborador apenas conduza os veículos aos quais está habilitado e que as suas faculdades no momento da condução, são as ideais para a prática. O sistema terá então que combinar a teoria com a prática, efetuando não só a gestão de informação de veículos mas também, o controlo de acesso a recursos, neste caso veículos validando assim esse acesso.

Deste modo, após o bom desenvolvimento ou implementação de uma já existente solução, o acesso a veículos poderá ser feito de forma automatizada sem ação por parte do gestor da frota, bem como, grande parte do processo administrativo. Uma primeira abordagem ao mercado será feita, no sentido de apurar se é possível combinar a parte administrativa com o controlo de acessos numa só solução existente, caso contrário é necessário efetuar a montagem de um puzzle. Puzzle esse que deverá assentar sobre a autenticação de utilizadores, verificação de documentos, identificação de chaves e repatriamento de informação automática, de modo a facilitar o trabalho administrativo da gestão da frota.

Palavras-chave: gestão de frota, controlo de documentos legais, licença de condução, acesso a veículos, teste alcoolemia, identificação de chaves, administração automática

Abstract

The Fleet Management Systems market has grown substantially as well as the implementation and diversification of its features. The market starts to be more oriented to small and medium-sized enterprises that need have cost controls within their fleet.

Indeed costs are important for any company and its fleet manager, however several other aspects need to be taken into account. Safety and liability for damage caused by company vehicles are also part of the equation. This means that, more and more companies should make the access control to their vehicles, in particular, the control of employee's driving license or alchool tests.

The proposed system in this thesis is based not only on the administrative part of fleet management, but also on the fulfillment of the law by the company, ie the company must ensure that the employee only leads the vehicles to which it is entitled and that his faculties at the time of driving are ideal for the practice. The system will then have to combine the theorical aspect with the practice, providing not only the administrative informations of veihcles as well as the control of access to resources, in this case vehicles and also validate the access to them.

Thus, after the successful development or implementation of an existing solution, access to vehicles will be a automated process without need of intervention by the fleet manager, as well as much of the administrative process will be automated. A first approach to the market will be made in order to figure out if it is possible to combine the administrative part of fleet management with the access control in one existing Solutions. Otherwise it is necessary to make like a a puzzle that should be based on user authentication , verification of documents, keys identification and automatic load of veihcle's information to the system, in order to make easier the task of the fleet manager.

Keywords: fleet management, control of legal documents, driving license, vehicle access, blood alcohol test, key identification, automatic control

Agradecimentos

Agradecer em primeiro lugar aos mesmos mencionados na dedicatória pelas razões óbvias, em segundo agradecer ao meu orientador, que nunca desistiu de mim e de me fornecer alternativas válidas para a conclusão do meu mestrado. Sem ele, tudo seria bastante mais complicado.

Agradecer por fim, mas não menos importante, a Deus! Obrigado por me dares força em seguir o meu caminho.

Índice

Lista de Figuras

Lista de Tabelas

Acrónimos e Símbolos

Lista de Acrónimos

ACL *Access Control List* (Lista de controlo de acessos)

AD *Active Directory*

AIO *All-In-On*

API *Application Programming Interface*

CCD *Charge-Coupled Device*

DC *Domain Controller*

DTC *Diagnostic Trouble Code*

ECU *Engine Control Unit*

EER *Equal Error Rate*

ERP *Enterprise Resource Planning*

FAR *False Acceptance Rate*

FRR *False Rejection Rate*

FSK *Frequency-Shift Keying*

GINA *Graphical Identification and Authentication*

GPS *Global Positioning System*

ICC *Integrated Circuit Card*

ICR *Intelligent Character Recognition*

IT *Information Technology*

ITF *Interrogator Talk First*

IWR *Intelligent Word Recognition*

KBA *Knowledge-Based Authentication*

LSA *Local Security Authority*

NFC *Near Field Communication*

NT	*New Technology*
NTLM	*NT Lan Manager*
OCR	*Optical Character Recognition*
OCR	*Optical Character Recognition* (Reconhecimento Ótico de Caracteres)
OpenCV	*Open Computer Vision*
OTP	*One-time password*
OWR	*Optical Word Recognition*
PC	*Personal Computer*
PIN	*Personal identification number*
PSK	*Phase-Shift Keying*
RFID	*Radio Frequency IDentification*
SAM	*Security Account Manager*
SAW	*Surface Acoustic Wave*
SC	*Smart Card*
SSO	*Single Sign-On*
TTF	*Tag Talk First*
UC	*Use Case* (Caso de uso)
UE	União Europeia
USB	*Universal Serial Bus*
UV	*Radiação ultravioleta*

1 Introdução

O primeiro capítulo desta dissertação de mestrado pretende ajudar o leitor a enquadrar-se na problemática apresentada, explicando o porquê do surgimento do tema bem como os objetivos que se pretendem alcançar com a dissertação, contribuindo então para a resolução de futuros problemas deste âmbito. Por fim apresenta-se a estrutura do documento.

1.1 Problema/Motivação

Boegli-Gravures SA [73] é uma empresa Suíça com cerca de setenta e cinco funcionários que opera no seio da engenharia mecânica de precisão. Encontra-se divida em três pólos, separados entre eles em aproximadamente 500 metros. O primeiro pólo, conta com os departamentos de *Customer Service / Export*, *Design, Accounting, Quality Control* e *Information Technology - IT Services*. O segundo pólo, denominado pólo de produção, é composto pelos departamentos de *Production*, *Research & Development* & *Engineering*. Por fim o terceiro pólo, é composto pelo *Stock* & *Warehouse* e *Montage*.

Sendo a estrutura assim dividida, torna-se necessário o vaivém constante entre os pólos, pelo que as viaturas da empresa são bastante requisitadas. Em primeiro lugar no que diz respeito ao trabalho quotidiano e em segundo lugar para todas as outras atividades normais de uma empresa (visita a fornecedores/clientes, deslocações relacionadas com o trabalho).

O problema presente nesta dissertação prende-se com a impossibilidade da organização em efetuar um controlo dos seus funcionários respetivamente ao uso das viaturas da empresa.

Segundo a lei Suíça, uma empresa é responsável pelo controlo e validação da admissibilidade dos seus funcionários para conduzirem em vias públicas. Isto é, sendo a empresa sediada na Suíça, esta deve assegurar que quando uma viatura é utilizada fora da empresa, o utilizador/funcionário da mesma tenha nesse dado momento uma permissão válida e não suspensa/apreendida. Assim, um funcionário não deve utilizar um veículo da empresa caso não seja portador de uma licença de condução válida ou esta esteja expirada.

Quando se refere a “não suspensa/não apreendida” significa que o funcionário tem em posse a sua carta de condução e esta não foi apreendida pelas autoridades competentes. Incorrendo legalmente não só o funcionário, mas também a própria empresa, caso o funcionário conduza nesta condição.

Obviamente, este processo pode ser efetuado pelo recurso ao ser humano. No entanto, situando a empresa, percebe-se o porquê da necessidade que este processo se efetue de uma forma automatizada sem necessidade de alocar recursos humanos para a gestão da frota. A utilização das viaturas é bastante elevada e dinâmica sendo os recursos humanos preciosos numa estrutura como esta. Além disso, a empresa tem vindo a crescer substancialmente, pelo que com ela o número de veículos também. Deste modo, a realização desta tarefa por via humana, implicaria quase por certo uma pessoa exclusivamente dedicada a essa tarefa. Além disso, a automatização deste processo seria uma grande vantagem em termos de autonomia e eficiência de trabalho, não só para os funcionários mas também para o gestor da frota automóvel da empresa, pois ambas as partes não precisam de se encontrar a cada vez que algum funcionário necessita de utilizar uma viatura.

1.2 Objetivos

O claro objetivo desta dissertação é sem dúvida conseguir controlar ao máximo o acesso aos recursos, neste caso as viaturas de serviço, ao mesmo tempo que assegura que os seus funcionários cumprem com os requisitos mínimos para conduzir uma viatura ou seja possuírem uma carta de condução válida e que estejam fisicamente aptos.

No entanto, mais objetivos adjacentes a estes surgem por parte da empresa, nomeadamente a rentabilização de recursos, neste caso, os funcionários e as viaturas; flexibilidade na gestão da frota e liberdade; mobilidade aumentada para os seus funcionários e por fim o controlo de custos associado à utilização e manutenção das viaturas.

Por outro lado, esta dissertação espera contribuir para o mercado de *software* com uma abordagem diferente da que se pode encontrar hoje em dia, abordagem essa que será explicada no capítulo de estado da arte. Assim, deverá ser possível, depois desta dissertação, obter uma melhor visão do que deve ser o futuro, não só no que toca a gestão de frota pesada mas também de viaturas ligeiras como também do progresso e necessidade da segurança contida nos documentos legais.

Assim, no sentido de sistematizar o que se pretende com este trabalho existem quatro questões que devem ser respondidas e resolvidas. As questões que se pretendem responder no âmbito deste trabalho são:

P1. Como garantir ao máximo possível, que o utilizador que se apresenta é quem diz ser?

P2. Como efetuar uma verificação do seu documento legal de habilitação de condução?

P3. Que mecanismos devem ser implementados para garantir a entrega e devolução correta das chaves das viaturas?

P4. Como obter informações automaticamente das viaturas a gerir?

Estas quatro questões levam à formulação da questão final:

P5. É possível combinar as soluções de P1, P2, P3 e P4 num só produto?

1.3 Contribuições

O trabalho de pesquisa aqui efetuado pretende contribuir com possibilidades e soluções atuais para a resolução do problema, essencialmente através do produto final. Assim, são várias as áreas que a dissertação lança no mínimo a discussão como a inovação de métodos de autenticação de utilizadores, melhores mecanismos de segurança em documentos legais e até a recusa ou permissão de acesso a dados dos veículos por alguns fabricantes.

A seguir, algumas contribuições concretas desta dissertação são salientadas:

- Propor uma nova abordagem para deteção de documentos legais contrafeitos, nomeadamente cartas de condução;
- Possibilitar uma plataforma capaz e flexível ao nível do modelo de negócio da empresa em questão e país;
- Oferecer um sistema que permita a redução de custos empresariais no que toca a gestão de viaturas;
- Oferecer também uma maior flexibilidade aos seus funcionários, ao nível do gestor da frota e ao nível dos utilizadores da mesma;

1.4 Estrutura do documento

Este documento está repartido em seis capítulos, que por sua vez estão ainda mais repartidos em secções de acordo com a temática a apresentar. Neste presente capítulo é efetuada uma introdução ao problema com vista a enquadrar e ajudar o leitor na perceção exata do problema e abrir foco aos objetivos pretendidos. No segundo capítulo (Estado da arte) é descrito o estado atual das soluções de mercado, que possam preencher os requisitos e objetivos analisando-as segundo as suas vantagens e desvantagens. Seguidamente, no terceiro capítulo apresentam-se os estudos das tecnologias de cada solução apresentada no estado da arte e também de tecnologias que possam ser úteis no caso de necessidade de implementação de uma solução ainda não existente.

No quarto capítulo (Desenvolvimento do protótipo) é efetuada a implementação do *software* de gestão de frota. Entenda-se implementação, a uma eventual escolha e consequente

adequação à empresa ou ao desenvolvimento de um protótipo de base, completamente desenvolvido à medida da empresa.

O quinto capítulo (Avaliação do produto) tem por objetivo efetuar a avaliação e teste do produto implementado, se cumpre definitivamente com os objetivos esperados à partida e fecha com o sexto capítulo, precisamente para constatar possíveis melhorias e progressos futuros a desenvolver, bem como uma conclusão e medição do estudo e trabalho efetuados.

2 Estado da arte

Como é de todo normal, um problema leva a uma motivação, motivação de o solucionar, que por sua vez levará à formulação dos objetivos. Nem sempre todos os problemas que aparecem quer ao nível pessoal quer ao nível profissional têm solução. Não deixa com isso de ser sempre possível a procura pela solução, até que se esgotem todas as possibilidades. Neste caso o problema não pode ser visto através de um único prisma, o prisma da gestão de frota, mas também visto pelo prisma da gestão de sistema tacográficos.

De uma forma genérica as aplicações de gestão de frota de veículos apresentam um conjunto de funcionalidades que estão essencialmente relacionadas com a gestão administrativa da frota. Ou seja, de controlo de quilómetros, controlo de custos de manutenção, agendamento de manutenções, controlo de expirações de *leasings*, controlo das cartas de condução entre outros. Por outro lado os sistemas tacográficos oferecem mais a possibilidade de controlo de acesso aos veículos, controlo exato de quilómetros, ou seja, relacionam-se mais com a gestão técnica da frota. Este tipo de sistemas dispensam a necessidade de introduzir estes dados técnicos manualmente, evitando erros e ações fraudulentas, pois através de interfaces eletrónicas com os veículos conseguem obter várias informações técnicas. Informações essas, muitas das vezes mesmo invisíveis ao condutor.

Deste modo, prevê-se que este problema seja em tudo deveras abrangente. Não se pretende unicamente para a sua resolução, um produto de "Gestão de Frota" mas também de identificação positiva de condutores, ou seja, garantir que o condutor é quem diz ser e está presente quando efetua um pedido de viatura. Também a verificação da autenticidade da carta de condução apresentada é óbvia pelos motivos já mencionados. Além disso, a gestão de frota aqui abordada não é direcionada para veículos pesados mas sim para veículos ligeiros convencionais, que à partida não são portadores de sistemas de controlo e gestão da sua condução, como por exemplo os tacógrafos. No entanto um tacógrafo pode ser adaptado a uma viatura ligeira, visto este se conectar à interface eletrónica da viatura.

Nas seguintes secções deste capítulo estudam-se as possibilidades existentes no mercado atual, enquadrando-as no problema e tentando-se satisfazer os objetivos propostos. Estes objetivos

propostos, como já mencionados na secção 1.2, são globalmente divididos em quatro questões que precisam ser respondidas e satisfeitas.

2.1 Sistema de gestão de frotas

Nesta secção pretende-se estudar soluções de gestão de frota existentes no mercado. Assim um resultado da pesquisa das melhores e mais razoáveis soluções será apresentado. Nas seguintes subsecções irão ser apresentadas dois sistemas de gestão de veículos automóveis. No final desta secção um sumário será efetuado para que seja possível uma análise simples e sucinta das soluções estudadas.

2.1.1 Sistema de gestão de frota Chevin

Nesta subsecção apresenta-se um estudo de uma solução de gestão de frota existente. Após uma pesquisa sobre aplicações de gestão de frota em inglês "*Fleet Management*", esta empresa apareceu bastante referenciada na internet, pois é utilizada por várias e grandes empresas [2]. Chevin [1], uma empresa multinacional, presente em Inglaterra, Estados-Unidos, Austrália e Bélgica, fornece sistemas adequados de gestão de frota e conta já com 25 anos desde o seu começo. Analisando as soluções da empresa, esta propõe duas vertentes do produto, uma versão *Web* e outra versão para o sistema operativo Windows, FleetWave e RoadBase, respetivamente.

Segundo a empresa, RoadBase evoluiu para a solução FleetWave pelas razões que as tecnologias *Web* trazem consigo, como uma maior flexibilidade entre sistemas, uma maior e mais fácil acessibilidade e uma maior simplicidade de instalação do sistema. Além disso, esta considera-a como uma verdadeira aplicação *Web* e não uma aplicação emulada na *Web*, o que a torna fluída e bastante expansível a longo prazo.

De entre os vários clientes da empresa, esta apresenta no seu *website* alguns clientes atuais [2]. De notar GM Motors, New York State Police, Coca-Cola Korea, Louisville Metro County Government entre outros. Nestes exemplos de clientes, tratam-se de frotas enormes e complexas de gestão como por exemplo a polícia de Nova Iorque, que sem dúvida tem uma frota extensiva, não só terrestre mas também aérea e marítima.

Através do estudo da aplicação FleetWave, será possível compreender as suas funcionalidades, características, como também as suas potencialidades e mais-valias na resolução do problema apresentado. Após uma leitura sobre as características da solução, podem-se realçar alguns pontos interessantes, que podem entrar em conta para a solução pretendida do problema. São funcionalidades interessantes que apesar de se prenderem mais com o aspeto administrativo da gestão de frota, são funcionalidades sempre uteis num qualquer sistema de gestão de frota. Apresenta-se então um resumo dessas funcionalidades e características:

- Conformidade de gestão frotas: o sistema permite ser adaptado a diferentes tipos de frota, terrestre, área, marítima.

- Conformidade de gestão de condutores: tal como no ponto anterior o sistema permite a adaptação a diferentes tipos de condutores, gestão de conformidades, exames obrigatórios periódicos, renovações de licenças entre outros.
- Relatórios detalhados da utilização dos veículos de modo a garantir a conformidade de utilização dos veículos em termos de utilização e quilometragem.
- Gestão de garantias presentes nos veículos que levam a uma gestão de fornecedores de serviços: oficinas de mecânica, fornecedores de peças e mecânicos de serviço, levando assim a economias e um seguimento detalhado de intervenções na frota.
- Comunicação possível com diferentes sistemas, nomeadamente *Enterprise Resource Planning* - ERP, fornecedores de combustível, fornecedores de manutenção entre outros.
- Diversos relatórios como o consumo de combustível, quilometragem entre outros.

Por fim, mas não menos importante, visualizou-se a interface gráfica com o utilizador. Trata-se de uma interface gráfica intuitiva com a nova tendência de interface Microsoft (por quadrados) com uma noção de visão global do trabalho/frota, em inglês muitas vezes designado de *dashboard*. A Figura 1 mostra o *dashboard* que serve o gestor da frota, onde vários indicadores e gráficos são apresentados como o custo de combustível por mês por exemplo.

Figura 1 – Interface gráfica do sistema FleeWave

De notar que FleetWave é flexível ao ponto de permitir ao utilizador a criação de campos, cálculos e texto de acordo com as preferências do gestor da frota. Existe também um portal onde cada condutor pode consultar as suas horas de conduções e inserir informação adicional, como por exemplo acidentes.

De notar também, a integração na solução de uma aplicação móvel (para sistemas Android/iOS) com o intuito de melhorar a interação com os condutores.

Na subsecção seguinte estuda-se uma outra solução de gestão de frota semelhante à FleetWave, de modo a que o estudo tenha uma maior visibilidade das possibilidades existentes no mercado.

2.1.2 Sistema de gestão de frota Fleetio

Como anteriormente referido, nesta subsecção efetuar-se-á um estudo sobre uma outra possível solução de gestão de frota. Através da mesma pesquisa efetuada que permitiu a descoberta de FleetWave, foi também possível obter a recomendação da solução Fleetio [3].

Fleetio é uma empresa Inglesa, com sede em Birmingham, que tal como Chevin, fornece uma plataforma semelhante. Apesar de se tratar de uma plataforma mais pequena, tem ainda assim algumas características que podem tornar este sistema interessante. Em primeira mão trata-se de uma solução livre, podendo ser utilizada pelo utilizador sem compromisso, o que torna o sistema mais atrativo à experimentação.

Assim, tal como no estudo apresentado da solução FleetWave, na subsecção 2.1.1, um levantamento das características é necessário ser feito. Este levantamento de características resultou na descoberta de algumas funcionalidades [4] interessantes fornecidas pela solução Fleetio.

Entre as mesmas características já presentes na solução FleetWave, como a possibilidade de gestão da conformidade de condutores e veículos, a execução de relatórios como por exemplo o gasto de combustível, ressaltam a vista outras características que poderão ser exploradas no intuito da satisfação do problema, pois estas características permitem uma flexibilidade e alargamento de requisitos bastante importantes:

- Possibilidade de utilização da mesma em modo *Application Programming Interface* - API em outras aplicações;
- Integração de GPS, permitindo saber as rotas e localização dos veículos;
- Integração com cartões de combustível;
- Integração com sistema de Geotab [56] que permite efetuar leituras do painel ou quadrante do veículo em questão, fornecendo informações sobre os quilómetros, paragens, avarias entre outros.

As características apresentadas permitem que se torne factível a integração desta solução, com a solução global. No que a interface gráfica diz respeito, como se pode verificar pelas Figuras 2 e 3 esta vai de encontro ao que são as novas e modernas interfaces gráficas *Web*. Intuitivas, simples e organizadas. Na Figura 2 é apresentado um *webform* de um exemplo de visualização de uma viatura, *webform* que seria utilizado pelo gestor da frota para efetuar a gestão desta.

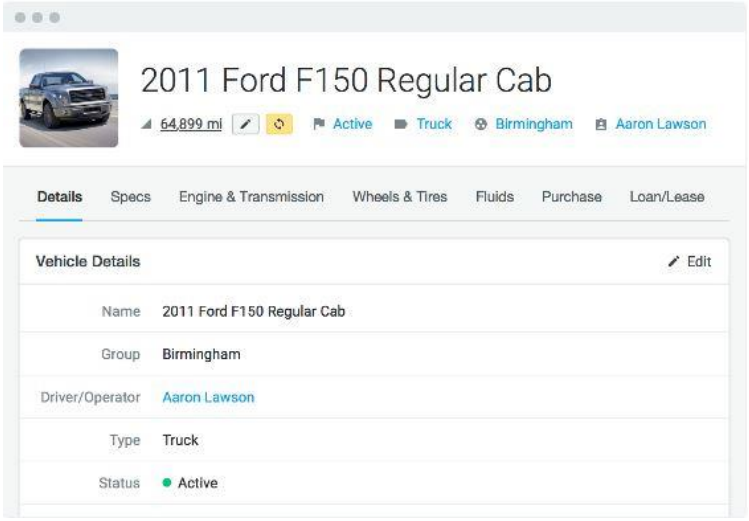


Figura 2 - Imagem de informações de um veículo armazenado no sistema.

De encontro ao que são as características proposta pela solução Fleetio, apresenta-se na Figura 3 um exemplo de uma interface gráfica com o utilizador em que é apresentado o estado atual da viatura previamente selecionada. É possível visualizar-se a localização da viatura através da integração *Global Positioning System* - GPS e também um resumo de anomalias da mesma (*Diagnostic Trouble Code* - DTC).

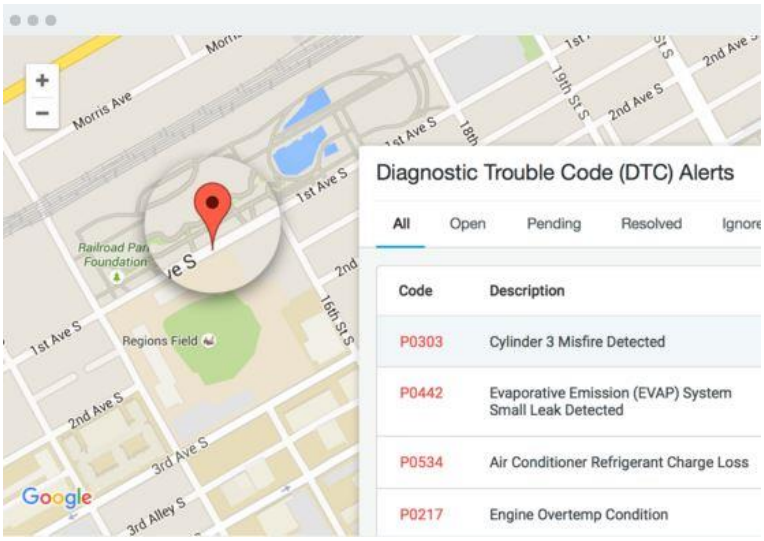


Figura 3 - Imagem representativa da localização do veículo e de anomalias detetadas.

Seguindo para a parte de referências a clientes, tal como efetuado para o sistema Chevin, apresentam-se no *website* da empresa, alguns testemunhos de clientes satisfeitos presentes. No entanto tratam-se de empresas locais, onde é sediada a empresa Fleetio, pelo que não são empresas multinacionais conhecidas.

Por último, uma comparação das diferentes versões de Fleetio deve ser efetuada. Como referido anteriormente, uma das vantagens desta solução é o fato de esta prever a sua livre utilização. Obviamente que uma versão livre não terá contida em si as mesmas funcionalidades da versão paga. Por estas razões é necessário perceber o que cada versão compreende.

Existem três versões do sistema, "*Free*", "*Basic*" e "*Advanced*", tendo este associado um preço de zero, três e 6 dólares por veículo por mês. Obviamente que consoante o preço algumas características estão presentes ou não. Na Tabela 1 é apresentado um resumo das características presentes em cada versão.

Tabela 1 – Características das diferentes versões de Fleetio.

	Free	*Basic*	*Advanced*
Veículos ilimitados	X	X	X
Utilizadores ilimitados	X	X	X
Gestão de serviços	Limitado	X	X
VIN *Decoder*	Máximo 10	X	X
Integração cartões combustível		X	X
Localização GPS		X	X
Acesso à API		X	X
Gestão de Inventário			X
Gestão de avarias			X
Integração *Geotab*			X

Resumindo, trata-se de um sistema de gestão de frota, no sentido real da definição, isto porque não leva em conta apenas a questão administrativa, ou seja, não resolve simplesmente os problemas de introdução de dados no sistema, mas oferece também soluções de monitoramento e alertas em tempo real do veículo, nomeadamente através de sistemas GPS. No entanto verifica-se ainda assim uma maior amplitude e probabilidade de resposta as necessidades do problema. Ao contrário da plataforma Chevin, Fleetion prevê uma maior automatização de processos nomeadamente com a integração da comunicação e gestão de avarias através de uma interface com a viatura (Integração Geotab).

2.1.3 Síntese

A parte final secção levanta e conecta duas ideias bastante distintas, começando a responder à pergunta P4 apresentada na secção 1.2 (Objetivos) do capítulo de Introdução. É necessário num sistema de gestão de frota não só a parte administrativa, como a gestão de utilizadores, custo entre outros mas também é necessária uma integração automatizada entre as viaturas e o sistema. Um gestor de frota deve ter acesso constante a dados das viaturas que apenas só são possíveis de obter se estes forem introduzidos manualmente, pelo que requer uma atenção extra e trabalho longo dependendo do tamanho da frota. Por exemplo, dados das viaturas como quilómetros entre outros, são dados importantes para o gestor de frota por razões óbvias de manutenção e alerta de sobrecargas de utilização. Estes dados podem ser obtidos através de processos automatizados ou inseridos manualmente pelos condutores.

No entanto, uma das motivações presente no problema é precisamente de automatizar este processo, reduzindo a possibilidade de erro e esquecimento.

A próxima secção vai precisamente de encontro ao que são processos automatizados de recolha de informação de veículos. Quer seja informação relativa aos quilómetros efetuados ou até de avarias presentes na viatura.

2.2 Sistemas de Tacógrafo

No seguimento da resposta à pergunta P4 e no encadeamento da última subsecção, que apresentava uma solução, que permitia integrar e automatizar o processo de recolha de dados das viaturas automaticamente, pretende-se nesta secção estudar uma tecnologia com essa potencialidade. A tecnologia em questão, está presente nas viaturas de transporte de mercadorias e passageiros pesados de hoje em dia, denominando-se de tacógrafo.

O tacógrafo tem a função de registar todas as atividades referentes ao veículo. Regista a velocidade, tempo de trajeto, tempo de pausa dos condutores entre outros dados relevantes para um relatório completo e detalhado dessa atividade.

2.2.1 História do Tacógrafo

Segundo Tabouret, Francis [5], os primeiros tacógrafos a surgir tiveram como alvo os meios de transporte ferroviários antes de 1900 como o "*Flaman*" [5], que era utilizado pelas companhias ferroviárias Suíças, apenas com o intuito de fazer respeitar os limites de velocidade aos seus condutores e assim garantir a regularidade e bom desenrolar dos seus trajetos.

Mais tarde nos anos 20 do século passado, apareceram os primeiros tacógrafos para veículos pesados, como é possível visualizar na Figura 4. Estes eram feitos através de discos de papel (Tacógrafo mecânico). Cada condutor era responsável pelo seu disco e isto permitia controlar a conformidade, imposta pela lei Europeia no que diz respeito aos tempos de condução permitidos

Figura 4 – Tacógrafo mecânico e disco condutor papel

Hoje em dia os tacógrafos são obrigatórios em veículos de transporte de mercadorias e passageiros no interior da União Europeia - UE e países signatários [6]. Uma lei internacional define a obrigatoriedade ou não da instalação deste componente. Através da transcrição seguinte em [6] *http://eur-lex.europa.eu/*, é possível obter a informação de quando este deve ser instalado.

> "O regulamento aplica-se ao transporte rodoviário de mercadorias por veículos com uma massa total superior a 3,5 toneladas e ao transporte rodoviário de passageiros por veículos adaptados para transportar mais de nove pessoas (incluindo o condutor).
>
> Independentemente do país de matrícula do veículo, o regulamento aplica-se aos transportes rodoviários efetuados no interior da UE e entre os países da UE, a Suíça e os países signatários do Acordo sobre o Espaço Económico Europeu."

O grande objetivo desta lei e consequente adaptação dos tacógrafos foi de fazer com que os condutores cumprissem as horas de trabalho periódicas permitidas. Obviamente, um condutor não deve conduzir uma viatura indefinidamente, independentemente do seu estado de fadiga entre outros fatores. É necessário que este cumpra os mecanismos de prevenção, evitando em muitos dos casos acidentes rodoviários. Assim de encontro a este objetivo, citam-se algumas leis implementadas pela união europeia [7]:

- Um tempo diário de condução máximo de nove horas. Não mais de duas vezes por semana, este limite pode ser alargado até dez horas;
- Um tempo semanal de condução não superior a 56 horas;
- Após um período de condução de quatro horas e meia, o condutor gozará uma pausa ininterrupta de pelo menos 45 minutos, a não ser que goze um período de repouso;

Assim, estas regras/leis são passiveis de serem verificadas com recurso ao tacógrafo, pois este regista toda a informação necessária para a recolha e leitura e conseguinte verificação.

2.2.2 Tacógrafo Digital

Com a evolução da tecnologia, os tacógrafos mecânicos evoluíram também eles para a era digital. Nos dias de hoje todos os veículos passiveis de aplicação de tacógrafos vêm já equipados com tacógrafos digitais (Figura 5). O sistema de tacógrafo digital é um sistema que conectado através de interfaces eletrónicas ao veículo, permite registar informações do veículo e do motorista como velocidade, tempo, distância, rotações do motor e informações de viagem.

Para isso, cada condutor é munido de uma carta de motorista profissional (Figura 6) contendo um circuito integrado em inglês designa-se este tipo de carta como *Smart Card* - SC que deverá inserir no tacógrafo. Sem esta, não é possível ligar o veículo. Assim através da inserção da carta de motorista, o veículo pode associar todos os eventos importantes ao condutor em trabalho.

Existem também outros tipos de cartões associados ao tacógrafo, com a intenção de controlo de acesso ao recurso, permitindo definir funcionalidades para os diferentes atores no sistema. Após uma pesquisa foi possível obter-se informação acerca de cada um dos intervenientes no sistema e respetivos cartões [8] que passa-se a explicar:

- Cartão de empresa (normalmente associado com um armazenamento sob a forma de USB) que permite ler e descarregar os dados registados no tacógrafo e efetuar sessões de trabalho próprias para cada veículo, ou seja, bloquear certos veículos a certos condutores;
- Cartão de mecânico que permite efetuar a manutenção periódica obrigatória dos tacógrafos (os ateliers de mecânica deverão ser acreditados pela união europeia);
- Cartão de controlador que permite as entidades competentes efetuar o controlo do tacógrafo, por exemplo em operações de controlo rodoviário;

Com a presença destes intervenientes no sistema, várias outras informações são registadas para além das informações de base como a identificação do veículo, distâncias percorridas ou avarias e anomalias. Por exemplo, através do cartão de controlador é possível saber a identidade dos agentes que efetuaram um controlo ao tacógrafo e o condutor, bem como a data e hora. Da mesma forma o identidade do mecânico e da empresa que efetuou o controlo técnico e manutenção periódica obrigatória do tacógrafo é registada, podendo à posteriori ser consultada.

Por todas as informações referenciadas aqui nesta secção, é possível ter-se uma visão completa da atividade do veículo em viagem, permitindo não só por parte das entidades competentes saber se o condutor está a infringir a lei, como permite também às empresas um controlo sobre o trabalho dos seus funcionários e um controlo sobre os seus veículos. Na Figura 5, é possível visualizar um exemplo de um tacógrafo digital. Na Figura 6, é apresentado um exemplo de uma carta de condutor, necessária para a utilização do tacógrafo e viatura.

Figura 5 – Exemplo de um tacógrafo digital

Figura 6 – Imagem de uma carta de condutor profissional

2.2.3 Síntese

Chegando ao fim desta secção uma maior visibilidade sobre a pergunta P4 é obtida e esta pode então ser vista como um objetivo atingível, dado que existem já atualmente mecanismos e sistemas com esse intuito. Existem mecanismos no mercado que permitem satisfazer esse requisito, no entanto, serão esses mecanismos razoáveis no contexto do problema? É mais uma questão que se levanta que será analisada posteriormente, aquando da decisão da escolha da arquitetura e implementação de uma ou partes dos sistemas avaliados neste capítulo.

2.3 Autenticação e Autorização de pessoas

A secção que tem agora início pretende obter informação relevante de modo a que a pergunta P1 possa ser respondida. Essa questão é uma das mais importantes a responder. É fundamental que a solução proposta possa identificar com a maior segurança possível o utilizador, neste caso, o condutor que se apresenta para a utilização de um veículo.

Em sistemas computacionais o processo de autenticação assenta os seus objetivos sob dois pilares fundamentais, o primeiro impedir o acesso a pessoas não autorizadas aos recursos e o segundo assegurar que a pessoa autorizada no sistema apenas tenha acesso aos recursos que realmente necessita. Autenticação prende-se com a identificação do utilizador do sistema e em segundo plano surge autorização que se prende com a verificação que o utilizador identificado tenha permissões e direitos atribuídos de maneira correta [9].

Por exemplo, quando um utilizador pertence a um "*Security Group*" de um domínio Windows, a sua identidade é verificada via um dos vários métodos de autenticação. Após a sua identificação no domínio, o utilizador recebe da parte do sistema um "*access token*" contendo informação sobre os grupos a que este pertence. Assim, quando o utilizador pretender aceder a um recurso, nomeadamente um ficheiro ou impressora, a lista de controlo de acessos em inglês *Access Control List* - ACL desse recurso é verificada contra o "*access token*" do utilizador, fornecendo assim uma autorização ou não a esse recurso.

Numa primeira fase é necessária a identificação do melhor mecanismo de autenticação. Qual é o mecanismo que melhor assegura o não repúdio? Qual é o mecanismo de autenticação com menor taxa de transmissão a terceiros? Sobretudo, qual o mecanismo mais razoável, que mais se adequa neste contexto global, processo e empresa? São estas as questões que esta secção pretende em primeiro clarificar.

Numa segunda fase, é evidente a necessidade da gestão de autorizações de um determinado utilizador e acesso aos recursos. Traduzindo o paradigma utilizador/recursos para o problema, falamos de condutor/veiculo.

2.3.1 Fatores de autenticação

A maneira como um utilizador pode ser identificado e autenticado num determinado sistemas recai sobre três categorias, baseada nos denominados fatores de autenticação. Ou seja, as variáveis que influenciam a autenticação perante o sistema [13].

A primeira categoria de fatores denominada como "fatores de conhecimento" é descrita como algo que o utilizador conhece, como por exemplo uma palavra-passe, um PIN, um padrão ou até mesmo uma resposta a uma pergunta.

A segunda categoria de fatores chamada de "fator de propriedade" é algo que o utilizador tem em sua posse. Um "*Hardware Token*", um "*ID Card*" ou até mesmo um "*Token Software*".

A terceira e última categoria de fatores chamada de "fator de característica" é neste caso algo que o utilizador é, como por exemplo uma impressão digital ou um padrão de retina, mas também pode ser algo que o utilizador faz, como por exemplo sua assinatura.

Estes três métodos formam os pilares básicos de um sistema de autenticação, que podem ser combinados entre eles, formando assim, um nível de segurança mais elevado por se tratar de uma autenticação que depende de mais variáveis para o seu sucesso. Esta combinação de fatores é denominada como "*Two-factor authentication*" ou "*Three-factor authentication*" [11].

Nas subsecções seguintes são apresentados estas três abordagens de autenticação. Começando pela autenticação baseada no conhecimento, de seguida a autenticação baseada na propriedade e por fim a autenticação baseada na característica. O estudo destas três abordagens permitirá verificar a questão número um, no sentido em que se pretende utilizar um sistema com a maior certeza possível, significando isso que os riscos de acesso indevido ou falsificação de identidade devem ser reduzidos ao máximo.

2.3.2 Autenticação baseada no conhecimento

Autenticação baseada no conhecimento em inglês *Knowledge-Based Autethentication* – KBA, é um mecanismo de autenticação que sugere à parte interessada em se autenticar, de fornecer informações privadas conhecidas por este. Estas informações podem ser dividas em dois grupos, informações estáticas que assentam sobre a base de um pré-acordo entre o sistema e o utilizador de segredo partilhado, e as informações dinâmicas que assentam sobre a premissa

de um conjunto de questões que o sistema apresentada, geradas e escolhidas aleatoriamente baseado em informação pessoal [10].

Diga-se que KBA do tipo estático pode basear-se então numa simples pergunta de "Qual o teu nome? E palavra-passe?", como também pode ser usado para que este prove realmente a sua identidade no caso de perda de credenciais, como no método comum de Pergunta/Resposta para reposição de credenciais. Por sua vez, a KBA do tipo dinâmico, não requer que um utilizador forneça respostas a determinadas perguntas previamente estabelecidas. É o sistema que se encarrega de gerar as suas perguntas e resposta baseadas em "data records" compostos por dados públicos e privados, como por exemplo "Qual o valor sua última compra efetuada?", quando um determinado utilizador de *homebanking* aceder a nossa conta bancária. Ou por exemplo "A quem enviou o seu último correio eletrónico?" para que um utilizador possa repor a sua palavra-passe de acesso a sua conta de correio eletrónico.

Estas pequenas perguntas "saídas do nada" tornam difícil a outro que não o próprio que se anuncia a tarefa de autenticação, visto que são questões não só espontâneas, mas também difíceis de saber por alguém que não o proprietário.

Obviamente, nos dois processos é necessário numa primeira fase o anúncio ao sistema, para depois o sistema possa efetuar uma prova desse anúncio. Este anúncio pode ser feito pelo nome de utilizador, ou pelo nome próprio, número de conta, entre outros fatores que possam identificar o utilizador de maneira única no sistema.

2.3.3 Autenticação baseada na propriedade

Autenticação baseada na propriedade, tal como o nome indica é um tipo de autenticação que se baseia em algo que o utilizador tem ao qual se denomina de "*Security Token*". Estes podem ser de variadíssimos tipos nomeadamente *harware* não amovível, *Universal Serial Bus* - USB, *cryptograpfic*, *software* entre outros [14].

Estes *security tokens* são usados para provar a identidade de quem se anuncia eletronicamente, entrando aqui em jogo a autenticação de dois fatores. Normalmente, o utilizador anuncia-se ao sistema através de um nome de utilizador e palavra-passe e de seguida o sistema efetua então a verificação de propriedade. Como por exemplo através da leitura de uma SC [17].

Ao contrário de KBA, um *security token* é um objeto físico que pode ele próprio ser o *token* ou gerá-lo, como por exemplo um *Personal Identification Number* - PIN. Assim surgem dois grupos de *security tokens*, os estáticos e dinâmicos [15].

Nos *tokens* de tipo estático, o aparelho não efetua qualquer cálculo ou computação, o aparelho apenas contem fisicamente escondida a palavra-passe do utilizador e esta é transmitida a cada autenticação. No tipo dinâmico ocorre precisamente o oposto. O aparelho de geração de *tokens* é responsável pela computação/cálculo da palavra-passe.

Para a computação da palavra-passe *token* pode ser usado o simples protocolo de "Desafio-Resposta" em que que o servidor de autenticação pergunta algo e o aparelho deve ser capaz de

responder corretamente ou também as mais recentes *One-time passwords* - OTP. O protocolo utilizado em OTP pode ser visto como um "Desafio-Resposta" no qual o desafio não é enviado pelo servidor, mas sim é publicamente conhecido (como por exemplo o dia e hora atual) [16].

São exemplo de *tokens* dinâmicos do tipo "Desafio-Resposta" os tradicionais métodos de acesso à conta bancária *online* [12], em que o servidor gera um conjunto de números, que introduzidos num aparelho de geração de *tokens* irá dar origem a resposta ao servidor. Como é óbvio, este cálculo e computação envolve o conhecimento do algoritmo de geração e até encriptação destes números por parte do servidor e do aparelho.

Na Figura 7 é apresentado um dispositivo capaz de gerar um *token* de acesso a uma conta bancaria *online*. Neste aparelho esta presente um *token* do tipo dinâmico desafio-resposta em que este se baseia em dados privados nomeadamente o cartão multibanco e respetivo PIN para a geração da pergunta e respetiva resposta (*token*).

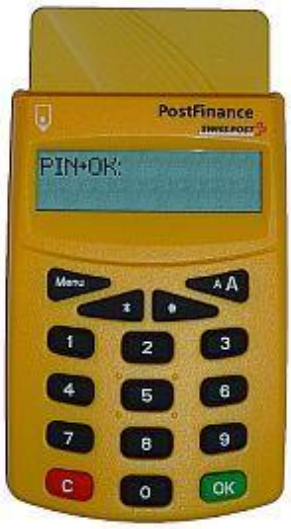


Figura 7 – Calculadora de "*security token challenge-response*" para acesso a "*HomeBanking*" do banco Suíço PostFinance [74].

Este tipo de autenticação baseada na propriedade é utilizado em sistemas de tacógrafo digital, já referidos anteriormente. Os tacógrafos digitais autentificam o condutor segundo o cartão apresentado do tipo SC. Este cartão apresentado, por sua vez contém um segredo estático, logo não há computação, que será passado ao tacógrafo e permitira autenticar o condutor no sistema.

2.3.4 Autenticação baseada na característica

A autenticação baseada na característica, tal como o nome deixa interpretar, é um método de autenticação que se baseia no que o utilizador é ou faz. Surge na literatura como "*inherence*

factors". Este tipo de autenticação é designado no domínio informático como autenticação biométrica [17].

A autenticação biométrica usa então as propriedades biológicas únicas no indivíduo para o identificar e autenticar perante o sistema, que pode ser através da impressão digital, retina do olho, face, palma da mão, voz ou por exemplo a assinatura. A assinatura, que não uma característica física/biológica do indivíduo, é algo que este faz diferentemente de todos os outros. Existem assim dois grandes grupos de identificadores biométricos, os físicos e os comportamentais [17,19].

No grupo de identificadores biométricos comportamentais, pode ser referida a assinatura, o modo de andar (*gait*), a sua voz ou até mesmo o ritmo de escrita em teclados. Este grupo de identificadores tem bastantes limitações por ser justamente algo que pode ser mais facilmente imitável e levar o sistema a ser enganado [20].

No grupo de identificadores físicos apresenta-se um dos mais antigos e populares identificadores, esse identificador denomina-se por impressão digital que trata o reconhecimento do padrão/desenho presente nos dedos humanos, que apresentam pontos característicos presentes na epiderme, mais especificamente as papilas. Designam-se por "pontos característicos" as particularidades papilares, que quando vistas pormenorizadamente oferecem as marcas no seu curso pelo dactilograma natural e pela sua impressão. Estas particularidades são as convergências, desvios, planuras, interrupções, fragmentos, etc. das cristas e dos sulcos [21].

Mas não só, o reconhecimento facial é também um tipo de autenticação biométrica bastante e até vulgarmente utilizado hoje em dia. Basicamente, este método reconhece a face de cada indivíduo através de padrões e distancias entre os diversos pontos de referência da face, como os olhos, orelhas entre outros. Outro identificador biométrico que tem vindo a ganhar terreno, é o reconhecimento da íris. Este identificador é considerado um dos mais exatos métodos de reconhecimento biométrico. Ao contrário da impressão digital, esta característica está menos exposta a degradação devido a sua proteção dentro da córnea [19].

Quais identificadores podem ser usados? A resposta é simples, qualquer um que responde as seguintes propriedades:

- Universal: alguma coisa que qualquer pessoa tem.
- Único: algo que seja diferente de pessoa para pessoa.
- Permanente: algo que se mantenha constante com o passar do tempo.
- Mensurável: algo que possa ser lido e medido.
- Eficiente: rapidez de medição, preciso e robusto.
- Aceitabilidade: por parte do indivíduo.
- Dificilmente imitável ou roubada, levando alguém a enganar o sistema.

Este tipo de autenticação tem ganho bastante peso no mundo atual, pelas razões obvias adjacentes da dificuldade de transmissão, cópia e imitação de alguns identificadores

biométricos. Obviamente existem outras restrições, como por exemplo legais, no que toca ao registo de dados biométricos, o que é compreensível. Uma palavra passe pode ser alterada, um dedo ou um olho torna-se mais difícil.

2.3.5 Síntese

Termina aqui a secção 2.3, relativa aos métodos de autenticação de pessoas em sistemas. Esta secção pretendia estudar os diversos métodos existentes atualmente para a autenticação de utilizadores em sistemas informáticos. Com este estudo pretendia-se responder à pergunta P1, que visa precisamente a autenticação dos condutores no sistema com a menor taxa de erro possível ou acesso fraudulento.

Após esta secção é possível sintetizar os diversos tipos de autenticação e identificar aqueles que mais se enquadram na resolução do problema, ou melhor, na resposta à pergunta P1. O objetivo presente na pergunta P1 não se prende somente com a identificação de um condutor mas também, garantir ao máximo possível o não repúdio por parte deste. Isto significa que o mecanismo de autenticação deve ser o mais exato possível, sem que possa este ser transmitido a outros ou roubado. Obviamente, não existem sistemas 100% seguros, mas existem mecanismos e técnicas que permitem uma maior confiabilidade no sistema. Esta secção respondeu positivamente ao que pretendido, no sentido que existem algumas possibilidades de autenticação de pessoas bastante avançadas e de mais difícil cópia ou roubo.

Existem ainda duas perguntas por responder. A pergunta P2 é a seguinte a ser investigada na secção imediatamente a seguir.

2.4 Identificação de documentos

A pergunta P2, pretende garantir que o condutor identificado e autenticado através dos métodos descritos na secção anterior, estejam na posse de um documento legal que o habilite a conduzir. Este documento legal denomina-se por carta de condução.

A resposta à questão P2 é um dos aspetos fundamentais do sistema, ou seja, um dos objetivos principais do sistema é que este seja capaz de garantir que um condutor não utiliza as viaturas da empresa sem estar na posse da sua carta de condução, sem que seja necessária a intervenção do ser humano. Esta secção pretende estudar diferentes possibilidades de identificação de documentos, satisfazendo o requisito subjacente na pergunta P2.

2.4.1 Contacteless, Contact-type e Hologramas

A identificação de documentos é algo que hoje em dia, é uma área pouco explorada pelos sistemas de informação comuns presentes no mercado. Esta área é mais utilizada pelas organizações governamentais pelas razões óbvias de autenticação e verificação de documentos em fronteiras, departamentos de estado entre outros. Dos vários documentos legais em uso hoje em dia, podem-se identificar alguns com recurso a identificação eletrónica nomeadamente

os passaportes com chip *contactless* ou documentos com chip *contact-type* como o cartão de cidadão português. Estes documentos permitem uma identificação automática do mesmo. Como os próprios nomes indicam, o chip *contactless* ao contrário do chip *contact-type* não necessita de contacto com o leitor como é o caso do Passaporte português e do cartão de cidadão respetivamente [23]. Todos os passaportes eletrónicos, contendo dados biométricos possuem um pequeno símbolo a indicar essa característica. Na Figura 8 é apresentado esse símbolo.

Figura 8 - Símbolo presente em passaportes biométricos [23]

Referindo os passaportes eletrónicos, também conhecidos como passaportes biométricos, estes são a combinação de papel e um pequeno chip com capacidade de armazenamento e uma antena de comunicação, que permite a comunicação sem fio com o leitor. A Figura 9 demonstra com uma melhor perceção a construção e acoplamento de todos os componentes. O chip presente no passaporte irá conter a informação denominada crítica do indivíduo ou seja, dados biométricos (foto, impressão digital, assinatura, íris), de maneira que esta informação é acompanhada de um certificado digital, gerado por uma infraestrutura de chaves públicas, habitualmente pertencentes ao governo. Este certificado digital torna-se difícil e extremente dispendioso de copiar, quando a estrutura que o gera implementa e segue os padrões e normas de segurança [24,26,27].

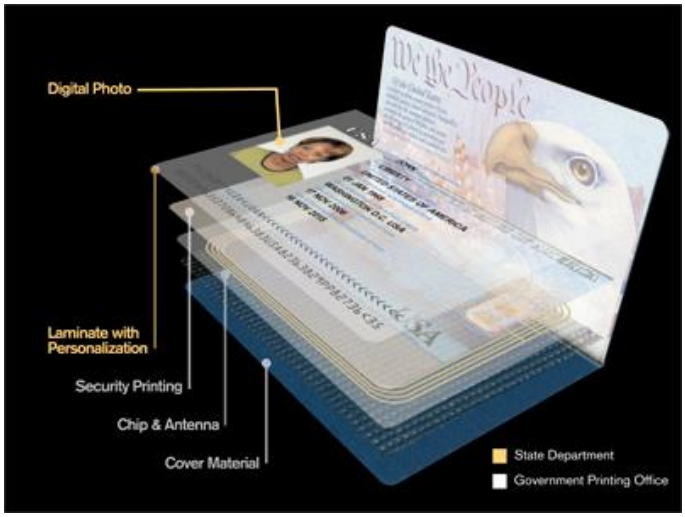


Figura 9 – Imagem representativa da composição do passaporte biométrico [76]

Este tipo de autenticação por chip, de imediato se associa a uma autenticação baseada na propriedade. Através de um passaporte eletrónico por exemplo, e usando mecanismos de encriptação e computação, num leitor de aeroporto, é possível que este detete qual o passaporte apresentado e por conseguinte identifique a quem pertence. Sendo depois tarefa adicional do sistema de reconhecer a pessoa perante o sistema, através de reconhecimento facial como é o caso em vários aeroportos mundiais (*e-Gates*) [30].

Regra geral passaportes eletrónicos usam chips de Comunicação por Campo de Proximidade em inglês *Near Filed Communication* - NFC. Esta tecnologia de pequeno alcance/alta frequência, permite a leitura do chip de até dez cm sensivelmente, tornando-se então uma extensão da norma ISO/CEI 14443, *standard* em cartas de Identificação Radiofrequência (*Radio Frequency IDentification - RFID*). Assim, um passaporte pode ser verificado através de técnicas de reconhecimento ótico de caracteres em inglês *Optical Character Recognition* - OCR e a implementação de uma leitura de RFID tão em voga nos dias de hoje. De notar que os dados contidos no chip NFC, não são somente dados biométricos mas sim todos os dados impressos no passaporte como nome, data de nascimento entre outros. Posto isto, e comparando os dados do chip como os captados através da tecnologia OCR e por fim com um reconhecimento facial do indivíduo que se apresenta com o passaporte, é possível verificar a identidade e autenticidade do indivíduo em causa, uma vez que uma foto do detentor do passaporte é guardada no chip NFC. Obviamente que o método de reconhecimento biométrico depende dos dados biométricos presentes no passaporte [28,29,31].

Já no caso do cartão de cidadão ou no cartão de condutor o princípio é o mesmo, com a diferença que o chip necessita de estar em contato com o leitor para comunicar com este. No exemplo do cartão de cidadão, este é composto por um chip integrado em inglês *Integrated Circuit Card* – ICC. ICC é o mesmo que SC. Este tipo de chip está também presente em cartões de telemóvel, cartões bancários e em outros variados sistemas de autenticação, onde são guardadas diversas informações consoante a aplicação em causa [32].

Mas não só em chips contendo informação residem os mecanismos de identificação de documentos. Um outro tipo de autenticação de documentos legais pode ser realizado pela impressão nos mesmos de hologramas de segurança. Estes hologramas nem sempre são vistos a olho nu pelo ser humano, por vezes é necessário recorrer a determinados focos e tipos de luz. Este tipo de elemento de segurança é difícil de falsificar pelas razões óbvias de complexidade e custo da tecnologia de fabrico. De referir também que um holograma não é possível de ser digitalizado, fotografado ou copiado, o que evita em principio, a sua reprodução fraudulenta.

O princípio de fabrico deste elemento baseia-se na sobreposição de níveis de imagens, que serão visíveis ou não segundo o angulo de visão e por vezes também visíveis somente com determinados focos e cor de luz como é caso de hologramas impressos com tinta invisível. Estes últimos, apenas conseguem ser visualizados com recurso a uma fonte de luz ultravioleta - UV, como é possível visualizar na Figura 10. Pode-se através deste método de autenticação tentar explorar o campo de reconhecimento de padrões, ou seja, extrair o padrão presente num documento que se saiba original, para de seguida se comparar com documentos futuros [33].

Figura 10 – Holograma apenas visível após incidência de uma fonte luminosa UV [75].

2.4.2 Síntese

Nesta secção foi explorada a resposta a pergunta P2. Em resumo, pode-se constatar que começam cada vez mais a ser adotadas medidas de segurança eletrónica dos documentos legais. Infelizmente, cartas de condução ainda não são visadas por qualquer tipo de identificação e autenticação eletrónica. Estas estão munidas no entanto estão de pequenos hologramas em formato de padrões. Pode-se definir que a autenticação destes documentos seja feita através de um reconhecimento de padrões (*Pattern Matching*), presentes nesses ditos hologramas de segurança.

A próxima secção abordará a pergunta P3, que tem como objetivo a deteção automática das chaves das viaturas.

2.5 Identificação de chaves de viaturas

A pergunta P3 formalizada no capítulo de introdução tem por objetivo a possibilidade de identificação da chave de uma viatura. Este objetivo sem dúvida permitirá um controlo sobre quem utiliza o quê na verdade. Visto pelo prisma da segurança, um condutor pode requisitar uma viatura e pegar numa outra chave de outra viatura, tornando os dados inconsistentes.

Assim, para que o processo de utilização de viaturas possa ser feito totalmente automatizado, é necessária a garantia por parte do sistema que a boa chave é entregue ao utilizador/condutor e a boa chave é devolvida por esse mesmo condutor. Nesta secção, um estudo sobre a possibilidade de identificação de chaves irá ser realizado bem como a apresentação de possíveis soluções existentes.

2.5.1 Estado atual

As viaturas mais recentes estão munidas com chaves capazes de comunicar com a viatura através de sinais elétricos emitidos sem recurso a cablagem, ou seja, as chaves estão equipadas com um *transponder*. Na gíria comum denominam-se este tipo de chaves como chaves inteligentes, em inglês "*smart keys*" [70]. Esta tecnologia será descrita mais à frente nesta subsecção.

O princípio de utilização de um veículo há muito deixou de ser meramente mecânico com recurso a uma chave simplesmente também ela mecânica. Nos veículos atuais quando o condutor pretende simplesmente abrir a viatura não basta só inserir a chave na fechadura. Um mecanismo de controlo eletrónico é acionado que verifica a autenticidade da chave, efetuado a leitura do chip da mesma. Além disso, também quando o condutor pretende ligar esse veículo a mesma deve entrar em comunicação com a *Engine Control Unit* - ECU. A ECU envia uma pergunta à chave e esta devolve uma resposta. Basicamente a ECU assegura-se que a chave é a correta, através de por exemplo um identificador único de cada chave que é comunicado por esta à pergunta da ECU.

Começam a surgir atualmente viaturas que não necessitam de chave inserida na ignição, isso deve-se precisamente ao fato de estas comunicarem com a ECU através dos denominados *transponders*, e que deixam cair por terra a necessidade da introdução da mesma na ranhura da ignição visto que o controlo pode ser feito unicamente eletronicamente. Nas primeiras versões de *smart keys*, esta necessitava estar na ranhura por razões de comunicação através do meio físico e também por razões de carregamento de eventuais baterias presentes na chave [34,35].

Para que este conceito de s*mart key* seja melhor entendido, é necessário também percebermos o conceito adjacente ao *transponder*.

2.5.2 Transponder

Um *transponder* é um aparelho eletrónico RFID concebido para receber e emitir sinais elétricos sem recurso a cablagem, o seu nome derivou então das palavras *transmitter* e "*responder*" (emissor e recetor). Este dispositivo quando recebe uma chamada pergunta pelo meio de uma onda rádio com uma frequência pré-determinada, responde através de uma outra frequência, isso acontece devido a um conversor interno de frequência. Tornando assim possível receber e enviar sinais simultaneamente, caso contrario, chocariam.

A primeira utilização de um *transponder* data da segunda Guerra Mundial, presentes em aviões, permitia aos pilotos indicar aos operadores de radar que eram um avião da força amiga. Estes primeiros eram composto por um chip eletrónico que tinha memória não volátil e uma bobine enrolada em volta deste, que sendo assim não necessita de energia constante para retenção da informação [36,37].

Existem dois tipos de *transponder*:

- Elétricos: que permitem um maior alcance como é o caso de uso destes em satélites e aviões. Porem estes requerem bastante energia e própria para operarem. Emitem o seu sinal em *broadcast*, o que significa que não esperam por serem interrogados para transmitir a sua informação.

- Magnéticos: estes são chamados de natureza passiva, ou seja, não necessitam de energia constante para operarem, logo não necessitam de uma fonte de energia própria, no entanto devido a esse fato, a distância de alcance é bastante reduzida (1 a 15 centímetros) pois é o leitor de RFID que fornece a energia ao *transponder* para que este possa operar. Funcionam na gama de frequências de 125 kHz, e por se tratarem de sinais radio frequência, não precisam estar diretamente visíveis [37,38].

2.5.3 Transponders em chaves de viaturas

As primeiras chaves que continham um *transponder* eram basicamente, como já descrito anteriormente, compostas por uma bobina enrolada em torno do chip. Quando o veiculo, mais precisamente a ECU, recebe a informação para se ligar, este envia um sinal eletromagnético através da ignição, que por sua vez é absorvido pela bobine. A bobine através deste campo de energia aciona o chip para a emissão de um sinal. Este sinal normalmente é uma sequência alfanumérica que corresponde a um código de identificação da chave. De seguida é responsabilidade da ECU de verificar este código e aceitar ou não ligar o motor [40,41].

A necessidade principal dos fabricantes automóveis era de evitar o roubo facilitado de viaturas. No entanto, com o evoluir das tecnologias estas foram sendo adaptadas e aproximadas cada vez mais do conforto quer das oficinais dos fabricantes quer dos proprietários. Hoje em dia não é só o código de identificação da chave que é registado na chave mas as mais variadíssimas informações como quilómetros, serviços efetuados, serviços a efetuar, estado da viatura, alarmes entre outras tão pertinentes para que o simples mecânico da oficina apenas precise da chave do proprietário para verificar os primeiros dados de base da viatura [40]. É sob este conceito que assenta o significado de *smart key*. A Figura 11 mostra um exemplo de um leitor de chaves utilizado pelos concessionários da marca BMW.

No entanto, não só informações pertinentes para o concessionário são armazenadas, também do ponto de vista do proprietário algumas informações são registadas na chave nomeadamente a posição do banco, as emissoras de radio preferidas, a intensidade do ar condicionado, a língua da computador de bordo entre outras. Em suma, se duas pessoas partilham um carro, imediatamente se percebe a razão destas informações numa chave por parte dos fabricantes, o conforto do cliente.

Figura 11 – Imagem representativa de um leitor de chave BMW, utilizada pelas oficinas [71].

Obviamente, que a evolução dos *transponders* e tecnologias de comunicação sem fios ajudaram a realizar este passo, mas sobretudo a culpa maior deve-se à evolução eletrónica e computacional presente numa viatura. Cada vez mais uma viatura não deve ser só vista no prisma e paradigma mecânico, devendo também ser contemplado o prisma eletrónico e informático. Qualquer viatura nos dias de hoje, tem associada eletrónica e computação desde a simples abertura de portas, até ao sistema de Navegação GPS e *Web*.

2.5.4 Síntese

O fim desta secção acaba por responder à última pergunta ainda em aberto, a pergunta P3. Através do estudo realizado nesta secção é completamente viável que as chaves atuais de viaturas possam ser identificadas, através de um identificador único contido no seu chip interno.

No entanto, esta possibilidade é algo um pouco distante da realização visto não haver abertura por parte dos fabricantes para o fornecimento de informações acerca de como efetuar a leitura das mesmas. Esta posição por parte dos fabricantes é completamente compreensível, visto nas chaves estarem guardados dados essenciais que permitem abrir e ligar uma viatura.

2.6 Sumário do capítulo

Neste capítulo foi possível obter uma resposta positiva às perguntas (P1-P4) formuladas na introdução. Uma abordagem separada ao problema, permitiu uma melhor compreensão das áreas e consequente melhor estudo de cada. Apresenta-se novamente a seguir as perguntas formuladas e respetivas respostas:

P1. Como garantir ao máximo possível, que o utilizador que se apresenta é quem diz ser?

a. Na autenticação biométrica reside uma maior confiabilidade. É o método de autenticação mais difícil de copiar e deste modo, de o utilizar de maneira indevida. Se o sistema pretende garantir ao máximo que o utilizador é quem diz ser, autenticação por conhecimento ou propriedade devem ser evitadas pois palavras-passe e cartões RFID são infelizmente no mundo do trabalho, facilmente utilizadas por vários.

P2. Como efetuar uma verificação do seu documento legal de habilitação de condução?

b. Em relação a cartas de condução o único método viável será a do reconhecimento dos padrões impressos em forma de holograma, visto ser um documento que não possui qualquer tipo de chip.

P3. Que mecanismos devem ser implementados para garantir a entrega e devolução correta das chaves das viaturas?

c. Foi também possível saber através do estado da arte que as chaves automóveis de hoje em dia possuem um chip interno com um determinado identificador que as distinguem umas das outras.

P4. Como obter informações automaticamente das viaturas a gerir?

d. Através do estudo de soluções de mercado de gestão de frota foi verificado que existem algumas soluções que oferecem um interface com a eletrónica do veículo e consequentemente, permitem a recolha de informações pertinentes do mesmo. Nomeadamente a solução Fleetio e os tacógrafos digitais.
e. Por outro lado a questão número P3 permitiu também provavelmente responder a esta questão, visto que as chaves das viaturas hoje em dia não só contem o tal identificador único que as distinguem entre elas, como também armazenam vários dados relativos ao veículo.

No entanto, a resposta à pergunta final P5 não pode ser satisfeita. Ou seja, não existem soluções atuais no mercado que permitam englobar numa só solução os quatro requisitos representados pelas perguntas em cima respondidas. Um sistema que aborde as várias tecnologias deve ser implementado, por ventura aproveitando partes de soluções já desenvolvidas como por exemplo a autenticação biométrica através de um componente e *Application Programming Interface* - API externos.

No próximo capítulo, irão ser aprofundadas as tecnologias por detrás das soluções apresentadas passiveis de serem integradas numa solução global. A boa compreensão destas irá proporcionar não só um melhor desenho da solução como também um melhor compromisso com as boas práticas da engenharia de *software.*

3 Tecnologias

O capítulo presente pretende, após o levantamento do estado da arte e consequente estudo das possibilidades, um estudo das tecnologias utilizadas nessas soluções que farão parte da solução final. Será portanto um capítulo que visa estudar e avaliar as possíveis características da solução a implementar.

Nas próximas secção, as tecnologias com potencial de integração na solução final serão aprofundadas de maneira a obter mais conhecimento sobre as mesmas e facilitar não só a implementação mas também utilização.

Nas primeiras duas secções irão ser abordadas tecnologias de autenticação em sistemas, seguidas de tecnologias de leitura de *transponders* e por fim, tecnologias de reconhecimento de texto e padrões. Estas tecnologias serão fundamentais para a boa compreensão e implementação do sistema final.

3.1 Integrated Windows Authentication

A autenticação por via do utilizador Windows (*Integrated Windows Authentication*) é algo já bastante utilizado nas aplicações de *software* dos dias de hoje. As aplicações aproveitam a existência de um possível existente domínio e consequente autenticação do utilizador no mesmo para a utilizarem posteriormente na aplicação.

Assim, após o utilizador iniciar sessão no domínio, este recebe como que um *token* que pode ser utilizado posteriormente para se identificar em outras aplicações. Com este *token*, o utilizador deixa de necessitar de rescrever as suas credenciais de autenticação como por exemplo: um nome de utilizador e palavra-passe. É necessário no entanto perceber como o processo de autenticação num domínio/AD funciona para que o *output* do mesmo seja passível de reutilização.

3.1.1 Interactive Logon

A partir da versão NT 4.0 de sistemas Windows, tornou-se obrigatório aos utilizadores se identificarem perante o sistema para acederem ao computador em questão. A este processo é chamado de autenticação. Assim, o sistema servidor controla a utilização de recursos locais e de rede através de mecanismos inter-relacionados de autenticação e autorização. Estes mecanismos entram em funcionamento na segunda fase de autenticação, ou seja, após o utilizador se autenticar no sistema.

De referir que os utilizadores podem ser identificados com recurso a uma base de dados local SAM em inglês *Security Account Manager,* ou com recursos à base de dados num *Active Directory* – AD. Caso um determinado computador esteja adicionado a um domínio, o *login* no computador pode ser efetuado localmente ou através de um controlador de domínio em inglês *Domain Controller* - DC. Caso este não pertença a um domínio então este processo terá de ser sempre local [46].

3.1.2 Processo de login em domínio

O *login* em domínios possibilita o acesso aos recursos em todos os pontos pertencentes ao domínio. Para isso, as contas de utilizador são armazenados num domínio do AD que por sua vez, o é replicado por cada DC.

Antes que um utilizador possa fazer *login* num computador utilizando uma conta de domínio, o computador deve estar associado a um domínio. Logo, se o computador tem acesso à rede, o utilizador pode fazer *login* num domínio se este possuir uma conta de utilizador.

Obviamente, a autenticação do computador em si no domínio é feita transparentemente para o utilizador (*Computer Logon*). Perante o domínio e o AD ambas entidades são consideradas "*equal security principals*" o que significa que estas devem estar identificadas perante o domínio/AD para que o acesso aos recursos se torne possível pelo utilizador.

Resumindo, o processo de *login* de utilizadores num domínio processa-se em primeira instância pela componente *Graphical Identification and Authentication* - GINA, que não mais é que a janela gráfica de introdução de dados de *login* (nome de utilizador e palavra-passe). Esta janela irá então criar um processo novo de *login* que é enviado (ainda localmente) à *Local Security Authority* - LSA. A LSA é então responsável por fornecer esta interface entre a GINA e o repositório de credenciais, encriptando os dados e efetuando verificações de *login*, alterações da conta (como mudanças de palavra-passe) entre outros. Por último a LSA irá também verificar se o processo de *login* em causa, é um processo a ser tratado localmente (SAM) ou um processo de domínio/AD. A Figura 12 apresenta a arquitetura de *login* num domínio.

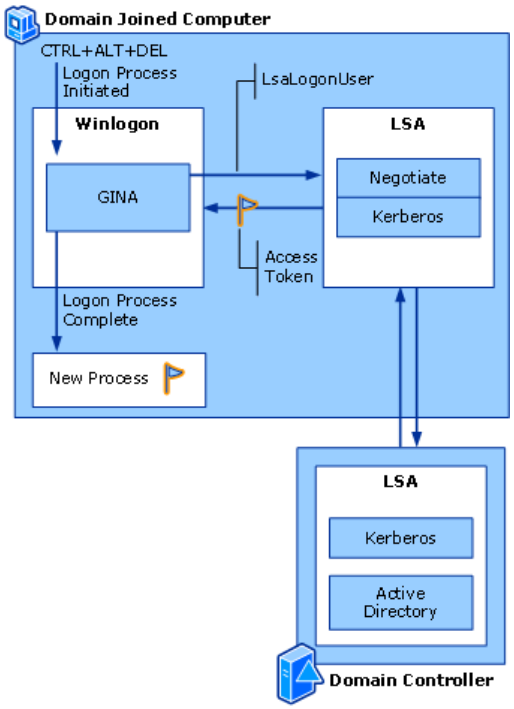


Figura 12 – Imagem representativa de uma identificação e autenticação num domínio [47].

Depois de determinado o tipo de *login*, ou o NT *Lan Manager* – NTLM ou o *Kerberos* validam o utilizador. Se o DC de autenticação está munido com o Windows 2000 ou superior, a LSA irá usar *Kerberos*, a tecnologia padrão de hoje em dia. No entanto a LSA pode escolher NTLM para processar *login* de domínio em versões de Windows NT 4.0 mistos [47].

3.1.3 Single Sign On

O método *Single Sign On* – SSO, como o próprio nome indica, é um método que permite a um utilizador aceder a diferentes recursos utilizando uma só identificação. Deste modo o método SSO usa as credenciais recebidas durante o processo de *login* interativo de domínio neste caso, para permitir que o utilizador se identifique na rede uma só vez e ter acesso a todos os recursos autorizados sem autenticação adicional. Os recursos de rede podem variar de dispositivos de *hardware*, como impressoras, para aplicações, ficheiros e outros tipos de dados, os quais podem ser localizados em toda a empresa em servidores de vários tipos, possivelmente em diferentes domínios e executando sistemas operacionais diferentes.

3.2 Autenticação íris

De entre todos os identificadores biométricos, como impressão digital, reconhecimento facial, geometria da mão, íris, retina entre outros, o identificador íris é um dos mais eficazes. A parte da íris de um olho é a parte colorida como mostra a Figura 13, esta parte é diferente de um olho para o outro da mesma pessoa e mesmo em gémeos as retinas são diferentes.

A íris tem diferentes características que sofrem mutação entre diferentes pessoas, a primeira e mais visível denomina-se malha trabecular. A malha trabecular dá um aspeto de divisão radial desta mesma, e é formada apenas com oito meses de gestação. Assim, para além de ter a vantagem de ser formada antes no nascimento da pessoa, tem também a vantagem de se manter a mesma durante toda a vida, não alterando com a idade. Outra vantagem da íris é que esta esta bem protegida quer pelas pálpebras quer pela córnea, estando pouco sujeita a danos. Também de referir, que o uso de lentes de contato ou óculos não tem interferência com a tecnologia de reconhecimento atual [20]. Na Figura 13 apresenta-se a representação da estrutura de um olho humano.

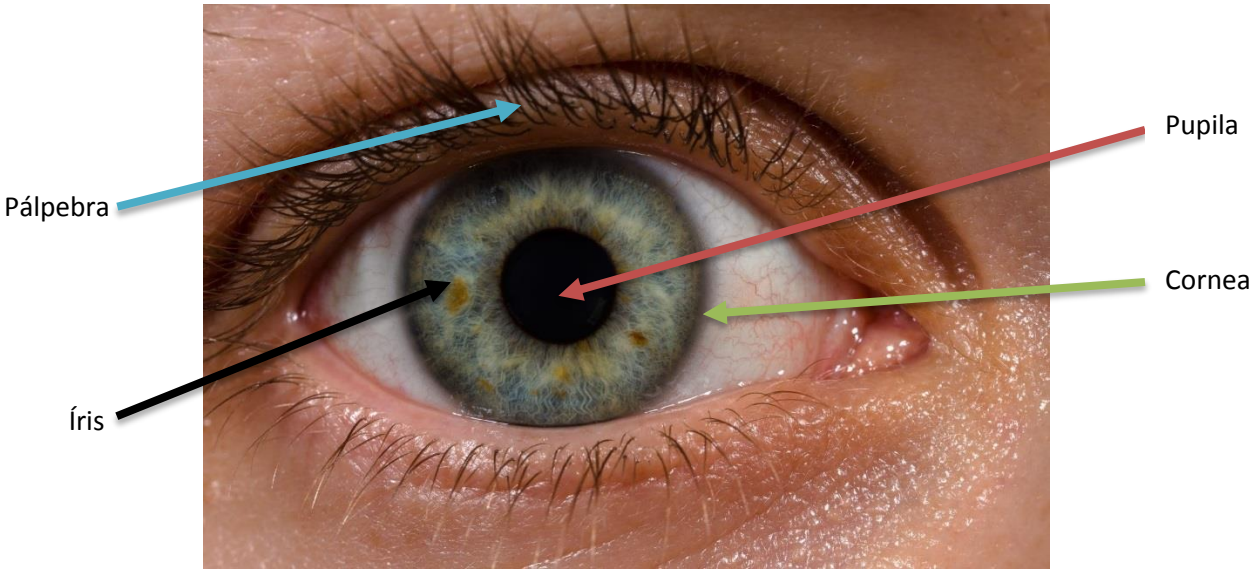


Figura 13 – Imagem de um olho humano.

3.2.1 Processo de reconhecimento

O processo de reconhecimento da íris é subdividido geralmente em três grandes passos. O primeiro passo prende-se com a captura da imagem da íris. Esta imagem pode ser capturada com recurso a uma camara *standard,* usando luz visível ou mesmo usando um luz infravermelha. Este processo pode ser manual ou automático, em que manual a lente da camara deve estar relativamente próxima para conseguir focar o objetivo, e automático em que pode estar um pouco mais afastado. Em modo automático, o que a camara faz, é reconhecer uma pessoa, ou melhor, reconhecer uma face, de seguida localiza os olhos na face e continuamente ate focar e capturar a íris do olho. Obviamente este modo automático torna o processo mais fácil e "*user-friendly*" [48].

Definida a localização da íris, esta precisa ser capturada com o melhor foco e qualidade de imagem. A aquisição de imagem da íris, por ser o primeiro passo do processo, torna-o fundamental. Uma má resolução e qualidade da imagem captada pode comprometer o desenrolar do processo. Sabendo que a íris é uma pequena parte do olho humano, com cerca de 1cm de diâmetro, a distância entre a camara e o olho deve ser reduzida de modo a que o foco seja o melhor. Segundo o Instituto CASIA [59], organização Chinesa especializada em

trabalhos de pesquisa na área da biometria, camaras CCD – *Charge-Coupled Device* são preferenciais no processo. Camaras CCD são capazes de transformar cada *pixel* da imagem num sinal elétrico, tornando o resto do processo de tratamento mais fácil. Estas, devem ainda seguir as normas ANSI/IESNA RP-27.1-96 e IEC 62471, que são os *standards* de produtos de radiação e laser no âmbito da segurança. Também a aquisição em tons de cinza simplifica o restante do processo [44].

O segundo passo consiste na extração da íris, ou melhor do tratamento da imagem. Para isso a imagem capturada precisa ser analisada, com o objetivo de identificar os limites interno e externo da íris, removendo toda a informação da imagem desnecessária como a pupila, as pálpebras e o resto do olho, resultando desta análise a localização precisa da íris circular e a extração dos valores da mesma [45].

Por fim, após a extração da íris, o último passo será o seu armazenamento para comparação. Este processo divide, filtra e mapeia os segmentos da íris em centenas de vetores (*phasors*). Este processo é também conhecido como 2-D *Gabor*, que pode ser facilmente compreendido como o "quê" e o "onde", da imagem adquirida. Este vetor é chamado de "*IrisCode 512-byte record*" [45,48].

3.2.2 Identificação e Verificação

Um sistema de autenticação biométrico pode proceder de duas maneiras, são elas a identificação ou verificação. Identificação é o processo de tentar encontrar a identidade da pessoa examinando as suas características biométricas [57].

No caso da identificação o sistema é munido com os padrões e características biométricas de todos à *priori*. Assim quando uma pessoa se apresenta ao sistema, este retira o seu padrão biométrico e compara-o contra todos os padrões existentes no sistema, ganhando aquele que se apresenta mais próximo do padrão apresentado mas que se encontre abaixo do nível máximo de diferença definido.

No caso da verificação, o utilizador é indicado à *priori*, e o sistema verifica o novo padrão somente contra esse utilizador indicado. No caso de o novo padrão não exceder o nível de diferença definido pelo sistema de autenticação, este é positivamente autenticado no sistema.

3.2.3 False Acceptance Rate, False Rejection Rate e Equal Error Rate

Os níveis acima indicados são denominados de pontuações ou pesos. Essas pontuações são usadas para expressar a similaridade entre um padrão apresentado e um padrão *template*. O padrão *template* pode ser por exemplo um padrão registado na base de dados biométricos dos utilizadores. Quanto maior for essa pontuação, maior é a probabilidade de o utilizador corresponder a um *template*. Ao mesmo tempo, uma pontuação mínima é definida, porque em verdade qualquer utilizador que se apresenta terá uma pontuação qualquer em relação a um qualquer *template* [57].

Em teoria, a pontuação de um utilizador que é quem diz ser, devia ser sempre maior que um intruso ou impostor, assim um mínimo de pontuação poderia ser definida para distinção entre o grupo de utilizadores verdadeiros e o grupo de intrusos ou impostores. Este mínimo ou limite é denominado com um *threshold*. No entanto na prática nem sempre isto acontece. Por vezes a pontuação do impostor pode ser mais elevada e mesmo com a escolha de um limite o impostor é autenticado [58,57].

Por exemplo, um limite (*threshold*) elevado pode ser escolhido em que realmente nenhum impostor é falsamente aceite pelo sistema. Por outro lado, os utilizadores verdadeiros com pontuações mais baixas que o impostor com a pontuação mais alta serão falsamente rejeitados.

Em oposição ao último paragrafo, um *threshold* baixo pode ser definido de maneira que todos os utilizadores verdadeiros sejam falsamente rejeitados. No então, sendo este *threshold* baixo, o impostor que tenha uma pontuação mais elevada que um utilizador verdadeiro pode ser falsamente aceite [57,58].

Para melhor perceber este conceito, considere-se a Figura 14 que apresenta as pontuações de uma amostra de padrões de impostores e as pontuações de uma amostra de utilizadores verdadeiros.

Figura 14 – Pontuações de impostores e de utilizadores verdadeiros [77]

Como pode ser verificado, existem impostores com maior pontuação que um verdadeiro utilizador, pois ambas as amostras se intersectam.

Assim, a taxa de falsos positivos em inglês *False Acceptance Rate* – FAR é o número de impostores falsamente aceites a dividir pelo número total de impostores da amostra e a taxa de falsas rejeições em inglês *False Rejection Rate* – FRR é o número de utilizadores falsamente rejeitos a dividir pelo número total de utilizadores verdadeiros da amostra. Um falso impostor irá sempre ser aceite, se o sistema tiver um FAR de um e zero se nenhum impostor deve ser aceite, ao mesmo tempo que se o sistema tiver um FRR de zero aceitara sempre os utilizadores verdadeiros e rejeitará a medida que este for crescendo ate um [58].

Resumindo, à medida que FAR diminui e FRR também o sistema funciona de maneira mais exata, sendo o sistema perfeito quando estes atingem zero. Para se ter uma melhor perceção da relação entre as pontuações e FAR/FRR veja-se a Figura 15 a seguir, em que é apresentada a distribuição de FAR e FRR pelas pontuações obtidas.

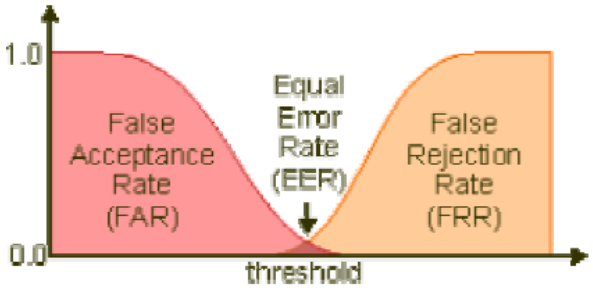


Figura 15 – Representação de FAR e FRR para cálculo de EER [77]

Na Figura 15, pode-se verificar que a taxa de impostores falsamente aceites diminui à medida que a pontuação aumenta, mas que a taxa de utilizadores verdadeiros rejeitados aumenta à medida que uma pontuação mais elevada é estabelecida. Não é possível que um utilizador verdadeiro obtenha em todas as suas comparações a mesma pontuação, pelo que esta varia, por força da luz, da imagem captada entre outros. Assim, à medida que uma pontuação mais elevada é requerida, a taxa de utilizadores rejeitados tende a crescer.

A escolha do *threshold* começa aqui a ser um problema, pois é necessário definir um limite ou uma pontuação mínima que não rejeite os verdadeiros utilizadores e que não aceite os impostores. No entanto, como visto anteriormente as pontuações intersectam-se não sendo possível assegurar que todos os verdadeiros utilizadores serão aceites e os impostores rejeitados. A partir deste ponto entra em então o cálculo do *threshold*. Esse cálculo é efetuado com recurso a FAR e FRR e pretende atribuir iguais hipóteses de sucesso ao sistema de rejeitar impostores e de não rejeitar utilizadores verdadeiros. Essa intersecção chama-se de *Equal Error Rate* – EER e definirá o limite/*threshold* em que essa igualdade acontece, ou seja, em que a taxa de impostores falsamente aceites é igual à taxa de utilizadores verdadeiros rejeitados.

3.2.4 IriShield

A marca Iritech [43] fornece soluções de reconhecimento biométrico pela íris que permitem ser conectados facilmente via interface USB, denominando-se estes produtos de IriShield Series. Existem modelos próprios e preparados a embutir numa solução de *hardware* física através dos seus módulos OEM (como pode ser verificado na Figura 16 e 17) e modelos já devidamente encastrados.

Figura 16 – OEM IriShield MO 2120 EVM [42]

Figura 17 – OEM IriShield BO 2121 [42]

Dentro dos modelos já encastrados, encontram-se o modelo MK 2120U presente na Figura 18 e o modelo BK 2121U presente na Figura 19 sendo o primeiro monocular e o segundo binocular. Ambos são semelhantes nas características, com a diferença que o modelo BK 2121U permite a deteção dos dois olhos ao mesmo tempo e uma distância maior.

Figura 18 – IriShield MK 2120U [42]

Figura 19 – IriShield BK 2121U [42]

Na Tabela 2 apresenta-se uma comparação dos produtos e preços segundo [43].

Tabela 2 – Tabela comparativa da gama de produtos IriShield

	MK 2120U	BK2121U	MO2120	BO2121
Modo de captura	Automático			
Distância de captura (cm)	4.7 – 5.3	13.5 – 14.5	4.7 – 5.3	14-15
Formato de imagem	640*480 8 Bit de escala de cinza			
Resolução	VGA			
Iluminação	LED infravermelho			
Interface conexão e fonte de energia	USB			
Consumo energético	250mA	430mA	250mA	430mA
Preço	189€	445€	179€	330€

Como se pode verificar a partir da Tabela 2, a grande diferença entre os produtos prende-se com a distância necessária entre o olho e a camara bem como a capacidade de deteção de um ou dois olhos simultaneamente. Todos os modelos seguem a norma ISO 19794-6 e IEC 62471 que regulam qualidade e formato da captação de dados biométricos como também a segurança na aquisição de dados fotobiológicos a partir de lâmpadas e camaras respetivamente.

De notar que os produtos IriShield possuem já um SDK a disposição que permite a sua integração em sistemas Windows, Linux, WinCE, Embedded Linux, Android e Mac OS com as linguagens de programação comuns a poderem ser utilizadas como C/C++, NET C#/VB e Java.

3.3 RFID

Não será possível perceber-se a técnica adjacente de *transponders* em chaves de viaturas sem perceber-se a tecnologia RFID. Um *transponder* nada mais é que um identificador RFID em inglês RFID *Tag* que responde a interrogações do meio. Esses *transponders* estão presentes nas chaves das viaturas.

A abreviação RFID significa *Radio Frequency IDentification*. Esta tecnologia consiste num acoplamento eletromagnético ou electroestático na radio frequência permitindo a identificação de um objeto, o seu trajeto, ou as suas características graças a emissão através do meio das suas informações. Hoje em dia, começa a ser utilizada a tecnologia em detrimento de código de barras, tendo como principal vantagem em relação aos códigos de barras a não necessidade de contacto quer físico quer visual pelo *scanner*.

3.3.1 Composição de um sistema RFID

Um sistema RFID consiste então em três partes fundamentais. O emissor-recetor (leitor) a antena e o *transponder* [55]. O *transponder* é então um chip interno, que contem informação a transmitir, ou seja o identificador. Assim, quando a antena recebe um sinal proveniente de uma emissor-recetor (*transceiver*) este é interpretado pelo controlador incorporado no chip que irá desencadear uma ação. A ação pode simplesmente ser um retorno de uma informação para o leitor. Na Figura 20 é apresentada uma esquematização de um sistema de RFID.

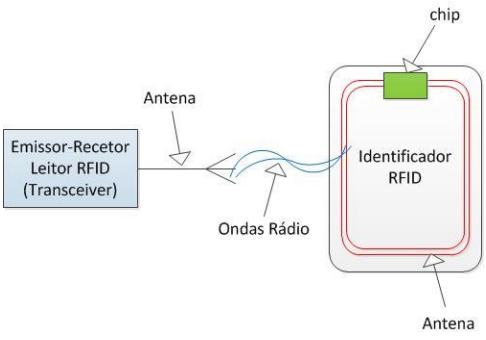


Figura 20 – Representação logica de sistema RFID

3.3.2 Classificação de sistemas RFID

A primeira classificação possível dos sistemas RFID é baseada sobre a presença ou não de um chip eletrónico nos identificadores RFID. De seguida, estes podem ser classificados como ativos ou passivos bem como identificadores de simples identificação ou de funções mais complexas.

3.3.2.1 Chips em Identificadores RFID

Os primeiros RFID no mercado não continham qualquer chip eletrónico. Neste tipo de identificadores encontram-se os identificadores *Surface Acoustic Wave* - SAW, que reagem consoante a onda/energia recebida alimentando ou não partes do circuito a superfície [51]. Esta superfície é composta basicamente por barras acústicas, que consoante essa energia e onda recebida são refletidas ou não. Outro tipo de identificadores sem recurso a chip são os identificadores "*transponder* 1 bit", este tipo de RFID composto por díodos capacitivos é ainda utilizado em sistemas de alarme e antirroubo pois permitem ao interrogador verificar se o identificador RFID está presente ou não no seu campo de ação. A mais recente e utilizada tecnologia, compreende os identificadores RFID composto por um circuito integrado (chip). Este circuito integrado pode ser uma simples "máquina" de estados ou informação como por exemplo uma memória não volátil ou um verdadeiro microprocessador [53].
Como já anteriormente identificado, um *transponder* de uma chave de viatura é claramente classificado como um transponder de chip integrado, visto as chaves armazenarem bastante informação nela.

3.3.2.2 Identificadores RFID ativos e passivos ou híbridos

A segunda classificação a efetuar aos sistemas RFID é a classificação dos seus identificadores como passivos ou ativos ou híbridos. Os identificadores passivos não possuem bateria própria, sendo apenas compostos por um antena e um circuito integrado/chip [52].
Como o nome implica, um RFID passivo espera por um sinal de interrogação de um *transceiver* para executar um ação. Assim sendo, quando o interrogador está na zona de cobertura do identificador e o interroga, este utiliza as suas ondas eletromagnéticas para as utilizar como energia. Esta energia é passada da antena ao chip que então se põe em funcionamento. Quando este começa o seu funcionamento, irá alterar o sinal e a onda eletromagnética recebida. Esta alteração é então depois detetada pelo leitor que irá interpretar a nova onda e transforma-la em informação. Esta técnica é conhecida como retro modulação. Por se tratarem de identificadores sem recurso a energia própria normalmente estes mesmos estão limitados em memória e frequência [39]. As frequências utilizadas na comunicação são baixas. Também por uma questão de transposição da matéria, é preferível a utilização de baixas frequências, visto que quanto mais altas forem as frequências mais difícil são de transpor o material [52].

Um identificador RFID ativo, ao contrário de um passivo, possui a sua própria energia interna e o seu próprio transmissor, permitindo que este funcione em *broadcast*. Obviamente, por se tratar de um tipo de indentificador com energia própria, a capacidade de memória e distância de propagação da informação é largamente superior aos identificadores de tipo passivo.

No entanto, convém não esquecer que estes identificadores estão na presença de uma energia externa que normalmente se traduz em baterias, que a longo termo devem ser substituídas. Dentro dos identificadores RFID ativos podem ainda se identificar dois tipos, os *transponders* que basicamente só respondem quando interrogados por um leitor e os *beacons* que precisamente fazem *broadcast* do seu sinal ou informação em intervalos de tempo definidos [39].

Por último, existem os identificadores RFID híbridos ou passivos assistidos por bateria externa [53]. Essa bateria externa não é utilizada para alimentar um emissor pois o princípio neste tipo de identificadores continua o mesmo que o princípio dos passivos (retro modulação), mas para alimentar o circuito eletrónico do identificador. Esta alimentação permite em teoria um melhoria em termos de performance e capacidade de memória e microprocessamento, permitindo a um identificador RFID deste género efetuar outras operações mesmo sem ser interrogado, como por exemplo a leitura da temperatura, luz entre outros.

3.3.2.3 Memória dos identificadores RFID

Qualquer que seja o tipo de identificador (ativo ou passivo) que possua um circuito integrado, pode-se classificar o mesmo quanto a sua permissibilidade de interação com a memória do circuito. Quer isto dizer que a memória do identificador pode ser classificada como uma memória de leitura apenas, ou também de escrita, repercutindo esta classificação no identificador RFID [53]. O objetivo de um identificador RFID é como dito anteriormente, a possibilidade de identificação automática de objetos. Este identificador deve então conter em memória o seu identificador único, tornando esta memória de leitura apenas, sendo depois responsabilidade do leitor RFID de obter informações referentes a esse identificador. No entanto, existem identificadores com uma segunda parte de memória que permite a sua leitura e escrita. Esta parte da memória pode então ser utilizada para a gravação de dados dinâmicos.

3.3.2.4 Protocolo Tag Talk First e Interrogator Talk First

Esta questão prende-se com o protocolo de comunicação entre o leitor e o identificador. No fundo, pretende estabelecer quem comunica em primeiro lugar, o leitor ou o identificador. Esta questão, apesar de parecer óbvia, quando se trata de sistemas RFID passivos, exige algumas interrogações quando vários identificadores se encontram juntos e no mesmo raio de ação do leitor.
É óbvio que em sistemas passivos a primeira coisa a fazer é a passagem de energia por parte do leitor ao identificador, mas isso não quer dizer que uma comunicação seja estabelecida. Uma vez alimentado, o identificador pode transmitir imediatamente, por exemplo, o seu número de identificação (protocolo em que o identificador inicia a comunicação - *Tag Talk First* - TTF), ou esperar ser interrogado pelo leitor (protocolo em que é o interrogador que inicia a comunicação – *Interrogator Talk First* - ITF). A escolha entre um protocolo e outro deve ser efetuada em função da gestão de leitores RFID e da eventual presença de vários identificadores no raio desses leitores, com o objetivo de evitar colisões de comunicação no meio [54].

Resumindo, a classificação de um sistema RFID tem como denominador comum de comparação o identificador. Este pode então ser classificado quanto a sua posse ou não de um circuito integrado e quanto a sua maneira de operação, ou seja, ativo, passivo ou hibrido. Por fim, os identificadores podem ser classificados quanto a sua permissibilidade em relação à memória e quanto ao seu protocolo de comunicação.

Como já referido anteriormente, o identificador de uma chave de viatura (RFID transponder) é claramente um identificador com recurso a um circuito integrado. Também este identificador é claramente um identificador passivo, pois responde a interrogações por parte da ECU, ficando por esclarecer ainda se este utiliza uma bateria externa para a alimentação deste circuito, tornando-o hibrido. É certo que as chaves utilizam baterias para a abertura de portas, pelo que a utilização dessa mesma bateria para uma maior performance do circuito integrado do identificador é altamente provável.

A presença de memórias com possibilidade de escrita pode ser confirmada, visto as chaves registarem os quilómetros atuais da viatura entre outras informações. Fica ainda por esclarecer o protocolo de comunicação. Não sendo um dado adquirido, o protocolo usado será provavelmente o ITF, visto ser a ECU que interroga a chave sobre a sua identificação e até porque, caso fosse o protocolo TTF era impossível por exemplo um proprietário de uma outra viatura viajar dentro de uma viatura que não fosse a dele em posse da chave da sua viatura, pois iria causar confusão e colisões na comunicação.

Na Figura 21 pode ser visualizado um quadro de classificação de identificadores RFID com circuito integrado, permitindo melhor estruturar e esquematizar as classes destes.

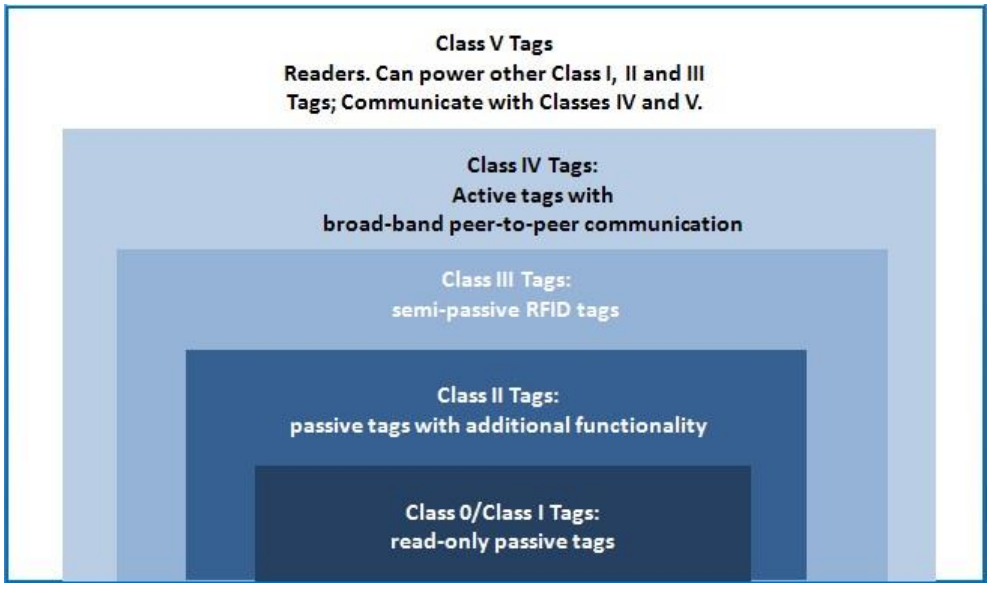


Figura 21 – Classes de um identificador RFID [53]

Após a identificação dos vários tipos de identificadores RFID, serão abordados nas seguintes subsecções a composição de um sistema RFID e as frequências destes bem como a técnica de transferência de informação presente em sistemas RFID.

3.3.3 Frequências de operação sistemas RFID

Um dispositivo RFID é considerado como um dispositivo não especifico de baixo alcance, então podem usar bandas de frequência sem a necessidade de licença, no entanto, estes dispositivos devem estar em conformidade com regulamentações locais como da European Telecommunications Standards Instute - ETSI [49]. Assim segundo [49] os sistema RFID podem operar em:

- ***Low Frequencies*: 125kHz – 134,2 KhZ**

Esta fatia do espetro muitas vezes referida como LowFID permite uma distância de cobertura ate meio metro. É globalmente utilizada para identificação de veículos.

- ***High Frequencies: 13,553 – 13,567 MHz***

Esta gama de frequências referida pela maioria como a gama 13,56 permite uma distância de até um metro. Esta gama é tipicamente utilizada para bilhetes eletrónicos, pagamentos de cartão bancário sem contacto, controlo de acessos entre outros.

- ***Ultra High Frequencies: 860MHz – 960MHz***

Permite distâncias a partir de um metro até ao máximo de dez metros. Esta gama requer um linha de visão para a comunicação e existem varias restrições ao seu uso. São usados para sistemas de proporção e escalar maiores como o seguimento de contentores, bagagem entre outros e normalmente são usados em conjunto com sistema Wi-Fi.

- ***Super High Frequencies: 2,446 GHz – 2,454GHz (2,45GHz)***

Esta gama permite distâncias superiores a três metros. São normalmente usadas quando se pretende cobrir uma grande distância com identificadores do tipo ativo, como por exemplo radares. No entanto, por serem de grandes distâncias estão mais sujeitas a interferências, pelo que neste tipo de frequências o dispositivo leitor RFID deve ouvir antes de falar, segundo as normas ETSI.

De notar que, quanto maior a frequência maior capacidade de alcance e de velocidade de transmissão de dados terá. No entanto, menor será a capacidade do sinal de ultrapassar os obstáculos do meio, como paredes, plásticos entre outros, bem como a sua necessidade de energia aumenta.

3.3.4 Transferência de dados/informação em sistemas RFID

A transferência de dados é como sabido efetuada através das ondas rádio. No entanto, estas devem ser interpretadas de maneira a transforma-las em informação para o emissor-recetor.A comunicação em sistemas RFID começa com o *handshake*. O *handshake* é iniciado pelo leitor que emite constantemente sinais RF esperando obter um sinal de volta.

Quando estamos na presença de identificadores RFID (transponder - considerando apenas os passivos) este irá modular o campo RF que será detetado pelo leitor. Assim o identificador, após absorção de alguma energia do leitor, irá começar a enviar informação modulada.

A informação pode então ser modulada diretamente, o que significa que a amplitude da modulação define a presença de zero ou um, ou seja, a maior amplitude (sinal elétrico) é interpretado como um e a menor como zero. Este tipo de modulação permite uma grande largura de banda de transferência mas é mais suscetível a interferências.

Por outro lado existem dois métodos que se distinguem da modulação direta, são eles a modulação por mudança da frequência em inglês *Frequency-Shift Keying* - FSK e modulação pela alteração da fase em inglês *Phase-Shift Keying* - PSK. O método FSK utiliza diferentes frequências para representar zero e um. Normalmente o modo utilizado é Fc/8/10. Em que zero é representado pela número de amplitudes moduladas num ciclo de período correspondente ao sinal RF do *handshake,* dividida por oito e o valor um dividido por dez [50,52]. Na Figura 22 é possível verificar um exemplo do mesmo.

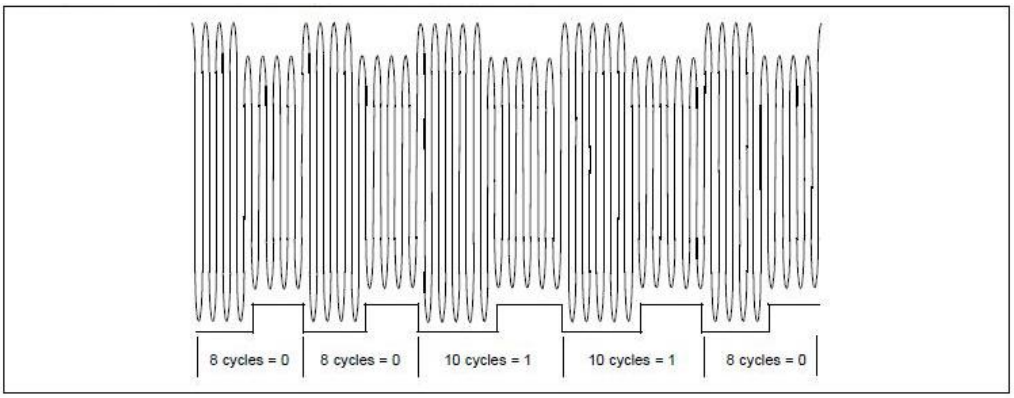


Figura 22 – Modulação FSK Fc/8/10 [52]

O método PSK é semelhante ao método FSK com a exceção que apenas uma frequência é usada. A distinção entre o valor zero e um é feita através da mudança da fase em 180 graus como pode ser verificado através da Figura 23.

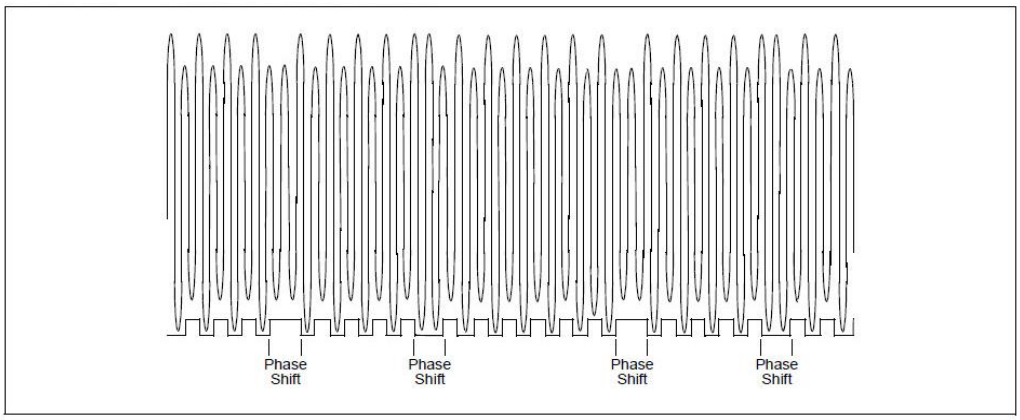


Figura 23 – Modulação PSK [52]

Na modulação PSK pode-se ainda encontrar dois tipos de interpretação da mudança de fase, as mais comuns são:

- Cada mudança de fase representa a mudança para zero.
- A inversão de fase representa uma inversão do valor transmitido no ciclo do período anterior correspondente ao sinal RF [52,50].

Nesta secção foi possível apresentar vastamente a tecnologia RFID, que será sem dúvida útil no processo de leitura de chaves de viaturas. É possível concluir que esta tecnologia é amplamente utilizada no mundo atual, o que a torna bastante diversificada entre as áreas de aplicação. Apenas conhecendo esta tecnologia será possível abordar a temática de leitura de chaves, pois uma chave de viatura é composta por um identificador RFID/*transponder*. Conseguindo interagir com a chave, o problema de verificação da chave presente será resolvido.

Na próxima secção será abordada a tecnologia OCR & *Pattern Recognition,* que também será fundamental na deteção de hologramas de segurança em cartas de condução como previamente explicado.

3.4 Tecnologia OCR & Pattern Recognition

Nesta secção pretende-se analisar uma tecnologia, que poderá responder à necessidade de leitura de informações em documentos, bem como o reconhecimento de certos hologramas. Essa tecnologia tem o nome de *Optical Character Recognition ou Optical Character Reader* – OCR.

3.4.1 História e Definição de OCR

A tecnologia OCR não é mais do que a transformação de uma imagem, documento impresso ou escrito à mão em informação eletrónica, ou seja, as formas contidas nas imagens são transformadas em caracteres ASCII. É uma tecnologia bastante usada como ponto de entrada de informação em sistema, como passaportes, documentos, faturas, cartões de visitas entre outros. Deste modo, documentos previamente impressos podem ser informaticamente procurados, editados e as suas informações utilizadas e propagadas por outros sistemas. OCR é um campo de pesquisa em *pattern recognition* [63].

Os primeiros traços desta tecnologia começaram a aparecem em 1914, quando Emanuel Goldberg desenvolveu uma máquina que lia caracteres e os convertia em código morse [60]. Paralelamente a isto Edmund Fournier d'Albe desenvolveu o *optophone* em 1913 que pode ser visto na Figura 24. O *optophone* transformava o texto de um documento em diferentes tons sonoros que diferenciavam as letras [61].

Figura 24 – Exemplo de Optophone [72]

Mais tarde, em 1976, a empresa Kurzweil Computer Products em conjunto com a National Federation of the Blind apresentou um sistema que reconhecia o texto e o reproduzia em formato sonoro, que ajudaria os invisuais a ouvir o que estava escrito. Mas seria somente em 2000 que a primeira plataforma *online* OCR se fez disponibilizar [62].

Dentro da grande tecnologia OCR existem várias variantes:

- *Optical Character Recognition* – OCR: visa texto impresso, um símbolo ou caractere de cada vez;
- *Optical Word Recognition* – OWR: visa também texto impresso mas analisa uma palavra de cada vez, baseando no espaço entre símbolos ou caracteres. Normalmente chamado OCR;
- *Intelligent Character Recognition* – ICR: visa não só o texto impresso mas também texto escrito à mão, analisando um símbolo ou caractere de cada vez;
- *Intelligent Word Recognition* – IWR: semelhante a ICR mas analisa uma palavra de cada vez baseando no espaço entre símbolos ou carateres.

3.4.2 Processo de reconhecimento

Supondo que o alfabeto apenas fosse composto por uma letra, por exemplo a letra A, o processo de reconhecimento de caracteres seria na mesma um processo ainda complicado. Isso deve-se ao fato de a letra A ser escrita de maneira diferente por cada um. Mesmo em documentos impressos a letra A pode estar impressa com tipos/fontes de letra diferentes.

Em termos gerais, há duas maneiras diferentes de resolver esse problema, ou pelo reconhecimento de caracteres na sua totalidade (*pattern recognition*) ou através da deteção das suas características individuais (*feature detection*) [63].

3.4.2.1 Feature Detection

Também conhecida como extração de características ou reconhecimento inteligente de caracteres (ICR), esta é uma maneira mais sofisticada de reconhecer caracteres. Isto pode ser explicado por uma razão simples. Supondo que um sistema de OCR é desenvolvido para o efeito e este é presenteado com um lote de diferentes cartas escritas com diferentes tipos de letras. Estando cada letra em cada carta impressa com uma forma diferente, como será o sistema capaz de detetar os padrões se estes são ligeiramente diferentes? Provavelmente algumas letras encaixarão no perfil enquanto outras provavelmente não [63,67].

No entanto, se regras de construção de letras forem aplicadas, como por exemplo, existem duas linhas angulares que se encontram num ponto no topo e no centro existe uma linha horizontal entre elas, que as une, então a letra é correspondente é a letra A. Aplicando esta regra, o sistema será capaz de detetar a maioria das letras A maiúsculas, independentemente da forma/tipo de letra. Ao invés de detetar a forma completa do padrão da letra A, o sistema identificará características indivíduas de cada uma, como linhas angulares, linhas paralelas, cruzadas entre outros.

Os mais modernos sistemas de OCR funcionam por *feature detection* ao invés de *pattern recognition*, pois esta abordagem permite uma maior flexibilidade e taxa de sucesso [63,64].

3.4.2.2 Pattern Recognition

Pattern recognition é a capacidade de identificar a presença de padrões em textos, objetos, som ou mesmo relações, tornando o processo de aprendizagem e de deteção de padrões explícito, tal que este possa ser implementado, parcial ou totalmente em computadores. O reconhecimento automático (sistemas computacionais), descrição, classificação (agrupamento de padrões em classes padrão) tornaram-se problemas importantes nos dias de hoje em uma variedade de disciplinas de engenharia e científicas como a biologia, psicologia, medicina, marketing, visão computacional, inteligência artificial entre outras. Em quase qualquer área da ciência em que uma decisão ou aquisição é tomada pela observação humana, *pattern recognition* pode ser usado para ajudar ou mesmo substituir o humano nessa tarefa [67].

O interesse em *pattern recognition* foi renovado recentemente, devido a aplicações que não são apenas um desafio, mas também, computacionalmente mais exigentes como *data mining*, classificação de documentos, organização e pesquisa em base de dados multimédia (imagem/vídeo) e em autenticação biométrica.

Um sistema de reconhecimento de padrões pode ser geralmente esquematizado pela seguinte ordem de processos/etapas [66,67]:

- Aquisição de dados e pré-processamento: é tirada uma foto de um objeto e removendo as partes irrelevantes como o fundo ou objetos ao lado;

- Representação dos dados: derivar propriedades de objetos relevantes (como o seu tamanho, forma e cor), que ofereçam de forma eficiente a informação pertinente necessária para o reconhecimento de padrões;
- Treino do sistema: conferir a definição de classe padrão ao sistema, muitas vezes, mostrando alguns exemplos típicos do padrão e as tomadas de decisão que envolveram esse padrão.

Existem algumas maneiras de abordar o processo de reconhecimento de padrões. Ou seja, existem diferentes métodos, que permitem definir um padrão e o reconhecer [65,67]:

- Template Matching: Os objetos e suas características são diretamente comparados com alguns exemplos de protótipos e representativos das classes subjacentes. Devido às grandes variações frequentemente encontradas nestes exemplos, esta abordagem não é a mais eficaz para o reconhecimento de padrões.
- Geometrical Classification: a classificação do padrão é representada por valores num espaço. Por exemplo, a classificação do sexo de uma pessoa consoante o peso e altura. Segundo a sua forma, estes dois valores serão transpostos para um cartesiano de relação entre os dois valores. Seguidamente através dos valores do ponto de X,Y do objeto e da separação do cartesiano (separação e limites entre masculino e feminino), é possível determinar o sexo. Supondo que os media de altura de uma mulher e M1 e peso P1 e de um homem H1 e P2, uma simples análise dos pontos obtidos poderá classificar a pessoa quanto ao sexo.
- Statistical Classification: este tipo de classificação difere do anterior pelo fato de não haver pré-estabelecido os valores da classificação. Utilizando o exemplo anterior através dos exemplos já inseridos no sistema com características semelhantes, a determinação do sexo da pessoa apresentada irá basear-se nas probabilidades e estatísticas das suas características encaixarem no sexo masculino ou feminino.
- Syntatical or Structure Classification: Nas duas abordagens anteriores, ou seja, a representação da altura e peso é demasiado simplista para a determinação do sexo, além disso é sabido que a forma do corpo de uma pessoa é uma melhor representação para determinar o seu sexo. Pode-se então decompor o corpo da pessoa em várias partes e descrever para cada uma a forma e as suas relações (a qual cada parte esta ligada por exemplo). Assim a determinação do sexo pode agora ser calculada através da forma das partes, das suas ligações ou ambos os fatores.

3.4.3 OpenCV

Open Source Computer Vision – OpenCV [69] é uma biblioteca de funções de programação destinada principalmente a visão computacional em tempo real, originalmente desenvolvido pelo centro de pesquisa da Intel na Rússia, mais tarde apoiados por Willow Garage e agora por Itseez [68]. A biblioteca é multiplataforma e livre para o uso sob a licença BSD de código aberto. Esta biblioteca possui módulos de processamento de imagens e vídeo, estrutura de dados,

álgebra linear entre outros. Esta biblioteca permite assim o reconhecimento de objetos, estruturas e outras formas, podendo ser incorporada nos mais diversos sistemas [69].

3.4.4 Linguagem de Programação e Plataformas compatíveis

OpenCV é uma biblioteca desenvolvida com a linguagem de programação C++ apesar de haverem traduções desta para Python, Java e MATLAB/OCTAVE. A interface de API principal é C++, mas também aqui esta biblioteca mostra grande adaptabilidade e flexibilidade por apresentar também a possibilidade de exploração da API em C#, Perl, e Ruby, o que encoraja a sua adoção por um mais vasto público da área da programação.

A biblioteca é suportada pelas mais variadas plataformas de sistemas operativos nomeadamente Windows, Android, Maemo, FreeBSD, iOS, BlackBery, Linux e OS X.

3.4.5 Áreas de aplicação

Como já previamente referenciado, a tecnologia de *pattern recognition* é nos dias de hoje, motivo de interesse em várias áreas de engenharia e ciência. Assim as áreas de aplicação desta biblioteca é vasta como por exemplo a identificação de objetos, a compreensão de movimentos (*gesture recognition*), reconhecimento facial, aprendizagem e ajuda na tomada de decisões, realidade virtual, reconhecimento de padrões, *Human-Computer interaction* – HCI entre outros. Na Figura 25 é possível visualizar um exemplo de reconhecimento de padrões (cartas) por parte da biblioteca OpenCV.

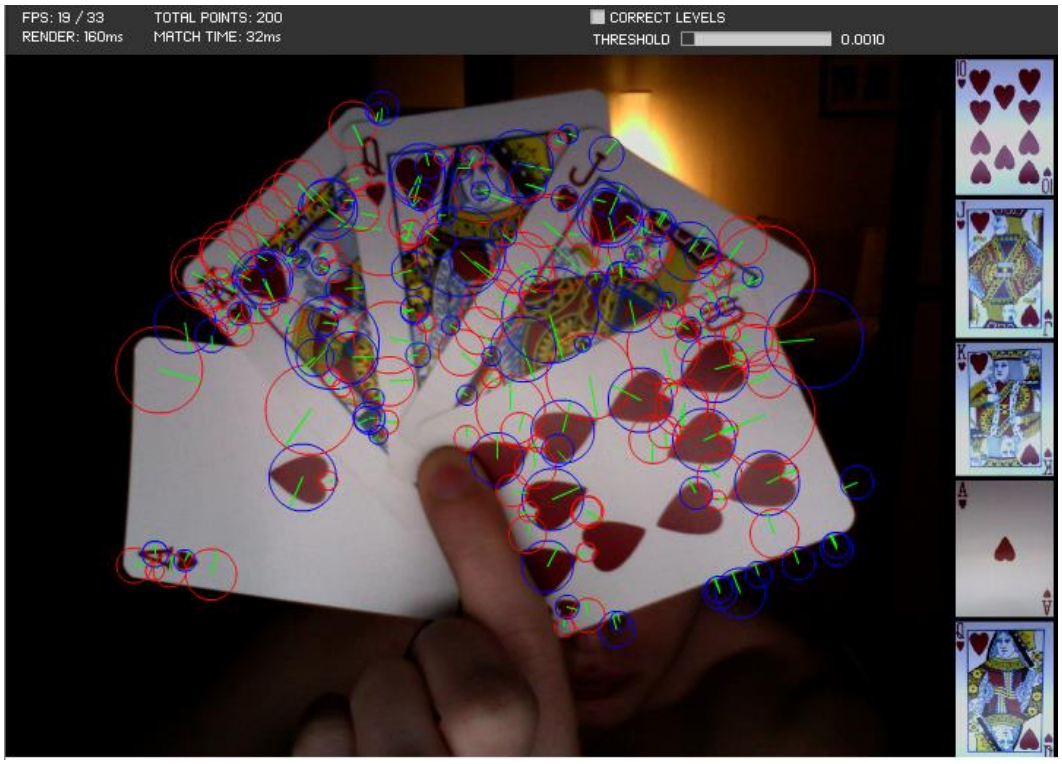


Figura 25 – Deteção de padrões em OpenCV [68]

3.5 Sumário do capítulo

Neste capítulo foi possível estudar e analisar diferentes tecnologias existentes no presente. O grande objetivo deste capítulo não se prendia somente com as respostas às perguntas P1-P4 mas principalmente à pergunta P5.

Após o estudo das tecnologias é possível afirmar-se que os requisitos da solução a implementar podem ser satisfeitos, bem como, podem ser incorporados numa só solução, respondendo então à pergunta P5. Existe de facto tecnologia de autenticação biométrica (íris) capaz de ser integrada em soluções variadas como é o caso de IriShield. Existe também a possibilidade de incorporar a leitura de RFID em soluções, através dos mais diversos leitores presentes no mercado. No entanto por se tratar de um objeto proprietário (chaves) a escolha do leitor esta longe de ser estabelecida. Por fim o reconhecimento de padrões e texto é possível através de API como o OpenCV.

Acredita-se que com a junção destas três tecnologias é possível a obtenção da solução global que preencha os requisitos e responda às perguntas P1-P5.

4 Desenvolvimento do protótipo

O capítulo que se segue pretende sistematizar o problema, levantando e definindo requisitos funcionais e não funcionais. De seguida é efetuado também o desenho da arquitetura pretendida do sistema proposto e consequente implementação onde serão apresentados os detalhes da solução.

4.1 Análise

Após a identificação do problema e enquadramento do mesmo, tornou-se mais simples a análise do mesmo e o levantamento de requisitos e necessidades por parte da empresa. O levantamento de requisitos é fundamental para que a solução proposta e implementada corresponda as expetativas e necessidades por parte dos utilizadores. Assim, de seguida são apresentados os requisitos identificados.

4.1.1 Levantamento de requisitos

O primeiro passo no processo de análise prende-se com a aquisição e tratamento de toda a informação necessária, que será indispensável para a definição das funcionalidades que a plataforma deve apresentar. Este primeiro passo designa-se como o levantamento de requisitos.

4.1.2 Requisitos Funcionais

Após algumas reuniões de discussão com os futuros utilizadores da plataforma foram recolhidas informações, que possibilitaram identificar os seguintes requisitos:

1. Permitir ao utilizador/condutor a utilização de uma viatura;
2. Identificação do utilizador aquando da requisição de chaves da viatura;
3. Verificação da sua carta de condução;
4. Evitar a troca de chaves de viaturas;
5. Instalação de dois repositórios de chaves de viaturas, cada um com compartimentos dedicados a cada chave de cada viatura;

6. Permitir o acesso às chaves das viaturas sem apresentação de carta de condução;
7. Denominar um responsável da plataforma que será responsável pela gestão das viaturas e condutores, tornando-o o supervisor/gestor da frota;
8. Efetuação de testes de alcoolemia aleatórios antes da utilização de viaturas;

Passe-se agora à explicação dos pontos acima identificados. No que diz respeito ao primeiro, segundo e terceiro ponto, trata-se do coração do problema, ou seja, é obrigatório que o utilizador possa utilizar uma viatura como é óbvio (este é o objetivo da plataforma), neste caso o condutor e que quando se dirija a um dos repositórios de chaves, seja corretamente identificado no sistema, com a maior segurança possível. Ao mesmo tempo, é necessária a validação da sua carta de condução. Apesar da carta de condução ter de ser verificada manualmente pelo gestor da frota aquando da inserção do condutor no sistema, este pode ter sido objeto de suspensão no passado recente e não estar na posse da mesma, estando então proibido de conduzir. Assim sendo, esta verificação do documento de condução é também um ponto obrigatório.

O quarto ponto, garantir que o utilizador leva e devolve a chave que requisita na plataforma, neste caso, no repositório, torna-se fundamental para garantir a coerência do sistema, quer a nível dos registos de utilização das viaturas, quer ao nível das permissões de acesso aos recursos. Ora vejamos:

- Um utilizador U1, que apenas pode conduzir a viatura V1, pede essa viatura V1 e esta é-lhe concedida, partindo o utilizador U1 com a mesma.
- De seguida o utilizador U2 que apenas pode conduzir a viatura V2, requisita a viatura V2 que também lhe é concedida, partindo também este com a mesma.
- Se ambos, no retorno e devolução das chaves trocarem o compartimento da chave, o sistema perderá a consistência acerca do local em que cada chave se encontra.

O quinto ponto, vai de encontro aquilo que é a estrutura física da empresa. A empresa encontra-se dividida em dois locais separados, como já referido anteriormente. O objetivo deste quarto ponto é permitir que uma viatura não esteja fisicamente ligada a um só local, pois as viaturas podem viajar de um local da empresa para o outro e serem nesse segundo local requisitadas para se deslocar a um terceiro destino. De notar que o compartimento dedicado a cada chave de cada viatura, permite precisamente esta flexibilidade de não permanente alocação de uma viatura a um local da empresa, permitindo também ao sistema manter a coerência entre os dois locais e viaturas presentes em cada um.

O sexto ponto pode-se denominar como uma "*back door*", ou seja, permite ao gestor da frota em caso de urgência, ou por exemplo no caso de alguém se esquecer dos seus documentos, permitir o acesso do mesmo sem a obrigatoriedade da apresentação da carta de condução. De notar que este acesso sem apresentação da carta de condução, apenas deverá ser possível por parte do gestor, ficando a cabo do mesmo, permitir o acesso às chaves por parte de algum condutor ou não. O objetivo do ponto número sete é de permitir o acesso as chaves em caso de avaria por parte de uma das partes da plataforma. (identificação do utilizador ou verificação

da carta da condução). Por último, a denominação do supervisor da plataforma (gestor da frota), permitirá ao mesmo ter um pouco mais de permissibilidade na plataforma. A intenção é que esta possa efetuar a gestão de viaturas (frota) e gestão de utilizadores numa primeira instância.

Por fim, o último ponto, não sendo uma obrigatoriedade, é uma medida muitas vezes implementada em várias empresas na entrada ao serviço dos seus funcionários. Algumas empresas tem um sistema aleatório de testes de alcoolemia, que se aciona quando o funcionário dá entrada na empresa. Neste caso, será no início do pedido da viatura, evitando talvez em alguns casos, o incumprimento da lei.

Os pontos até aqui abordados são pontos críticos e essenciais do "*core*" do sistema. Porém, alguns outros requisitos puderam ser identificados ao longo dos encontros de discussão do sistema, principalmente relacionados diretamente como o denominado supervisor da plataforma, que será também ele o gestor da frota:

9. Possibilidade de suspender/bloquear utilizadores;
10. Possibilidade de suspender/bloquear viaturas;
11. Permitir ao supervisor a atribuição correta de permissões de acesso e condução a viaturas por parte dos utilizadores/condutores;
12. A gestão de reservas de viaturas;
13. Registo e consulta simplificado do diário de bordo das viaturas e informações (manutenções, apólices seguro, revisões);

Estes últimos cinco pontos tornaram-se óbvios com o desenrolar das discussões, pelo que não sendo requisitos obrigatórios para a resolução do problema, são requisitos importantes para que a gestor da frota em cima possa ser feita de uma maneira correta e sóbria.

Se faz sentido a identificação e autenticação dos condutores aquando da utilização das viaturas, faz sentido também a plataforma permitir a gestão destes e destas respetivamente, arrastando para si a gestão do nível de permissões de acesso a recursos, neste caso viaturas. Assim, pode e deve também ser integrado no sistema a gestão de reservas de viaturas, pois o sistema deve negar o acesso a viaturas que o gestor da frota prevê não estarem disponíveis. Estas podem estar indisponíveis por vias de uma requisição, ou para efeitos de manutenção por exemplo.

Por último, o registo e consulta do diário de bordo é importante para o gestor, pois este deve saber onde esteve a viatura V1, conduzida por quem e num dado momento, ou até os quilómetros feitos pela viatura hoje, ontem ou este ano. Não só para efeitos de atribuição de determinadas infrações mas também para efeitos de manutenção das viaturas.

A partir deste momento uma plataforma de *BackOffice* torna-se imperativo para estes últimos requisitos funcionais. O gestor deverá poder efetuar estas operações a partir do seu posto de trabalho. O repositório de chaves deverá estar num local próximo da saída para as viaturas.

4.1.3 Casos de uso

Definidas as necessidade ou requisitos da solução é necessária a esquematização dos casos de uso desta. Casos de uso, em inglês *Use Cases* - UC, não é mais que uma representação das funcionalidades propostas por um sistema, que está fortemente relacionada com os requisitos funcionais do sistema. No ponto anterior, apresentou-se uma descrição das funcionalidades pretendidas (requisitos funcionais), pelo que neste ponto, através da Figura 26, apresenta-se um diagrama de UC descritos, bem como uma narrativa da sequência de ações a desempenhar pelo ator de maneira a contemplar e perfazer essas mesmas funcionalidades.

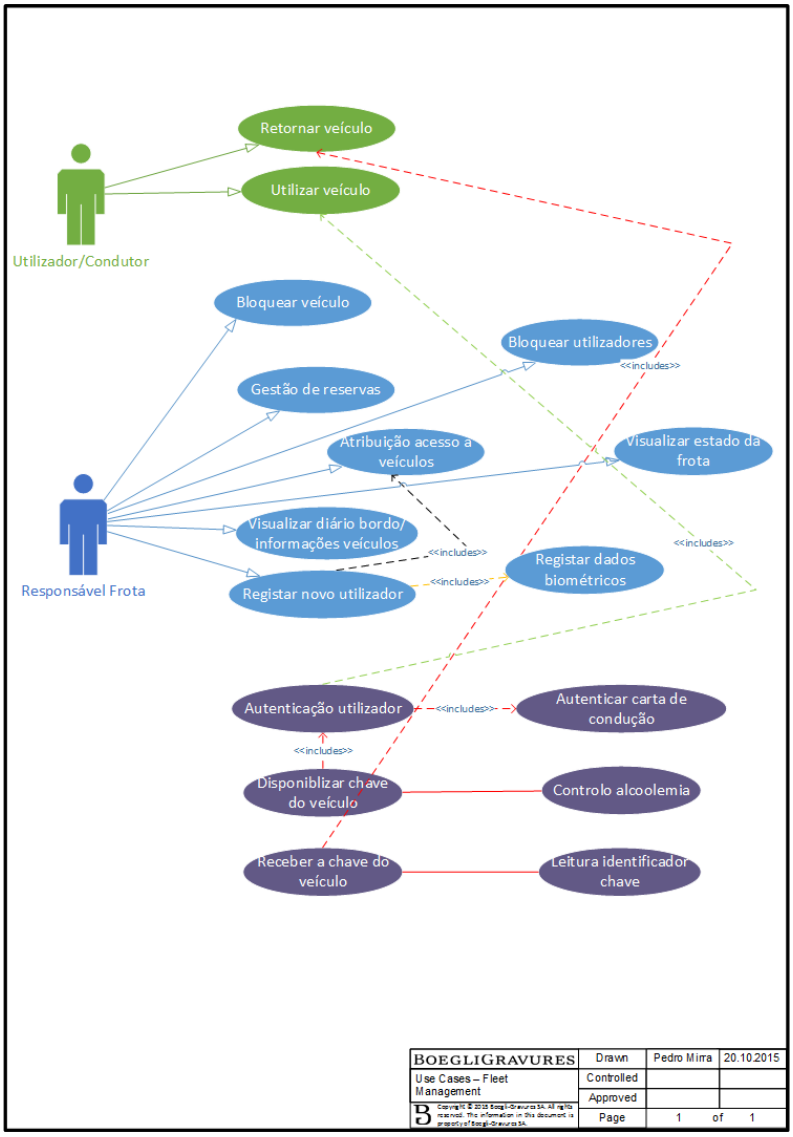


Figura 26 – Diagrama de casos de uso

Nesta subsecção foram definidos os casos de uso do sistema, parte fundamental para a boa implementação de qualquer sistema informático. Antes do desenvolvimento e implementação

é necessário conhecer ao certo o que se pretende com o sistema e suas funcionalidades, esquematiza-las através de um processo e prever os pressupostos e exceções de cada uma.

Para complementar e melhor esquematizar o fluxo do *software*, serão apresentados na próxima subsecção precisamente os processos que se formam a partir das funcionalidades e casos de uso. O anexo 1 apresenta as narrativas dos casos de uso identificados.

4.1.4 Processos do sistema proposto

Esta subsecção pretende esquematizar os processos (*Workflows*) das funcionalidades requisitadas e a implementar no sistema. Assim, entenda-se por processo como um conjunto de tarefas a executar no sistema, para levar a cabo a função pretendida por parte do utilizador.

4.1.4.1 Registar novo utilizador

O processo de registo de um novo utilizador é o processo responsável pela criação de um novo utilizador de veículos da empresa. Tem como objetivo permitir que o gestor da frota possa introduzir um novo utilizador.

Numa primeira fase o gestor da frota introduz as informações básicas do utilizador como o nome, número de carta de condução entre outras. Por fim, efetua o registo dos dados biométricos do utilizador em causa. Na Figura 27 é apresentado um diagrama de fluxo do processo em causa. De notar que no anexo 1 é apresentada a narrativa deste processo, através da descrição do caso de uso correspondente.

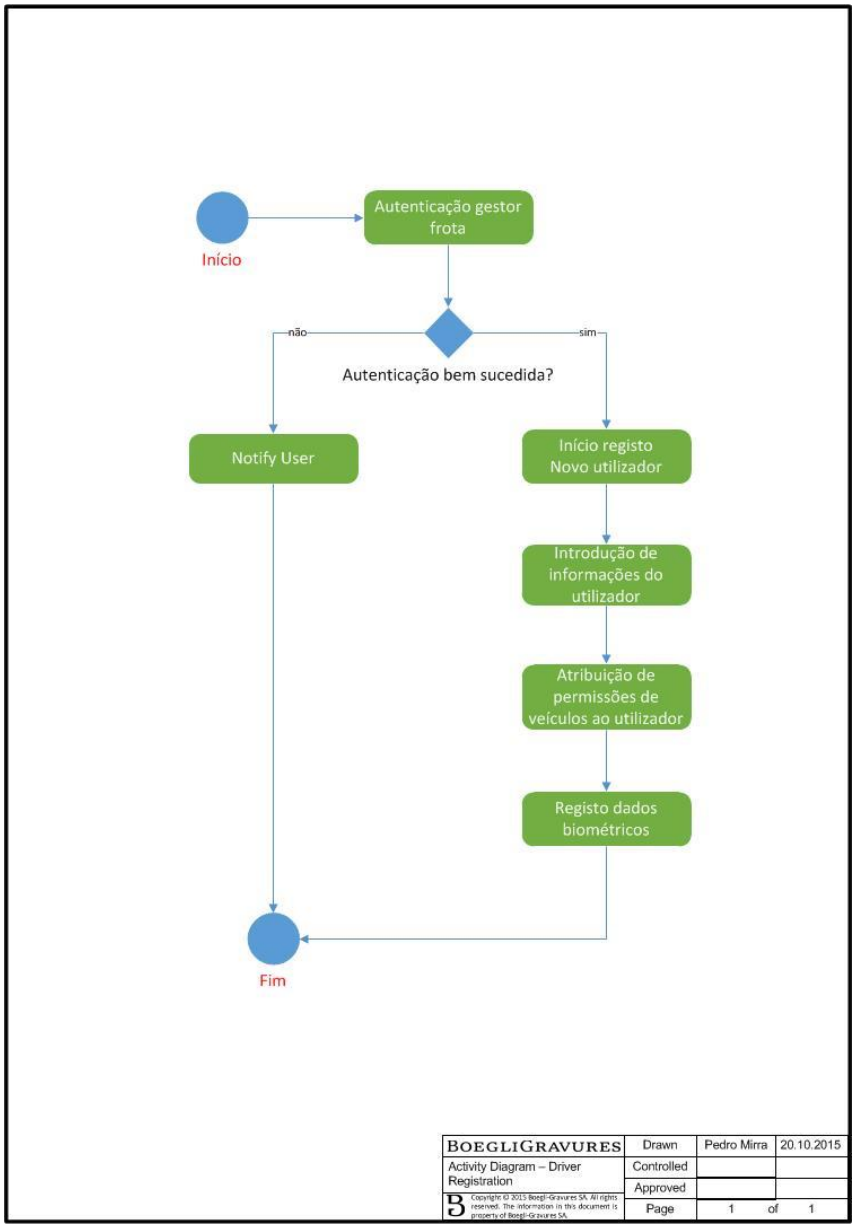


Figura 27 – Processo de registo de novo condutor

4.1.4.2 Utilizar veículo

O processo de requisição de uma viatura é o processo responsável pela liberação e entrega das chaves de um veículo a um utilizador que o requisita. Tem como objetivo permitir que o utilizador fique em posse de um veículo para utilização.

O utilizador começa por se autenticar no ponto de requisição e devolução de chaves (repositório de chaves), bem como valida a sua carta de condução. De seguida, mediante a disponibilidade ou permissões de acesso o utilizador poderá pegar na chave do veículo escolhido.

Na Figura 28 apresenta-se um diagrama de fluxo do processo em causa. De notar que no anexo 1 é apresentada a narrativa deste processo, através da descrição do caso de uso correspondente.

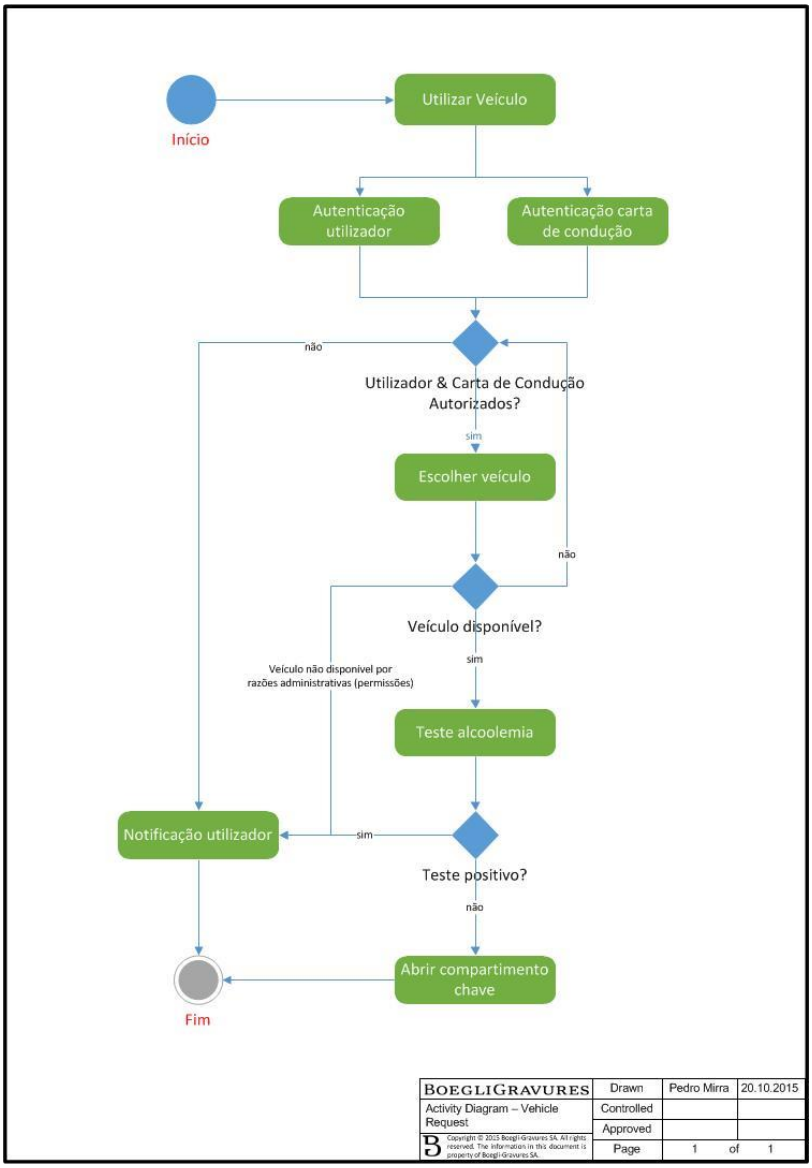


Figura 28 – Processo de requisição de viatura

4.1.4.3 Retornar veículo

O processo de devolução de uma viatura é o processo responsável pelo bom recebimento da chave de um veículo que esteve até ao momento em utilização. Tem como objetivo permitir que o utilizador devolva o veículo requisitado anteriormente.

O utilizador deverá no ponto de requisição e devolução de chaves (repositório de chaves), indicar que pretende devolver um veículo. O sistema escolherá um compartimento a abrir, para

que este possa pousar a chave. De seguida, o sistema fará todas as verificações necessárias para evitar inconsistências de informação. Na Figura 29, um diagrama de fluxo do processo em causa é apresentado. De notar que no anexo 1 é apresentada a narrativa deste processo através da descrição do caso de uso correspondente.

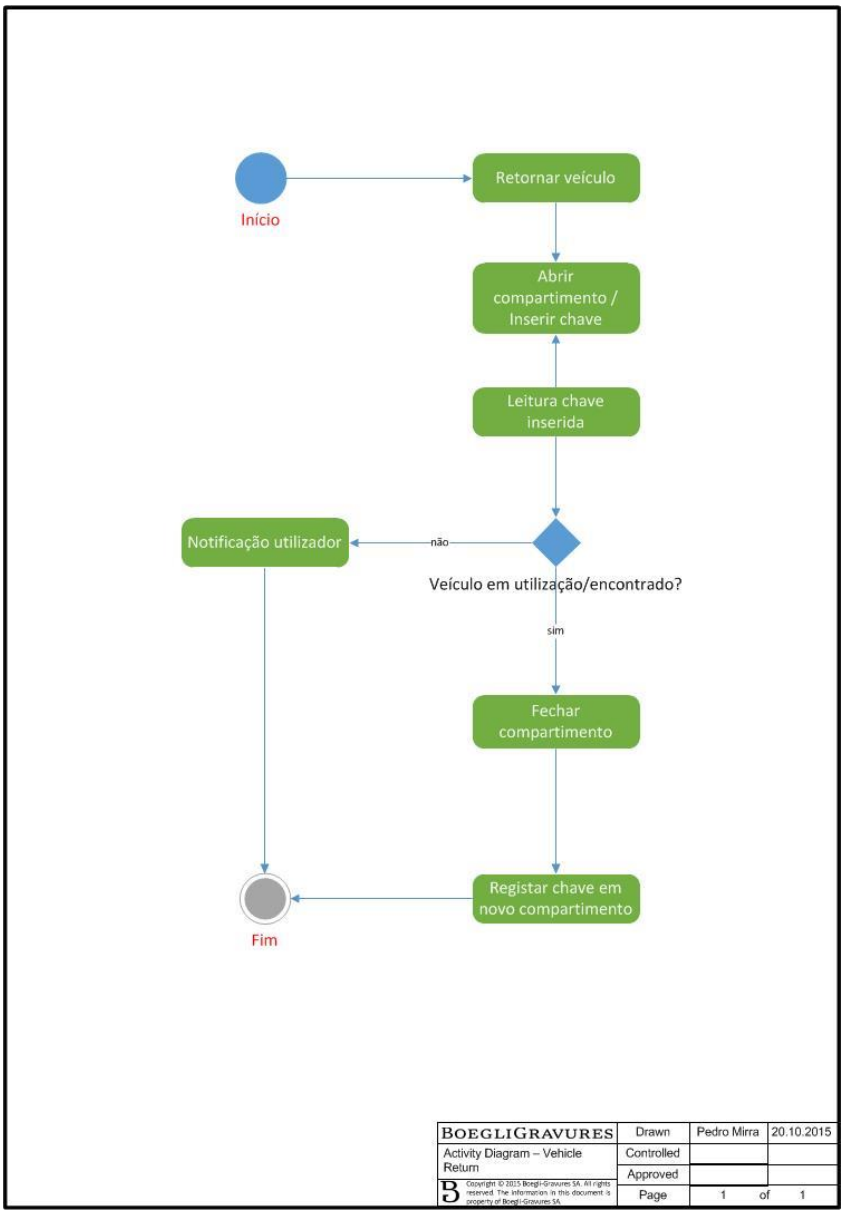


Figura 29 – Processo de devolução de viatura

4.1.5 Requisitos Não Funcionais

Os requisitos não funcionais relacionam-se com a qualidade de cada sistema ou plataforma implementada. Deste modo, os requisitos não se prendem com questões de funcionalidades que o sistema deverá fornecer, mas sim com o modo como as fornece. Tendo em vista e relacionando-se então com os padrões de qualidade como, a segurança, desempenho, flexibilidade e a usabilidade. Estas quatro premissas devem ser cumpridas, que para além dos requisitos funcionais, permitirão que o sistema seja de qualidade e confiança, não só do ponto de vista dos utilizadores mas também por parte de quem o implementa.

- Segurança

É necessário que o acesso à aplicação de repositório das chaves e o acesso a um eventual e *Backoffice* se efetue apenas por pessoas autorizadas. Assim, no que ao repositório diz respeito, é fundamental que a pessoa que se apresenta para utilizar uma viatura seja ela própria e não um colega, que lhe "emprestou" as credenciais de acesso e carta de condução. Por sua vez é também necessário assegurar que é apresentada uma carta de condução válida e correspondente ao utilizador que se identifica no sistema. Por outro lado, o acesso ao *Backoffice* deve ser só possível por pessoas autorizadas, ou seja, o gestor de frota e administradores da aplicação. Os dados relativos a utilizadores e outros considerados sensíveis deverão estar protegidos de acessos indevidos.

- Desempenho

O processo de autenticação dos utilizadores e gestores deverá ser um processo rápido, sem que este perturbe a fluidez do negócio. Não se pode perder demasiado tempo com um processo que apenas tem a finalidade de "disponibilizar" uma chave. Do mesmo modo, este deverá responder com rapidez às ações do gestor da frota, como por exemplo, bloquear um utilizador. Por fim o processo de entrega de chaves deverá também ele ser rápido e eficaz.

- Flexibilidade

O sistema a implementar terá que ser flexível ao ponto de permitir "*backdoors*" para a utilização das viaturas, caso outros componentes do sistema estejam no momento inaptos, como por exemplo o sistema de verificação de carta de condução, ou simplesmente porque o gestor da frota necessita da chave para efetuar um controlo de veículo (manutenção). Deverá também estar construído de maneira que permita uma rápida reparação *hardware* em caso de falha.

- Consistência

Sendo um sistema que estará presente em dois locais, este deverá sempre em todo o caso manter a consistência entre eles. Se o supervisor bloqueia uma viatura, esta devera ser bloqueada nos dois locais, ou se o utilizador utiliza uma viatura a partir de um local e a entrega no outro local, o sistema deve ser capaz de encontrar essa informação e manter a coerência entre as viaturas presentes em casa um dos locais e a proveniência entre outros.

- Usabilidade

Como não poderia deixar de ser, qualquer plataforma, aplicação ou sistema deve sempre ser intuitiva e agradável ao utilizador de forma a garantir o máximo de aproveitamento da plataforma. Esta deve ser fácil de utilizar e com uma interface simples e limpa.

4.1.6 Conclusão da Análise e Sistema proposto

Após as várias discussões acerca dos objetivos da aplicação foi possível sintetizar e expor os requisitos funcionais e não funcionais vistos anteriormente. A partir do estudo do Estado da Arte e com base no levantamento de requisitos, é possível concluir que não existe no mercado uma aplicação/plataforma que satisfaça o problema na totalidade como já adiantado na secção 2.6 Sumário do capítulo 2 - Estado da Arte.

Existem alguns sistemas que permitem efetuar uma gestão de frota no que à parte administrativa diz respeito, outros que permitem satisfazer o problema de recolha de dados das viaturas, que não sendo um "*have to have*" é um "*nice to have*", como por exemplo os sistemas de tacógrafos ou a própria solução de gestão de frota Fleetio. Explorando ainda mais o problema, verifica-se que não existem sistemas com a validação imediata da carta de condução, existem apenas sistemas preparados para alertar acerca de eventuais expirações da mesma. Por fim, não foi possível também encontrar soluções preparadas para a identificação e leitura de chaves das viaturas.

De mais, a adaptação de sistemas de tacógrafo seria necessária em cada veículo da empresa. Sendo que a gama de veículos que se pretende aqui controlar pertence a gama de veículos ligeiros de passageiros, esta gama não é são passível de tais sistemas. Pelo menos por lei, tal é que, nem o fabricante disponibiliza esta gama de viaturas com estes sistemas incluídos de base, pelo que a adaptação seria um extra. Assim, como em caso de adaptação de tacógrafos digitais, cartas de condutor seriam necessárias para cada utilizador das viaturas, que acarreta como é normal custos também extras, sem garantir esta (carta de condutor), que o condutor esteja em posse de uma carta de condução no dado momento.

Isto significa que, a verificação da carta de condução seria sempre necessária. A única vantagem seria um possível maior controlo e facilidade de obtenção de dados referentes aos veículos, visto que veículos possuidores de tacógrafo registam dados no mesmo como já referido anteriormente.

Resumindo, o problema principal deve ser divido em três partes. A identificação do utilizador/condutor sem repúdio; identificação e validação da carta de condução do utilizador que o habilita ou não a utilizar uma viatura; identificação de cada viatura, neste caso de cada chave. Esta combinação torna difícil a satisfação de todos os requisitos num só produto, pelo que é efetivamente mais razoável e mesmo mais correto a criação de uma plataforma/sistema à medida das necessidades e requisitos anteriormente já expostos, ou com recurso a tecnologias e "subproduto" já existentes no mercado para cada uma das três partes do problema e agrupa-las num só sistema/plataforma.

4.1.6.1 Decisão de identificação do condutor

Como já dito anteriormente, o processo de disponibilização de chaves deve ser rápido, seguro e fluído. Sendo que o sistema terá como local de destino, um local perto da saída, propõe-se que seja um computador *All-In-On* - AIO, com ecrã táctil, ou um computador de tamanho reduzido (*small factory Personal Computer - PC*), por razoes de simplicidade e estética. Pretendendo-se uma identificação do utilizador rápida e segura, principalmente com um nível de não repúdio baixa, terá que ser escolhida uma autenticação biométrica. Este tipo de autenticação não só permite baixos níveis de não repúdio, como é hoje em dia uma tecnologia rápida e eficaz, não sujeita a perda, e menos sujeita a danos.

A introdução de um sistema de autenticação por via de KBA ou propriedade não é desejável, no sentido em que estas podem ser mais facilmente perdidas, roubadas ou mesmo "emprestadas", tornado estas tecnologias mais facilmente repudiadas, quando existe alguém que se pretende responsabilizar de algo. Também de referir que a autenticação por via de KBA torna-se mais morosa que uma autenticação biométrica.

Uma autenticação por propriedade é sem dúvida a mais rápida, por exemplo através de cartões RFID, no entanto como já dito anteriormente esta é mais suscetível a perda, roubo ou danos, não garantindo que a pessoa que se autentica, está efetivamente presente como é garantido no caso de autenticação biométrica em casos normais.

Então, qual mecanismo ou método de autenticação biométrica utilizar? Hoje em dia existem alguns em voga, sendo os mais populares a impressão digital, o reconhecimento da íris e o reconhecimento facial. Todos são poderosos e funcionam relativamente bem, obviamente, a impressão digital é um dos mais antigos e mais testados métodos, pelo que o seu grau de confiabilidade (extremamente alto) não pode ser comparados com os restantes e mais novos métodos. Também deve ser referido que a autenticação por impressão digital é de fácil utilização e um método bastante comum em sistemas que utilizem autenticação biométrica.

No entanto, sendo a empresa, uma empresa de microengenharia industrial, os funcionários deparam-se algumas vezes com as mãos gordurosas, devido ao óleo e outros produtos usados em produção. Também, os dedos são mais suscetível de danos contrariamente à íris no trabalho quotidiano da empresa, pelo que, esta variante torna-se mais suscetível a erro e falha de identificação. Por outro lado o reconhecimento facial é um método de implementação relativamente barato, no entanto tem vindo a perder terreno para os restantes métodos, não só por ser altamente influenciável pela luz, como é mais sujeita a alterações e danos, neste caso, com o avançar da idade, ou alteração do visual da pessoa por exemplo.

A identificação pela íris será o mais adequado método a implementar neste caso de estudo. O reconhecimento da íris é extramente preciso e rápido e o menos suscetível a danos e mudança com a idade por exemplo. Nos últimos anos, este método tem ganho terreno aos seus concorrentes, permitindo a baixa do custo deste método que inicialmente era elevado. [78]

4.1.6.2 Decisão de identificação do gestor frota

Este último paragrafo não estará diretamente relacionado com a identificação do condutor, mas sim com a autenticação do gestor da frota. Como mencionado anteriormente, uma plataforma de *BackOffice* é expetável no sistema global. Estando a presente empresa equipada com um sistema de domínio AD*,* é perfeitamente viável que a autenticação do utilizador na aplicação de *BackOffice* se faça através do seu *login* Windows, integrando o processo de autenticação de domínio na aplicação. As restrições e atribuições de direitos de acesso podem ser geridas através de grupos de segurança do AD, o que seria uma vantagem.

4.1.6.3 Decisão de identificação e validação da carta de condução

Esta parte será talvez o maior desafio do sistema global. Como já referido anteriormente, uma carta de condução não contem nenhum elemento de segurança a não serem os hologramas. Não existe chip *contacless*, como nos passaportes, não existe chip de contacto nem outro componente eletrónico capaz de identificar uma carta de condução com recurso a *hardware*. A verificação deste documento deverá ser feita através da análise dos hologramas de segurança, nomeadamente os padrões do mesmo. A técnica de OCR irá ajudar a efetuar a leitura dos dados inscritos na carta e poderia resolver o problema, mas imagine-se que o utilizador apresenta uma fotocópia da sua carta de condução? A técnica de OCR provavelmente iria detetar as informações na carta, mas não seria capaz de validar se esta se tratava verdadeiramente de um documento ou uma fotocópia. O condutor pode ter ficado com a sua licença suspensa ontem e hoje apresentar uma fotocópia. Assim, é necessário que se efetue uma verificação aos únicos elementos de segurança presentes numa carta de condução ou seja os hologramas.

A verificação da presença de hologramas poderá ser feita através do recurso a técnicas de *pattern matching*, usadas para a comparação de imagens. Neste caso, é necessário como é normal, executar comparações com padrões retirados à *priori* de uma carta de condução válida e autêntica. Além disso, é necessário definir padrões de acordo com o país da carta de condução que é apresentada, pois os hologramas variam de país para país como é óbvio. Será assim necessário, não só a deteção dos hologramas presentes na carta de condução, eliminando uma boa parte de possíveis apresentações fraudulentas, mas também a deteção dos dados presentes na mesma sob a forma de texto. Só assim o sistema será capaz, não só de verificar a autenticidade da mesma, mas também de a associar ao condutor que se identificou no sistema por via do reconhecimento da íris.

4.1.6.4 Decisão de identificação da chave da viatura

A identificação da chave apresentada ao sistema terá de ser feita através de leitores de *transponders*. Não é justificável a instalação de tacógrafos digitais, não só pelo custo, mas sobretudo porque não resolvem literalmente o problema. A chave terá sempre de ser identificada para garantir que o condutor irá utilizar a viatura correta. O tacógrafo apenas iria ter utilidade na aquisição de dados de diagnóstico da viatura, pois este não impediria que a viatura se ligasse ou não.

Anteriormente já foi demonstrado que é possível uma leitura da chave em modelos mais recentes, pelo que esse será o caminho a explorar e a seguir. Porém, como também já foi referido, os fabricantes automóveis são bastante fechados no capítulo da eletrónica, pois se forem demasiados abertos, a segurança da viatura pode ser comprometida e ser alvo de pirataria, como foi no caso da BMW e Jeep. Assim uma alternativa para identificar chaves poderá ter lugar, no caso da impossibilidade de adquirir diretamente do *transponder* da chave a sua identificação.

Sabe-se também que as chaves contêm hoje em dia variadíssimas informações relativas à viatura. Por esse prisma é factível que dados de diagnóstico como serviços a efetuar, quilómetros ou mesmo o nível de combustível sejam importados no sistema/plataforma aquando da leitura da chave, na medida em que a interação com esta seja possível.

4.2 Desenho

Nesta secção, uma arquitetura do sistema será apresentada, com o objetivo de esquematizar e separar tarefas física e logicamente. A boa arquitetura de um sistema é determinante para o seu bom funcionamento, como também poderá trazer enormes benefícios no futuro em caso de melhorias ou implementações de novas funcionalidades.

Deste modo, a fase de desenho de um projeto ou solução é tão ou mais importante que a fase de implementação, pois esta vai decidir e traçar o futuro da mesma, trazendo com isso as possíveis falhas a longo-termo ou não.

Na Figura 30 a seguir é apresentada uma arquitetura simples do sistema pretendido e proposto. O sistema será composto por dois componentes principais, o *Authentication System* responsável pela autenticação do utilizador e carta de condução e pelo *BackOffice*, responsável pela gestão de informações de apoio ao componente *Authentication System*. Por fim, o sistema conta ainda com dois componentes de suporte, um servidor de base de dados e um domínio/AD já existente.

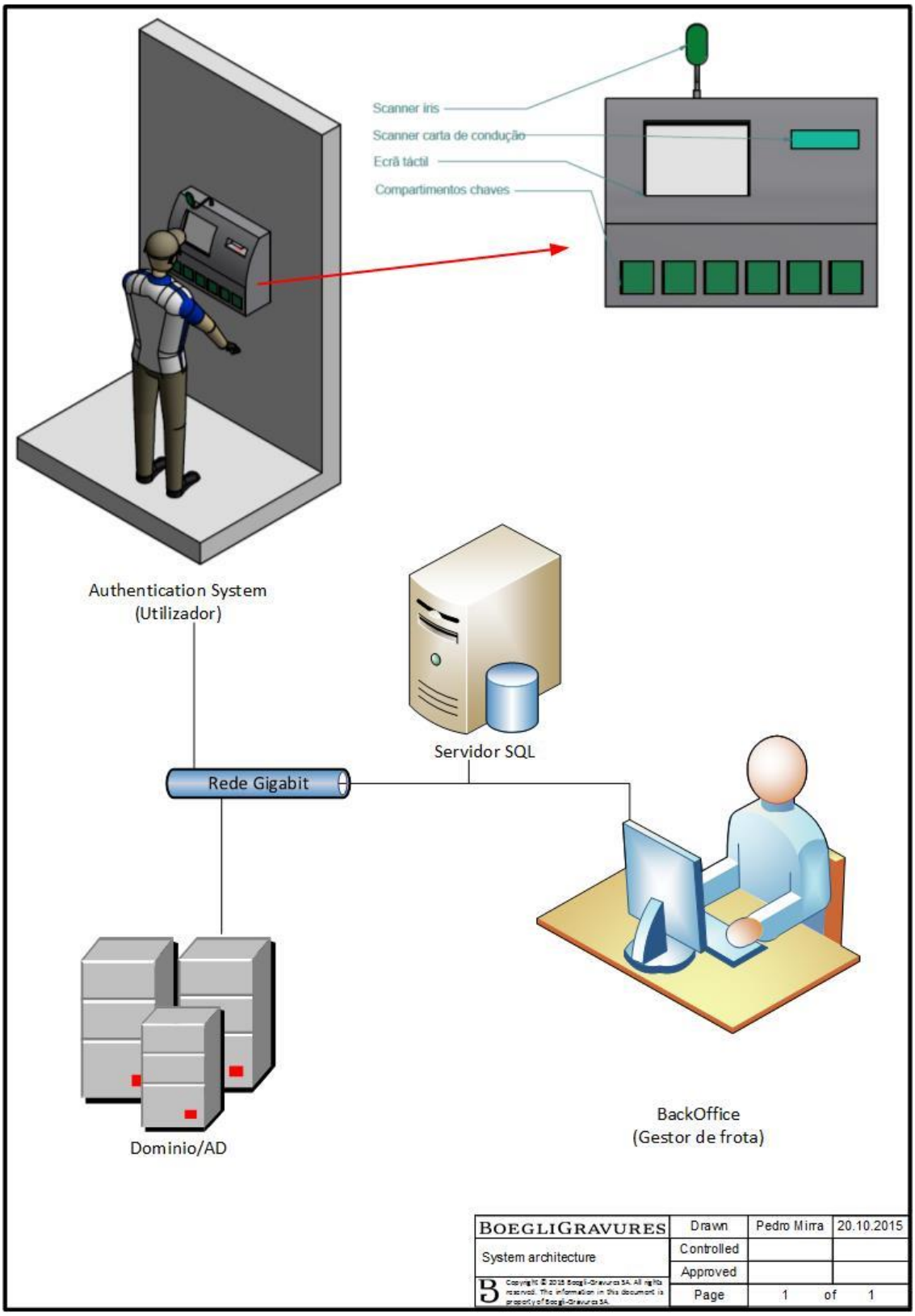


Figura 30 – Arquitetura do sistema

De seguida são abordados os componentes que fazem parte da arquitetura do sistema em cima proposto.

4.2.1 Componentes do sistema

De maneira que o sistema seja mais flexível e de mais fácil construção, um desenvolvimento por módulos é aconselhável. Reforçando a ideia de um desenvolvimento modular, apoia-se o fato de serem três partes de domínios diferentes, pelo que facilita a esquematização e a organização do processo e funcionalidades. A Figura 31 ilustra o diagrama de componentes desejado para a solução. Partindo do princípio das três partes acima descritas, pode-se efetuar uma separação modular do sistema.

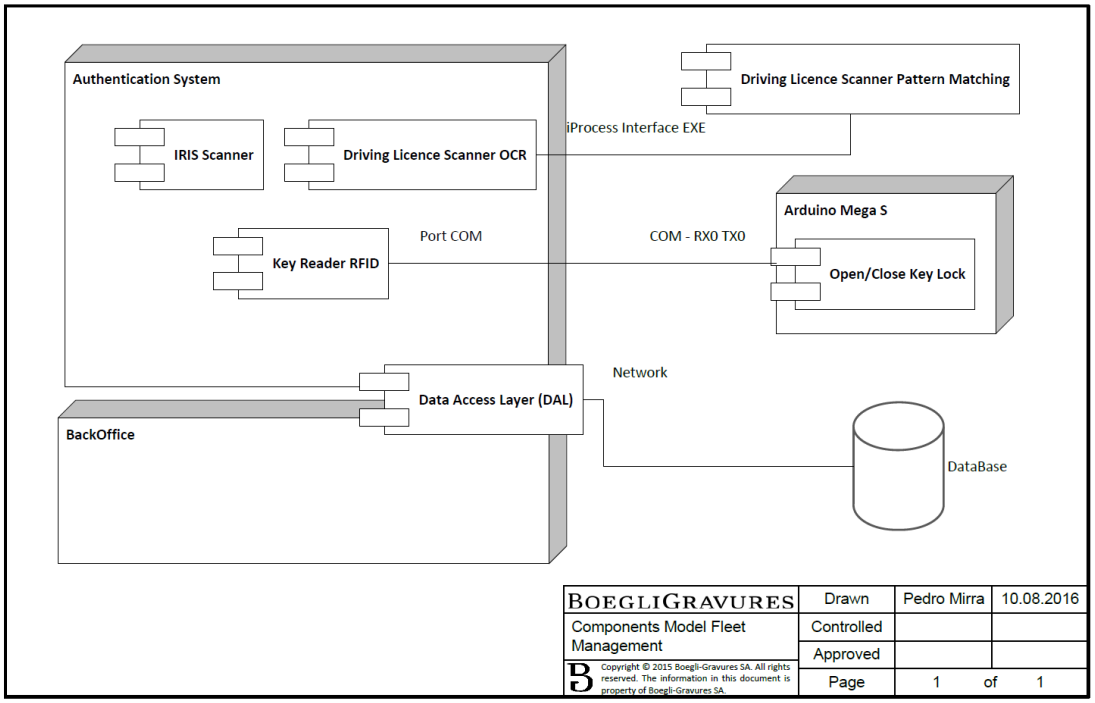


Figura 31 – Diagrama de componentes da solução

A arquitetura global do sistema está representada na Figura 31 e é composta por três partes fisicamente separadas (Arduíno Mega S é incorporado no componente *Authentication System*), que por sua vez podem estas também terem componentes físicos amovíveis. A estrutura conta ainda com uma base de dados de apoio à aplicação. De seguida são descritos cada um dos componentes:

- **Authentication System**

O *Authentication System* é o componente composto pelo computador denominado de repositório de chaves. Este componente será duplicado num segundo local. Trata-se de um computador com recurso a ecrã táctil e será responsável pela autenticação dos utilizadores,

validação dos documentos e identificação das chaves. Estas responsabilidades poderão como dito anteriormente, ser amovíveis em subcomponentes. Será aqui instalado a parte principal do sistema a implementar que contempla:

- *Iris Scanner*

Tal como o nome indica, este pequeno componente, será englobado no *Authentication System* e terá a responsabilidade de efetuar a leitura da íris dos utilizadores e transmiti-la ao componente pai.

- *Driving Licence Scanner*

O componente *Driving Licence Scanner* irá ser responsável por fazer a captação de imagem da carta de condução do utilizador/condutor e em seguida a verificação OCR e do holograma.

- *Key Reader*

O *Key Reader* é um componente importante para o sistema. Este será o responsável pela identificação e leitura das chaves das viaturas, repatriando estas informações para o componente *Authentication System*.

- Arduíno Mega S

Um Arduíno é um pequeno componente físico. Caracteriza-se como um microprocessador com varias entradas e saídas de sinais, analógicos e digitais. Este componente será útil para o controlo de fechaduras de cada compartimento das chaves.

- **BackOffice**

O *BackOffice* não é mais que uma segunda parte do sistema, que permitirá ao gestor/supervisor da aplicação, funcionalidades de gestão de utilizadores, viaturas, reservas entre outras. Este poderá ser instalado em qualquer posto Windows com conexão à rede (domínio/*active directory)* e servidor de base de dados da aplicação.

- **Data Access Layer - DAL**

O componente DAL é o componente responsável pelo acesso à informação da base de dados. É também o componente que integra a lógica de negócio da aplicação, sendo então responsável por manter a coerência e conformidade da informação. Este componente é partilhado entre o componente *BackOffice* e *Authentication System.*

- **DataBase**

A base de dados, tal como num outro qualquer sistema, servirá de suporte à plataforma no seu todo. Será através dela que os dois locais de repositórios de chaves serão alimentados e sincronizados, bem como o *BackOffice.* Na base de dados irão estar presentes informações acerca dos utilizadores e respetivos dados biométricos, viaturas, reservas e padrões de cartas de condução a comparar entre outros dados úteis ao sistema.

4.2.2 Modelo de dados

O modelo de dados tem como função servir de base de organização da informação e de seguida dar alma à base de dados. O modelo de dados conterá a informação necessária à aplicação e servirá também como ponto de sincronização entre os diferentes locais de repositórios de chaves. As alterações e ações por parte do cliente deverão ser tidas em conta na base de dados para evitar incoerências. De seguida, explica-se a estrutura da base de dados, assim como se explica o porquê desta, sabendo que obviamente, esta base de dados evoluirá com o tempo, através de novas necessidades e melhorias por parte da aplicação. Assim, uma estrutura tendo em conta as boas práticas de desenho de base de dados é apresentada na Figura 32.

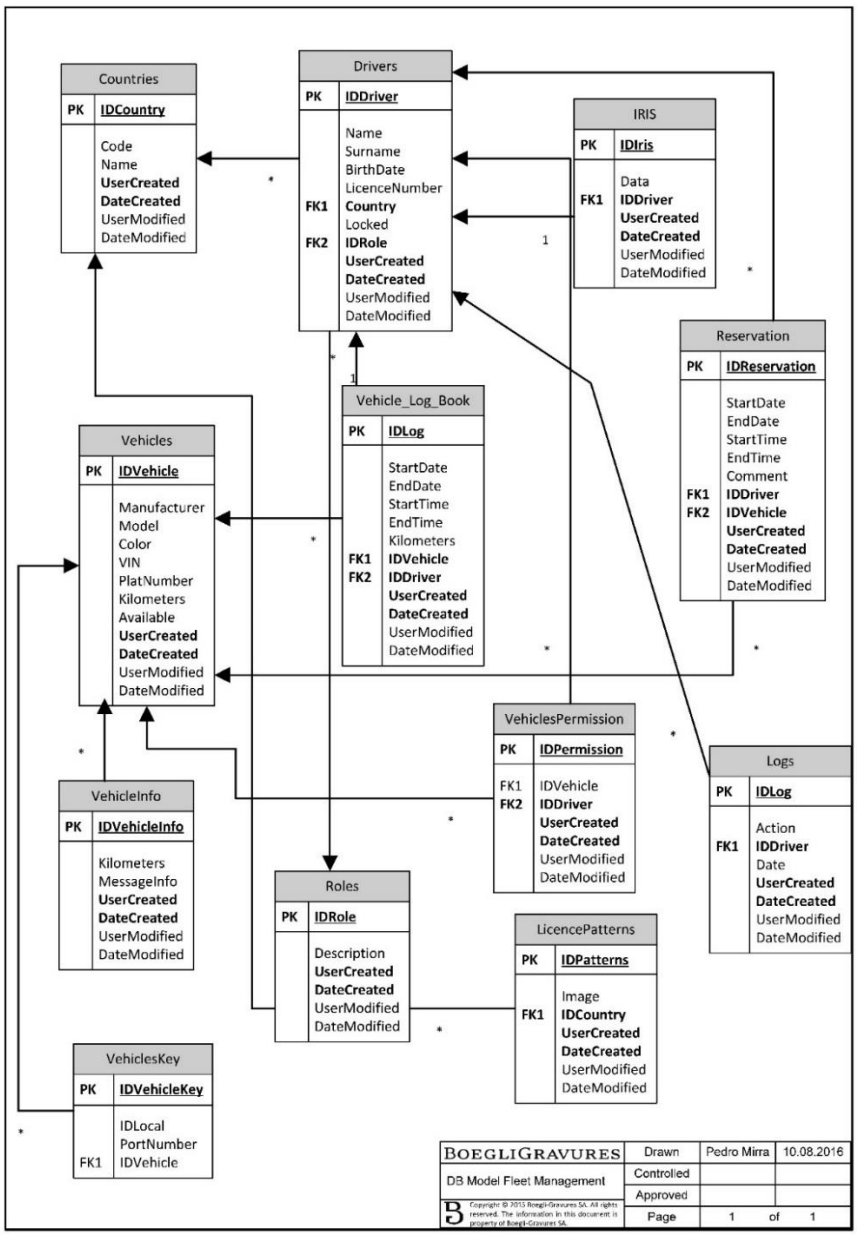


Figura 32 – Modelo de dados

- A tabela "*Supervisors*" conterá informação relativa aos gestores da frota. A separação desta entidade da entidade "Drivers" prende-se com o fato de um gestor nem sempre ser um condutor e vice-versa. Desta forma em termos de gestão e implementação do *software*, são duas abordagens diferentes.

- A tabela "Drivers" irá conter informações acerca dos condutores, nomeadamente o nome, número de carta de condução, proveniência, foto e atributos de gestão como "*Enabled*" ou "*DeletedDriver*". O atributo "*Enabled*" permitirá bloquear ou não o condutor a utilizar as viaturas, enquanto "*DeletedDriver*" o "apaga" do sistema. Na verdade não o apaga, apenas lhe mudará um estado. Este estado, analisado pelas aplicações cliente (*Authentication System e BackOffice)*, permitirá decidir a sua apresentação no sistema ou não. Não se pretende apagar condutores em definitivo do sistema por razões de traçabilidade.

- A tabela "Countries" permitirá conter uma lista de países. Esta lista será depois utilizada nas tabelas de "Drivers" e "*LicencePaterns*" para identificar no caso da entidade "Drivers" a proveniência da carta de condução. Esta proveniência é importante, pois países diferentes têm hologramas diferentes, logo padrões diferentes. Esta última entidade, "*LicencePatterns*" armazenará os padrões e hologramas a reconhecer nas cartas de condução para o determinado país.

- A tabela "Iris" como o próprio nome o deixa adivinhar, trata-se de uma tabela que armazenará os dados biométricos do condutor, neste caso, da sua íris.

- A tabela "*Vehicles*" servirá de repositório de informação de base de uma viatura, nomeadamente a marca, o modelo, o VIN, matrícula entre outros. De notar mais uma vez os seguinte atributos da entidade em causa, "*Available*" e "*DeletedVehicle*". O atributo "*DeletedVehicle*" e "*Avaliable*" são em tudo semelhantes aos atributos "*DeletedDriver*" e "*Enabled*" da entidade "Drivers" e as suas funções equiparam-se respetivamente.

- A tabela "*Vehicle_Info*" funciona como uma entidade auxiliar de informações sobre as viaturas, em que nesta não estarão presentes informações de base mas sim informações/alertas recolhidos da chave ou introduzidos manualmente pelo gestor da frota.

- A tabela "*Vehicle_Log_Book*" será o local de armazenamento do diário de bordo das viaturas, onde por cada utilização da viatura, um registo será criado. Assim, um diário de bordo será mantido por cada viatura, que dirá ao gestor que "O condutor C1 utilizou a viatura V1, de uma data D1 a uma data D2 e os quilómetros atuais são Q1", por exemplo.

- A tabela "*Vehicles_Permission*" permitirá atribuir ou retirar o acesso a viaturas a determinados condutores. Um registo nesta entidade entre a identificação do condutor através do atributo "*IDDriver*" e a identificação da viatura que este tem acesso através do atributo "*IDVehicle*", permitirá ao sistema determinar se este tem permissão de acesso à viatura.

- Por fim a tabela "*Logs*" terá unicamente como objetivo o registo de todas as ações efetuadas no sistema, de maneira a manter uma traçabilidade num aspeto global, permitindo ao administrador da aplicação saber todo o fluxo do sistema.

De notar que em todas as tabelas existem os seguintes quatro atributos *"UserCretead", "DateCreated", "UserModified", "DateModified".* Estes quatro atributos permitem também ao administrador identificar para cada registo, quem foi o responsável pela criação ou modificação e também a respetiva data.

4.2.3 Diagrama de classes

Nesta secção é apresentado o diagrama de classes. Este diagrama é a esquematização da estrutura e relações das classes que servem de modelo para os objetos da solução. O diagrama de classes apresentado na Figura 33 permite obter uma imagem do sistema a desenvolver, servindo e facilitando depois na construção da aplicação em termos de estrutura e comunicação entre os objetos.

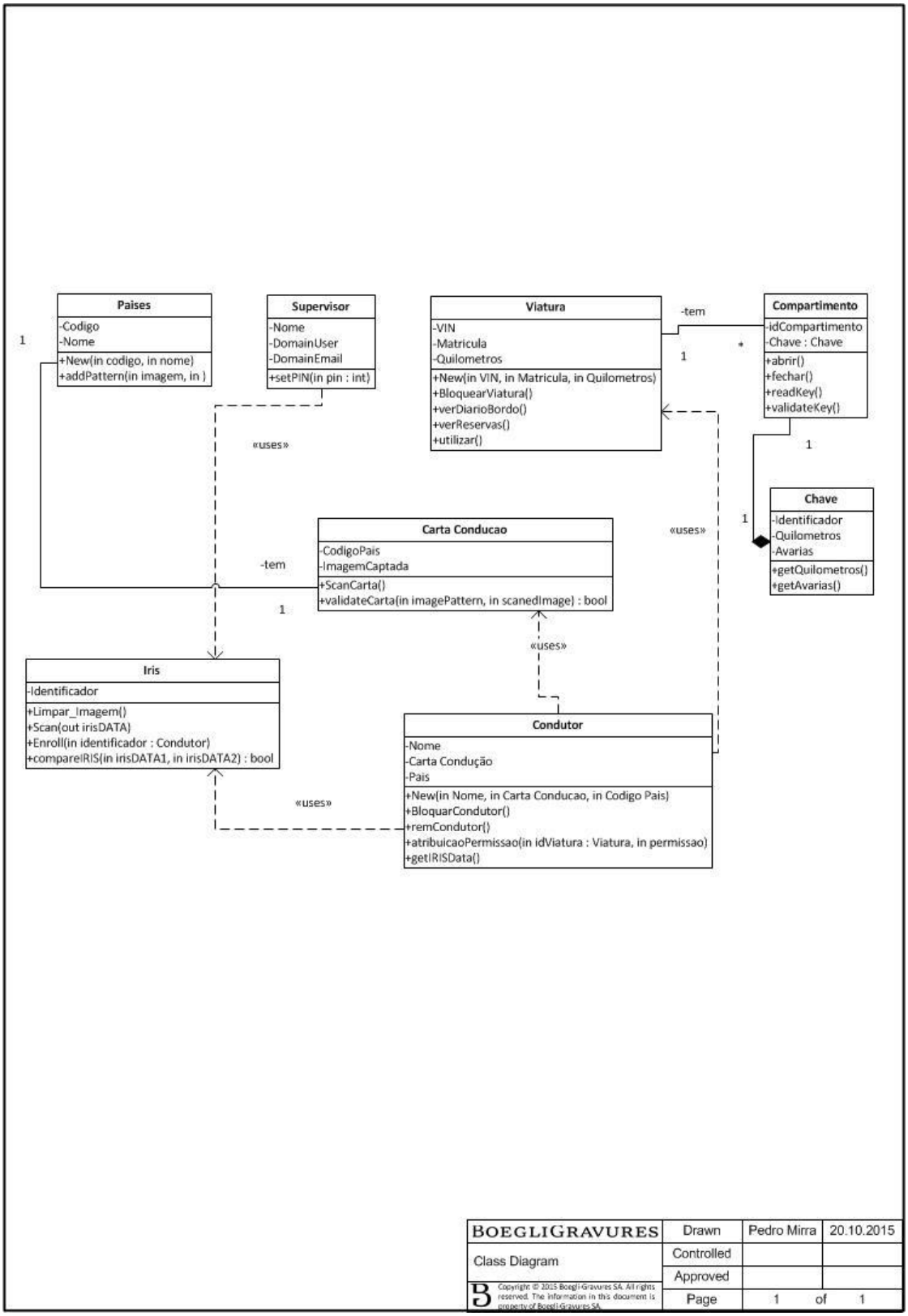


Figura 33 – Diagrama de classes

4.2.4 Interface gráfica

Nesta secção serão apresentados alguns exemplos pretendidos para a interface gráfica. Esta deve ser simples e de fácil uso, prevendo um manuseamento da componente *Authentication System* através de um ecrã táctil.

4.2.4.1 Authentication System

Para o componente *Authentication System* foram projetadas as janelas da interface gráfica apresentadas a seguir pelas Figuras 34, 35, 36, 37 e 38.

A Figura 34 apresenta a janela principal de entrada no sistema de autenticação (*Authentication System)*. Esta janela é composta por três botões que permitem o início do processo de autenticação, a devolução de uma chave e a autenticação como gestor/supervisor da frota.

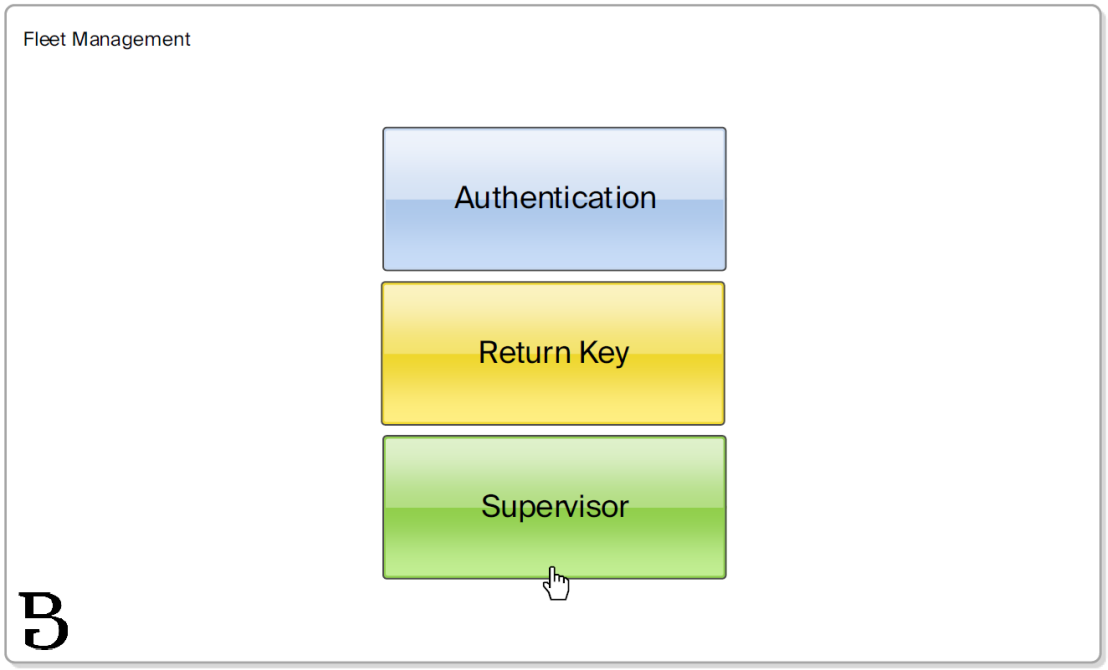


Figura 34 – Authentication System, janela principal

A Figura 35 mostra a janela de autenticação do condutor e verificação da carta de condução. Esta janela apenas contém um barra de carregamento, indicativa do estado do processo de autenticação do condutor e sua carta de condução.

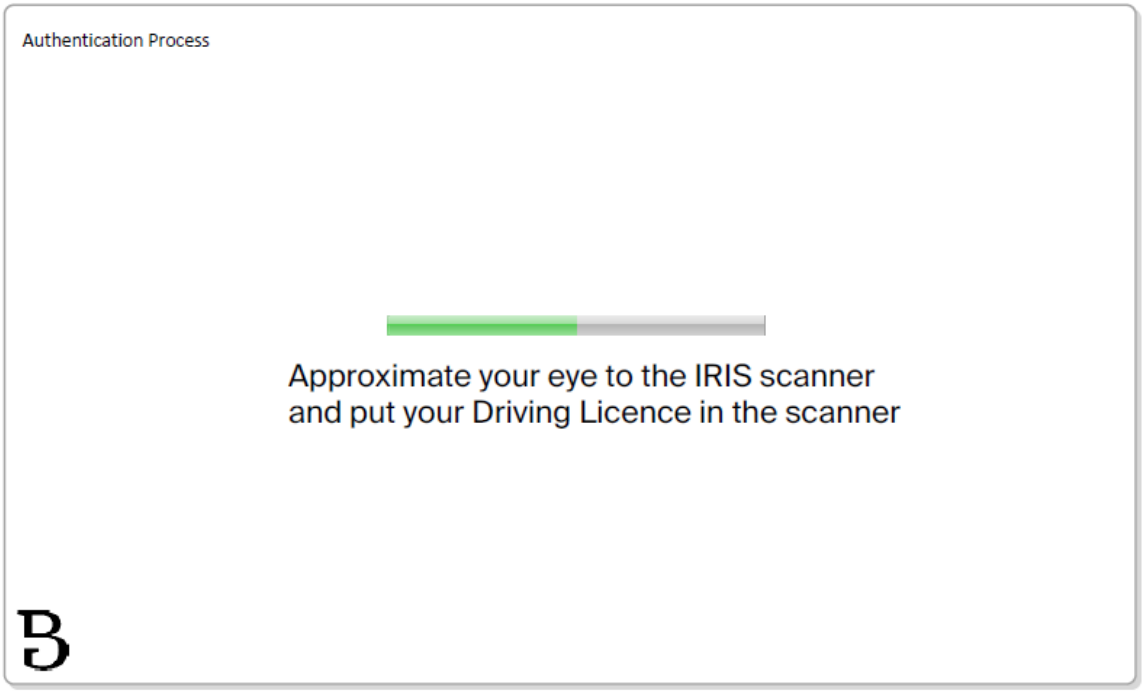


Figura 35 – Authentication System, autenticação utilizador/condutor

A Figura 36 apresenta a janelas de escolha de viaturas por parte dos utilizadores/condutores. Esta janela sucede à janela anterior caso o utilizador e sua carta de condução sejam autenticados no sistema. É composta por um cabeçalho contendo informações do condutor autenticado e por uma lista de viaturas disponíveis para o mesmo poder escolher. Cada linha desta lista é composta pelas informações do veículo e um botão para ativar a escolha.

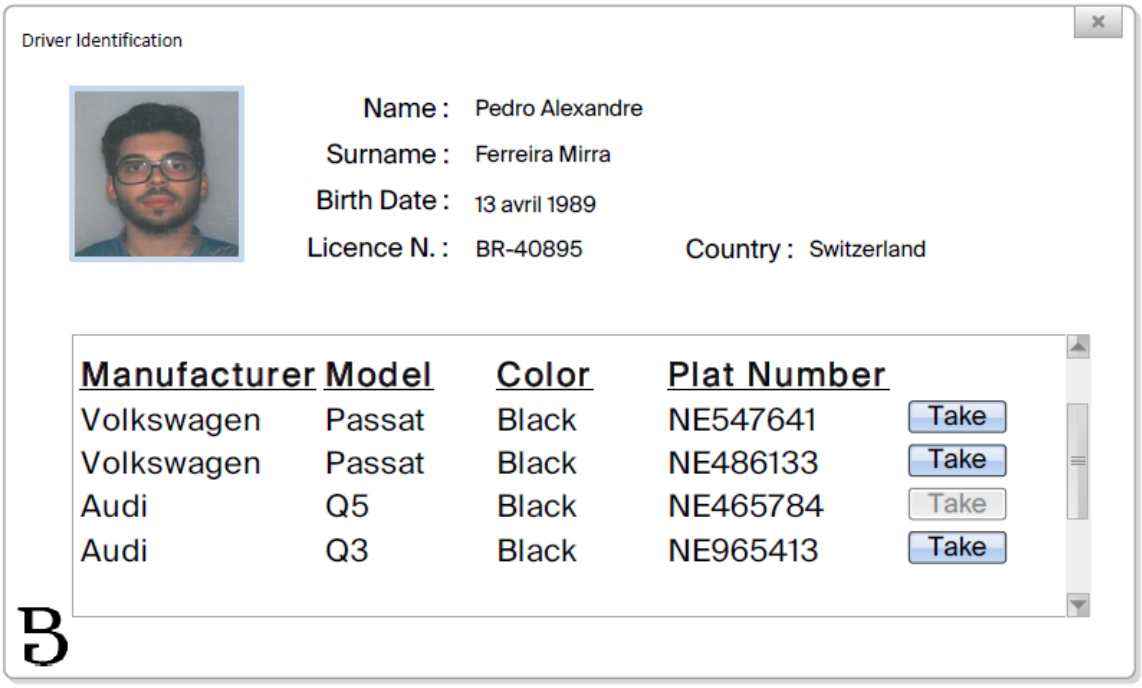


Figura 36 – Authentication System, escolha de viaturas por parte do utilizador/condutor.

A Figura 37 apresenta a janela de autenticação do gestor de frota no componente *Authentication System*. Esta é composta por um teclado numérico constituído por doze botões, permitindo ao gestor da frota inserir o seu PIN de identificação e consequentemente autenticar-se.

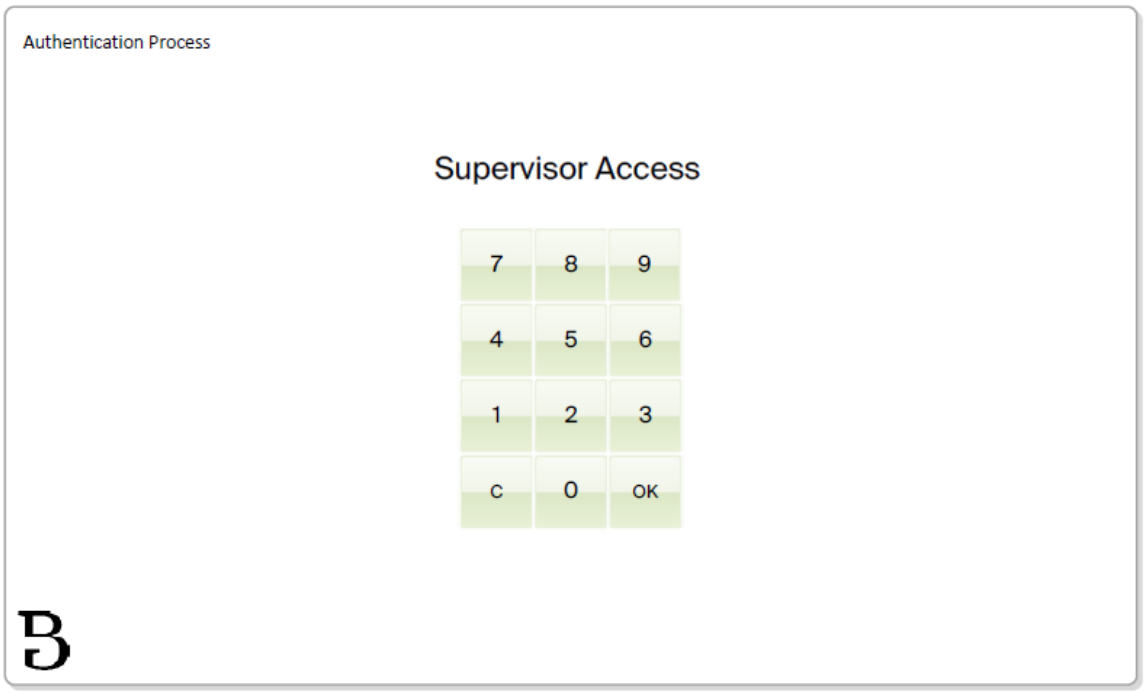


Figura 37 – Authentication System, autenticação gestor de frota

A Figura 38 mostra a janela de registo dos dados biométricos do utilizador/condutor. Esta permite ao gestor de frota efetuar o registo de dados biométricos dos utilizadores no sistema. É composta por uma lista de utilizadores registados no sistema e suas informações, bem como um botão de ação por cada utilizador, permitindo o início do processo de registo dos dados biométricos.

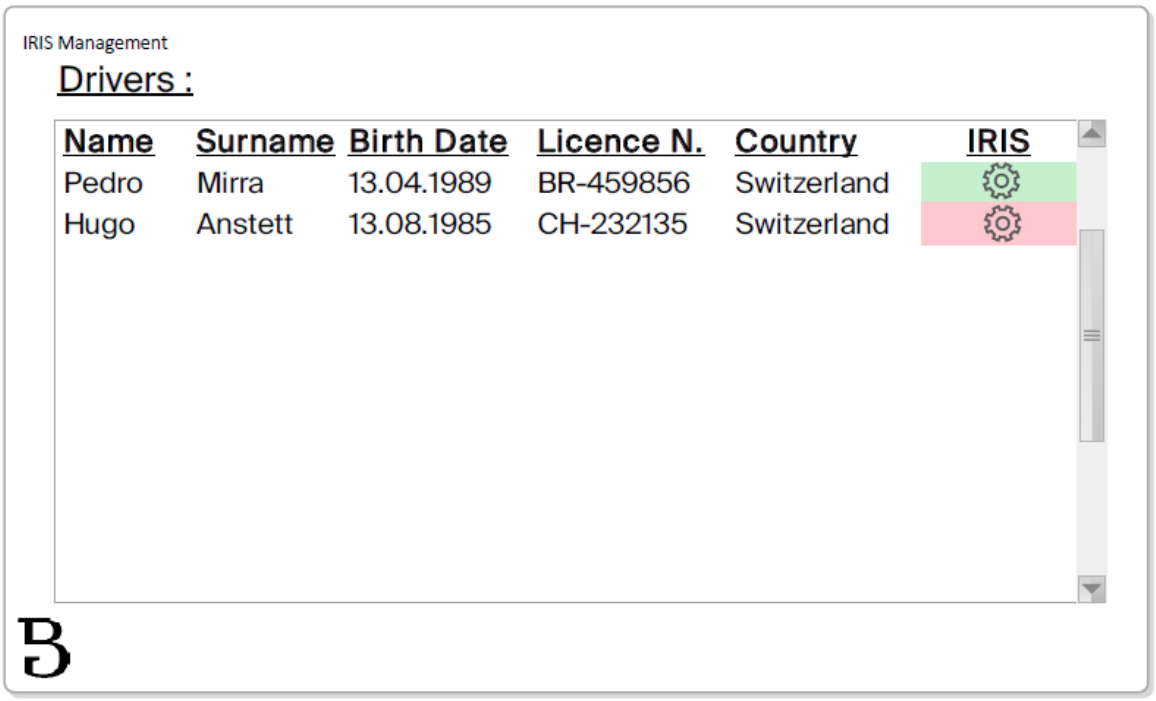


Figura 38 - Authentication System, registo dados biométricos de utilizadores/condutores.

Observação: A célula IRIS em vermelho significa que o utilizador ainda não gravou os seus dados biométricos ao contrário da cor verde. Através do clique no símbolo de "engrenagem", será possível efetuar o registo dos dados biométricos para o utilizador.

4.2.4.2 BackOffice

Para o componente *BackOffice* foram projetadas as janelas da interface gráfica apresentadas a seguir pelas Figuras 39, 40, 41 e 42.

A Figura 39 apresenta a janela principal do componente *BackOffice*. Esta é composta por três botões permitindo ao Supervisor/gestor da frota direcionar-se aos menus de gestão de utilizadores, gestão de veículos ou reservas.

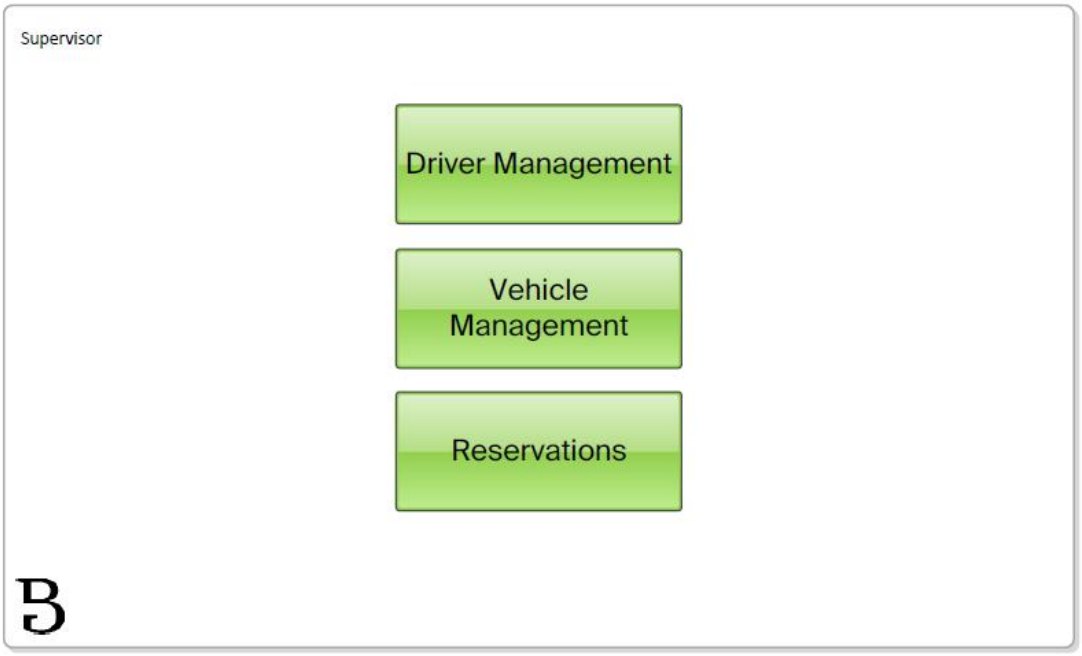


Figura 39 – BackOffice, janela principal

A Figura 40 demonstra a janela de gestão do utilizador/condutor. Esta janela permite ao gestor da frota a manipulação dos dados do utilizador e a atribuição de permissões sobre viaturas do mesmo. Esta é composta por um cabeçalho que contém as informações do utilizador e uma lista das viaturas presentes no sistema. Esta lista contém as informações principais das viaturas e uma *checkbox* que se ativada, permite o acesso a essa viatura por parte do utilizador em questão.

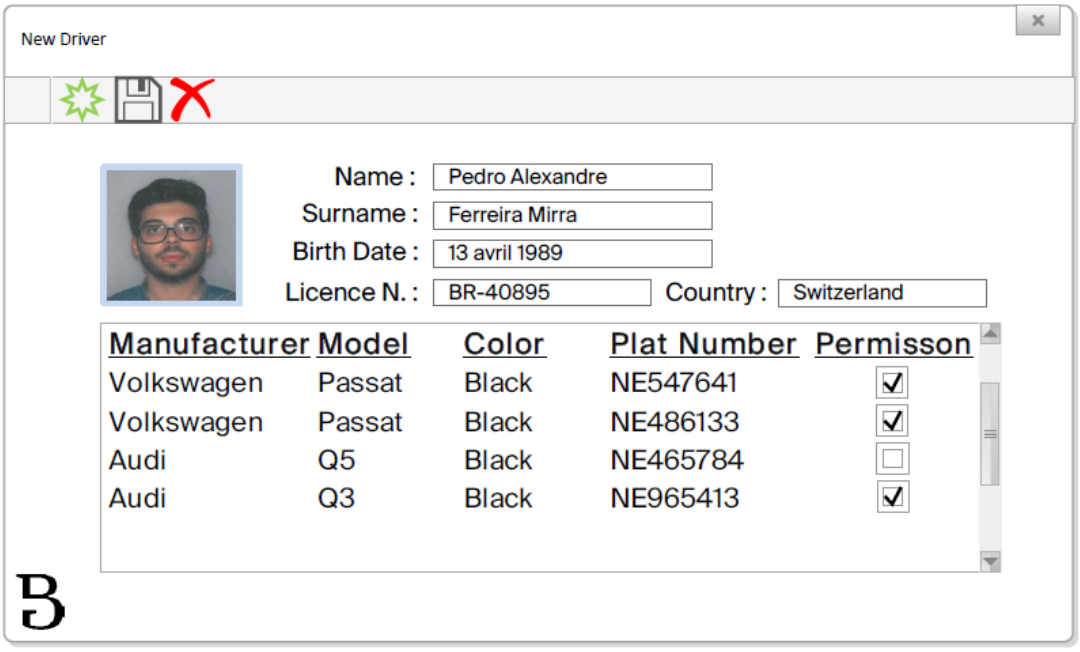


Figura 40 - BackOffice, gestão utilizadores/condutores e suas permissões

A Figura 41 apresenta a janela de gestão de viaturas e visualização do diário de bordo. Esta é composta por um cabeçalho que contém as informações do veículo e uma lista que representa o registo de utilização do mesmo. Esta lista é composta pelo início e fim da utilização, os quilómetros após o fim da utilização e o utilizador.

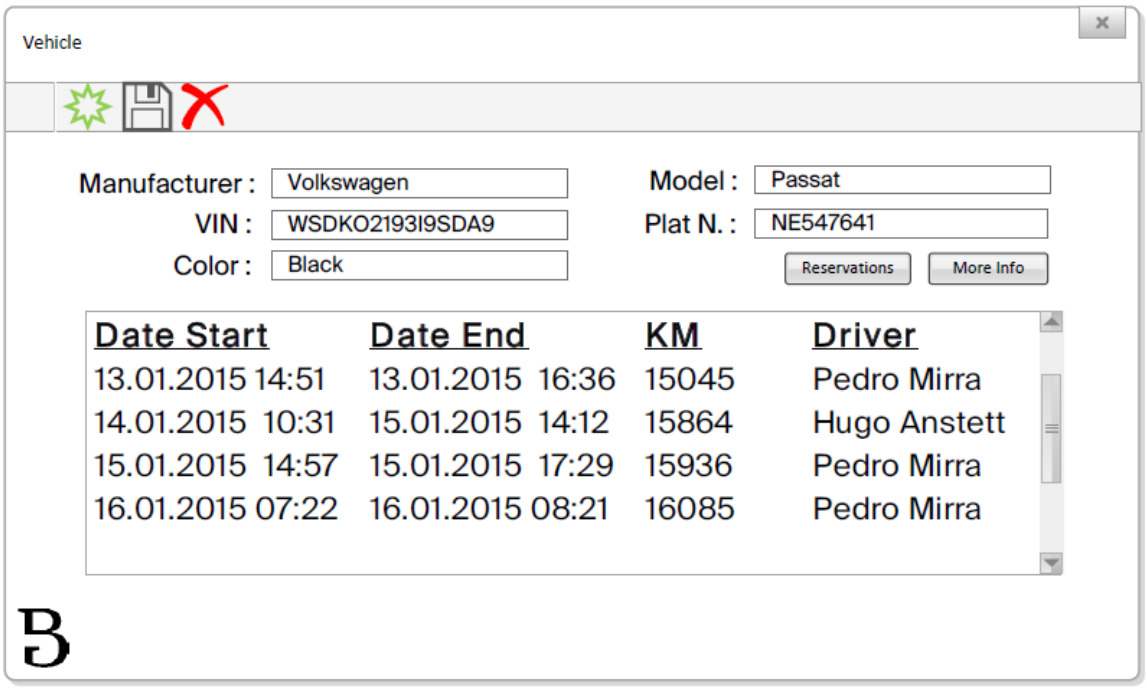


Figura 41 - BackOffice, gestão viaturas e diário de bordo

Na Figura 42 é mostrada a janela de introdução de reservas de viaturas. Esta janela permite ao supervisor/gestor da frota introduzir reservas sobre um veículo, garantindo que este esteja disponível quando for necessário. O supervisor escolhe a data de início e fim da reserva, bem como o veículo a ser reservado e por quem será utilizado.

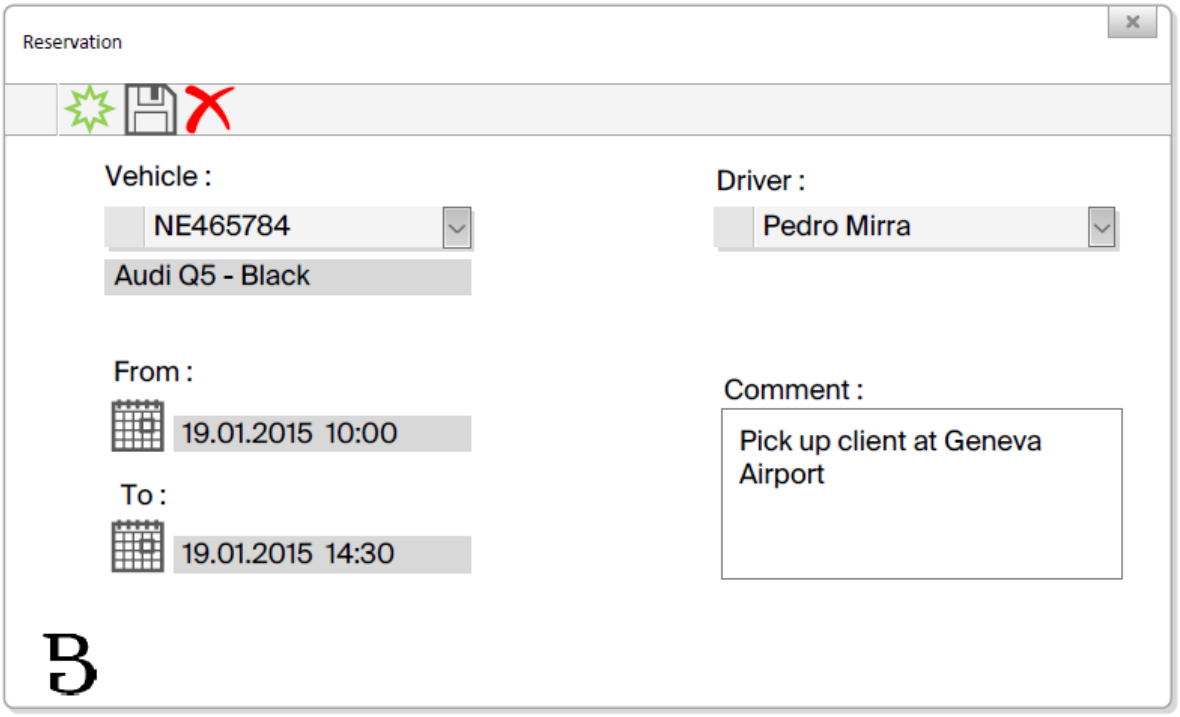


Figura 42 - BackOffice, introdução de reservas de viaturas

4.3 Implementação

Nesta secção irá ser explicada não só a implementação como o seu método. Como sabido anteriormente, o problema global foi modularizado em quatro questões a responder/resolver:

P1. Como garantir ao máximo possível, que o utilizador que se apresenta é quem diz ser?

P2. Como efetuar uma verificação do seu documento legal de habilitação de condução?

P3. Que mecanismos devem ser implementados para garantir a entrega e devolução correta das chaves das viaturas?

P4. Como obter informações automaticamente das viaturas a gerir?

O método global de desenvolvimento do projeto utilizado foi o processo ágil – iterativo e incremental, em que todo o processo de definição e implementação da solução passa pelo levantamento de requisitos, planeamento, desenho, implementação, distribuição e acompanhamento. De notar que a etapa de implementação teve como método escolhido a programação modular, em que cada componente e seus objetos foram desenvolvidos e testados separadamente antes de serem integrados na solução global com a exceção do componente *Data Access Layer* - DAL. Este último, visto ser partilhado pelos dois principais componentes foi desenvolvido paralelo, ou seja, foi sendo incrementado à medida que novas funções de acesso aos dados foram sendo necessárias.

Esta metodologia permitiu uma menor distância entre o pretendido pela empresa e o produto final, visto os componentes serem implementados e testados separadamente. Permitiu também uma melhor definição das questões P1, P2, P3 e P4, evitando derrapagens do projeto devido a más definições de requisitos. Na secção a seguir é apresentada a implementação do primeiro e mais importante componente da solução, o componente *Authentication System*, bem como os seus subcomponentes e ligações.

Assim, torna-se óbvio e lógico a implementação da solução global de uma forma modular ao nível de funções de cada componente (subcomponentes). No entanto, para além da resolução destes, é necessário ter em conta toda a infraestrutura necessária para o bom funcionamento da solução final. Na secção anterior (4.2 – Desenho) a modularização do problema principal é esquematizada, onde é possível verificar que existem duas partes bem distintas. A primeira parte, correspondente ao componente *Authentication System*, que é na verdade o coração da solução, pois é este que permite a resolução e execução das tarefas formalizadas nas perguntas P1, P2, P3 e P4.

A segunda parte mas não menos importante, corresponde ao componente *BackOffice*. Este componente apesar de não estar relacionado com a resolução/execução das tarefas P1 a P4, é importante para o bom desenrolar da solução final, na medida que permite capacitar a solução final de resposta às necessidades funcionais básicas, como inserção/remoção de utilizadores/viaturas, reservas de viaturas entre outras já explicitadas na secção 4.1 – Análise. A implementação deste segundo componente irá ser brevemente apresentada, sem bastante detalhe, visto ser apenas um componente de suporte à solução global que não está diretamente implicado na resolução do problema principal.

O primeiro componente *Authentication System*, é então composto por subcomponentes com tarefas bem distintas. Alguns destes como o *Iris Scanner* e *Key Reader* estão completamente incorporados na solução sob a forma de classes/objetos devido a sua "simplicidade" de utilização, outros, como o *Driving Licence Scanner*, estão separados da solução global (bibliotecas de acesso DLL/executáveis externos) com o objetivo de manter a arquitetura do sistema global o mais uniforme e limpa possível.

O subcomponente *Driving Licence Scanner* por exemplo, necessita de bibliotecas (OpenCV) que obtêm um maior rendimento quando executadas através da linguagem de programação C++. Para finalizar, o ponto comum entre ambos é a base de dados. É através desta que os dois componentes "comunicam". Assim, um componente de acesso a esta é partilhado pelos dois (*Data Access Layer* – DAL). Este componente é obviamente externo aos dois principais componentes e apresenta-se sob o formato de biblioteca DLL desenvolvida em linguagem de programação C#.NET.

4.3.1 Authentication System

Este componente contém os subcomponentes/objetos responsáveis pela resolução e tarefas das perguntas/problemas a resolver P1 a P4. É um programa desenvolvido em linguagem C# utilizando o *framework* .NET 4.6. Este componente contém todos os subcomponentes necessários às suas tarefas e será instalado num computador com recurso a um ecrã táctil. Este componente está presente nos dois pontos de requisição de chaves (repositórios), locais onde as chaves serão armazenadas e os utilizadores poderão requisitar e devolver as chaves. Será também o local de "registo da íris" dos utilizadores, ou seja, após a inserção do utilizador/condutor no sistema por parte do gestor através do componente *BackOffice*, o utilizador deverá efetuar o seu registo biométrico na presença do gestor da frota no componente *Authentication System*. Para o efeito, um método de *login* para gestores neste componente é providenciado. Este *login* de supervisor permite também ao gestor da frota aceder às chaves sem necessidade de se autenticar, formando como uma "*backdoor*" de acesso em caso de avaria de algum dos componentes que impossibilite a utilização do sistema.

A interface gráfica é bastante simples e prática. Na janela principal ("*home*"), três opções: Autenticação, Devolução de Chave, Autenticação de Supervisor/Gestor. Na seguinte Figura 43, a janela principal ("*home*") é apresentada.

BOEGLIGRAVURES

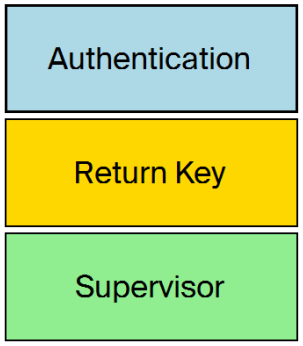


Figura 43 – Janela principal componente Authentication System

A opção Autenticação, como o próprio nome indica, permite ao utilizador se identificar e autenticar perante o sistema ao mesmo tempo que valida a sua licença de condução. Em seguida é apresentada a lista de veículos disponíveis para seu uso dependendo claramente das suas permissões, de reservas efetuadas e de disponibilidade da viatura no dado momento.

A Figura 44 mostra a janela após *login* do utilizador "Pedro Mirra".

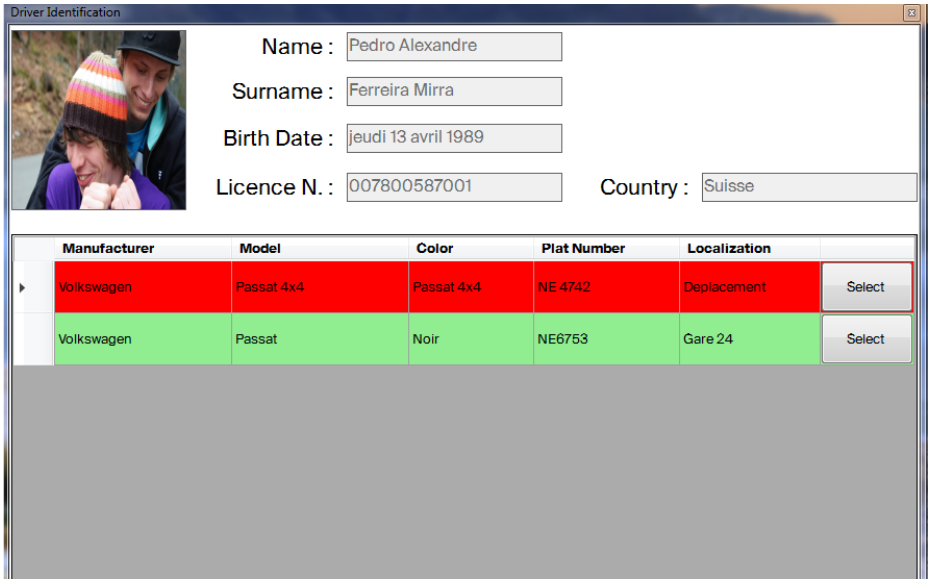


Figura 44 – Janela de utilização de veículos após *login* bem-sucedido

A segunda opção, devolução de chave, permite aos utilizadores devolverem a chave que têm em posse. Não existem nenhuma janela específica associada a esta função. Após clique, uma pequena barra de carregamento é mostrada para informar o utilizador que deve pousar a chave no repositório indicado. Em paralelo é chamado o componente *Key Reader* que se encarrega de efetuar a identificação da chave. Após a identificação da chave, o componente *Authentication System* sabe então de qual viatura se trata, quem a requisitou e pode então fazer a sua aceitação ou recusar a chave por algum motivo, nomeadamente, erro de leitura da chave ou inconsistência dos dados.

Por último, a terceira opção, Autenticação de Supervisor, permite ao gestor da frota efetuar *login* para registos biométricos da íris ou por exemplo, para abrir os compartimentos sem necessitar de efetuar *login* biométrico ou apresentar a licença de condução. Estas funcionalidades são uteis em caso de avaria do sistema ou dificuldade de leitura da licença de condução por exemplo.

O *login* efetua-se por intermédio de um código numérico, definido pelo próprio gestor no componente de *BackOffice*. Este código numérico (PIN) é único no sistema, independentemente do número de gestores, ou seja, o código do gestor A é único no sistema assim como o código do gestor B (caso existam múltiplos gestores de frota), à semelhança do que acontece em sistemas de alarme. Este código não é armazenado em *plain text* mas sim o seu *hash.*

Na Figura 45, a janela de acesso em modo Supervisor é apresentada (de relembrar que o componente *Authentication System* será instalado num computador com um ecrã táctil, sem periféricos de entrada como teclado ou rato).

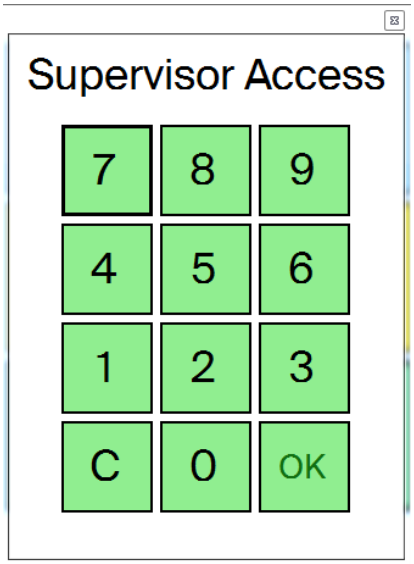


Figura 45 – Janela de *login* de supervisores

Após *login,* é possível ao gestor de frota abrir os compartimentos automaticamente ou definir novos dados biométricos para um utilizador, ou seja, "registar a íris". É também possível ao gestor efetuar uma foto em modo UV de uma licença de condução para obter o seu padrão. Obviamente esta última funcionalidade apenas é necessária quando um novo utilizador do sistema contém uma licença de condução de um país diferente e consequente padrão diferente, como por exemplo a França. Deste modo é necessário que o gestor capte os padrões (hologramas) do novo país a gerir. Na Figura 46 a seguir é possível visualizar a lista de utilizadores do sistema através da qual o gestor pode efetuar o registo biométrico da íris.

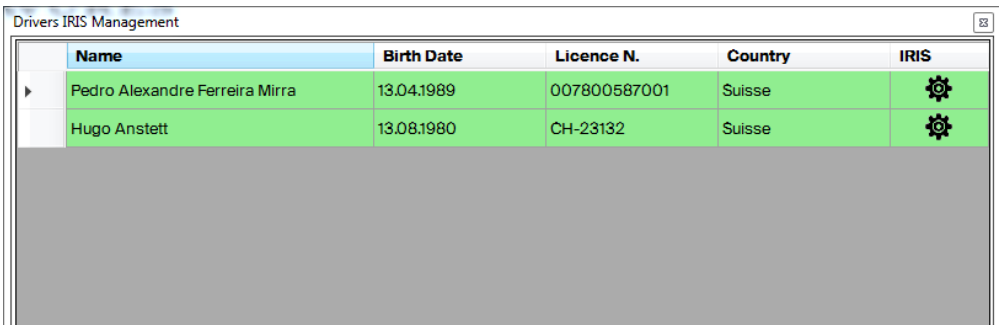


Figura 46 – Janela de registo da íris

Neste caso, os dois utilizadores apresentam-se sobre a cor verde pois a sua íris já se encontra registada. No caso de ausência de dados biométricos a cor vermelha seria a cor de fundo da linha do utilizador. Não obstante, os dados biométricos podem ser registados de novo, por exemplo se o utilizador decidir trocar a íris/olho a utilizar para a identificação e autenticação.

O fluxo de dados neste componente é bastante óbvia. O componente *Authentication System* utiliza o subcomponente *Iris Scanner* para obter a identificação do utilizador presente. Em paralelo utiliza o subcomponente *Driving Licence Reader* que retorna o texto reconhecido da licença de condução pelo método OCR e se esta é uma licença válida (verificação de

holograma). Deste modo, o componente pode saber quem se apresenta e que carta de condução foi apresentada, para de seguida verificar através da base de dados se estes dois identificadores coincidem ou não, visto na base de dados estarem armazenados todos os dados necessários do utilizador (dados biométricos, número de licença de condução, validade, etc.).

No entanto este componente apenas faz sentido se nele se incorporarem todos os subcomponentes esquematizados na secção 4.2.1 – Arquitetura Global, responsáveis pelas tarefas descritas no parágrafo anterior. Assim, nas seguintes subsecções são explicados estes subcomponentes.

4.3.1.1 Subcomponente Iris Scanner

O subcomponente *Iris Scanner* é responsável pelo registo e consequentemente, pela boa identificação e autenticação do condutor/utilizador no sistema. Este subcomponente utiliza a íris humana como método de autenticação biométrico. Se se pretende garantir ao máximo possível, que o utilizador que se apresenta é quem diz ser (P1), então uma forma de autenticação segura e de difícil transmissão é o mais indicado, como é o caso da íris humana.

O Hardware escolhido para o efeito foi o apresentado na secção 3.2.4 – Irishield, modelo MK 2120UO. Este dispositivo monocular, para além de ser "*ready to use*" é extremamente versátil em termos de compatibilidade de sistemas, fornecendo também uma API de utilização em várias linguagens de programação. A API consiste em uma biblioteca DLL pronta a ser integrada na tecnologia .NET, de onde as principais funções a serem utilizadas serão de "registo da íris" e de "comparação da íris" representadas pelas funções na Figura 47 "*EnrollCapture(String)*" e "*Compare11WithTemplate(DataBuffer, float)*" respetivamente.

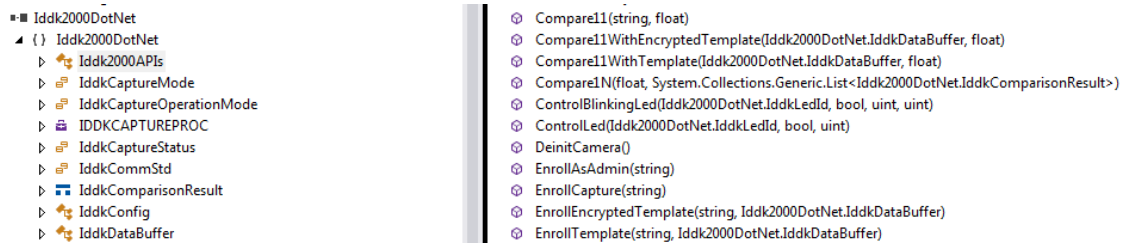


Figura 47 – API Irishield - Funções

Para a captura e registo da íris, o dispositivo/API em questão utiliza como base de dados uma parte da sua memória local, pelo que é necessária a extração da íris registada para envio à base de dados da solução global, pois esta será utilizada em dois locais separados e distintos. No extrato de código seguinte verifica-se na Figura 48 o processo de inicialização do dispositivo e captura da íris, e na Figura 49, a extração do mesmo para envio à base de dados da solução.

```
IddkCaptureStatus captureStatus = IddkCaptureStatus.Idle;   // INICIALIZACAO DO DISPOSITIVO
 string enrollID = "";
IddkSystemRole userRole = IddkSystemRole.Admin;
ret = apis.GetCaptureStatus(out captureStatus);

if (ret == IddkResult.OK)
{
    ResetErrorLevel(ret);
    if (captureStatus != IddkCaptureStatus.Complete)
    {
        CapturingProcess(true, false, false);
    }
}
else
{
    HandleError(ret);
}
 enrollID = IDDriver.ToString();

/* We check the camera status */
ret = apis.GetCaptureStatus(out captureStatus);
if (ret == IddkResult.OK)
{
    // INICIALIZACAO DO PROCESSO DE CAPTURA
    ResetErrorLevel(ret);
    if (captureStatus == IddkCaptureStatus.Complete)
    {
        if (!CheckImageQuality(true))
        {
            return;
        }
        ret = apis.EnrollCapture(enrollID); // CAPTURA DA IRIS
        if (ret == IddkResult.OK)
        {
            userRole = IddkSystemRole.User;
            ret = apis.SetUserRole(enrollID, userRole);
            if (ret != IddkResult.OK)
            {
               HandleError(ret);
            }
```

Figura 48 – Processo de inicialização e captura da íris

```
 IddkDataBuffer dataEnroll = new IddkDataBuffer();
 apis.GetEnrolleeTemplate(IDDriver.ToString(), dataEnroll); //EXTRACAO DA IRIS REGISTADA
 try
 {
     fac.objDrivers.insertIRIS(IDDriver, UserSettings.IdSupervisor, dataEnroll.Data); // ENVIO PARA A BASE DE DADOS
     MessageBox.Show("User enrolled with success!", "Success", MessageBoxButtons.OK, MessageBoxIcon.Information);
     apis.UnenrollTemplate(IDDriver.ToString());
 }
 catch (Exception ex)
 {

     MessageBox.Show(ex.Message);
 }
 /* Commit to gallery */
 //   ret = apis.CommitGallery();
 //if (ret != IddkResult.OK)
 //{
 //    Console.Out.Write("\nCommitGallery ... failed \n");
 //    HandleError(ret);
 //}

 ClearCapture();
```

Figura 49 – Extração e registo da íris na base de dados

A segunda principal funcionalidade a ser utilizada nesta API é a função *Compare11WithTemplate.* Esta função permite capturar em tempo real uma íris que se apresente na camara de captura com um *template*/íris existente. De notar que existe uma função na API que permite efetuar o *login* diretamente, mas a não utilização da memória local do dispositivo, torna necessário capturar a íris apresentada e comparar com uma íris externa (proveniente da base de dados), pelo que a função *login* incorporada na API é impossível de ser utilizada.

Assim, é necessário capturar a íris apresentada e de seguida compara-la com todas as íris presentes na base de dados. Sendo a solução utilizada por menos de 15 utilizadores/condutores, para um maior conforto destes e rapidez do processo de utilização do sistema por parte do utilizador, optou-se por seguir a filosofia de identificação/autenticação automática pelo sistema. Quer isto dizer que o utilizador não necessita de se identificar perante o sistema, ou seja, não necessita de informar o sistema que é um dado utilizador para de seguida efetuar a autenticação.

O sistema irá por sua vez percorrer toda a lista de utilizadores e comparar a íris capturada com as íris presentes na base de dados, selecionar a que é mais próxima da íris capturada e de seguida validar ou não a sua autenticação. A validação e consequente autenticação dependerá do *threshold* escolhido. Este *threshold*, que varia de zero a um, não mais é que a interseção entre o FRR e FAR, definindo o limite mínimo de proximidade da íris a autenticar no sistema. Neste caso o limite escolhido foi de 0.75, ou seja 75% de proximidade, como pode ser visto na seguinte Figura 50.

```
DataTable dt = fac.objDrivers.getIRIS();
foreach (DataRow row in dt.Rows) // Loop over the rows.
{
    int idDriver = (int)row[0];
    byte[] irisTOcheck = (byte[])row[1];
    float threshold, threshold2 =0;
    IddkDataBuffer iris = new IddkDataBuffer();
    iris.Data = irisTOcheck;

    result = apis.Compare11WithTemplate(iris, out threshold);
    if(threshold > threshold2)
    {
        threshold2 = threshold;
        if (threshold2 > 0.75)
        {
            logedINDriver = idDriver;
         }
    }
    ClearCapture();
```

Figura 50 – Processo de identificação/autenticação da íris

Através destas duas implementações/funções, a resolução da pergunta P1 fica exemplificada, permitindo então a autenticação dos utilizadores/condutores pelo meio dum fator biométrico. A chamada a este subcomponente é feita pelo componente principal *Authentication System* de uma maneira simples, dependendo da funcionalidade pretendida: “Autenticação” ou “Registo de dados biométricos”. Na Figura 51 um exemplo de utilização/chamada a este subcomponente que está desenvolvido sob a forma de objeto “*Windows Form*”. De notar que a chamada à

função de registo de dados biométricos apenas é possível através de um acesso a este componente como gestor/supervisor de frota.

```
frm = new AuthenticationForm();
frm.ShowDialog();
idDriverLogged = frm.logedINDriver;
```

Figura 51 – Utilização chamada do subcomponente de autenticação

4.3.1.2 Subcomponente Driving Licence Reader

Este subcomponente é responsável por validar uma carta de condução apresentada. Desse modo, este subcomponente é divido em duas partes. A primeira parte tem como função o reconhecimento OCR do texto presente na mesma, e a segunda parte o reconhecimento do padrão da carta de condução. É necessário detetar não só o numero de carta de condução apresentado, como também detetar os hologramas/padrões impressos na mesma através de tinta invisível (visível apenas à luz UV) para evitar a apresentação de falsificações ou até fotocópias.

Assim, duas interfaces com duas *webcams* foram efetuadas para obter uma maior performance e rapidez do processo. Uma *webcam* terá a função de adquirir uma foto a preto e branco da parte frontal da licença de condução, enquanto uma segunda webcam adquire em paralelo uma foto no escuro com luz UV incidente na parte traseira da licença, onde estão impressos os hologramas de segurança. Mesmo que os hologramas estejam presentes nas duas faces, como se verifica no caso de uma carta de condução Suíça, torna-se mais simples e rápido para o sistema, a não necessidade de interface com luzes artificiais para cada foto a obter pela *webcam*.

A obtenção destas fotos/imagens é como já dito anteriormente, efetuada pela interação com duas *webcams* e uma API de acesso a *webcams* genérica chamada *AForge* [80], opensource. Na Figura 52 é mostrado o método de utilização da API *AForge* para obtenção das imagens das *webcams*.

```
private FilterInfoCollection videoDevices;
private VideoCaptureDevice videoSource; //CAMARA OCR
private VideoCaptureDevice videoSource2; //CAMARA PATTERN
Threshold filter = new Threshold(90); //FILTRO PRETO E BRANCO


Bitmap bmpTEXT, bmpPATTERN;

1 reference
private void video_NewFrame(object sender, NewFrameEventArgs eventArgs)
{

    // get new frame FOR OCR
    var bitmap = (Bitmap)eventArgs.Frame.Clone();
    var bmp8 = Grayscale.CommonAlgorithms.BT709.Apply(bitmap);
    filter.ApplyInPlace(bmp8);        //APLICACAO FILTRO PRETO BRANCO
    bmpTEXT = (Bitmap)bmp8.Clone();
}
1 reference
private void video_NewFrame2(object sender, NewFrameEventArgs eventArgs)
{
    // get new frame FOR PATTERN
    var bitmap2 = (Bitmap)eventArgs.Frame.Clone();
    bmpPATTERN = (Bitmap)bitmap2.Clone();
}
```

Figura 52 – Inicialização e utilização da API AForge

Os passos seguintes à obtenção das imagens é o reconhecimento OCR e o reconhecimento do padrão/hologramas. O reconhecimento de OCR é feito através do recurso a uma libraria *opensource* de OCR, chamada *Tesseract* de Charles Weld [81]. Na Figura 53 a seguir é possível visualizar a utilização desta mesma.

```
1 reference
private void capturePermis_DoWork(object sender, DoWorkEventArgs e)
{

        while ((textOCR.ToString().Length < 6) && (workerCapturePermisComplete == false))
        {
            try
            {
            // LOCALIZAR A BIBLIOTECA DE PALAVRAS E LINGUA A UTILIZAR
            using (var engine = new TesseractEngine(@"C:\tessdata", "fra", EngineMode.Default))
                {
                    using (var img = bmpTEXT)
                    {
                        using (var page = engine.Process(img))
                        {
                            textOCR = page.GetText();
                        }
                    }
                }
            }
            catch (Exception ex)
            {
                //     MessageBox.Show(ex.Message);
            }
        }

}
```

Figura 53 – Utilização da biblioteca de reconhecimento OCR *Tesseract*

Esta biblioteca é obtida através de *NuGet Packages,* presente na ferramenta de desenvolvimento Microsoft Visual Studio [82] e inserida na solução, no entanto os dicionários de palavras apesar de gratuitos, devem ser obtidos separadamente. Neste caso a língua a escolher é irrelevante, pois o identificador que se pretende obter do reconhecimento OCR é independente da língua. Este identificador, o número de carta de condução, é constituído maioritariamente por números e letras, não contendo palavras dos dicionários de línguas.

No extrato de código apresentado na Figura 53 é possível visualizar a inicialização do motor de reconhecimento OCR através da chamada à função *TesseractEngine* da libraria *Tesseract* e a obtenção do texto através da função *Process*(). De referir que a obtenção do texto tem como *input* a imagem *bitmap*, obtida da *webcam*.

Obtido o texto presente na licença de condução é necessária a sua validação. Ou seja, é necessário verificar se o documento apresentado é efetivamente uma licença válida e não simplesmente uma fotocópia. Para isso, um reconhecimento dos hologramas de segurança é efetuado. À semelhança do reconhecimento da íris, a libraria OpenCV [69] disponibiliza funções de reconhecimento de formas e padrões em imagens. É então possível, através dum dado *template*, procurar numa dada imagem por esse mesmo *template*, e assim verificar se o mesmo está presente ou não na dada imagem.

Assim, o primeiro passo é obter um *template* a procurar nas licenças de condução. Aplicando uma luz UV num ambiente escuro sobre uma licença de condução Suíça, um padrão de hologramas é obtido. Na Figura 54 é mostrado o resultado obtido deste procedimento.

Figura 54 – Imagem resultante da incisão de luz UV sobre a licença de condução Suíça

Como é possível verificar, um padrão formado por três elipses está presente no documento de habilitação de condução. Para maior facilidade de comparação e procura de padrões, um filtro de preto e branco é aplicado sobre a mesma imagem e o *template* final é então obtido. Este *template* final está presente na seguinte Figura 55.

Figura 55 – *Template* a ser procurado nos documentos apresentados

Será esta a forma/*template* detetada caso um documento válido (licença de condução) seja apresentado, no caso de ser uma carta de condução Suíça. Esta deteção é efetuada através de um subcomponente externo (executável) implementado em C++, que terá como *input* o *template* a procurar (Figura 55), a imagem onde se pretende procurar o *template* (imagem proveniente da *webcam* 2 – Figura 54) e o *threshold* de *Matching,* que corresponde à percentagem mínima com que o padrão/*template* deve ser reconhecido. Obviamente, devido ao ruido de imagem, luz UV, qualidade de impressão/desgaste do documento que serão sempre diferentes de uma aquisição para a outra, é impossível definir um valor aproximado dos 100%. No entanto, um *score* mínimo de 70% de semelhança foi definido. Limite este, que permite sem margem para dúvidas, obter um grau de confiança bastante elevado na deteção do *template*.

Este subcomponente externo utiliza então a biblioteca OpenCV para efetuar o reconhecimento de formas. Estas funções de reconhecimento de formas baseiam-se nos limites/mudança de cor para efetuar o desenho através de milhares de pontos. Será então depois a proximidade e derivação destes pontos com os pontos do *template* a procurar, que determinam se a imagem contem um *template* aproximado ou não. Na seguinte Figura 56 é possível visualizar a utilização da biblioteca OpenCV. O retorno da execução será "*YES" ou "NO*" caso o *template* seja encontrado ou não respetivamente.

```
if(!GM.CreateModel(grayTemplateImg,lowThreshold,highThreashold))
{
    cout<<"ERROR: could not create model...";
    return 0;
}
TM.DrawContours(templateImage,CV_RGB( 255, 0, 0 ),1);
cout<<" Shape model created.."<<"with  Low Threshold = "<<lowThreshold<<" High Threshold =
CvSize searchSize = cvSize( searchImage->width, searchImage->height );
IplImage* graySearchImg = cvCreateImage( searchSize, IPL_DEPTH_8U, 1 );

// Convert color image to gray image.
if(searchImage->nChannels ==3)
    cvCvtColor(searchImage, graySearchImg, CV_RGB2GRAY);
else
{
    cvCopy(searchImage, graySearchImg);
}
//cout<<" Finding Shape Model.."<<" Minumum Score = "<< minScore <<" Greediness = "<<greedi
//cout<< " -----------------------------------\n";
clock_t start_time1 = clock();
score = TM.FindTemplate(graySearchImg,minScore,greediness,&result);
clock_t finish_time1 = clock();
total_time = (double)(finish_time1-start_time1)/CLOCKS_PER_SEC;

if(score>minScore) // if score is atleast 0.4
{
    //cout<<" Found at ["<<result.x<<", "<<result.y<<"]\n Score = "<<score<<"\n Searching T
    cout<<"YES";
    TM.DrawContours(searchImage,result,CV_RGB( 0, 255, 0 ),1);
}
else
    cout<<"NO";
```

Figura 56 – *OpenCV* reconhecimento de padrões em imagens

Na Figura 57 a chamada a este subcomponente externo é apresentada.

```
1 reference
private bool Check_Authentic_Permis(int idDriver, int idCountry)
{
   bool resp = false;
   DataTable dt = fac.objPatterns.getPatterns(idCountry);
    foreach (DataRow row in dt.Rows)
    {
        MemoryStream ms = new MemoryStream((byte[])row["Image"]);
        Image img = System.Drawing.Image.FromStream(ms);
        img.Save("tempPattern.JPG", System.Drawing.Imaging.ImageFormat.Jpeg);

        //CHECK IF PATTERN EXISTS IN THE IMAGE PROVIDED BY CAMERA
        var proc = new Process
        {
            StartInfo = new ProcessStartInfo
            {
                FileName = "FindTemplate.exe",
                Arguments = "-t tempPattern.JPG -l 10 -h 100 -s tempPermis.JPG -m 0.7 -g 0.9",
                UseShellExecute = false,
                RedirectStandardOutput = true,
                CreateNoWindow = true
            }
        };
        proc.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
        proc.Start();
        string line = "";
        while (!proc.StandardOutput.EndOfStream)
        {
            line = proc.StandardOutput.ReadLine();
            // do something with line
            MessageBox.Show(line);
        }
        if (line.Contains("YES") == true)
        {
            resp = true;
            System.IO.File.Delete("tempPattern.JPG");
            break;
        }
        else
        {
            System.IO.File.Delete("tempPattern.JPG");
        }
    }
    return resp;
}
```

Figura 57 – Chamada ao subcomponente externo *FindTemplate.exe*

Conclui-se esta secção com a resposta/resolução à pergunta P2. Deste modo é possível ser efetuada a validação de uma licença de condução, que passa pela leitura do seu número de licença e reconhecimento dos hologramas de segurança. Obviamente, falsificações bem-feitas não serão detetadas, pois a solução baseia-se em um número de licença e um padrão/*template* a reconhecer, não num infinito número de pontos de verificação possíveis. No entanto, o objetivo da solução não é detetar todas as falsificações, mas sim garantir ao máximo possível que o utilizador/condutor apresenta a sua carta de condução e não uma fotocópia por exemplo.

4.3.1.3 Subcomponente Key Reader

Nesta secção é explicada a implementação do subcomponente *Key Reader,* que tem como tarefa a leitura dos identificadores da chaves para assim poder manter a coerência de acesso a recursos no sistema, bem como possibilitar a identificação/verificação da chave que será devolvida pelos utilizadores.

Refletindo, a chave não necessita de ser identificada no sistema antes da sua entrega. Em efeito, será a consistência dos dados de localização da chave no armário digital que fará o sistema entregar a chave correspondente ao veículo escolhido pelo utilizador/condutor. Esta apenas necessita ser verificada na sua devolução, permitindo manter a consistência dos dados e assegurar que a boa chave foi devolvida.

Tomando de exemplo a seguinte Figura 58, ilustrativa de um armário digital, é possível perceber o conceito da organização da informação.

1 **Veiculo A**	**2** **Veiculo B**
3 **Veiculo C**	**4** **Livre**
5 **Livre**	**6** **Veiculo D**

Figura 58 – Ilustração conceptual de um armário digital

Na Figura 58, cada posição do armário (1-6) corresponde a um veículo num dado momento. Então, para a entrega de um determinado veículo, por exemplo o B, sabe-se que é necessário "abrir" o compartimento número dois para que a chave seja entregue.

Será então posteriormente no retorno da chave por parte do utilizador/condutor ao sistema, que este deverá identificar a chave, para a fazer corresponder ao veículo B que por sua vez irá ser depositado num compartimento qualquer, desde que este esteja livre. Em suma, cada compartimento de cada local de repositório corresponderá a um veículo, que por sua vez é caraterizado por uma determinada chave.

Porém, a leitura de uma chave de um veículo é tarefa árdua. Não só é extremamente difícil encontrar a frequência de cada uma, como também, é difícil descodificar as informações da mesma. Existem de facto no mercado, leitores pré concebidos para determinadas chaves de determinados modelos de veículos. No entanto, não existem leitores para todos, principalmente para os mais recentes modelos, o que torna esta opção menos flexível e robusta, pois a cada aquisição de um novo veiculo, o sistema poderia enfrentar problemas de compatibilidade de leitura da chave. De acrescentar que nem todas as chaves usam a mesma frequência, pelo que, um leitor para cada banda de frequência ou um leitor multifrequência

seria necessário. No que toca a leitores multifrequência é necessário referir que os preços são bastante mais elevados.

Pelas razões acima mencionadas, sugere-se a utilização de um identificador RFID comum (RFID Tag) a incorporar na chave da viatura. Este identificador deve então ser acoplado com a chave de maneira que a sua troca/remoção física seja percetível, pelo menos ao ser humano (gestor da frota). Por exemplo, um porta-chaves selado mecanicamente. Este método permitiria ao gestor da frota perceber se alguém teria violado o identificador e tomar as medidas necessárias.

Infelizmente, deixa de ser possível responder com sucesso à pergunta P4 recorrendo a solução de leitura da chave do veículo para obter informações do mesmo, nomeadamente aos quilómetros. Não se tratando este de um ponto fulcral para o bom desenvolvimento da solução, remete-se este problema para *posteriori*. Na secção de conclusões e trabalho futuro algumas sugestões serão designadas.

Resumindo, um tipo de identificador comum NFC que usa os métodos de comunicação RFID foi escolhido. A frequência do mesmo é de 13.56 MHz com o protocolo clássico MIRAFIRE 1k 50. O leitor do mesmo tipo foi escolhido em conjunto com os identificadores, respeitando as características e compatibilidades dos mesmos. O leitor NFC/RFID escolhido tem como interface com o computador a porta USB e é compatível em plataformas Windows 32 e 64 bits. O preço de cada identificador ronda os 90 cêntimos de euro e o preço do leitor os 47 euros.

Inicialmente a ideia seria de possuir apenas um leitor de RFID/NFC por cada local de repositório, ou seja, dois leitores. No entanto, esta abordagem exige que: após a leitura da chave, esta seja dirigida para o seu compartimento, implicando um mecanismo de abertura e fecho de ramos em canais dirigidos ou então uma espécie de mecanismo de roleta (formato piza), rodando esta até a abertura libre (no caso de retorno), ou rodando até à fatia da chave pretendida (armário digital no caso de requisição). Um mecanismo deste género, em que a condução das chaves é "robotizada", seria sempre não só mais dispendioso como também uma maior fonte provável de problemas e manutenção.

Após uma análise de preços, simplicidade e expansibilidade do sistema, optou-se por escolher a abordagem de compartimentos completamente controlados separadamente. Isto é, cada compartimento tem a sua própria abertura/porta que é aberta através de um impulso elétrico numa fechadura eletromagnética. Esta abordagem requer porém um leitor RFID/NFC por compartimento, no entanto situa-se sempre num patamar de preços mais baixos, comparativamente a um sistema de ramos dirigidos/roleta. Também a possibilidade de expansão torna-se mais ampla, no sentido em que se porventura é necessário a introdução de uma nova chave, apenas um novo compartimento com um leitor RFID/NFC necessita ser incorporado. Se se pensar em mecanismos de roleta ou canais dirigidos, estes sempre ficam limitados ao espaço.

Existem atualmente cinco viaturas na empresa, pelo que são necessários cinco identificadores e dez leitores de RFID/NFC perfazendo um total de aproximadamente 500€ para a o material

de identificação das chaves, incluindo já o componente Arduíno, que será responsável pela abertura e fecho dos compartimentos através de fechaduras eletromagnéticas.

A primeira implementação diz respeito à leitura do identificador RFID/NFC, assim no subcomponente de leitura de chaves foi usada a API .NET PCSC de Daniel Mueller [79]. Esta API *opensource* é de simples utilização e bastante flexível em termos de normas ISO dos leitores e identificadores. Através desta implementação a solução para a pergunta P3 fica parcialmente implementada. Parcialmente, porque é ainda necessário implementar um mecanismo de abertura e fecho dos compartimentos.

Na seguinte Figura 59 um extrato do código de inicialização do leitor RFID/NFC e consequente leitura ou tratamento de exceções. Exceções que podem ser por exemplo: o identificador não se encontra presente no leitor, o identificador encontra-se presente no leitor mas a sua leitura não é possível entre outros.

```
var readerName = readerNames[0];
if (readerName == null)
{
    return -1;
}

using (var rfidReader = new SCardReader(context))
{

    var sc = rfidReader.Connect(readerName, SCardShareMode.Shared, SCardProtocol.Any);
    if (sc != SCardError.Success)
    {
   // listBox1.Items.Add("The KEY couldn't be readed!\n");
        return 0;
    }

    var apdu = new CommandApdu(IsoCase.Case2Short, rfidReader.ActiveProtocol)
    {
        CLA = 0xFF,
        Instruction = InstructionCode.GetData,
        P1 = 0x00,
        P2 = 0x00,
        Le = 0  // We don't know the ID tag size
    };

    sc = rfidReader.BeginTransaction();
    if (sc != SCardError.Success)
    {
   // listBox1.Items.Add("The KEY is present, but not readable!");
        return 1;
    }

    //    richTextBox1.AppendText("Retrieving the UID .... ");

    var receivePci = new SCardPCI(); // IO returned protocol control information.
    var sendPci = SCardPCI.GetPci(rfidReader.ActiveProtocol);

    var receiveBuffer = new byte[256];
    var command = apdu.ToArray();

    sc = rfidReader.Transmit(
        sendPci,            // Protocol Control Information (T0, T1 or Raw)
        command,            // command APDU
        receivePci,         // returning Protocol Control Information
        ref receiveBuffer); // data buffer

    if (sc != SCardError.Success)
    {
        MessageBox.Show("Error: " + SCardHelper.StringifyError(sc));
    }

    var responseApdu = new ResponseApdu(receiveBuffer, IsoCase.Case2Short, rfidReader.ActiveProtocol);
    idReaded = BitConverter.ToString(responseApdu.GetData()); // RETRIEVE ONLY DE ID OF THE RFID TAG //
    rfidReader.EndTransaction(SCardReaderDisposition.Leave);
    rfidReader.Disconnect(SCardReaderDisposition.Reset);
```

Figura 59 – Utilização API PCSC para leitura de identificadores RFID/NFC

A resposta completa à pergunta P3 passa então pela programação do controlador Arduíno, que será responsável pela abertura e fecho das fechaduras dos compartimentos. Este subcomponente será ligado ao componente pai (*Authentication System)* através de uma porta série, por onde toda a comunicação entre ambos passará.

Para se abrir então um compartimento, é então necessário enviar esse comando para a porta série, onde o Arduíno irá estar à escuta. A escrita na porta série não é mais do que o envio do comando e o número do compartimento a abrir. Se por exemplo é requerida a chave do veículo A (ver Figura 58) o compartimento a abrir será o número um, assim o comando enviado ao Arduíno proveniente do componente *Authentication System* será "A1". Assim que o componente *Authentication System* não detete mais a chave do veículo A nos leitores RFID e a porta se encontre fechada (corrente elétrica na fechadura) o comando a enviar será "F1" (fechar fechadura 1). No extrato de código apresentado na Figura 60 é possível visualizar a instanciação da porta série e a escrita na mesma.

```
SerialPort serialPort1;
bool portFound;
1 reference
private Boolean SetComPort()
{
    serialPort1.PortName = "COM1";
    serialPort1.BaudRate = 9600;

    serialPort1.Open();
    if (serialPort1.IsOpen)
    {
        return true;
    }
    else
    {
        return false;
    }
}
1 reference
private void stopPortCom()
{
    if (serialPort1.IsOpen)
    {
        serialPort1.Close();
    }
}

2 references
private void SendCommand(char command, char compartimento)
{
    // If the port is closed, don't try to send a character.
    if (!serialPort1.IsOpen) return;

    // If the port is Open, declare a char[] array with one element.
    char[] buff = new char[2];

    // Load element 0 with the key character.
    buff[0] = command;
    buff[1] = compartimento;
    // Send the one character buffer.
    serialPort1.Write(buff, 0, 1);

}
```

Figura 60 – Envio de comandos porta série (Arduíno)

No entanto, o extrato de código da Figura 60 não mais é que a parte do componente *Authentication System*, ainda é necessária a programação do componente Arduíno para que este seja capaz de interpretar os comandos recebidos e os execute. A programação deste componente é apresentada na secção seguinte.

4.3.2 Arduíno Mega S

Como já referido anteriormente, este componente é fisicamente independente do componente *Authentication System*. Um Arduíno é um microcontrolador, que pode ser programado de maneira a interagir através de sinais analógicos e digitais com outros componentes elétricos/magnéticos, como é o caso de uma fechadura eletromagnética.

A forma de programação de um microcontrolador é um pouco diferente da forma de programação convencional, no que à estrutura diz respeito. Um microcontrolador está em constante execução (*loop*), ou seja, está em constante escuta e execução de tarefas atribuídas, tal como um processador de um computador. Desse modo, a logica de programação baseia-se num ciclo infinito, pelo que o controlo de estados e operações é importante. De referir que os microcontroladores Arduíno possuem a sua própria ferramenta de desenvolvimento e utilizam C como linguagem de programação.

Após a receção do comando proveniente do subcomponente *Key Reader* na porta série, o Arduíno deve efetuar a sua interpretação. A estrutura do comando a executar é composta por dois caracteres, o primeiro para a operação e o segundo para o número do compartimento.

Cada compartimento está associado a um pino digital de saída do Arduíno. Este Arduíno em questão é composto por 54 entradas/saídas digitais, às quais se designam como pinos. Considera-se que o compartimento um está associado ao pino digital um, o compartimento dois ao pino digital dois e por conseguinte. Assim, quando o Arduíno recebe o comando da porta série deverá interpretar os dois caracteres e ativar ou desativar o sinal (corrente elétrica) no pino correspondente, consoante se pretenda abrir ou fechar a fechadura. Na Figura 61 pode-se visualizar uma parte do código do microcontrolador onde é possível verificar a leitura da porta série e a ação no compartimento/pino correspondente. A leitura é efetuada para um *array* de duas posições (*inData*), em que a primeira contem a ação e a segunda o número do compartimento e consequente pino.

Este componente ainda não está completamente acabado. É ainda preciso verificar que a porta foi fechada para de seguida fechar a fechadura eletromagnética (os ímanes necessitam estar encostados para que a fechadura seja selada). Para isso, dois cabos para cada compartimento são necessários. Um cabo para transmitir a voltagem à fechadura para fechar ou abrir e um segundo cabo que passará eletricidade e por conseguinte formará um sinal de entrada sempre que os ímanes estejam encostados, formando assim uma espécie de circuito elétrico. Este ultimo permitirá saber se a porta está fechada ou não.

sketch_aug30a §

```
char inData[2];
char inChar;
byte index = 0;

void setup()
{
    Serial.begin(9600);
}

void loop()
{
 while(Serial.available() > 0)
 {
     if(index < 2)
     {
         inChar = Serial.read();
         inData[index] = inChar;
         index++; //
         inData[index] = '\0'; // Null terminate the string
     }
 }
 if (inData[0] == 'A')
 {
  // ABRIR FECHADURA
  digitalWrite(inData[1] , HIGH);
  delay(1000);
  inData[0] = '0';
  index = 0;

 }else if (inData[0] == 'F')
 {
  // FECHAR FECHADURA
  digitalWrite(inData[1] , LOW);
  delay(1000);
  inData[0] = '0';
  index = 0;
 }

}
```

Figura 61 – Programação microcontrolador Arduíno

4.3.3 Montagem dos componentes

Como em qualquer outro projeto/solução em que é necessária a interação com o exterior, nomeadamente objetos (carta de condução/olho humano/identificadores RFID), torna-se evidente a necessidade de acoplamento/montagem dos componentes necessários para tal.

Nesta solução existem vários componentes físicos necessários para o bom desenrolar da mesma, nomeadamente um *scanner* da íris humana, duas webcams para a leitura da licença de condução ou até os leitores RFID/NFC em cada compartimento.

A montagem está encarregue a um parceiro externo, parceiro esse experimentado no desenho de máquinas industriais. Para além do desenho e conceção da carcaça, este será também

responsável pela montagem dos vários dispositivos a utilizar, nomeadamente computador, leitores RFID, *webcams,* fechaduras, Arduíno, etc. bem como toda a cablagem necessária.

Um primeiro esboço do pretendido está já desenhado. Na seguinte Figura 62 é mostrado então o esboço do que será um dos repositórios de chaves na sua totalidade, dando assim corpo e alma ao projeto/solução.

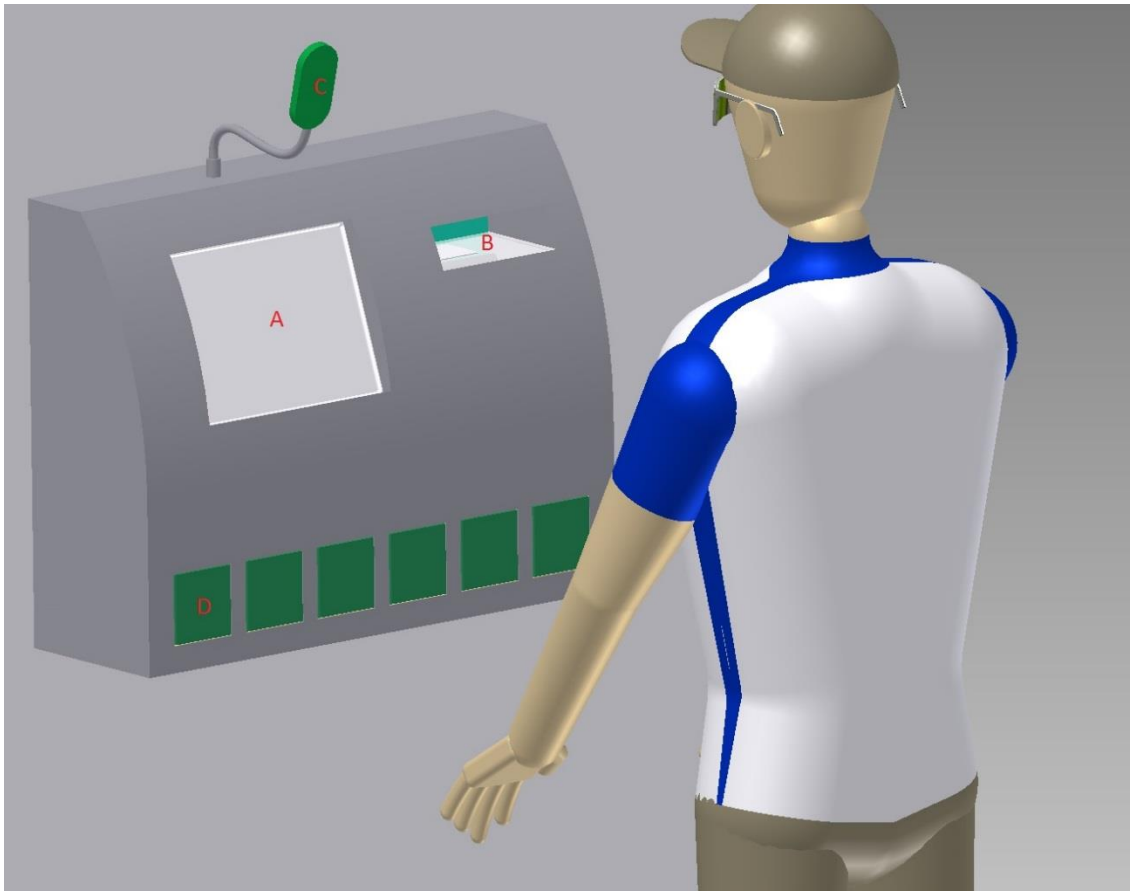


Figura 62 – Montagem da solução final

Efetuando a explicação de cada parte do repositório de chaves, a letra A designa um ecrã táctil que está ligado a um computador de pequeno tamanho. Este computador irá conter o componente *software Authentication System* de onde o utilizador poderá manusear o sistema e efetuar o levantamento e devolução das chaves.

A letra B corresponde ao local onde o utilizador irá introduzir a sua licença de condução, que deverá sempre estar na mesma posição. Para isso, encostar ao canto esquerdo no fundo é uma hipótese para que a posição seja constante. De notar que uma *webcam* se encontra no topo superior da abertura e outra no inferior, em conjunto com as luzes UV e ambiente.

A letra C representa o *scanner* da íris do utilizador, que conforme é possível verificar pela imagem, é passível de ajustamento. O pequeno tubo entre o mesmo e a caixa metálica é maleável, permitindo assim o ajuste do scanner conforme a altura do utilizador por exemplo.

Por fim, a letra D corresponde aos compartimentos das chaves. No interior de cada compartimento existe então um leitor RFID que permitirá a identificação da chave. No anexo 2, 3 e 4 a parte de montagem é apresentada com mais detalhe, bem como um orçamento para o componente *Authentication System*.

Aqui termina a explicação do componente principal da solução, *Authentication System*. É este componente o motor de todo o projeto. Na próxima secção será apresentado o componente *BackOffice*.

4.3.4 BackOffice

Nesta secção será abordado o componente *BackOffice*, que não sendo o componente mais importante da solução, não deixa de ser uma peça importante do puzzle.

Como o nome sugere, este componente é responsável pelas tarefas de base do sistema, nomeadamente a gestão de utilizadores, gestão de viaturas, gestão de reservas e gestão de padrões de licenças de condução. Por gestão de viaturas entenda-se a gestão de informações das mesmas como manutenções, apólices de seguro e revisões. É através deste componente que o gestor da frota gere os dados a utilizar pelo componente *Authentication System*. Por se tratar de uma ferramenta que se baseia maioritariamente em acessos à base de dados da aplicação, opta-se por efetuar uma breve explicação.

Este componente foi desenvolvido com recurso a linguagem de programação C#, utilizando a última versão do *framework* .NET, a versão 4.6, à semelhança do componente *Authentication System.*

4.3.4.1 Autenticação BackOffice

Este componente será instalado nos postos de trabalho dos gestores da frota e o acesso ao mesmo será baseado no *login* Windows de cada (*Integrated Windows Authentication*). A empresa está munida de um domínio Windows, deste modo não é necessário gerir o controlo de acesso à aplicação. Apenas é necessário saber o utilizador atualmente autenticado no sistema e interrogar o domínio para saber se este pertence ao grupo de gestores de frota. Mas como pode o domínio saber que este utilizador é um gestor de frota? Não sabe, porém um grupo organizacional foi criado no domínio, em que nesse grupo se inserem os supervisores da aplicação/gestores de frota, sendo tarefa do componente *BackOffice* encontrar o utilizador nesse grupo ou não. No seguinte extrato de código da Figura 63 é possível verificar o processo acima descrito.

```
1 reference
public MainForm()
{
    InitializeComponent();
    domainctx = new PrincipalContext(ContextType.Domain, "boegli", "DC=boegli,DC=local");
    UserSettings.UserName = Environment.UserName;
    userPrincipal =  UserPrincipal.FindByIdentity(domainctx, IdentityType.SamAccountName, UserSettings.UserName);
}

1 reference
private bool LOGIN_SUPERVISOR()
{
    return (userPrincipal.IsMemberOf(domainctx, IdentityType.Name, "BG_Fleet_Management_Supervisor"));
}
```

Figura 63 – Autenticação do utilizador no componente *BackOffice*

No extrato acima pode-se verificar que a identificação do utilizador é obtida através da instrução "*Environment.Username*" e que de seguida é verificado se esse utilizador faz parte do grupo de supervisores. Grupo esse que foi criado ao nível do domínio e chamado de "*BG_Fleet_Management_Supervisor*". Deste modo, para que um utilizador tenha acesso ao componente de *BackOffice* e seja nomeado supervisor, apenas é necessário que o Administrator do domínio, o adicione ao grupo acima mencionado.

Após boa autenticação, o utilizador é então presenteado com a janela principal, que segue as mesmas linhas de *design* do componente *Authentication System* como é possível verificar na Figura 64.

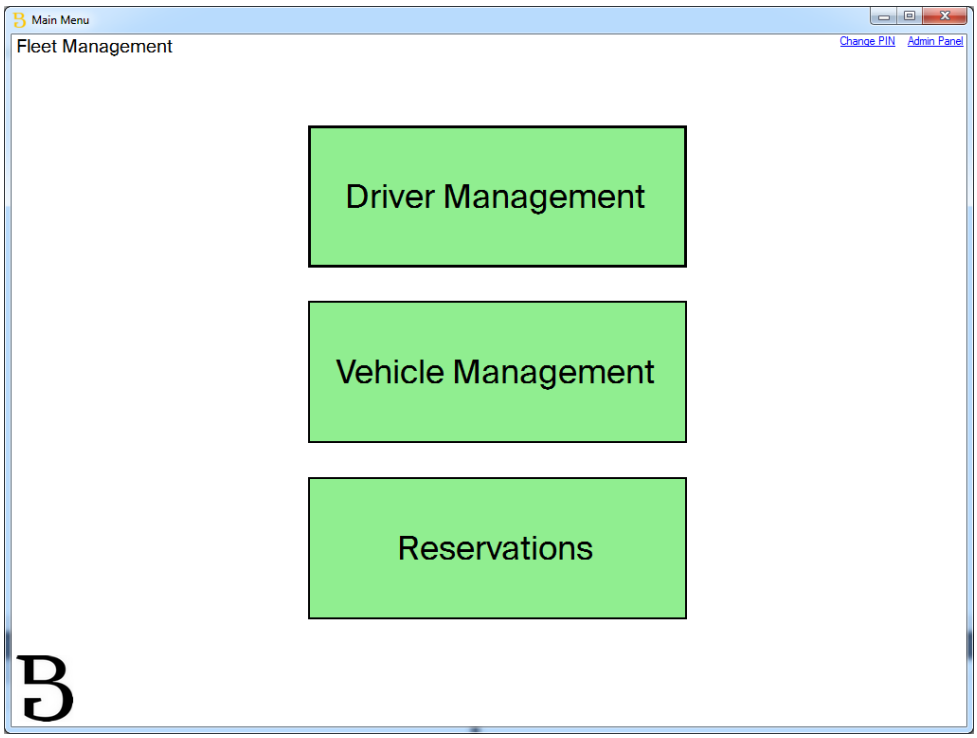


Figura 64 – Apresentação do componente *BackOffice*

4.3.4.2 Alterar PIN Supervisor

Uma das funcionalidades do *BackOffice* é a possibilidade do gestor alterar o seu PIN de acesso ao componente *Authentication System*. Como explicado anteriormente, o processo de registo de um novo utilizador é feito através do componente *BackOffice,* mas o registo dos dados biométricos (íris) é feita no componente *Authentication System*. Deste modo, é necessário que o gestor tenha acesso ao componente *Authentication System* em modo supervisor para poder fazer então o registo biométrico do utilizador ou eventualmente atualizá-lo. De notar também que o gestor de frota pode necessitar de aceder ao componente *Authentication System* em modo supervisor, para poder abrir os compartimentos em caso de manutenção/avaria do sistema.

Como já referido na secção 4.3.1 o *login* é efetuado através deste PIN (único no sistema) armazenado na base de dados em formato *hash,* ou seja, o componente de *BackOffice* verifica se este já existe na base de dados e caso não exista este é então inserido como novo PIN do supervisor em questão.

Na Figura 65, é apresentado o método de verificação de existência do *hash* para o PIN pretendido e consequentemente a sua codificação. Para efeito, uma classe foi criada com esse intuito.

```
2 references
public class HashPIN
{
    private const int PBKDF2IterCount = 1000; // default for Rfc2898DeriveBytes
    private const int PBKDF2SubkeyLength = 256 / 8; // 256 bits
    private const int SaltSize = 128 / 8; // 128 bits

    //Creates a new hashed password according to the password in plain text received
    1 reference
    public static string CreateHashPassword(string password)
    {
        byte[] salt;
        byte[] subkey;
        using (var deriveBytes = new Rfc2898DeriveBytes(password, SaltSize, PBKDF2IterCount))
        {
            salt = deriveBytes.Salt;
            subkey = deriveBytes.GetBytes(PBKDF2SubkeyLength);
        }
        byte[] outputBytes = new byte[1 + SaltSize + PBKDF2SubkeyLength];
        Buffer.BlockCopy(salt, 0, outputBytes, 1, SaltSize);
        Buffer.BlockCopy(subkey, 0, outputBytes, 1 + SaltSize, PBKDF2SubkeyLength);
        return Convert.ToBase64String(outputBytes);
    }


    //check if the plain text received matches of an HASH
    //used to make Login and verify if the password (in plain text) introduced by the user
    //matches is hash in the database

    1 reference
    public static bool VerifyHashedPassword(string hashedPassword, string password)
    {
        byte[] hashedPasswordBytes = Convert.FromBase64String(hashedPassword);

        // Wrong length or version header.
        if (hashedPasswordBytes.Length != (1 + SaltSize + PBKDF2SubkeyLength) || hashedPasswordBytes[0] != 0x00)
            return false;

        byte[] salt = new byte[SaltSize];
        Buffer.BlockCopy(hashedPasswordBytes, 1, salt, 0, SaltSize);
        byte[] storedSubkey = new byte[PBKDF2SubkeyLength];
        Buffer.BlockCopy(hashedPasswordBytes, 1 + SaltSize, storedSubkey, 0, PBKDF2SubkeyLength);
        byte[] generatedSubkey;
        using (var deriveBytes = new Rfc2898DeriveBytes(password, salt, PBKDF2IterCount))
        {
            generatedSubkey = deriveBytes.GetBytes(PBKDF2SubkeyLength);
        }
        return storedSubkey.SequenceEqual(generatedSubkey);
    }
}
```

Figura 65 – Extrato código codificação/verificação *hash*

Em suma, o PIN pretendido é comparado como todos os *hash* armazenados na base de dados, e se um deles coincidir significa que esse PIN já está a ser utilizado por um outro supervisor, caso contrário o PIN é então codificado e armazenado na base de dados. Caso o PIN já existir, um supervisor que contenha esse PIN vê bloqueado o acesso em modo supervisor até que mude também ele o seu PIN (pois este foi descoberto). Uma notificação via correio eletrónico é enviada.

Nas próximas subsecções serão apresentadas pequenas funcionalidades de apoio ao gestor de frota, que não mais são que inserção, edição ou remoção de registos da base de dados da solução, que permitem um maior conforto e controlo por parte do mesmo na utilização da solução.

4.3.4.3 Inserção de padrões (hologramas)

A inserção de padrões (hologramas) para comparação com a licença de condução apresentada, não mais é que uma tabela da base de dados onde as imagens deste são armazenados em relação a um dado país. Trata-se de uma simples janela de inserção e remoção na base de dados, esta janela é apresentada na Figura 66.

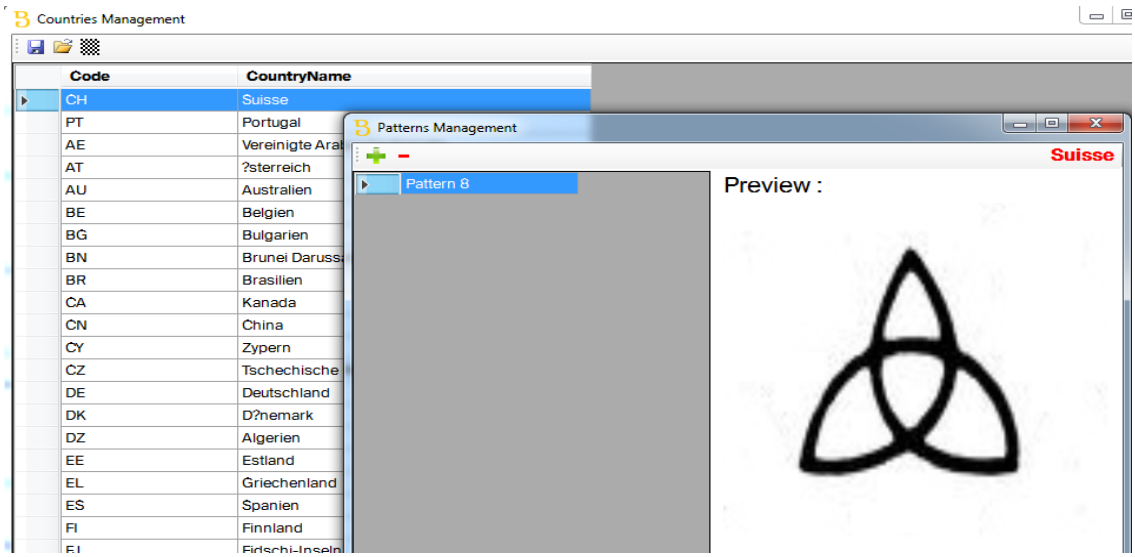


Figura 66 – Janela de gestão de padrões (hologramas)

4.3.4.4 Gestão de reservas

Esta secção termina com a apresentação da funcionalidade de gestão de reservas. Esta funcionalidade permite ao gestor efetuar reservas de viaturas para um determinado utilizador, impedindo assim que num intervalo de tempo, essa viatura seja utilizada por qualquer outro utilizador. Como não poderia deixar de ser, quando o gestor de frota pretende efetuar uma reserva, o componente *BackOffice* necessita de verificar que não hajam sobreposições com outras reservas/utilizadores. Por exemplo, se a viatura pretendida já esta reservada para outro utilizador, o gestor não pode reservar a viatura nesse intervalo a não ser que elimine a reserva já existente. Outro aspeto será o utilizador em questão, ou seja, não será feita uma reserva para

um utilizador que já tenha outra reserva nesse mesmo intervalo, pois o mesmo não consegue conduzir 2 veículos em simultâneo.

Estas verificações são feitas ao nível do componente DAL. Será este componente, que através de consultas à base de dados irá retornar a resposta ao componente *BackOffice*, permitindo a inserção ou não da reserva. Na secção a seguir 4.3.5, é apresentado o componente DAL onde é possível verificar algumas destas verificações de consistência da informação. De notar que, será depois o componente *Authentication System* o responsável por permitir ou impedir o levantamento dos veículos tendo em conta as reservas presentes da base de dados. Na Figura 67 apresenta-se a janela responsável pela gestão das reservas.

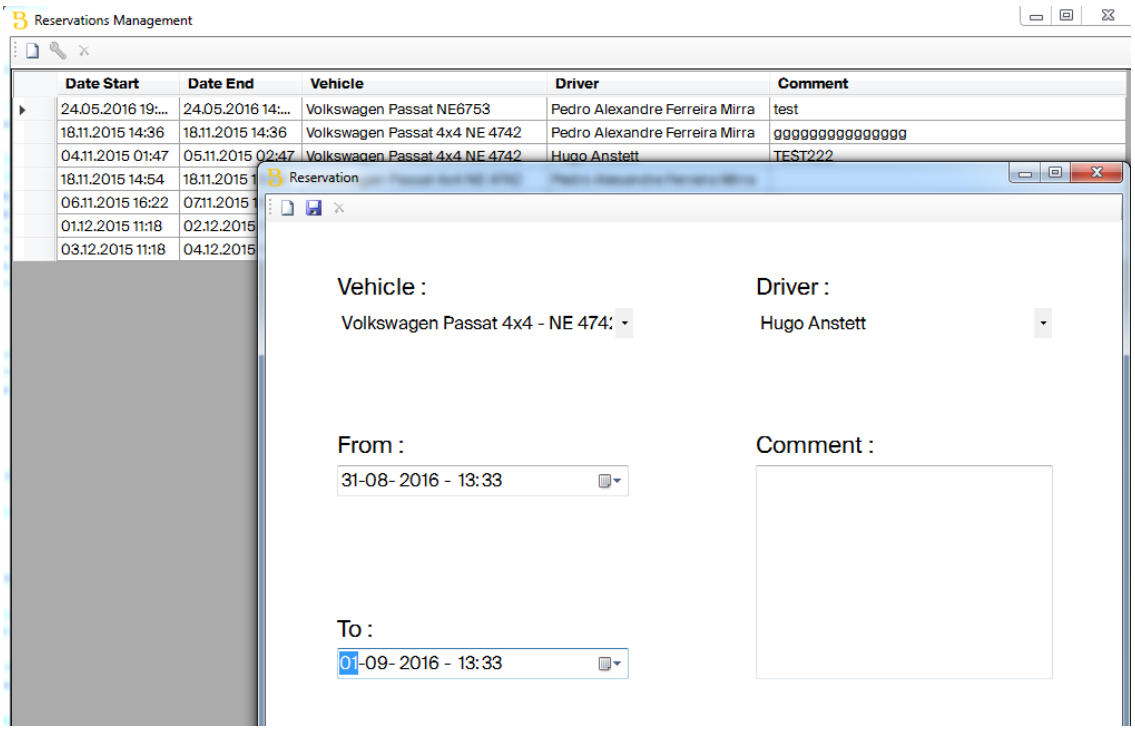


Figura 67 – Janela de gestão de reservas

Aqui termina a apresentação do componente de *BackOffice,* que em conjunto com o componente *Authentication System,* formam a parte visível pelos utilizadores da solução. Na próxima e última secção deste capítulo, será apresentado o componente DAL, que é responsável pelo acesso à informação da base de dados.

4.3.5 Data Access Layer - DAL

Nesta última secção deste capítulo é apresentado o componente DAL. Este componente como já explicado anteriormente é o componente responsável pelo acesso à informação pelos dois componentes principais: *Authentication System* e *BackOffice*.

Deste modo, a camada DAL modeliza através de classes o acesso à informação consoante o objeto pretendido (Veículos, condutores, etc.) como pode ser visualizado na Figura 68 a seguir. O acesso a estas classes de objetos dá-se através da classe de entrada principal (*Factory* – Figura

68) que em seguida acede a estes últimos. Resumindo, a DAL funciona como um controlador de acesso à informação, efetuando mecanismos de prevenção de inconsistências, a "lógica de negócio".

```
public Vehicles objVehicles;
public Reservations objReservations;
public Drivers objDrivers;
public Countries objCountries;
public Supervisors objSupervisors;
public Patterns objPatterns;
12 references
public Factory()
{

    objVehicles = new Vehicles();
    objReservations = new Reservations();
    objDrivers = new Drivers();
    objCountries = new Countries();
    objSupervisors = new Supervisors();
    objPatterns = new Patterns();
}
```

Figura 68 – Classe Factory, que permitem o acesso aos diversos objetos

É através deste componente que são inseridos, atualizados ou removidos os dados/informações da solução, pelo que este componente é maioritariamente composto por métodos de acesso à base de dados. De referir que a base de dados da solução foi desenvolvida em SQL. Na Figura 69 um pequeno extrato de código deste componente é apresentado.

```
1 reference
public bool getConflitReservation(DateTime _startDate, DateTime _endDate, int _idDriver, int _idVehicle, out DataTable dt)
{
    string query = "dbo.spGetConflitReservation";
    SqlParameter[] sqlParameters = new SqlParameter[4];
    sqlParameters[0] = new SqlParameter("@paramStartDate", SqlDbType.DateTime);
    sqlParameters[0].Value = Convert.ToString(_startDate);
    sqlParameters[1] = new SqlParameter("@paramEndDate", SqlDbType.DateTime);
    sqlParameters[1].Value = Convert.ToString(_endDate);
    sqlParameters[2] = new SqlParameter("@paramIDDriver", SqlDbType.Int);
    sqlParameters[2].Value = Convert.ToString(_idDriver);
    sqlParameters[3] = new SqlParameter("@paramIDVehicle", SqlDbType.Int);
    sqlParameters[3].Value = Convert.ToString(_idVehicle);
    dt = conn.executeSelectQuery(query, sqlParameters);
    if (dt.Rows.Count > 0)
    {
        //EXISTEM RESERVAS QUE SOBREPOEM O INTERVALO PROPOSTO
        return true;
    }
    else
    {
        //PODE RESERVAR PARA A DATA PROPOSTA
        return false;
    }
}
```

Figura 69 – Classe Reservations, método para verificar sobreposições de reservas

Como é possível verificar pela Figura 69, a manipulação da informação é efetuada através de procedimentos armazenados na base de dados, em inglês designados como *stored procedures.* Esta metodologia permite não só uma maior organização de tarefas entre a DAL e a base de dados como uma maior segurança, visto a DAL não conter linguagem SQL, passando apenas os

parâmetros para a sua execução. Na Figura 70 é apresentado o procedimento que é chamado pelo método da Figura 69 (*spGetConflitReservation*).

```
ALTER PROCEDURE [dbo].[spGetConflitReservation]

@paramStartDate as datetime,
@paramEndDate as datetime,
@paramIDDriver as int,
@paramIDVehicle as int

AS
BEGIN
SELECT        Reservation.StartDate,
              Reservation.EndDate,
              Vehicles.Manufacturer + ' ' + Vehicles.Model  + '-' +Vehicles.PlatNumber as Vehicle,
              Drivers.Name + ' ' + Drivers.Surname as Driver
FROM          Reservation
                INNER JOIN
                     Drivers ON Reservation.IDDriver = Drivers.IDDriver
                       INNER JOIN Vehicles ON Reservation.IDVehicle = Vehicles.IDVehicle
 where
 ((Reservation.StartDate < @paramStartDate and Reservation.EndDate > @paramStartDate) or
 (Reservation.StartDate < @paramEndDate and Reservation.EndDate > @paramEndDate) and Vehicles.IDVehicle = @paramIDVehicle)
 or
 ((Reservation.StartDate < @paramStartDate and Reservation.EndDate > @paramStartDate)) or
 ((Reservation.StartDate < @paramEndDate and Reservation.EndDate > @paramEndDate) and Drivers.IDDriver = @paramIDDriver)
 or
 ((Reservation.StartDate > @paramStartDate and Reservation.EndDate < @paramEndDate) and Vehicles.IDVehicle = @paramIDVehicle)
  or
 ((Reservation.StartDate > @paramStartDate and Reservation.EndDate < @paramEndDate) and Drivers.IDDriver = @paramIDDriver)
END
```

Figura 70 – Procedimento armazenado para acesso a reservas sobrepostas

4.4 Sumário do capítulo

Aqui termina o capítulo referente à implementação. As respostas a P1, P2, P3 e outras funcionalidades básicas foram atingidas. Como já dito anteriormente, a resposta a P4 será abordada no capítulo 6 – Conclusões e trabalho futuro, visto não ter sido possível para já, a aquisição automática de dados referentes aos veículos como os quilómetros. Por fim a resposta à pergunta P5 é naturalmente adquirida com a construção e aglomeração das resoluções/respostas às perguntas P1, P2, P3 e P4.

Através de API's e bibliotecas já existentes, foi possível combinar e efetuar as funcionalidades pretendidas para a solução, pelo que a implementação assentou sobre a modularidade e evolução da solução global iterativamente, permitindo uma maior simplicidade e organização clara das funções e objetivos de cada componente.

No próximo capítulo serão abordados os métodos e testes a efetuar, que permitam garantir o bom funcionamento e possível manutenção futura do sistema. Depois da fase de implementação existem sempre pequenos ajustes e modificações que por vezes apenas são detetados através de testes e experimentações. Desse modo, a fase de testes é imprescindível, como em qualquer outro pojeto. Não só pela deteção de possíveis erros, que impeçam a sua entrega e utilização pelo cliente, como também poderão trazer novas ideias para futuras melhorias.

5 Avaliação do Produto

A avaliação do sistema implementado deverá assentar sobre as premissas de resolução dos objetivos propostos em primeiro lugar (perguntas P1, P2, P3, P4 e P5). É sobretudo este indicador que permitirá avaliar o sucesso do mesmo. No entanto, existem outros fatores que entrarão em jogo nas contas finais. O tempo é um bem precioso, que deve ser bem gerido e aproveitado, não significando isto que a solução deve ser implementada o mais rapidamente possível. A rapidez por vezes é inimiga da perfeição, pelo que a prioridade será sempre a qualidade e satisfação dos objetivos propostos.

O desempenho do sistema é algo a contabilizar na avaliação do sistema. Um dos requisitos do sistema proposto é que este seja rápido, fluído e que não atrase os processos de trabalho do quotidiano, pelo que, este deve ser executado com a maior performance possível.

Por último, a segurança do sistema proposto é um fator muito importante. De nada serve ter-se um sistema, rápido, objetivo e de fácil utilização se este não estiver seguro de possíveis intrusos. Visto ser um sistema que pretende fazer cumprir a lei, podendo levar mesmo à responsabilização do utilizador em certos casos, o acesso a este deverá ser seguro, diminuindo os riscos de intrusão indevida e prevenir a alteração/sabotagem dos dados/informações do mesmo.

A solução aqui implementada implicou a abordagem de áreas completamente distintas. A autenticação biométrica, o reconhecimento de padrões e o controlo e automação, torna esta solução, uma solução complexa e de difícil integração. Como já referido anteriormente a solução está em curso de montagem e os testes finais ainda não podem ser executados completamente. Ou seja, a versão *beta* ainda não foi possível ser entregue.

Melhor dizendo, os testes propriamente ditos apenas podem ser efetuados quando o primeiro protótipo estiver criado e montado devido a várias razões. Uma delas prende-se com a luz UV e a distância entre a *webcam* e a licença de condução, que deve ser testada nas condições finais, pois a distância entre a *webcam* e a licença de condução influenciarão a qualidade de captura e a quantidade de luz UV a emitir.

Outra das razões tem a ver com a qualidade e segurança de diferenciação de utilizadores, ou seja, do processo de autenticação biométrico. Para que o processo de autenticação seja sólido e funcional, este deve ser testado com uma amostra de utilizadores significativa, para que uma confirmação do bom funcionamento de autenticação fique provada. Até ao momento apenas "quatro" utilizadores foram testados no sistema de autenticação.

Por fim, outra das razões prende-se claramente com a qualidade e fluidez da solução. Estes dois parâmetros apenas devem ser julgados pelos utilizadores da mesma.

5.1 Metodologia de avaliação

Para a efetuação dos testes de qualidade, o componente *Authentication System* e o componente *BackOffice* foram testados segundo os casos de uso, percorrendo todos os processos e iterações possíveis na aplicação pelo programador. Também as funções e métodos foram testados utilizando todos os diferentes *inputs* e por consequência os diferentes *outputs*. Em suma, o método "*white-box testing"* foi aplicado. Estatísticas foram criadas apenas para o método de autenticação escolhido, neste caso o reconhecimento da íris para o método de validação da licença de condução, demonstrados nas secções a seguir 5.1.1 e 5.1.2 respetivamente. Por se tratar de uma solução altamente modular, os testes foram sendo efetuado consoante a implementação dos módulos (capítulo 4). Após a criação do primeiro protótipo serão efetuados os testes comuns de "*black-box",* que funcionará como método de aceitação por parte da empresa e utilizadores. Em conjunto, inquéritos de satisfação serão realizados e dirigidos aos utilizadores da solução.

5.1.1 Autenticação ÍRIS

Os testes efetuados para a autenticação da íris tiverem como intervenientes apenas duas pessoas até ao momento, em que cada uma foi registada duas vezes. Cada registo corresponde a um olho diferente, pelo que consideram-se quatro pessoas no total.

Sendo a rapidez e fluidez uma das prioridades principais dos utilizadores, optou-se por efetuar uma identificação e autenticação numa só etapa ao invés de efetuar a identificação separadamente da autenticação. Ou seja, o utilizador não se anuncia ao sistema para de seguida se autenticar (apresentar a íris). Este apenas apresenta a sua íris ao *scanner* para de seguida ser comparada com todos os utilizadores registados na base de dados. No final, o sistema irá verificar qual o utilizador registado na base de dados que mais se aproxima da íris apresentada e caso esta ultrapasse os 80% de semelhança, então o sistema autentica o utilizador.

Obviamente o sistema seria mais rápido a efetuar a autenticação se à partida ele soubesse o utilizador em questão. No entanto por razões de fluidez e simplicidade e por se tratar de um sistema a utilizar no máximo por vinte pessoas, a comparação com todos os utilizadores não tem um impacto significativo na performance do sistema.

Nas Tabelas 3, 4, 5 e 6 a seguir são mostrados os sucessos/insucessos do processo de autenticação efetuado pelas duas pessoas e seus dois respetivos olhos bem como os tempos de autenticação. O processo foi efetuado dez vezes para cada olho. De notar que estes tempos incluem a captação da íris pelo *scanner* do sistema. A coluna "Íris DataBase" corresponde à íris da base de dados à qual o sistema fez a correspondência, em que P1 = Pessoa 1, P2 = Pessoa 2, OD = Olho Direito e OE = Olho Esquerdo.

Tabela 3 – Tabela experimentações pessoa 1, olho direito (P1OD)

Experiência	Tempo (s)	Íris DataBase	Semelhança (%)
1	5,1	P1 OD	87%
2	5,4	P1 OD	83%
3	5,0	P1 OD	91%
4	6,3	P1 OD	85%
5	5,9	P1 OD	94%
6	6,0	P1 OD	93%
7	6,7	P1 OD	81%
8	4,8	P1 OD	83%
9	5,5	P1 OD	88%
10	5,3	P1 OD	81%

A média de tempo dos testes de autenticação foi de 5,6 segundos com uma taxa de sucesso de 100% (nos total de dez testes efetuados, dez foram autenticados com sucesso). A média de semelhança dos testes de autenticação com sucesso foi de 86%.

Tabela 4 – Tabela experimentações pessoa 1, olho esquerdo (P1OE)

Experiência	Tempo (s)	Íris DataBase	Semelhança (%)
1	6,4	P1 OE	93%
2	5,6	P1 OE	90%
3	5,3	P1 OE	93%
4	5,3	P1 OE	89%
5	5,4	P1 OE	87%
6	5,9	P1 OE	92%
7	6,0	P1 OE	88%
8	6,8	P1 OE	36%
9	6,8	P1 OE	88%
10	5,7	P1 OE	83%

A média de tempo dos testes de autenticação foi de 5,92 segundos com uma taxa de sucesso de 90% (no total de dez testes efetuados, nove foram autenticados com sucesso). A média de semelhança dos testes de autenticação com sucesso foi de 89%.

Tabela 5 – Tabela experimentações pessoa 2, olho direito (P2OD)

Experiência	Tempo (s)	Íris DataBase	Semelhança (%)
1	5,0	P2 OD	91%
2	5,2	P2 OD	17%
3	5,2	P2 OD	83%
4	5,3	P2 OD	95%
5	6,7	P2 OD	88%
6	6,6	P2 OD	88%
7	5,9	P2 OD	82%
8	5,1	P2 OD	80%
9	5,8	P2 OD	91%
10	6,0	P2 OD	91%

A média de tempo dos testes de autenticação foi de 5,68 segundos com uma taxa de sucesso de 90% (no total de dez testes efetuados, nove foram autenticados com sucesso). A média de semelhança dos testes de autenticação com sucesso foi de 88%.

Tabela 6 – Tabela experimentações pessoa 2, olho esquerdo (P2OE)

Experiência	Tempo (s)	Íris DataBase	Semelhança (%)
1	5,6	P2 OE	94%
2	6,4	P2 OE	88%
3	6,0	P2 OE	88%
4	6,0	P2 OE	89%
5	6,1	P2 OE	91%
6	5,9	P2 OE	83%
7	5,4	P2 OE	87%
8	5,3	P2 OE	81%
9	5,9	P2 OE	86%
10	5,1	P2 OE	94%

A média de tempo dos testes de autenticação foi de 5,77 segundos com uma taxa de sucesso de 100% (no total de dez testes efetuados, dez foram autenticados com sucesso). A média de semelhança dos testes de autenticação com sucesso foi de 88%.

O processo de aquisição biométrico da íris caracteriza-se por ser um processo complexo, pelo que, segundo os dados obtidos, considera-se que o tempo de aquisição e o sucesso de autenticação é passível de uma nota bastante positiva. O tempo médio total de todos os testes foi de 5,74 segundos com uma taxa de sucesso de 95%.

No entanto, por se tratar de uma amostra de população bastante reduzida, testes de reconhecimento da íris com recurso a mudanças do ambiente, nomeadamente da luz,

reconhecimento da íris com óculos e sem óculos, lentes de contato entre outros fatores suscetíveis de mudança serão efetuados após a entrega do primeiro protótipo.

O protótipo será posto à disposição dos utilizadores com o integrador a acompanhar a utilização. Será nesta fase feito o registo automático por parte do sistema (*logs)*, de todas as interações com o mesmo.

5.1.2 Validação licença de condução

Nesta secção e à semelhança da secção anterior, são demonstrados os testes efetuados ao subcomponente responsável pela validação da licença de condução. É necessário efetuar dois tipos de validação neste subcomponente: o reconhecimento OCR e o reconhecimento do padrão/holograma. Nesta primeira fase de avaliação do subcomponente foram utilizadas duas licenças de condução de diferentes pessoas mas do mesmo país (Suíça).

Novamente, a rapidez e fluidez da solução é uma das prioridades mais importantes para os utilizadores. Desse modo, a leitura dos dados da licença (reconhecimento OCR) e o reconhecimento de padrões são feitos em paralelo, que por sua vez são paralelos ao processo de reconhecimento da íris, ou seja, o utilizador apresenta a licença de condução ao mesmo tempo que apresenta a sua íris ao *IRIS scanner.*

Este processo utiliza duas *webcams* e uma fonte de luz UV. Uma das *webcams,* em conjunto com uma fonte de luz UV, é colocada dentro de uma caixa ao abrigo da luz ambiente. Esta caixa contém apenas uma abertura do mesmo formato que a licença de condução mas um pouco mais reduzida em tamanho, para que a licença seja de seguida pousada sobre essa abertura com a parte traseira virada para essa pequena abertura. A segunda *webcam* é colocada por cima de modo a captar as informações da licença. A parte frontal da licença é fotografada bem como a parte traseira. Esta parte traseira é no entanto fotografada com a luz UV a incidir na mesma como já explicado anteriormente.

O *threshold* de aceitação do padrão foi definido em 70% de semelhança, o que já é um valor bastante elevado, visto uma aquisição fotográfica alterar sempre as propriedades luminosas e de cor a cada aquisição/foto. Nas Tabelas 7 e 8 a seguir, mostram-se os sucessos/insucessos do processo de reconhecimento e validação da carta de condução efetuado pelas duas pessoas e suas duas respetivas licenças de condução. Este processo foi repetido dez vezes para cada licença de condução. De notar que, apenas um padrão retirado de uma das licenças é usado como base de comparação, ou seja, é possível a adição de várias amostras do mesmo padrão, aumentando assim a probabilidade de sucesso de validação.

Tabela 7 – Tabela experimentações licença condução 1

Experiência	Tempo OCR (s)	OCR	Tempo Padrão (s)	Semelhança Padrão
1	1,5	Sucesso	2,4	74%
2	1,6	Sucesso	2,3	75%
3	1,6	Sucesso	2,2	75%
4	1,5	Sucesso	2,2	61%
5	1,4	Sucesso	2,4	76%
6	2,3	Sucesso	2,3	75%
7	1,6	Sucesso	2,3	74%
8	1,6	Sucesso	2,3	74%
9	1,8	Sucesso	2,3	74%
10	1,6	Sucesso	2,1	79%

A média de tempo dos testes de reconhecimento OCR e do padrão/holograma foi de 1,65 e 2,3 segundos respetivamente, com uma taxa de sucesso de 90% (no total de dez testes efetuados, nove cartas de condução foram reconhecidas com sucesso). A média de semelhança dos testes de reconhecimento do padrão/holograma com sucesso foi de 75%.

Tabela 8 – Tabela experimentações licença condução 2

Experiência	Tempo OCR (s)	OCR	Tempo Padrão (s)	Semelhança Padrão
1	1,9	Sucesso	2,2	68%
2	1,4	Sucesso	2,3	79%
3	1,6	Sucesso	2,3	77%
4	1,5	Sucesso	2,2	79%
5	1,4	Sucesso	2,3	81%
6	1,4	Sucesso	2,5	79%
7	1,7	Sucesso	2,5	79%
8	1,6	Sucesso	2,5	78%
9	1,6	Sucesso	2,4	78%
10	1,6	Sucesso	2,4	78%

A média de tempo dos testes de reconhecimento OCR e do padrão/holograma foi de 1,57 e 2,4 segundos respetivamente, com uma taxa de sucesso de 90% (no total de dez testes efetuados, nove cartas de condução foram reconhecidas com sucesso). A média de semelhança dos testes de reconhecimento do padrão/holograma com sucesso foi de 79%.

O processo de reconhecimento de padrões é um processo complexo, pelo que, segundo os dados obtidos, nomeadamente: tempo médio total reconhecimento OCR (1,61 segundos), tempo médio de reconhecimento do padrão/holograma (2,4 segundos), bem como uma taxa de sucesso de 90% final, considera-se que o processo global é passível uma nota bastante positiva. No entanto, à semelhança do processo de reconhecimento da íris, por se tratar de uma amostra de população bastante reduzida, mais testes serão efetuados com todos os utilizadores

da aplicação e suas respetivas licenças de condução, independentemente do país de emissão das mesmas.

5.1.3 Validação da solução global e aceitação

Como já anteriormente explicado, a experimentação da solução a 100% apenas pode ser efetuada uma vez que o protótipo esteja montado. É extremamente difícil ou mesmo impossível, ocupar cada um dos utilizadores durante um dia para efetuar testes com o mesmo. Deste modo os testes por método de caixa negra, em inglês denominado "*black-box testing"*, serão efetuados. Quer isto dizer que o protótipo será criado e posto à disposição dos utilizadores. Assim, não só a funcionalidade e simplicidade da solução poderão ser julgadas, como também a estabilidade dos subcomponentes e métodos implementados. Esta experimentação servirá também como aceitação do produto final (*hardware e software).*

Todos os componentes do sistema serão postos em modo simulação, nos respetivos locais à disposição dos utilizadores (*Authentication System* e *BackOffice*), que com uma pequena formação deverão começar a utilizar os mesmos. Este modo simulação permite registar informações de utilização do produto. Deste modo, dados de performance do sistema serão obtidos automaticamente. Esses dados serão registados com recurso à medição de tempo decorrido nas operações efetuadas, (operações baseadas nos caso de uso), no que diz respeito ao indicador de performance. Em suma, os processos funcionais do sistema serão monitorizados.

Os dados resultantes desta monitorização serão utilizados para efeito de estatística e consequente avaliação final do produto. Estas estatísticas deverão ser formuladas para cada subcomponente da solução individualmente, para uma maior facilidade não só de qualificação de cada "módulo"/subcomponente mas também para facilitar a supressão de possíveis erros e falhas da solução global a nível modular. A realização de inquéritos de satisfação é também um método de avaliação do sistema, principalmente no que à usabilidade e simplicidade do sistema diz respeito. A seguir é apresentada uma lista com os dados que deverão ser registados e agrupados segundo o componente e processo/caso de uso. Por fim uma explicação dos inquéritos a realizar é efetuada.

5.1.3.1 Componente Authentication System

Este componente deverá registar para o processo de requisição de chaves as seguintes informações: utilizador, data e hora início processo, data e hora de fim do processo, sucesso da autenticação da íris, percentagem de semelhança da íris, sucesso de reconhecimento OCR da licença condução, sucesso de validação do holograma, percentagem de semelhança do holograma e erros do processo.

No que toca ao processo/caso de uso de devolução de chaves, as seguintes informações devem ser registadas: data e hora início processo, data e hora de fim do processo, sucesso da leitura RFID da chave e erros do processo.

Por fim, o processo de autenticação do supervisor neste componente através do seu PIN bem como as suas ações devem ser monitorizadas. Para isso, as seguintes informações devem ser registadas: data e hora início do processo, data e hora fim do processo, sucesso registo íris de um utilizador e os erros do processo.

5.1.3.2 Componente BackOffice

Este componente, por se tratar de um componente orientado à manipulação da base de dados, registará as operações de manipulação dos dados. Este será utilizado como um *log* que poderá ajudar na resolução de erros no sistema, especialmente de inconsistências de informações. Os tempos de manipulação deste componente não serão monitorizados pois não se trata de um componente crítico para a fluidez do trabalho quotidiano.

5.1.3.3 Inquéritos de satisfação

A última forma de avaliação da solução se baseará em reuniões de discussão planificadas entre os atores do sistema e o integrador/programador para o apuramento da satisfação dos utilizadores. Destas reuniões um inquérito de satisfação dirigido a cada ator será realizado por parte do integrador/programador. Esta troca de informações permitirá obter uma boa avaliação da funcionalidade e usabilidade da solução global, obtendo ordens de grandeza do sucesso da solução e possíveis melhorias futuras ou novas funcionalidades. No anexo 5 é apresentado o inquérito a efetuar.

5.2 Sumário do capítulo

Neste capítulo foi demostrado uma pequena parte das experimentações e avaliações já efetuadas, mas sobretudo sobre as experimentações e avaliações futuras e respetivo planeamento. É extremamente complicado obter uma base de dados de informações de teste, confiável e utilizável quando um produto é modular como o presente e sobretudo com recurso a vários dispositivos externos, sem que um protótipo esteja desenvolvido fisicamente (montado).

Assim, apesar dos poucos testes efetuados até ao presente, reforça-se a ideia de efetuar os testes necessários num futuro próximo, de modo a efetuar a validação comprovada do produto e suas funcionalidades no seu âmbito global. Obviamente, testes do tipo caixa branca podem sempre ser efetuados, o que sucedeu a cada implementação de um subcomponente do sistema. No entanto, ninguém melhor que os utilizadores finais e o tempo para testarem um sistema.

6 Conclusões e trabalho futuro

Neste último capítulo serão apresentadas as conclusões finais do trabalho efetuado. Uma contextualização do problema será apresentada, seguida de uma avaliação do trabalho efetuado relativamente aos objetivos definidos no início do trabalho. Também os pontos que não foram até ao momento realizados serão deliberados, com o intuito de os incorporar em desenvolvimentos futuros. Por fim, é feita a apreciação final sobre o estudo e protótipo desenvolvidos neste trabalho.

6.1 Conclusões

O mercado de aplicações de gestão de frota começa cada vez mais a fazer parte de sistemas adquiridos por pequenas e médias empresas. O controlo de custos relacionados com a frota é fundamental a nível financeiro de qualquer empresa. Como já dito anteriormente, não só é necessário ter um bom controlo e vigilância de custos, como também é importante para a empresa cumprir os requisitos legais.

Esses requisitos vão desde a verificação das licenças de condução até ao teste de alcoolemia. De nada serve ter um bom controlo de gastos com a frota em termos de seguros, inspeções e manutenções se depois as poupanças efetuadas são gastas em possíveis contraordenações ou mesmo indeminizações. Assim, é necessário que o sistema efetue o controlo de acesso a recursos, ou seja, o controlo de acesso aos veículos. Um dado colaborador pode não estar habilitado para conduzir um determinado veículo de uma determinada categoria, ou simplesmente, pode estar impedido pelas autoridades judiciais de conduzir. Por estes motivos, é imprescindível que o gestor de frota da empresa controle estes parâmetros antes de entregar as chaves de uma viatura ao seu colaborador, caso contrário este poderá estar em incumprimento da lei e provocar danos à empresa.

Dado então o problema, o objetivo principal deste estudo era permitir um controlo de acesso às viaturas de forma automatizada, sem necessidade de recurso a um ser humano. Ou seja, um sistema capaz de autenticar o utilizador e o seu documento de habilitação de condução,

evitando que um dado utilizador possa conduzir um veículo sem estar na posse de uma carta de condução válida.

Este objetivo foi repartido em quatro questões que são agora relembradas:

P1. Como garantir ao máximo possível, que o utilizador que se apresenta é quem diz ser?

P2. Como efetuar uma verificação do seu documento legal de habilitação de condução?

P3. Que mecanismos devem ser implementados para garantir a entrega e devolução correta das chaves das viaturas?

P4. Como obter informações automaticamente das viaturas a gerir?

Estas quatro questões levam à formulação da questão final:

P5. É possível combinar as soluções de P1, P2, P3 e P4 num só produto?

Após o estudo de mercado, verificou-se que as soluções de gestão de frota existentes estavam mais orientadas para a parte administrativa, ou seja, não existem soluções de gestão de frota que efetuem o controlo de acesso aos veículos e sobretudo, que controlem os documentos legais que habilitam um indivíduo a conduzir (carta de condução).

Por estas razões, optou-se pelo desenvolvimento de uma solução que englobasse todas estas funcionalidades, principalmente o controlo de acesso a veículos através da autenticação de utilizadores e verificação da sua carta de condução respondendo dessa forma à questão P5. No que as questões P1, P2, P3 e P4 diz respeito, estas foram respondidas através das implementações demonstradas no capítulo 4.

Assim, a solução para a pergunta P1 foi a implementação de um sistema de autenticação biométrico da íris, que apesar de não ser infalível, apresenta uma maior segurança para o sistema global. Deste modo, é garantida uma autenticação menos suscetível a falha e menos suscetível a roubo de identidade.

A solução para a pergunta P2 foi conseguida através do reconhecimento OCR, que permite corresponder a carta de condução apresentada com o utilizador autenticado através da solução da pergunta P1, combinado com o reconhecimento de padrões. Este reconhecimento de padrões baseia-se na deteção dos hologramas de segurança presentes nas cartas de condução, que servirão de base de autenticação e veracidade das mesmas. Por sua vez, esta deteção baseia-se nas formas desse holograma, visíveis apenas quando uma luz UV é incidida sobre este, evitando assim o engano do sistema através de fotocópias e outras imitações de mais fácil fabrico. Novamente, tal como a autenticação da íris este método não é infalível. Uma falsificação de uma carta de condução poderá ser autenticada, dependendo da qualidade da falsificação em si.

A solução à pergunta P3 foi conseguida através da adição de identificadores RFID nas chaves dos veículos. Deste modo, recorrendo a um leitor RFID compatível, é possível identificar a chave

apresentada ao sistema. Obviamente, o identificador deve ser adicionado à chave de maneira a que este não possa ser removido e trocado por outro identificador de outra chave. Caso isso aconteça, deverá ser percetível aos utilizadores, principalmente ao gestor da frota.

Por fim, a solução à pergunta P4 não foi ainda possível de ser realizada. Esta será alvo de desenvolvimento futuro, tal como o teste de alcoolemia, que apesar desta última não ser uma funcionalidade principal a obter, seria sem dúvida uma mais-valia. Estas duas funcionalidades serão abordadas na próxima secção.

6.2 Trabalho futuro

Os objetivos principais foram de facto realizados. No entanto fica ainda em aberto a resposta/solução à pergunta P4. Devido à escolha efetuada, a aquisição de dados dos veículos de forma automática não é atualmente possível.

É assim necessário estar atento à evolução dos fabricantes automóveis, verificando regularmente se estes permitem interfaces simples de leitura de informações das chaves no que a informações de avarias e manutenção diz respeito. Porém, é possível num futuro próximo adicionar uma mais-valia à solução global, que é explicada de seguida.

Como visto durante a dissertação, existem hoje em dia soluções de gestão de frota que permitem localizar os veículos e consequentemente traçar os percursos efetuados. Desse modo, a aplicação de um localizador GPS em cada veículo, irá permitir à solução global obter informações de percurso dos mesmos (dispositivo conectado via internet). Em consequência, o preenchimento do diário de bordo será automatizado bem como a atribuição de percursos a utilizadores e seus respetivos quilómetros.

Com o diário de bordo preenchido automaticamente, alertas de manutenção a efetuar poderão ser enviados ao gestor de frota, em função dos quilómetros dos veículos. De notar que hoje em dia, a maior parte dos fabricantes têm bem definidos os *deadlines* para manutenções em termos de tempo e quilómetros, com grupos de peças e trabalhos bem definidos em cada manutenção.

Por fim o teste de alcoolemia será integrado num futuro próximo. Não sendo este um objetivo principal, não deixa de ser uma mais-valia para uma solução que pretende fazer cumprir a legislação ao máximo possível. Esta funcionalidade deverá basear-se no princípio modular da solução, em que um dispositivo capaz de efetuar o teste de alcoolemia e sua API deverão ser integradas na solução global.

6.3 Apreciação final

Após a conclusão dos estudos e consequente protótipo, pode-se afirmar que os objetivos principais foram atingidos, com a exceção da obtenção de informações dos veículos

automaticamente (P4), como explicado na secção anterior. Também os objetivos secundários como a gestão de reservas, o bloqueio de utilizadores e veículos, a gestão de acesso a veículos entre outros foram cumpridos.

No entanto, o sistema final ainda não está completo, faltando ainda a montagem final. Só a montagem final da solução, como já explicado no capítulo anterior, permitirá efetuar testes de desempenho, funcionalidade e satisfação da empresa na sua globalidade. Será esse o ponto de partida porventura, para mais melhorias e implementações futuras de novas funcionalidades até aqui não identificadas.

Em suma, a dissertação aqui apresentada em tudo é assentada nos pilares e essência da Engenharia. O processo de pesquisa de possíveis soluções a utilizar, o processo de análise e por fim o processo de implementação de uma solução apoiada nos métodos de boa programação, assim como a utilização de módulos já existentes contribuíram para o sucesso da solução implementada. De assinalar também que esta dissertação promoveu a aplicação dos conhecimentos adquiridos no âmbito das várias unidades curriculares, que fazem parte da disciplina como: a pesquisa e escrita técnico-científica, análise de valor de negócio e experimentação e avaliação, que resultaram num enorme enriquecimento de competências profissionais.

7 Referências

[1] "About Us." [Online]. Available: http://www.chevinfleet.com/us/about_us.asp. [Accessed: 19-Jan-2016].

[2] "Case Studies." [Online]. Available: http://www.chevinfleet.com/us/case_studies.asp. [Accessed: 19-Jan-2016].

[3] "Contact Fleetio." [Online]. Available: https://www.fleetio.com/contact. [Accessed: 19-Jan-2016].

[4] "All Features - Fleetio." [Online]. Available: https://www.fleetio.com/all-features. [Accessed: 19-Jan-2016].

[5] F. Tabouret, "Le Chronotachygraphe," *Le Tigre*, no. 29, 2013.

[6] "EUR-Lex - 32014R0165 - PT - EUR-Lex." [Online]. Available: http://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1453198803482&uri=CELEX:32014R0165. [Accessed: 19-Jan-2016].

[7] "EUR-Lex - 32006R0561 - PT - EUR-Lex." [Online]. Available: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32006R0561. [Accessed: 19-Jan-2016].

[8] O. D. E. Instalação and D. E. T. Digital, "MANUAL DE PROCEDIMENTOS RELATIVOS À IMPLEMENTAÇÃO DO TACÓGRAFO DIGITAL."

[9] "Understanding and selecting authentication methods - TechRepublic." [Online]. Available: http://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/. [Accessed: 19-Jan-2016].

[10] D. Jablon, "Methods for Knowledge - Based Authentication David Jablon," pp. 1–26, 2004.

[11] D. de Borde, "Two-factor authentication." Siemens Insight Consulting, 2007.

[12] F. F. I. E. Council, "Authentication in an Internet Banking Environment." 2008.

[13] L. Li, "Technology designed to combat fakes in the global supply chain," *Bus. Horiz.*, vol. 56, no. 2, pp. 167–177, Mar. 2013.

[14] "Jeton d'authentification — Wikipédia." [Online]. Available: https://fr.wikipedia.org/wiki/Jeton_d%27authentification. [Accessed: 19-Jan-2016].

[15] "GOLD OTP Challenge Response Authentication Token - SafeNet, Inc." [Online]. Available: http://www.safenet-inc.com/multi-factor-authentication/authenticators/one-time-password-otp/gold-challenge-response-token/. [Accessed: 19-Jan-2016].

[16] “authentication - static vs dynamic vs challenge response - Information Security Stack Exchange.” [Online]. Available: http://security.stackexchange.com/questions/31711/static-vs-dynamic-vs-challenge-response. [Accessed: 19-Jan-2016].

[17] “About Smart Cards : Frequently Asked Questions » Smart Card Alliance.” [Online]. Available: http://www.smartcardalliance.org/smart-cards-faq/. [Accessed: 19-Jan-2016].

[18] A. K. Jain and A. Ross, *Introduction to Biometrics*. Springer, 2008.

[19] “Biometrics: Overview.” Biometrics.cse.msu.edu, 2007.

[20] A. Babich, “Biometric Authentication . Types of biometric identifiers,” pp. 1–56, 2012.

[21] J. Wayman, J. Wayman, A. Jain, A. Jain, D. Maltoni, D. Maltoni, D. Maio, and D. Maio, “An Introduction to Biometric Authentication Systems,” *Biometric Syst.*, pp. 1–20, 2005.

[22] “History of Fingerprinting - How Fingerprinting Works | HowStuffWorks.” [Online]. Available: http://science.howstuffworks.com/fingerprinting3.htm. [Accessed: 19-Jan-2016].

[23] “Biometric Passport.” [Online]. Available: https://en.wikipedia.org/wiki/Biometric_passport. [Accessed: 20-Jan-2016].

[24] “Infraestrutura de Chaves Públicas – Wikipédia, a enciclopédia livre.” [Online]. Available: https://pt.wikipedia.org/wiki/Infraestrutura_de_Chaves_P%C3%BAblicas. [Accessed: 20-Jan-2016].

[25] “PKI - Infra-estrutura de Chaves Públicas.” [Online]. Available: http://www.gta.ufrj.br/ensino/eel879/Anos-anteriores/2008-2/trabalhos_vf/hugo/index.html. [Accessed: 20-Jan-2016].

[26] S. Gold, “The biometric passport imperative,” *Biometric Technol. Today*, vol. 2013, no. 2, pp. 5–6, 2013.

[27] H. Liping and S. Lei, “Research on trust model of PKI,” *Proc. - 4th Int. Conf. Intell. Comput. Technol. Autom. ICICTA 2011*, vol. 1, pp. 232–235, 2011.

[28] “e-Passports | Homeland Security.” [Online]. Available: http://www.dhs.gov/e-passports. [Accessed: 20-Jan-2016].

[29] “Posts about e-Passport on CRISISBOOM.” [Online]. Available: http://crisisboom.com/tag/e-passport/. [Accessed: 20-Jan-2016].

[30] “What do I need to know about using e-passport gates? | Find Laws, Legal Information, News & Solicitors - Findlaw UK.” [Online]. Available: http://findlaw.co.uk/law/immigration_emigration/other_immigration_law_topics/travelling_to_the_uk/30368.html. [Accessed: 20-Jan-2016].

[31] G. Avoine, K. Kalach, and J. J. Quisquater, “ePassport: Securing international contacts with contactless chips,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5143 LNCS, pp. 141–155, 2008.

[32] “Que informação contém e para que serve o chip%3f.” [Online]. Available: https://www.cartaodecidadao.pt/index.php%3Foption=com_content&task=view&id=7&Itemid=35&lang=pt.html. [Accessed: 20-Jan-2016].

[33] “How holograms work - Explain that Stuff.” [Online]. Available: http://www.explainthatstuff.com/holograms.html. [Accessed: 20-Jan-2016].

[34] “Transponder car key - Wikipedia, the free encyclopedia.” [Online]. Available: https://en.wikipedia.org/wiki/Transponder_car_key. [Accessed: 20-Jan-2016].

[35] “Start Volkswagen Car without immobilizer.” [Online]. Available: https://www.youtube.com/watch?v=q4fYDbQD8Q0. [Accessed: 20-Jan-2016].

[36] “Transponder History and RADAR Identification of Aircraft.” [Online]. Available: http://www.experimentalaircraft.info/homebuilt-aircraft/avionics-transponder-2.php. [Accessed: 20-Jan-2016].

[37] S. Ahuja and P. Potti, “An Introduction to RFID Technology,” *Commun. Netw.*, vol. 2, no. 3, pp. 183–186, 2010.

[38] S. Preradovic, N. C. Karmakar, and I. Balbin, “RFID transponders,” *IEEE Microw. Mag.*, vol. 9, pp. 90–103, 2008.

[39] “Active RFID vs. Passive RFID: What’s the Difference?” [Online]. Available: http://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid. [Accessed: 20-Jan-2016].

[40] T. S. Key, S. Key, A. Audi, A. Audi, A. Audi, A. Audi, A. Audi, A. Audi, A. Audi, R. Audi, Q. Audi, Q. Audi, and Q. Audi, “Maintenance concept,” pp. 16–19, 2009.

[41] “Transponder car key - Wikipedia, the free encyclopedia.” [Online]. Available: https://en.wikipedia.org/wiki/Transponder_car_key#Transponder. [Accessed: 20-Jan-2016].

[42] “IriShield | Iris Camera | Iris Scanning.” [Online]. Available: http://www.iritech.com/products/hardware/irishield%E2%84%A2-series#. [Accessed: 21-Jan-2016].

[43] “Iris Scanner | Iris Biometrics Technology | Iris Recognition.” [Online]. Available: http://www.iritech.com/. [Accessed: 21-Jan-2016].

[44] J. Daugman, “How Iris Recognition Works,” *Essent. Guid. to Image Process.*, vol. 14, no. 1, pp. 715–739, 2009.

[45] J. Daugman, “Iris Recognition,” *Am. Sci.*, vol. 89, no. 4, p. 326, 2001.

[46] “What is Interactive Logon?: Logon and Authentication.” [Online]. Available: https://technet.microsoft.com/en-us/library/cc780095(v=ws.10).aspx. [Accessed: 21-

Jan-2016].

[47] “How Interactive Logon Works: Logon and Authentication.” [Online]. Available: https://technet.microsoft.com/en-us/library/cc780332(v=ws.10).aspx. [Accessed: 21-Jan-2016].

[48] A. J. Justino, I. S. Gaspar, and J. Cristina, “Biometria : Reconhecimento de Íris,” pp. 5–9, 2012.

[49] “RFID Frequencies | RFID Frequency Bands & Spectrum | Allocations.” [Online]. Available: http://www.radio-electronics.com/info/wireless/radio-frequency-identification-rfid/low-high-frequency-bands-frequencies.php. [Accessed: 25-Jan-2016].

[50] “Operation Of RFID Systems.” [Online]. Available: http://www.tutorialsweb.com/rfid/operation-of-rfid-systems.htm. [Accessed: 25-Jan-2016].

[51] O. T. Worldwide, “The Global SAW Tag - a New Technical Approach to RFID,” *Reading*, 2004.

[52] P. Sorrells, “Passive RFID Basics,” *Microchip Technol. Inc*, pp. 1–7, 2010.

[53] “Classification des tags RFID.” [Online]. Available: http://www.centrenational-rfid.com/classification-des-tags-rfid-article-19-fr-ruid-17.html. [Accessed: 25-Jan-2016].

[54] “RFID: How it works.” [Online]. Available: http://www.cord-ex.com/news/2015/12/rfid-how-it-works/. [Accessed: 25-Jan-2016].

[55] “Basic Components of RFID Systems.” [Online]. Available: http://fr.slideshare.net/PeterSam67/basic-components-of-rfid-systems. [Accessed: 25-Jan-2016].

[56] “Dispositif de gestion de véhicules.” [Online]. Available: https://www.geotab.com/fr/vehicle-management-device/. [Accessed: 26-Jan-2016].

[57] (SYRIS Technology Corp), “About FAR, FRR and EER,” *Tech. Doc.*, pp. 0–4, 2004.

[58] “The relation between FRR and FAR.” [Online]. Available: http://abibiometrics.org/the-relation-between-frr-and-far.html. [Accessed: 27-Jan-2016].

[59] “中国科学院自动化研究所.” [Online]. Available: http://english.ia.cas.cn/. [Accessed: 27-Jan-2016].

[60] “History of Computers and Computing, Internet, Dreamers, Emanuel Goldberg.” [Online]. Available: http://history-computer.com/Internet/Dreamers/Goldberg.html. [Accessed: 29-Jan-2016].

[61] M. Jameson, “The Optophone: Its Beginning and Development,” *Bull. Prosthet. Res.*, pp. 25–28, 1966.

[62] “Kurzweil Computer Products - Everything2.com.” [Online]. Available: http://everything2.com/title/Kurzweil+Computer+Products. [Accessed: 29-Jan-2016].

[63] “How does OCR document scanning work? - Explain that Stuff.” [Online]. Available: http://www.explainthatstuff.com/how-ocr-works.html. [Accessed: 29-Jan-2016].

[64] “How Does Optical Character Recognition Work?” [Online]. Available: http://www.nedocs.com/blog/how-does-optical-character-recognition-work. [Accessed: 29-Jan-2016].

[65] A. K. Jain and R. P. W. Duin, “Introduction to Pattern Recognition 1,” 2004.

[66] L. Zheng and X. He, “Classification Techniques in Pattern Recognition,” *Signal Processing*, 2007.

[67] Reh, “OCR — Optical Character Recognition,” *Orthopädie & Rheuma*, no. December, 2012.

[68] “itseez-vision that works!” [Online]. Available: http://itseez.com/. [Accessed: 29-Jan-2016].

[69] “OpenCV | OpenCV.” [Online]. Available: http://opencv.org/. [Accessed: 29-Jan-2016].

[70] “Smart Key Systems - Can other people unlock my car door with their remote? | HowStuffWorks.” [Online]. Available: http://electronics.howstuffworks.com/gadgets/automotive/unlock-car-door-remote2.htm. [Accessed: 29-Jan-2016].

[71] BMW, “Prestations de service BMW Service: Le service chez BMW.” [Online]. Available: http://www.bmw.fr/fr/topics/offers-services/personal-services/bmw-service.html.

[72] Look for diagnosis, “Gangrena di fournier.” [Online]. Available: http://www.lookfordiagnosis.com/mesh_info.php?term=gangrena di fournier&lang=5.

[73] Boegli-Gravures SA, “Home - Boegli Gravures,” 2016. [Online]. Available: http://www.boegli.ch/. [Accessed: 14-Aug-2016].

[74] “PostFinance ersetzt ihre E-Banking-Kartenleser - onlinepc.ch.” [Online]. Available: http://www.onlinepc.ch/internet/online/postfinance-ersetzt-ihre-e-banking-kartenleser-356224.html.

[75] “Hologram Products Overt Covert Security Features - Holographic Overlay with Invisible UV Exporter from New Delhi.” [Online]. Available: http://www.idcardhologram.com/hologram-products-overt-covert-security-features.html.

[76] “L’ePasseport en pleine expansion.” [Online]. Available: http://www.crime-expertise.org/lepasseport-le-controle-didentite-biometrique-en-pleine-expansion/.

[77] “FACE-TEK Face Recognition Management Systems.” [Online]. Available: http://www.face-tek.com/e_bias_detail.php?BiasID=3.

[78] “Iris recognition technology comes of age | SecurityInfoWatch.com.” [Online]. Available: http://www.securityinfowatch.com/article/12262537/iris-recognition-technology-comes-of-age.

[79] “NuGet Gallery | PCSC 3.5.1.” [Online]. Available: https://www.nuget.org/packages/PCSC/.

[80] “AForge.NET :: Computer Vision, Artificial Intelligence, Robotics.” [Online]. Available: http://www.aforgenet.com/.

[81] “NuGet Gallery | A .Net wrapper for tesseract-ocr 3.0.2.” [Online]. Available: https://www.nuget.org/packages/Tesseract/.

[82] “Microsoft Visual Studio 2015.” [Online]. Available: https://www.microsoft.com/france/visual-studio/.

8 Anexos

8.1 Anexo 1 – Casos de uso

8.1.1 UC.1 Caso de uso "Use a vehicle"

A. Formato casual

O utilizador, neste caso o condutor, seleciona a opção autenticação do componente *Authentication System*, que como dito anteriormente é o componente responsável pelo repositório de chaves. De seguida apresenta o seu olho ao sistema, através do dispositivo de captura da iris ao mesmo tempo que apresenta a sua carta de condução. O sistema deteta o condutor e apresenta-lhe uma lista de veículos disponíveis para utilização ou não, consoante a boa ou má autenticação.

B. Formato completo

Ator principal

Condutor

Partes interessadas e seus interesses

Condutor e Supervisor da frota. Permitir que o condutor escolha e utilize uma viatura sem intervenção do supervisor.

Pré condições

Condutor deve estar registado no sistema assim como os seus dados biométricos. Deve também estar na posse da sua carta de condução. A viatura escolhida deve estar disponível.

Pós condições

O condutor foi autenticado e autorizado a utilizar uma viatura que escolheu.

Fluxo principal de sucesso

1. O condutor apresenta a iris ao sistema em conjunto com a carta de condução.
2. O sistema autentica e apresenta a lista possível de viaturas.
3. O condutor seleciona a viatura pretendida.
4. O sistema efetua a abertura do compartimento da chave pretendida.

5. O condutor pega nas chaves e fechar o compartimento

Fluxos alternativos

1. O supervisor efetua *login* através do seu código PIN.
2. O sistema apresenta a lista de todas as viaturas e respetivo compartimento.
3. O supervisor seleciona o compartimento a abrir.
4. O sistema pede ao supervisor que indique o motivo da abertura do compartimento.
5. O supervisor escolhe o motivo.
    a. Caso o motivo seja devido ao esquecimento da carta de condução por parte do condutor, o sistema pede que o supervisor indique o condutor em questão.
6. O sistema abre o compartimento.
7. O supervisor pega na chave e volta a fechar o compartimento.

Exceções

1. O condutor não é autorizado a entrar no sistema.
2. Não existem veículos disponíveis no repositório atual.
3. O supervisor não é autorizado através do PIN introduzido.
4. Um teste de alcoolemia é solicitado.
    a. O condutor acusou álcool.

Pressupostos

1. O sistema de reconhecimento de iris e de cartas de condução estão instalado e funcionais.
2. O condutor esta registado no sistema bem como as suas credenciais biométricas.
3. O condutor não está na posse de uma viatura.

8.1.2 UC.2 Caso de uso "Return a vehicle"

A. Formato casual

O utilizador, neste caso o condutor, seleciona a opção devolução no componente *Authentication System*. De seguida o próximo compartimento livre é aberto. O utilizador coloca a chave no compartimento. O sistema efetua a identificação da chave e se for uma chave que estivera em utilização este aceita-a e fecha o compartimento.

B. Formato completo

Ator principal

Condutor

Partes interessadas e seus interesses

Condutor e Supervisor da frota. Permitir que o condutor devolva uma viatura sem intervenção do supervisor.

Pré condições

O condutor deve estar na posse de uma chave de viatura (UC.1).

Pós condições

A chave é identificada com sucesso e o compartimento é fechado

Fluxo principal de sucesso

1. O condutor inicia o processo de devolução.
2. O sistema abre um compartimento livre.
3. O condutor coloca a chave no compartimento indicado pelo sistema.
4. O sistema efetua a validação da chave.
5. O condutor fecha o compartimento da chave.

Fluxos alternativos

1. O supervisor efetua *login* através do seu código PIN.
2. O sistema apresenta a lista de todas as viaturas e respetivo compartimento.
3. O supervisor seleciona o compartimento a abrir.
4. O sistema pede ao supervisor que indique o motivo da abertura do compartimento.
5. O supervisor escolhe que pretende devolver a chave pertence a viatura associada a esse compartimento.
6. O sistema abre o compartimento.
7. O supervisor coloca a chave.
8. O sistema efetua a validação da chave
9. O supervisor fecha o compartimento da chave.

Exceções

1. Não existem veículos a devolver.

2. O supervisor não é autorizado através do PIN introduzido.

Pressupostos

1. O sistema de reconhecimento de iris está instalado e funcional.
2. O condutor está na posse de uma chave.

8.1.3 UC.3 Caso de uso "New Driver registration"

A. Formato casual

O supervisor através do componente *BackOffice* seleciona a opção "*Driver Management*" e de seguida a opção "New Driver". O sistema apresenta um formulário com os diferentes dados do condutor a preencher bem como as atribuições de viaturas permitidas ao mesmo. O supervisor introduz e grava os dados.

Na segunda parte do processo o supervisor desloca-se a um dos componentes *Authentication System* (repositórios) com o condutor em causa. De seguida efetua *login* nesse componente através do seu PIN. O supervisor seleciona a opção de visualização da lista de condutores do sistema. O supervisor seleciona da lista o condutor pretendido e escolhe a opção "Novos dados biométricos". O condutor em causa aproxima o olho do dispositivo de reconhecimento biométrico. Os seus dados biométricos são gravados no sistema e associados ao condutor gravado no componente *BackOffice*.

B. Formato completo

Ator principal

Supervisor

Partes interessadas e seus interesses

Supervisor da frota. Permitir que o condutor tenha acesso ao sistema.

Pré condições

O supervisor deve ter uma sessão de domínio Windows aberta.

Pós condições

O condutor foi registado no sistema e poderá utilizar as viaturas da empresa.

Fluxo principal de sucesso

1. O supervisor regista os dados do condutor através do componente *BackOffice*.
2. O supervisor acede ao componente *Authentication System* através do seu PIN.
3. O supervisor visualiza através deste último componente a lista de condutores atuais do sistema.
4. O supervisor seleciona da lista o condutor pretendido e escolhe a opção "Novos dados biométricos".
5. O sistema pede a apresentação do olho do condutor em causa.
6. O condutor aproxima o olho do dispositivo de reconhecimento biométrico.
7. O sistema grava os dados biométricos do condutor.

Fluxos alternativos

Não estão previstos fluxos alternativos.

Exceções

1. O supervisor não é autorizado a aceder ao componente de *BackOffice*.
2. O supervisor não é autorizado a aceder ao componente *Authentication System* através do PIN introduzido.
3. O condutor não se encontra presente.

Pressupostos

1. O supervisor iniciou a sua sessão Windows no domínio da empresa.
2. O sistema de reconhecimento de iris está instalado e funcional.
3. O condutor encontra-se presente na segunda parte do processo.

8.1.4 UC.4 Caso de uso "Vehicles Reservations"

A. Formato casual

O supervisor através do componente *BackOffice* seleciona a opção "*Reservations*" e de seguida a opção "*New Reservation*". O sistema apresenta um formulário com os diferentes dados a preencher bem como a viatura a reservar, o condutor afetado e a data e hora de início e fim previsto. O supervisor introduz e grava os dados.

B. Formato completo

Ator principal

Supervisor

Partes interessadas e seus interesses

Supervisor da frota. Permitir que o condutor tenha acesso a viatura na data e hora previamente pretendida, evitando que a viatura seja utilizada por outro condutor.

Pré condições

A reserva da viatura não deve intercetar no espaço temporal com outra reserva da mesma viatura.

O condutor não deve estar afeto a outra reserva que seja intercetada pela nova reserva.

Pós condições

O condutor utilizará garantidamente a viatura no tempo pretendido.

Fluxo principal de sucesso

1. O supervisor regista os dados da reserva através do componente *BackOffice*.
2. O sistema deteta a sobreposição de outras reservas da mesma viatura ou do mesmo condutor.
3. A reserva é efetuada.

Fluxos alternativos

Não estão previstos fluxos alternativos.

Exceções

1. O supervisor não é autorizado a aceder ao componente de *BackOffice*.
2. A viatura escolhida para a reserva possui já uma reserva que se sobrepõe ao espaço temporal da nova reserva.
3. O condutor possui já uma reserva que se sobrepõe ao espaço temporal da nova reserva.

Pressupostos

1. O supervisor iniciou a sua sessão Windows no domínio da empresa.

2. O componente de *Authentication System* não deve permitir a utilização da viatura por outro condutor que não o da reserva no espaço temporal da mesma.

8.1.5 UC.5 Caso de uso "Fleet status check"

A. Formato casual

O supervisor através do componente *BackOffice* seleciona a opção "*Vehicle* Management" e de seguida escolhe na lista de viaturas apresentadas pelo sistema a viatura pretendida. O sistema apresenta os diferentes de base da viatura, como a marca, modelo, matriculo entre outros. O supervisor escolhe a opção "*More info*". O sistema apresenta dados relativos a anomalias, serviços e outras informações recolhidas da viatura.

B. Formato completo

Ator principal

Supervisor

Partes interessadas e seus interesses

Supervisor da frota. Permitir que o supervisor tenha uma perceção do estado atual da viatura.

Pré condições

As informações da chave da viatura devem ter sido lidas pelo menos uma vez.

Pós condições

O supervisor obtém informações do estado da viatura.

Fluxo principal de sucesso

1. O supervisor seleciona a viatura pretendida através do componente *BackOffice*.
2. O sistema apresenta as informações de base da viatura.
3. O supervisor seleciona a opção "*More info*".
4. O sistema apresenta dados relativos a anomalias, serviços e outras informações recolhidas da viatura em questão.

Fluxos alternativos

Não estão previstos fluxos alternativos.

Exceções

1. O supervisor não é autorizado a aceder ao componente de *BackOffice*.
2. A viatura escolhida não contem dados relativos a anomalias, serviços entre outros.

Pressupostos

1. O supervisor iniciou a sua sessão Windows no domínio da empresa.
2. A viatura encontra-se registada no sistema e as informações da chave desta foi já lida pelo menos uma vez pelo sistema.
3. A chave da viatura pode ser lida pelo sistema.

8.1.6 UC.6 Caso de uso "View Vehicle LogBook"

A. Formato casual

O supervisor através do componente *BackOffice* seleciona a opção "*Vehicle Management*" e de seguida escolhe na lista de viaturas apresentadas pelo sistema a viatura pretendida. O sistema apresenta os diferentes de base da viatura, como a marca, modelo, matriculo entre outros bem como uma lista com os registos de utilização da viatura.

B. Formato completo

Ator principal

Supervisor

Partes interessadas e seus interesses

Supervisor da frota. Permitir que o supervisor conheça o histórico da utilização da viatura.

Pré condições

A viatura deve ter sido utilizada pelo menos uma vez.

Pós condições

O supervisor acede ao histórico de utilização da viatura.

Fluxo principal de sucesso

1. O supervisor seleciona a viatura pretendida através do componente *BackOffice*.
2. O sistema apresenta as informações de base da viatura.
3. O sistema apresenta a lista de registos de utilização da viatura, contendo as informações uteis ao supervisor.

Fluxos alternativos

Não estão previstos fluxos alternativos.

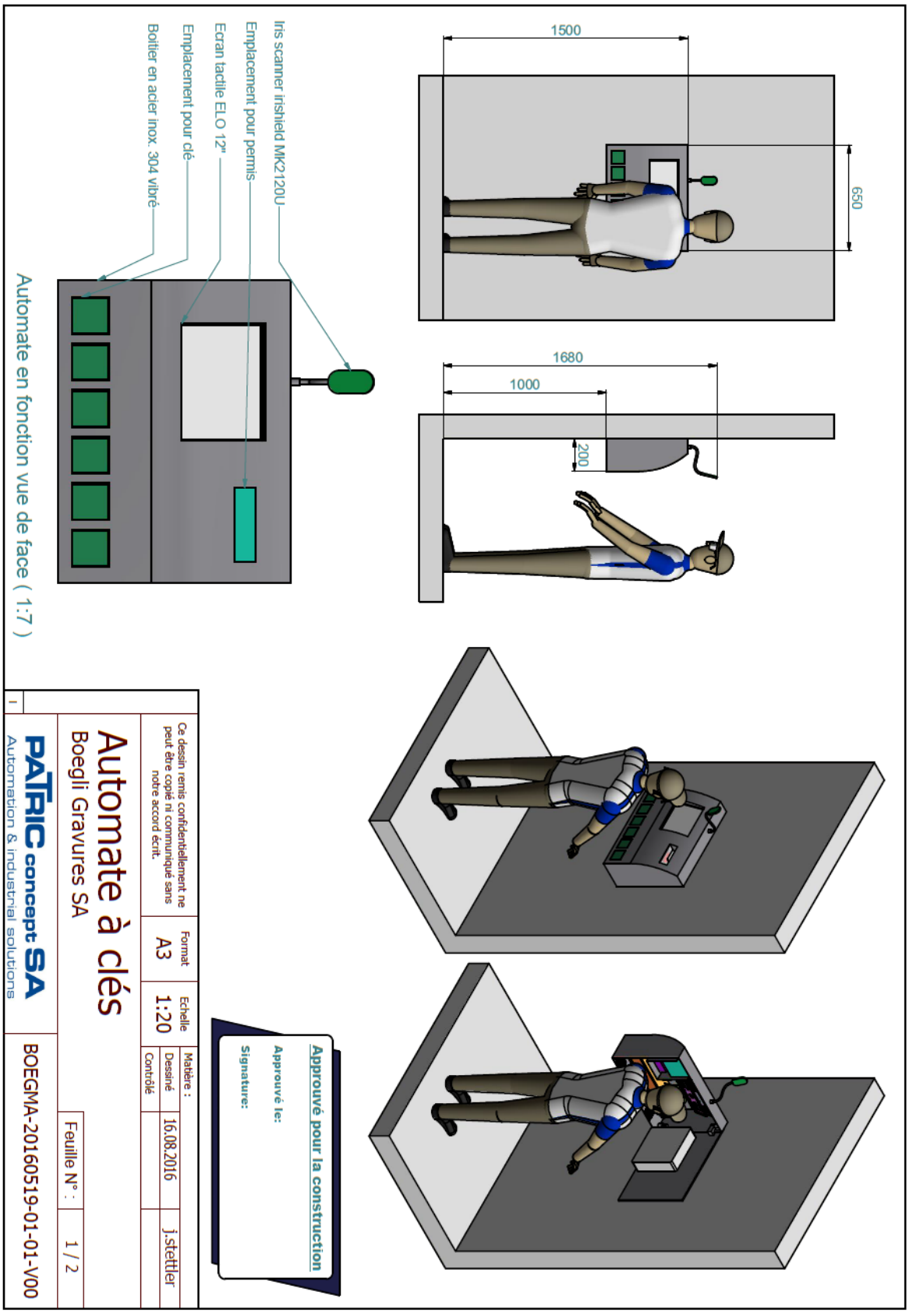
Exceções

1. O supervisor não é autorizado a aceder ao componente de *BackOffice*.
2. A viatura escolhida ainda não foi utilizada por nenhum condutor.

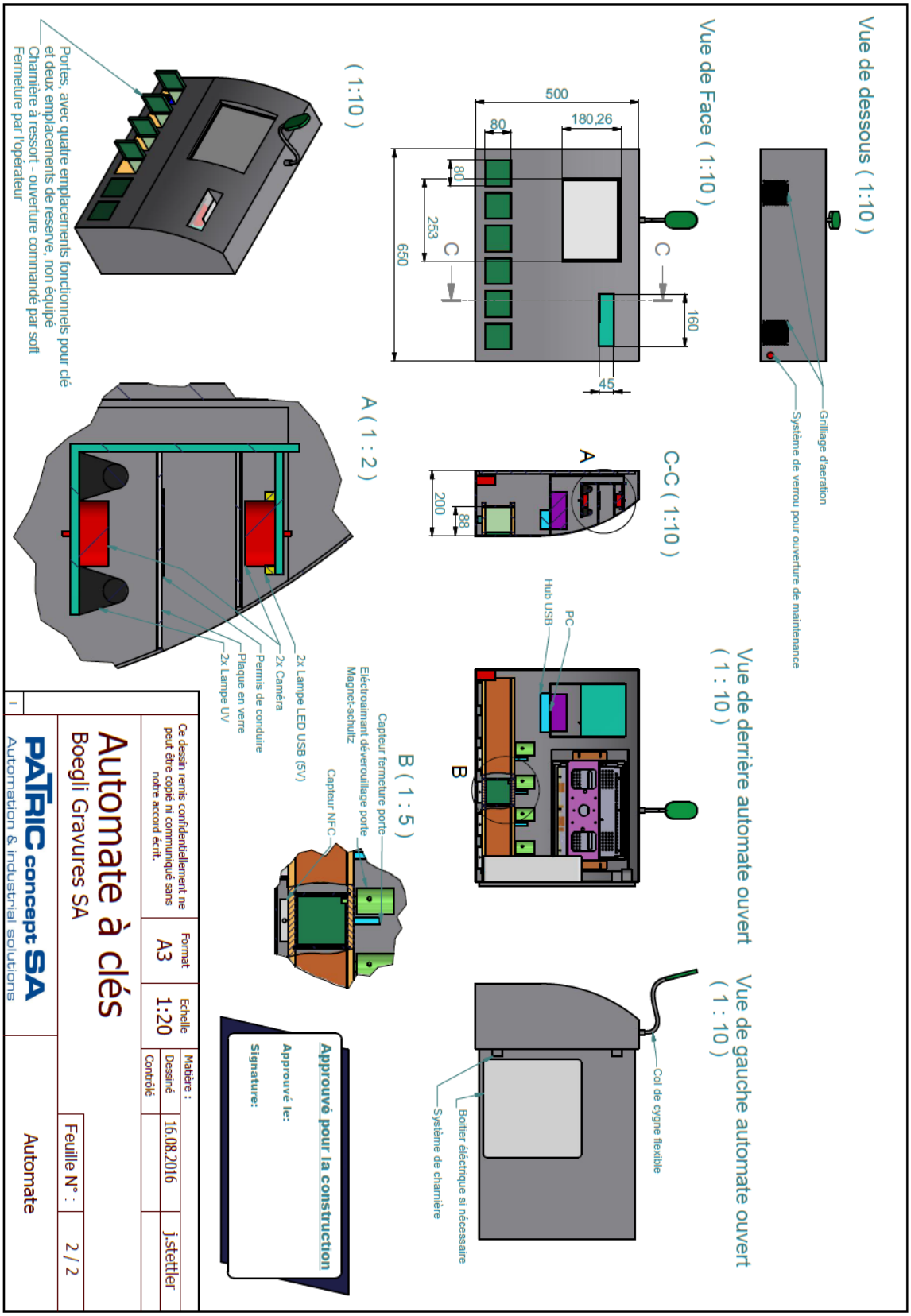
Pressupostos

1. O supervisor iniciou a sua sessão Windows no domínio da empresa.
2. A viatura encontra-se registada no sistema e já foi utilizada pelo menos uma vez no sistema.
3. A chave da viatura pode ser lida pelo sistema.

8.2 Anexo 2 – Montagem Authentication System parte 1



8.3 Anexo 3 – Montagem Authentication System parte 2



8.4 Anexo 4 – Orçamento de custos de montagem e integração

O orçamento a seguir apresentado, diz respeito a um componente *Authentication System*. De lembrar que a empresa necessitará de dois, pois esta está fisicamente divida em três polos/edifícios separados. Este orçamento pode ser contabilizado como o orçamento final, visto os restantes componentes não necessitarem de material físico propriamente dito e a programação da solução ter sido feita internamente na sua totalidade. O componente de *BackOffice* denomina-se por um componente de *software,* que será instalado no computador do gestor da frota e a base de dados será colocada em servidores de produção já existentes. Na Tabela 9 a seguir é apresentado o orçamento.

Tabela 9 – Tabela comparativa da gama de produtos IriShield

Posição	Artigo	Descrição	Quantidade	Preço Unitário
1	IriShield 2120U	Scanner íris	1	189 €
2	ACS ACR122U	Leitor RFID	5	47 €
3	Tag RFID	Mifare 1K	5	0.90 €
4	Logitech HD C525	Webcam	2	54 €
5	Samsung DB10E-T	Ecran Táctil	1	472 €
6	Intel NUC NUC5i7RYH	Computador com RAM, Disco e SO	1	835 €
7	Arduino Mega 2560	Microcontrolador Portas	1	59 €
8	Montagem e Integração Completa	Materias para construção, Cablagem, Montagem	1	7'200 €
			Total C/IVA	9'103 €
			Total S/IVA	8'375 €

IVA de 8%

8.5 Anexo 5 – Inquérito de satisfação

Avaliação do software Fleet Management

Este inquérito tem por objetivo avaliar a prestação do software Fleet Management junto dos seus utilizadores.

Nome completo: _____

1

O software Fleet Management é fluído e rápido na execução das tarefas?

- ○ Sim, muito
- ○ Mais ou menos sim
- ○ De velocidade média
- ○ Mais ou menos não
- ○ Absolutamente não

2

É a interface do nosso software fácil de usar?

- ○ Sim, muito
- ○ Mais ou menos sim
- ○ De dificuldade média
- ○ Mais ou menos não
- ○ Absolutamente não

3

A documentação que acompanha o nosso sofware é:

- ○ Muito útil
- ○ Mais ou menos útil
- ○ Normal
- ○ Mais ou menos inútil

- Absolutamente inútil

4

O software Fleet Management cobre todas as necessidades?

- Definitivamente sim
- Provavelmente sim
- Não sei
- Provavelmente não
- Definitivamente não

5

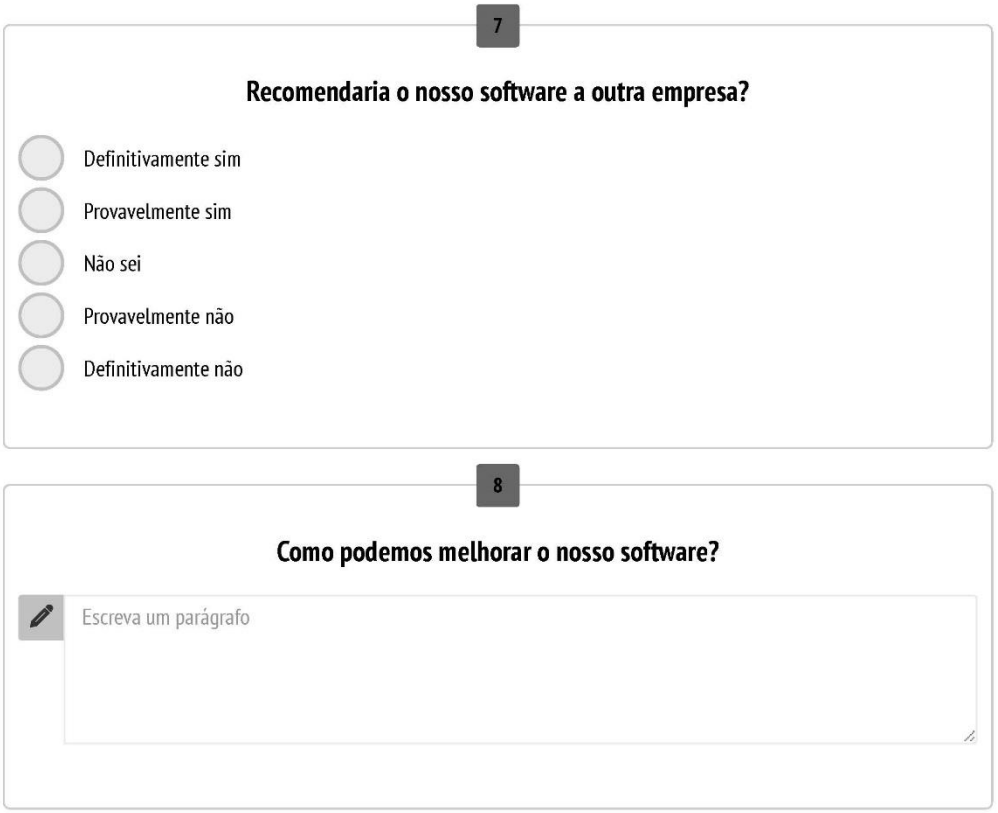
Com que frequência „congela“ ou „falha“ o nosso software?

- Muito frequentemente
- Frequentemente
- Às vezes
- Quase nunca
- Nunca

6

Está satisfeito/a com o funcionamento do nosso software?

- Muito satisfeito/a
- Satisfeit/a
- Médio satisfeito/a
- Insatisfeito/a
- Muito insatisfeito/a


7
Recomendaria o nosso software a outra empresa?
Definitivamente sim
Provavelmente sim
Não sei
Provavelmente não
Definitivamente não
8
Como podemos melhorar o nosso software?
Escreva um parágrafo