Instituto Politécnico de Viseu

Escola Superior de Tecnologia e Gestão de Viseu

Joel Carlos Campos Correia

Certificação de Software de Facturação

Tese de Mestrado
em Sistemas de Informação para as Organizações

Professor Doutor Jorge Alexandre de Albuquerque Loureiro

Dezembro de 2011

Resumo

A portaria de n.º 363/2010 (1), de vinte e três de Junho do ano de dois mil e dez, que regulamentou a certificação prévia dos programas informáticos de facturação, requereu que as Software Houses que comercializam aplicações de facturação, preparassem um conjunto de funcionalidades que permitam que um software garanta o cumprimento da lei e minimize a possibilidade de fugas fiscais. De entre estas funcionalidades, destaca-se a criação de assinaturas de modo a utilizar o método de encriptação RSA com SHA1, e a emissão do ficheiro SAF-T-PT (2) (3).

Este projeto e dissertação está focado em descobrir quais as soluções técnicas/funcionais necessárias para submeter uma aplicação à certificação prévia dos programas informáticos de faturação do Código do Imposto sobre o Rendimento das Pessoas Coletivas. Além disso, esta dissertação pretende averiguar sobre as principais dificuldades sentidas durante no processo de certificação, para esta finalidade, como forma de recolha de dados, foi usado o questionário.

Esta dissertação de mestrado incide sobre o processo de certificação do software de faturação e sua implementação real, no programa de facturação "Facturas e Recibos .NET", através da alteração deste software. O programa encontra-se no mercado desde Maio de 2007, sendo utilizado por empresas de áreas de actividade diversas, nomeadamente: turismo, comércio de produtos e serviços. A certificação do software "Facturas e Recibos .NET" é indispensável para manter e permitir angariar novos clientes, que tenham como necessidade de escolha um programa certificado dentro do mercado nacional de programas certificados.

Em relação às assinaturas digitais, o estado da arte, no que diz respeito a programas ou livrarias de implementação de métodos de encriptação RSA com SHA1, o OpenSSL (1) é, sem dúvida, um programa na vanguarda da criação de chaves privadas e públicas e aplicação de métodos de encriptação ou verificação dessas chaves. Outras livrarias de encriptação se destacam, tais como o Microsoft Framework e Bouncy Castle.

Das alterações realizadas no software, destacam-se como pontos cruciais: a criação de um estado de preparação de documentos; a gestão dos números dos documentos; a robustez essencial no momento de geração da assinatura de um documento; a necessidade de existência de um método de conversão e associação de documentos.

Através questionário conseguiu-se averiguar as principais dificuldades experimentadas, estas ocorreram principalmente na fase dos testes de conformidade, podendo ser minimizadas através da uniformização e exposição clara da composição dos testes de conformidade.

Palavras-chave

Certificação de Software, SAF-PT, RSA, SHA1, Open SSL, encriptação

Abstract

The Decree-Law No. 363/2010 (1) of the 23rd of June of two thousand and ten, that regulates the certification of the invoices software, requires that the Software Houses that produce and sell applications for invoice proposal, prepare a set of features which ensure that the software observes the law. One of the important features is the signature creation using the RSA encryption with SHA1, that is documented in file SAF-T-PT (2), (3) restrictions. Another feature is the association of invoice information.

This project aims on finding the necessary technical solutions required to submit an application to the certification of the billing software, respecting the Tax requirements. In addition, this dissertation intends to find out about the main difficulties experienced during the certification process, for this purpose, as a data collection a questionnaire was used.

This thesis focuses on the certification process of the invoice's software, with a case study implementation on the existing invoice program "Facturas e Recibos .NET". The Invoice program "Facturas e Recibos .NET" is on the market since May 2007, being used by companies in different areas, such as: tourism, goods and services. It is a web based software developed on Microsoft technology .NET and CSharp programming language. There is a need to maintain existing customers and gather new ones that will need to choose a certificate program within the national market possibilities of certified programs.

The state of art in digital signatures and the programs and methods of RSA encryption with SHA1 is OpenSSL, which is a program for the creation of private and public keys. Other software libraries of encryption are Microsoft Framework and Bouncy Castle Framework.

On the changes made to the software, stand out as crucial points: the need of existence of a state of preparation of documents; management of document numbers; the robustness of method on key generation at the time of signing a document; a method to convert and association documents.

The questionnaire allowed to determine the main difficulties experienced, These occurred mainly during the conformance testing phase, this difficulties can be minimized by standardizing and expositing of the composition of the compliance testing phase.

KeyWords

Software certification, SAF-PT, RSA, SHA1, Open SSL, encryption

Agradecimentos

Aproveito para agradecer a uma série de pessoas, cujo contributo contribuiu para a elaboração desta dissertação. Em primazia, um agradecimento ao meu professor orientador de estágio Dr.º Jorge Loureiro pelas orientações e conselhos prestados. Ao Engenheiro Informático Fernando Pereira da empresa CambraGest, cuja troca conjunta de ideias e partilha de informação permitiu fazer do processo de certificação do software "Facturas e Recibos .NET" um processo menos moroso e mais claro. Aos meus colegas de Mestrado nomeadamente ao António Mesquita, Filipe Brás Almeida e José Afonso pelo companheirismo e amizade.

Oliveira do Hospital, 27 de Dezembro de 2011

Joel Carlos Campos Correia

Índice

Índice de Figuras

Índice de Tabelas

Lista de Definições e Acrónimos

.NET	Plataforma para desenvolvimento e execução de sistemas e aplicações da Microsoft
ASP	Active Server Pages
API	Application Programming Interface ou Interface de Programação de Aplicações
C#	C Sharp é uma linguagem de programação orientada a objectos
DGCI	Direcção Geral do contribuinte e Impostos
DSPCIT	Direcção de Serviços de Planeamento e Coordenação da Inspecção Tributária
IIS	Internet Information Services
IVA	Imposto de Valor Acrescentado
MD4	Message-Digest Algorithm
PEM	Privacy Enhanced Mail
PDF	Portable Document Format
RSA	Ron Rivest, Adi Shamir and Len Adleman (inventores do algoritmo)
SAFT-PT	Standard Audit File for Tax Purposes - Versão Portuguesa
SHA	Secure Hash Algorithm
XML	eXtensible Markup Language

1 Introdução

A certificação de software, teve início no mês de setembro de 2010, requerendo para isso uma análise aprofundada das leis e regras técnicas que o regulamentam, bem como uma compreensão dos procedimentos económicos e financeiros dos agentes envolvidos.

1.1 Processo de compra e venda

O processo de compra e venda de bens ou serviços prestados, rege-se pela emissão de documentos comprovativos legais da transacção efectuada. A Figura 1, ilustra um exemplo das fases deste processo.

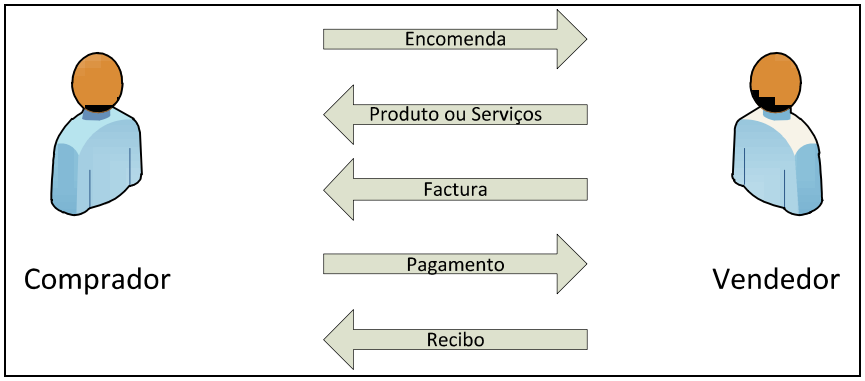


Figura 1 - Transacção de venda

Sendo a Factura o documento emitido mais comum no processo quando o pagamento não é imediato, como refere Proiete, o recibo é o documento que comprova o pagamento da factura (4), estando presente na gestão financeira e contabilística.

1.2 Evasão fiscal

Com do aparecimento dos sistemas de informação, rapidamente a emissão escrita de facturas foi substituída por programas informáticos. Porém, novos problemas de relacionados com situações de evasão fiscal surgiram. Como é referido no Relatório de Actividades Desenvolvidas de Combate à Fraude e Evasão Fiscais 2008, das principais formas de fuga ao fisco destacam-se a economia paralela, emissão de facturas falsas, a não declaração de valores correctos (5), existem também outras situações mais especificas como a substituição ou eliminação de documentos, eliminação de linhas dos documentos, alteração de quantidades, preços e alteração da entidade no cabeçalho do documento.

A necessidade de assegurar o controlo fiscal, para que se evitassem situações de evasão fiscal levou a DGCI[1] a regulamentar a certificação prévia dos programas informáticos de

[1] Direcção Geral do Contribuinte e Impostos

facturação. Tudo isto, através da definição de regras para que os programas de facturação garantam a inviolabilidade da informação registada, permitindo, consequentemente, que apenas os programas que respeitem tais requisitos possam ser comercializados e utilizados.

O programa de Facturação "Facturas e Recibos .NET" encontra-se no mercado dos software's de facturação desde Maio de 2007, sendo utilizado por empresas que facturam mais de 250 000 € por ano, por consequente, é necessário que o programa esteja devidamente certificado, para que as empresas o possam utilizar. Para submeter o software à certificação, terá de haver tudo um estudo dos requerimentos e a respectiva implementação prática tendo como base as soluções idealizadas.

Em termos técnicos a certificação baseia-se principalmente num esquema de assinaturas, para garantir a autenticidade dos dados é requerida uma assinatura impressa no documento, onde o 1.º, 11.º, 21.º e 31.º carácter têm de constar na factura impressa (6). Para assegurar a originalidade da assinatura esta tem como forma de cálculo a assinatura anterior e dados referente à própria factura, deste modo no caso de haver alterações no documento ou eliminação de documentos anteriores, a assinatura nunca será igual. Conferindo o documento impresso que foi entregue ao cliente e comparando-o com a assinatura presente na base de dados do programa, os caracteres da assinatura têm de ser iguais. Usando a chave pública é possível validar a assinatura consoante a os elementos que serviram como base de criação, esses elementos são: a assinatura anterior, a data do documento, a data e hora de finalização do documento e o valor total da factura.

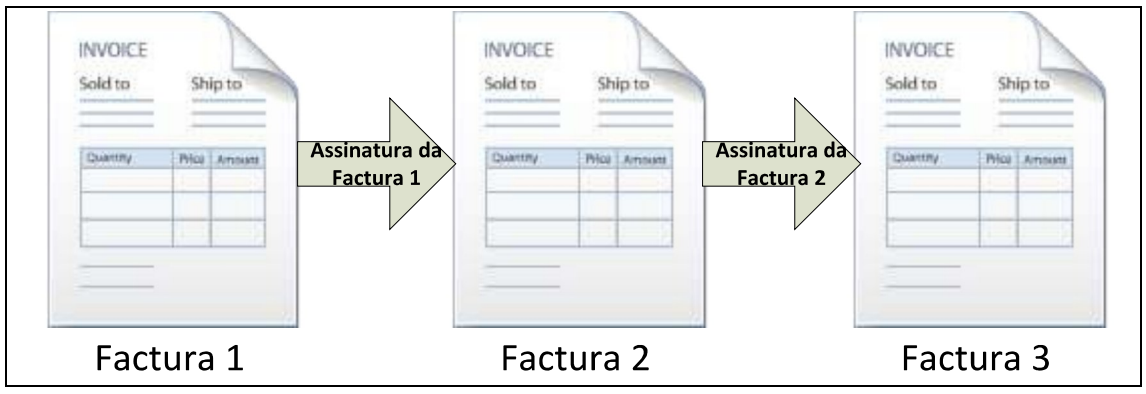


Figura 2 - Passagem da assinatura para o documento seguinte.

Como pode verificar na Figura 2, está ilustrado o esquema de passagem de informação das assinaturas entre documentos do mesmo tipo, caso existisse alteração nos valores dos documentos a validação das chaves feitas posteriormente numa auditoria iria acusar documentos inválidos. No site da DGCI, está disponível uma aplicação que valida o ficheiro SAF-T-PT e as assinaturas nele contidas (7).

1.3 Evolução da legislação

Após o surgimento dos sistemas de informação foram publicadas legislações e portarias que com o objectivo de obrigar à inclusão de um conjunto de funcionalidades garantisse a integridade operacional, a integridade da informação arquivada electronicamente. Na Tabela 1 são listadas as principais portarias ordenadas cronologicamente e seus principais pontos relevantes.

Ano de Publicação	Portaria/legislação	Resumo
1990	Decreto-Lei n.º 198/90 (8)	• Numeração das Facturas • Controlo do acesso ao sistema • Funções de controlo de integridade, exactidão e fiabilidade • Funções de controlo para detecção de alterações directas • Preservação de toda a informação necessária à reconstituição
2003	Decreto-Lei n.º 147/2003 (9)	• Documentos de transporte • Processamento dos documentos de transporte • Circuito e validade dos documentos de transporte
2003	Decreto-Lei n.º 256/2003 (9)	• Elementos a constar nas facturas • Transmissão e conservação por meios electrónicos
2007	Portaria n.º 321-A/2007 (2)	• Emissão do ficheiro SAF-T-PT
2009	Portaria n.º 1192/2009 (3)	• Alteração da estrutura ficheiro SAF-T-PT
2010	Portaria n.º 363/2010 (10)	• Certificação prévia dos programas informáticos de facturação

Tabela 1 - Evolução Histórica da Legislação

Todos estes decretos-lei obrigam os programas de facturação a terem implementado funções de autenticação, vulgo formulário de acesso com login e password, sistema de numeração dos documentos, funções de controlo, como por exemplo integridade referencial na base de dados através do uso de chaves estrangeiras e chaves primárias e possibilidade de emissão do ficheiro SAF-T PT.

2 Certificação

A organização para a Cooperação e Desenvolvimento Económico (OCDE) que tem como objectivo promover políticas que melhorem o desenvolvimento económico e bem-estar social, da qual Portugal faz parte, sugeriu um conjunto de orientações a ser seguidas por empresas que desenvolvem software de gestão comercial e contabilidade (11).

Estas orientações são relativas a requisitos de auditoria fiscal, destes destacam-se princípios de integração de mecanismos de controlo para uma protecção fiscal efectiva, a produção de resumos de auditorias através de um ficheiro electrónico que consequentemente permite o envio e comunicação automática via electrónica e a criação de procedimentos que garantam a integridade e legibilidade da informação. (11)

Seguindo estes princípios o governo português aprovou a legislação em que se destaca a obrigatoriedade de emissão do ficheiro SAF-T-PT, ficheiro este, que pode ser pedido pelos técnicos inspectores fiscais. Para que através deste ficheiro, obtenham uma descrição pormenorizada de toda a facturação da empresa e a certificação de software de Facturação. (12)

2.1 Ficheiro SAF-T PT

De modo a facilitar a inspecção da actividade tributária e tomando como exemplo outros países, a DGCI publicou a portaria número 321-A do ano de 2007 (12), que refere a obrigatoriedade dos sujeitos passivos de IVA que usarem um programa de facturação, terem de disponibilizar um ficheiro em XML com os detalhes e totais da facturação e contabilidade. Deste modo, facilitam o trabalho dos inspectores, que de uma maneira rápida têm acesso a um ficheiro com a informação de determinado ano, após dois anos em vigor.

A alteração da portaria foi publicada na portaria n.º 1192 de 2009 (13) cujos principais pontos estão relacionadas com o facto de serem os próprios programas e *software houses*[2] tem como requisito emitir o ficheiro SAF-T PT, isto devido ás situações que surgiram onde programas próprios eram desenvolvidos só para emitir o respectivo ficheiro. Esta situação acontecia quando o software não estava a ser mais suportado (atualizado) pela empresa que o desenvolveu ou devido ao custo da actualização ser mais caro que a criação de um programa que emitisse o ficheiro SAF-T-PT.

A nova portaria de 2010 também adicionou mais campos comparativamente à versão inicial do SAF-T-PT. Nesta portaria (10), a estrutura do ficheiro SAF-T PT já foi pensado para

[2] Empresas que produzem aplicações informáticas

suportar a informação relativa à assinatura electrónica, requisito principal da certificação, pois já inclui os campos como a assinatura (hash) e a versão da chave privada (hashcontrol).

2.2 Abrangência

A portaria n.º 363 de 2010 regulamenta a certificação prévia dos programas informáticos de facturação. No entanto, exclui as empresas que reúnam, pelo menos, uma das seguintes condições:

a) Utilizem software produzido internamente ou por empresa integrada no mesmo grupo económico, de que sejam detentores dos respectivos direitos de autor;
b) Tenham operações exclusivamente com clientes que exerçam actividades de produção, comércio ou prestação de serviços, incluindo os de natureza profissional;
c) Tenham tido, no período de tributação anterior, um volume de negócios inferior a (euro) 150 000€;
d) Tenham emitido, no período de tributação anterior, um número de facturas, documentos equivalentes ou talões de venda, inferior a 1000 unidades.

2.3 Etapas do processo

O processo de certificação desenrola-se do seguinte modo: o requerente da empresa que produziu o software ou entidade que detém os direitos de autor solicita o inicio do processo, via online, através do portal das finanças em https://www.portaldasfinancas.gov.pt/pt/consultaM24.action, usando o formulário online modelo 24 (ver Figura 3).

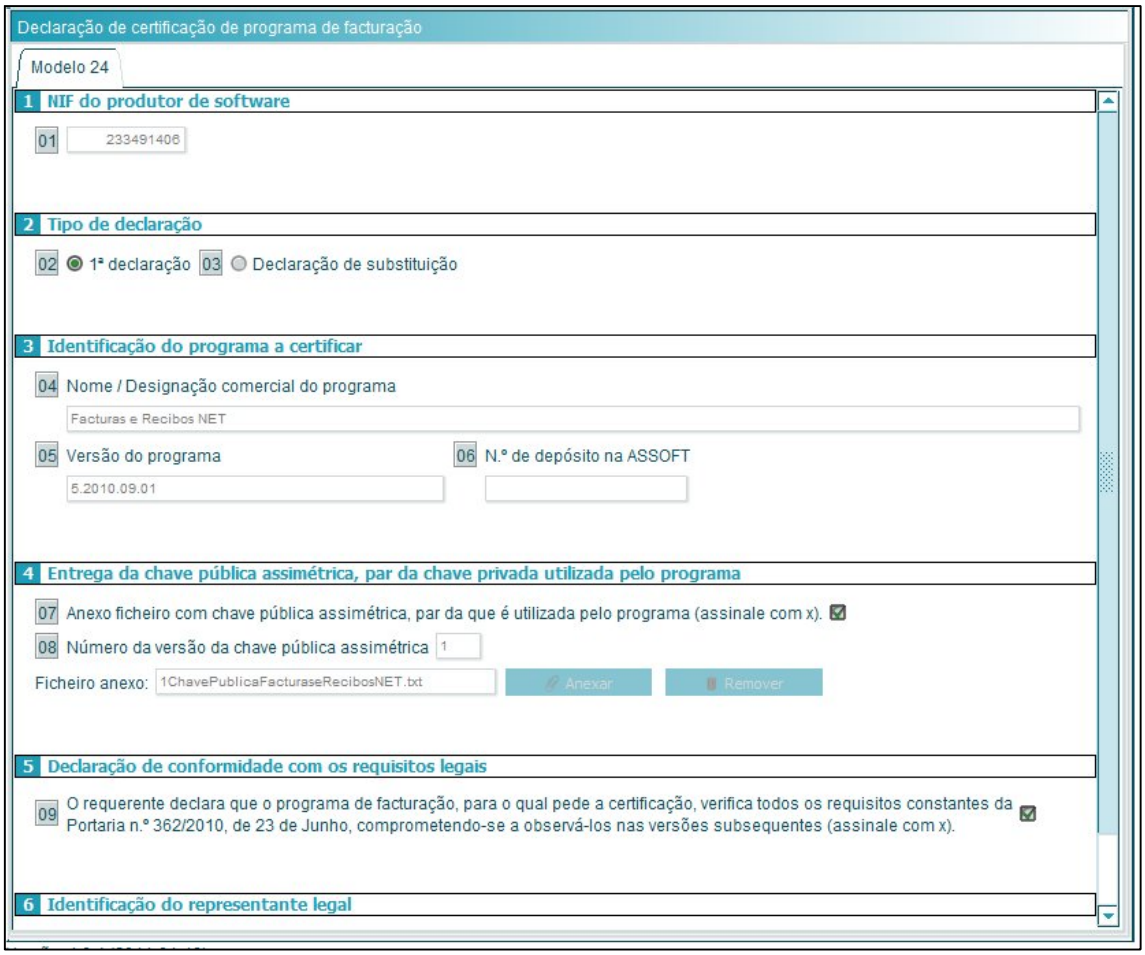


Figura 3 - Requerimento de certificação de Software (Modelo 24).

Após a recepção do requerimento a DGCI envia uma carta para a morada da entidade requerente, a solicitar o envio de um exemplo do ficheiro SAF-T PT produzido pela aplicação informática, documentos em formato ficheiro pdf com todas as diferentes tipologias de documentos existentes e a chave pública submetida com o requerimento. Na Figura 4, é resumido todo este processo.

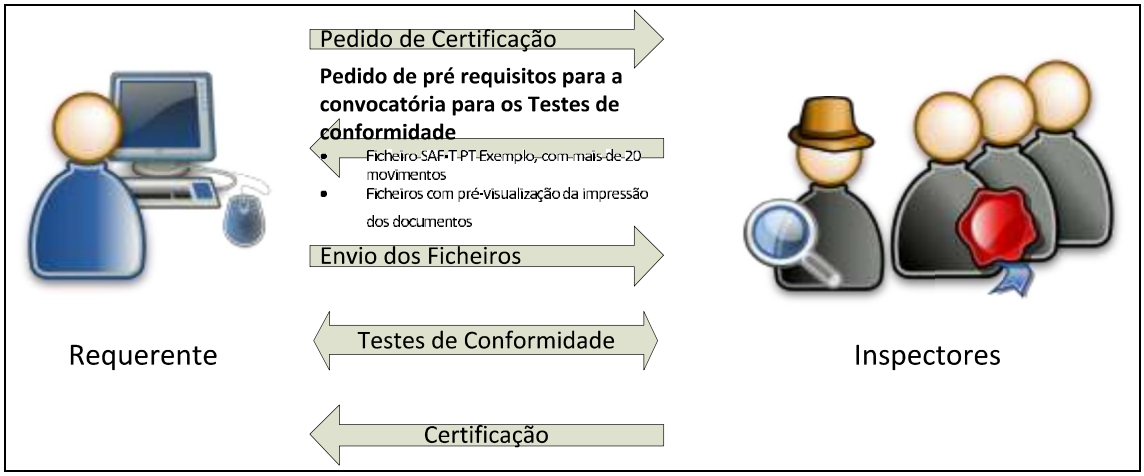


Figura 4 – Fases do processo de certificação.

No ficheiro SAF-T-PT terão de constar mais de vinte documentos emitidos com os campos Hash e HashControl (3) devidamente preenchidos, devendo estar registados em pelo menos dois períodos/meses diferentes, deverão abranger as diferentes topologias de documentos e conter documentos com o estado de anulado. Se o programa também gerar documentos do tipo de "Guias de Remessa"[3] ou "Orçamentos", este deverá igualmente conter documentos com o campo OrderReferences devidamente preenchido. O ficheiro deverá ser previamente validado usando o software disponível no site da DGCI (7).

Após a recepção dos ficheiros por parte da DGCI, estes são verificados seguindo uma bateria de testes que listo:

- Validação da estrutura do ficheiro SAF-T-PT;
- Verificação dos valores totalizadores e controlo linha a linha;
- Verificação das menções e informação que conta dos documentos.

Caso os requerimentos analisados até ao momento estejam conforme o requerido, será agendada a reunião presencial para os testes de conformidade.

[3] Documento que acompanha a documentação da carga a ser enviado para o destinatário

3 Tecnologias

Na área da segurança da informação, mais concretamente na certificação, é necessário recorrer a diversas tecnologias por forma a garantir autenticidade da informação e dos processos automatizados por sistemas de informação.

3.1 Criptografia

Enviar e receber informações confidenciais é uma necessidade que existe há centenas de anos. O aparecimento da internet e a sua consequente facilidade de transmitir dados de maneira precisa e rápida, tornou a criptografia uma ferramenta fundamental para permitir que apenas o emissor e o recetor tenham acesso à informação enviada.

Alecrim menciona que o termo criptografia advém da união das palavras gregas "kryptós" e "gráphein", que significam respetivamente, "oculto" e "escrever". A criptologia estuda os princípios e técnicas que codificam a informação, transformando-a da sua forma original para outra incompreensível, para que apenas o seu emissor e recetor possam decifra-la e interpretá-la (14).

A maior parte dos dados é digital, logo representada por bits, a criptografia utiliza algoritmos que utilizam uma determinada chave ou pares de chaves, para codificar e descodificar a informação.

É referido na Wikipédia que o método de criptografia que utiliza um par de chaves é denominado de criptografia de chave pública, em que existe uma chave pública e uma chave privada. A chave pública é do conhecimento de todos, a chave privada é apenas do conhecimento do seu dono (15).

Nos algoritmos de criptologia de chave pública uma mensagem encriptada com a chave pública pode apenas ser desencriptada com a chave privada correspondente. Este tipo de algoritmos garante a autenticidade e a confidencialidade da mensagem.

Mas estudo da criptologia não é apenas a cifragem e decifragem de dados, é um ramo da teoria da informação mas com a contribuição de outros campos da matemática e do conhecimento (15).

A criptoanálise é o estudo das formas de tentar descobrir o texto cifrado, quando não se é o destinatário, ou de tentar esconder o significado de uma mensagem, isto utilizando técnicas de criptografia.

A Criptologia é o campo que engloba a Criptografia e a Criptoanálise e basicamente é formada pelo estudo de algoritmos criptográficos que podem ser implementados em computadores.

3.1.1 RSA

A wikipedia refere que os matemáticos Diffie e Hellman desenvolveram um método de criptografia que revolucionou os sistemas de criptografia existentes até então. Este sistema de criptografia foi aperfeiçoado por pesquisadores do Instituto MIT, Ronald Rivest, Adi Shamir e Leonard Adleman, dando origem ao algoritmo RSA, denominação resultante das iniciais os seus autores.

RSA é o algoritmo de criptografia de dados considerado dos mais seguros sistemas de chaves públicas, baseia-se em teorias clássicas de números e foi o primeiro algoritmo a permitir criptografar a assinatura digital.

Barbosa et. al, referem que o algoritmo RSA é o resultado de cálculos matemáticos, um para encriptar e outro para desencriptar as mensagens, utilizando uma chave pública e uma chave privada. A chave pública é utilizada para encriptar e é conhecida por todos, a chave privada para desencriptar a mensagem e deve ser mantida em segredo. Para entender o RSA os conhecimentos necessários são básicos. É preciso entender o que é um número primo, um número diferente de um e só divisível por um ou por ele mesmo. E o conceito de aritmética modular, em que o modo de encontrar um resultado modular é dividindo o resultado não modular pelo módulo e considerar o resto. (16)

3.1.2 SHA1

SHA-1 ou Secure Hash Algorithm - Algoritmo Hash Seguro, é uma função criptográfica usada para calcular a versão condensada de uma mensagem produzindo um valor hash de 160-bits. É utilizado em diversas aplicações e protocolos de segurança e serve para garantir a integridade da mensagem. Este algoritmo foi criado pela NSA (National Security Agency). (17)

O SHA-1 foi criado baseando-se em princípios idênticos aos utilizados no algoritmo MD4, anteriormente criado pelo professor do MIT, Ronald L. Rivest.

De acordo com o que é citado na Wikipédia o hash é utilizado para assegurar a integridade da mensagem, onde o emissor submete a mensagem a um algoritmo hash que produzirá um valor hash. Este valor é enviado para o recetor junto com a mensagem. O recetor vai averiguar a integridade da mensagem verificando se o valor hash obtido é igual ao valor hash gerado na origem, caso sejam diferentes é porque a mensagem foi alterada.

De modo a garantir a irreversibilidade e a singularidade do valor hash gerado, o algoritmo hash é composto por fórmulas matemáticas complexas. Se um único bit da mensagem for alterado o valor hash gerado será completamente diferente.

Este valor hash poder ser a entrada para o Algoritmo da Assinatura Digital, que comprova a assinatura da mensagem. Normalmente é mais eficaz criar uma assinatura para o valor hash, já

que este é muito menor que a mensagem original. O recetor e o emissor utilizam o mesmo algoritmo hash para gerar e verificar a assinatura digital.

Qualquer alteração feita numa mensagem irá alterar o seu valor hash, logo a sua assinatura não poderá ser confirmada. O algoritmo SHA1 pode ser utilizado juntamente com o algoritmo de assinatura digital, para transferências bancárias, distribuição de software, envio de emails.

3.1.3 Chaves públicas e chaves privadas

A par das portarias, a DSPCIT[4] disponibilizou uma série de exemplos de geração de chaves públicas e privadas (6) usando o para isso o programa de geração de assinaturas OpenSSL. Este programa disponibiliza um conjunto de funções básicas de criptografia e pode ser utilizado em ambiente Linux ou Windows. As chaves são ficheiros no formato PEM (18) (19). A Figura 5 ilustra o processo de geração e posterior validação da assinatura, em que utilizando uma livraria externa ou desenvolvendo um software, se poderá recorrer a um método que combine a chave privada com a informação para gerar uma assinatura – data de emissão da factura, valor total, série e número da factura – pode ser posteriormente confirmada através da chave pública.

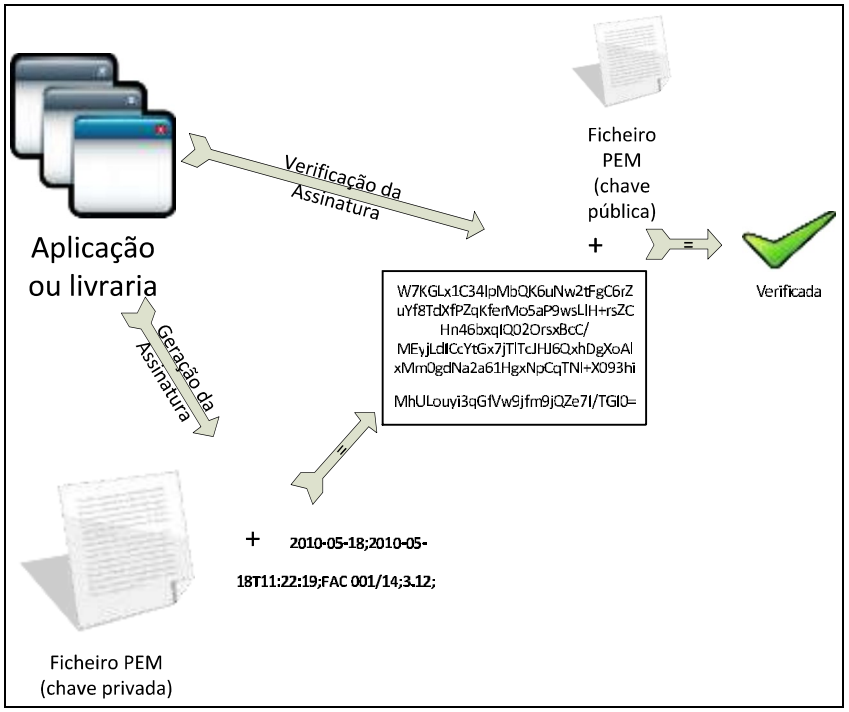


Figura 5 - Processo de Geração da Assinatura.

As tecnologias escolhidas para a implementação das funcionalidades requeridas, dependem do tipo de tecnologia já usada pelo programa de facturação.

[4] Direcção de Serviços de Planeamento e Coordenação da Inspecção Tributária

3.1.4 Ficheiro PEM

O ficheiro PEM é o ficheiro que contém os bytes das chaves públicas e privadas. Este tipo de ficheiro é utilizado como formato predefinido de exportação para o OpenSSL, mas não tem suporte nativo da Microsoft, para que o método de encriptação importe as chaves no processo de geração da assinatura. Para colmatar esta falta é necessário construir um mecanismo de importação.

3.2 ASP.NET

O ASP.NET é o sucessor da tecnologia ASP (Active Server Pages), é uma plataforma pertencente à Microsoft para o desenvolvimento de aplicações web. Baseia-se no Microsoft Framework .NET, uma aplicação desenvolvida em ASP.NET têm de ser compilada antes de ser executada, o servidor IIS é o responsável pela disponibilização destas aplicações.

3.3 Livrarias Criptográficas

Para o método de geração da assinatura acima descrita, é necessário a escolha de uma livraria criptográfica. Sendo que esta dissertação de mestrado incide sobre o processo de certificação do software de facturação e a sua implementação real, no programa de facturação "Facturas e Recibos .NET" e estando este desenvolvido em tecnologia ASP.NET da Microsoft, uma das alternativas é o uso do Microsoft Framework versão 2.0 nomeadamente a Livraria System.Security.Cryptography (20), como é ilustrado na Figura 6 esta livraria suporta métodos de encriptação SHA1, MD5, TripleDES e Rijndael. Destas opções, a escolhida por obrigação imposta pela DGCI é a SHA1.

Figura 6 - Biblioteca Security no Microsoft Framework 2.0.

Outra opção será a utilização de bibliotecas externas, tais como a versão em C# do Bouncy Castle API (21), disponível para download em http://www.bouncycastle.org/csharp/.

Livraria	Compatibilidade
Microsoft Framework 2.0	• Não importa públicas e privadas de PEM
Bouncy Castle API	• Importa chaves públicas e privadas de ficheiros PEM

Tabela 2 - Resumo comparativo das livrarias criptográficas.

Na escolha do método de encriptação é necessário ponderar a compatibilidade na importação das chaves privadas/públicas em formato PEM (Privacy-Enhanced Mail) (18). A DGCI aconselha a utilização do Open SSL para a geração das chaves de encriptação no formato PEM (18). Como é resumido na Tabela 2, a livraria Bouncy Castle consegue importar directamente ficheiro PEM, sem ser necessária a programação de uma interface de conversão de chaves PEM num outro formato. No caso de se usar a livraria nativa da Microsoft, torna-se necessário a implementação de um método de conversão do ficheiro PEM num formato compatível com o Microsoft Framework 2.0.

4 Arquitetura

A arquitetura de dados do software teve de suportar incrementos por forma a suportar as novas funcionalidades a serem desenvolvidas.

4.1 Arquitetura de dados

Para a implementação das alterações necessárias à certificação do software torna-se necessário alterar a estrutura da base de dados, para que esta comporte a informação associada à assinatura. Um dos requisitos presentes na Especificação das regras técnicas estipula que "O produtor de software deverá assegurar que a chave privada utilizada para a criação da assinatura que é do seu exclusivo conhecimento, deverá estar devidamente protegida no software" (6), para tal procedeu-se à encriptação das chaves, que são guardadas na base de dados do programa na tabela chaves. Esta tabela tem como campos a chave_privada e chave_publica, sendo o campo id_chave a chave primária, um número sequencial único e representativo da versão das chaves.

No anexo 3, está representado o diagrama de classes correspondente à tabela de chaves e movimentos, duas das tabelas afetas a este projeto. Como novos campos na tabela movimentos temos os seguintes: data_alteracao, hash, hash_control, texto_a_assinar, finalizada, anulada, motivo_anulacao , id_chave_versao. A data de alteração refere-se ao momento exato em que o movimento foi por ultimo alterado, o hash contem a chave codificada, que é baseada numa composição de valores (data da alteração da factura,data de emissão da factura, valor total, série e número da factura e assinatura anterior), esta composição é também guardada no campo texto_a_assinar, embora este seja um campo redundante. O hash_control representa a versão das chaves usadas, é também um campo redundante e duplicado pois a chave estrangeira id_chave_versao também guarda o mesmo valor. O campo booleano finalizado distingue o estado do movimento/documento, o campo booleano anulado define se o documento está assinalado como anulado tendo como campo complementar o campo motivo_anulacao.

4.2 Arquitetura do software

A arquitetura do software proposta para a assinatura digital passa pela criação de dois métodos, embutidos num módulo. Estes métodos são iguais na finalidade mas distintos em termos de modo de algoritmo usado.

No primeiro método é usado a biblioteca freeware Bouncy castle, no segundo método é usada a biblioteca interna da Microsoft complementada com a livraria de OpensslKey que fornecerá a forma de importação das chaves públicas e privadas.

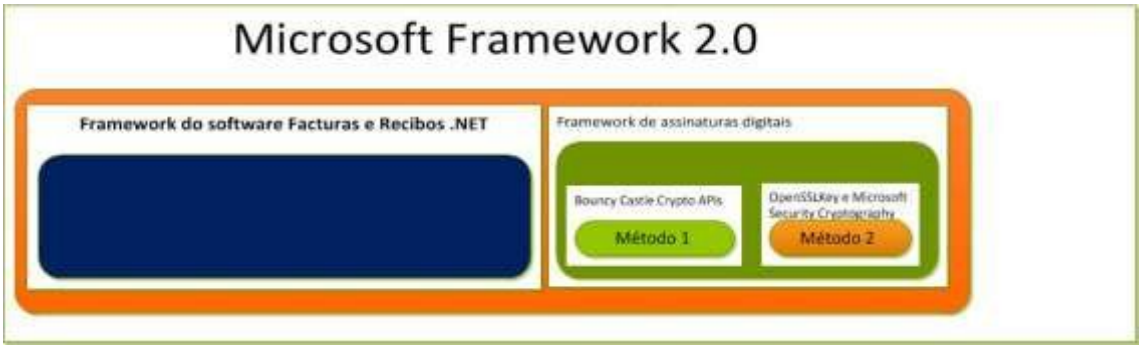


Figura 7 - Módulos e livrarias

Como podemos observar na Figura 7, será desenvolvido um módulo, vulgo DLL[5], assente no Microsoft Framework 2.0 que permitirá ao modulo principal do programa "Facturas e Recibos .NET" invocar as funções de encriptação. Optando por uma arquitectura modular, temos a vantagem de minimizar o impacto da alteração do software, facilitando a integração dos métodos e a todo o momento os métodos podem ser actualizados, corrigidos ou até substituídos.

4.3 Arquitetura de processos

Para uma reestruturação bem-sucedida do software é fundamental planear a estratégia, a implementar nos processos principais e no fluxo de trabalho do adjacente ao negócio, para que o sistema de informação se destina.

4.3.1 Assinatura dos documentos

É necessário idealizar uma arquitetura de processos coerente e fidedigna pois a assinatura dos documentos é um momento crucial onde se terá de garantir a veracidade da assinatura. Se algo falhar pode comprometer todos as facturas emitidas adiante, para isso é necessário implementar um processo de assinatura e verificação das chaves, com possibilidade de rollback e controlo de concorrência na base de dados.

As facturas têm um número identificativo único, tem de ser obrigatoriamente sequencial e ordenado temporalmente. Sendo este um programa multi-utilizador, poderão existir dois ou mais utilizadores em simultâneo a manipular facturas diferentes. Poderá haver situações que exijam a troca de números, para tal implementou-se um processo de troca de números, estando ilustrado na Figura 8.

[5] Dynamic-link library

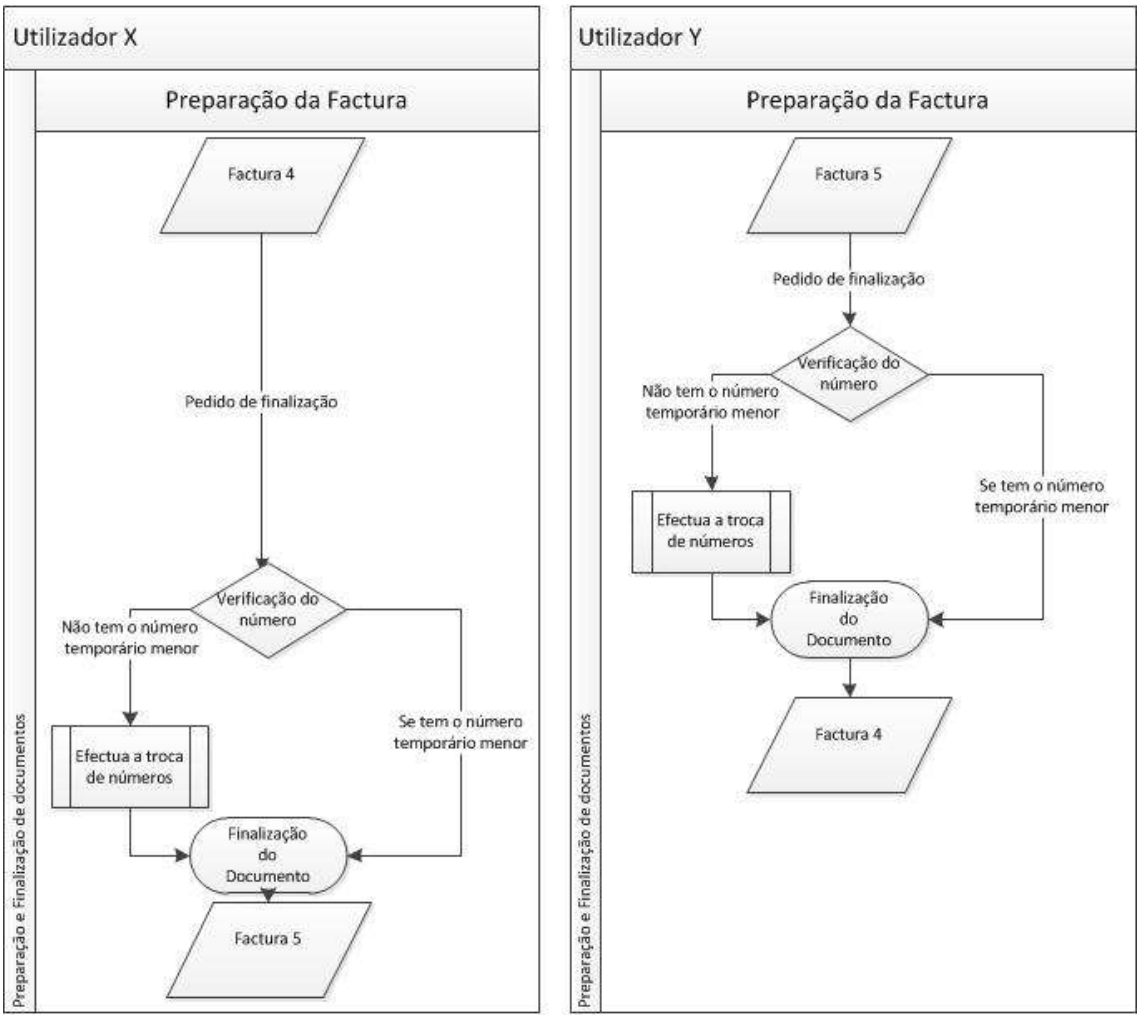


Figura 8 - Diagrama de Fluxo do processo de troca de números temporários.

Como exemplificado na figura anterior, pode acontecer o caso do utilizador X estar a preparar a Factura 4, ao mesmo tempo que o utilizador Y está a preparar a Factura 5, porem o utilizador Y finaliza primeiro a Factura 5. Como a ultima Factura finalizada é a número 3, a seguinte terá de ser a 4, consequentemente terá de existir uma troca de número entre a factura 4 e 5. Num programa com multiutilizadores e com a implementação de um estado de preparação de documentos, oferece-se ao utilizador a possibilidade de iniciar a criação de um documento sem a restrição de o ter de finalizar no próprio momento, este facto levanta a necessidade de implementar métodos de gestão de documentos pendentes, sendo a gestão dos seus números um dos aspetos essenciais.

Para protecção da unicidade numérica de cada documento, além da interface do programa em termos de base de dados, assegurou-se que o campo Número da Factura é único. Em termos práticos a sintaxe SQL usada foi a seguinte: *"CONSTRAINT u_numero_id_serie_id_tipo_movimento UNIQUE(numero, id_serie,id_tipo_movimento)".*

Para a troca poder acontecer, existe o valor zero disponível como valor temporário de troca, ou seja, usando o exemplo descrito na situação acima na tabela x, podemos constatar as várias mudanças de número de um documento consoante decorre este processo de troca de números.

Valor Temporal Virtual (milissegundos)	Número da Factura do Utilizador X	Número da Factura do Utilizador Y	Descrição
1	4	5	Início da troca de número
2	0	5	Utilização de número temporário
3	0	4	Troca do número de uma das facturas
4	5	4	Troca do número da outra factura

Figura 9 - Processo de troca de números de documentos temporários.

Após a troca ser efectuada com sucesso na base de dados, é instanciado o processo de criação da assinatura, verificação da validade da mesma (através da chave pública), e em caso de sucesso do passo anterior, mudança do estado do documento para finalizado. Todos estes passos são assegurados através da utilização de transacções em Microsoft SQL SERVER.

4.3.2 Fluxo de documentos

O processo de criação dos vários tipos de documentos terá de seguir a linha de negócio correspondente á facturação. A portaria de n.º 363/2010, de vinte e três de junho do ano de dois mil e dez, que regulamenta a certificação prévia dos programas informáticos de facturação, vem a requerer que as Software Houses que comercializam aplicações de facturação preparem um conjuntos de funcionalidades para que o software garanta a inviolabilidade das facturas depois de emitidas, de modo a evitar fraudes. Este novo contexto, requer mudanças na ideologia dos software's, sendo que estes passam a estar orientados para o cumprimento de normas, deixando para segundo plano a usabilidade, por consequente, obrigam à mudança de interfaces e fluxos de utilização.

Figura 10 - Conversão e associação de documentos.

O programa e sua interface têm de estar preparada para lidar com este fluxo de documentos e assegurar a associação dos mesmos. Em termos funcionais, a solução passa por desenvolver formulários de conversão de documentos e mecanismo de registo interno na base de dados da associação entre documentos ou linhas das facturas. Por exemplo em relação às notas de crédito estas têm de estar associadas a uma Factura, Venda-a-Dinheiro ou Nota de Débito como está esquematizado na Figura 10.

5 Desenvolvimento

A par das restrições técnicas e funcionais, o software tem de ter em conta todas as legislações inerentes ao processo de compra e venda, através das quais terão de ser criados fluxogramas de processos devidamente protegidos de forma a garantir os constrangimentos legais.

5.1 Metodologia

O modelo de desenvolvimento usado foi o modelo espiral, neste modelo as etapas são cíclicas e evolutivas, distinguem-se quatro estágios expõe Boehm no livro "A Spiral Model of Software Development and Enhancement". No estágio 1 procede-se à identificação de objetivos da fase, soluções e restrições. No estágio 2 são construídos protótipos e efetuadas simulações das funcionalidades desenvolvidas, o seguinte estágio consiste no desenvolvimento e evolução do protótipo, desenho, codificação e testes. No estágio final quatro procede-se à revisão das etapas anteriores e ao planeamento da próxima fase, dando inicio ao um novo ciclo. (22)

A escolha deste modelo recaiu devido ao facto que as funcionalidades a desenvolver carecem de pesquisa e amadurecimento, pois trata-se de um tema recente, necessitando de novas formas de abordagem para o desenvolvimento de funcionalidades.

5.2 Módulo de software

Tendo como base uma livraria de nome “OpenSSLKey” (23) foi desenvolvida uma solução em linguagem c# usando o Visual Studio 2008. Na Figura 11 está representada uma imagem do módulo desenvolvido. Desta solução faz parte a livraria externa OpenSSLKey composto por um ficheiro em linguagem de programação CSharp: OpenSslRsaKey.cs e também dois ficheiros em linguagem CSharp, que contêm as funções desenvolvidas de encriptação e verificação da assinatura gerada.

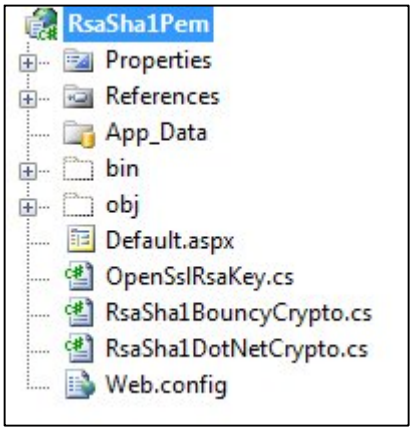


Figura 11 - Biblioteca de encriptação em C#.

Através da criação de um módulo estruturado em namespace[6] de nome "`RsaSha1Pem`", no qual estão incluídas duas classes: "RsaSha1BouncyCrypto" e "RsaSha1DotNetCrypto", as mesmas contêm dois métodos estáticos: "`Sign`" e "`Verify`" como o próprio nome indica, o primeiro método devolve uma assinatura, tendo como base a informação passada como parâmetro, bem como a chave privada.

No método "`Verify`", os parâmetros de entrada são a data a verificar, a respectiva assinatura e a chave pública. Na Figura 12, está representada a função de assinatura que foi desenvolvida usando a Biblioteca Bouncy Castle (21).

```
public class RsaSha1BouncyCrypto
{
    /// <summary>
    /// Sign the data with private key
    /// </summary>
    /// <param name="data">data string</param>
    /// <param name="privateKey">entire private key text from private key PE file.</param>
    /// <returns>Base64 signature text</returns>
    public static string Sign(string data, string privateKey)
    {
        //sign
        System.IO.TextReader TextReaderPrivateKeyBouncyCastle1 = new System.IO.StringReader(privateKey);
        Org.BouncyCastle.OpenSsl.PemReader PEMReaderBouncyCastle1 = new Org.BouncyCastle.OpenSsl.PemReader(TextReaderPrivateKeyBouncyCastle1);
        Org.BouncyCastle.Crypto.AsymmetricCipherKeyPair keyPair = PEMReaderBouncyCastle1.ReadObject() as Org.BouncyCastle.Crypto.AsymmetricCipherKeyPair;

        byte[] testData = Encoding.UTF8.GetBytes(data);
        //Need to use SHA1WithRSA, to be consistent with Openssl sign command.
        Org.BouncyCastle.Crypto.ISigner sigBouncyCastle1 = Org.BouncyCastle.Security.SignerUtilities.GetSigner("SHA1WithRSA");
        sigBouncyCastle1.Init(true, keyPair.Private);
        sigBouncyCastle1.BlockUpdate(testData, 0, testData.Length);
        byte[] signature = sigBouncyCastle1.GenerateSignature();
        return Convert.ToBase64String(signature);
    }
```

Figura 12 - Função Sign usando a Biblioteca Bouncy Castle.

5.3 Requisitos Funcionais

Os requisitos funcionais são verificados na fase dos testes de conformidade. Caso alguma funcionalidade não garanta os requisitos técnicos e funcionais do pedido de certificação, a aprovação da certificação ficará pendente durante trinta dias, até que se realizem novos testes de conformidade. Enumeram-se abaixo alguns dos pontos-chave que a aplicação terá de garantir:

- *Garantir a associação entre documentos de venda e os que lhe servem de suporte;*
- *Produzir/exportar correctamente o ficheiro SAF-T;*
- *Não permitir a associação do mesmo documento de suporte (orçamento/encomenda) de uma transacção a várias Facturas/documentos equivalentes e de clientes diferentes;*
- *Não permitir a repetição da associação do mesmo documento de suporte (orçamento/encomenda) de uma transacção a várias facturas/documentos equivalentes e de clientes diferentes;*
- *Existir controlo e monitorização dos documentos de suporte associados a uma transacção.*

[6] Espaço de nomes é um agregador abstrato que fornece contexto para os itens que armazena

Foram implementadas as seguintes funcionalidades de forma a responder aos requisitos enunciados:

- Disponibilização de um método de conversão/transformação automática de documentos;
    - A criação de uma Nota de Crédito, passa obrigatoriamente pelo processo de transformação/conversão da respectiva Factura associada;
    - Ao converter uma guia de remessa numa Factura, as quantidades e linhas são todas incluídas no documento de venda a gerar, não sendo permitida a edição das suas quantidades;
    - Impossibilidade de converter duas vezes a mesma guia de remessa;
    - Garantia de associação a documentos de suporte do mesmo cliente;
- Alertas com listagem das guias de remessa por facturar, por forma a alertar o utilizador do programa para a necessidade de cumprir a lei e emitir a factura referente à guia de remessa.

Adicionalmente no programa de facturação reduziu-se a existência de tipos de documentos a sete, isto porque estes documentos abrangem todo o tipo de situações:

1. FT Factura
2. VD Venda a dinheiro
3. ND Nota Débito
4. NC Nota Crédito
5. GR Guia de Remessa
6. ORC Orçamento
7. ENC Encomenda

Esta opção foi tomada devido a não ser necessário estar a duplicar todos os tipos de documentos que tem a mesma finalidade, que apenas diferem na nomenclatura, como por exemplo a Guia de Remessa tem a mesma função de uma Guia de Transporte.

Nos testes de conformidade, os técnicos da DGCI aconselharam a não utilização da anulação de movimentos de venda/documentos, apesar de não ser uma imposição da Portaria. A justificação tem a ver com o facto de para reduzir ou anular contabilisticamente uma Factura, Venda a Dinheiro ou Nota de Débito terá de ser emitida uma Nota de Crédito (4).

Por forma a ter obrigatoriamente a Nota de Crédito associada a um outro documento (Factura, Venda a Dinheiro ou Nota de Débito), a criação da Nota de crédito é feita obrigatoriamente por um processo de conversão de documentos.

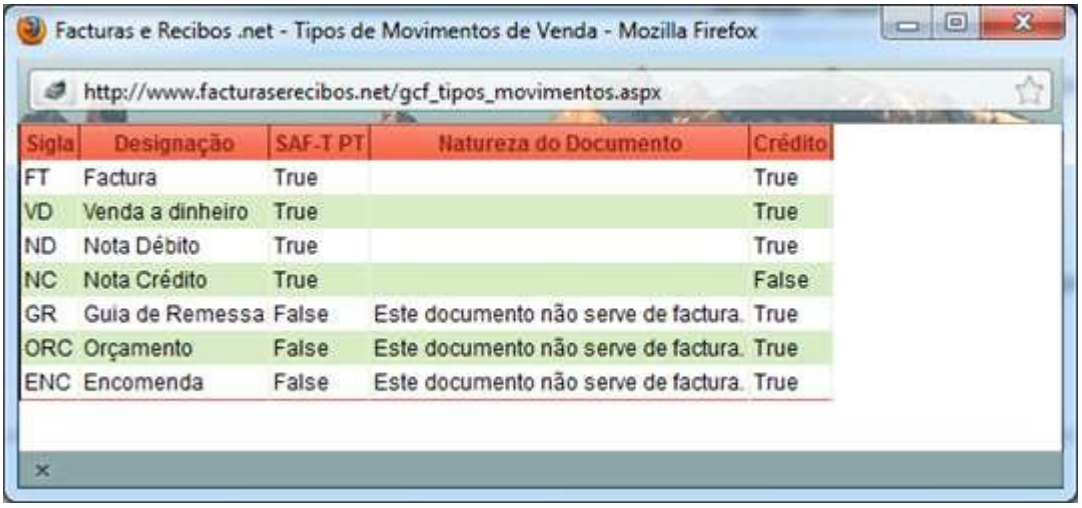
5.4 Especificação das Regras Técnicas para a certificação de Software

De seguida vão ser abordados os tópicos do documento de “Especificação das Regras Técnicas para a certificação de Software (6)”, disponibilizado pela DSPCIT. E também vai ser

explicada as formas encontradas de responder a cada um dos requisitos e o seu impacto na actualização do software.

5.4.1 Documentos emitidos pelos programas de facturação

Na Figura 13 listam-se os tipos de documentos emitidos pelo programa Facturas e Recibos .NET.



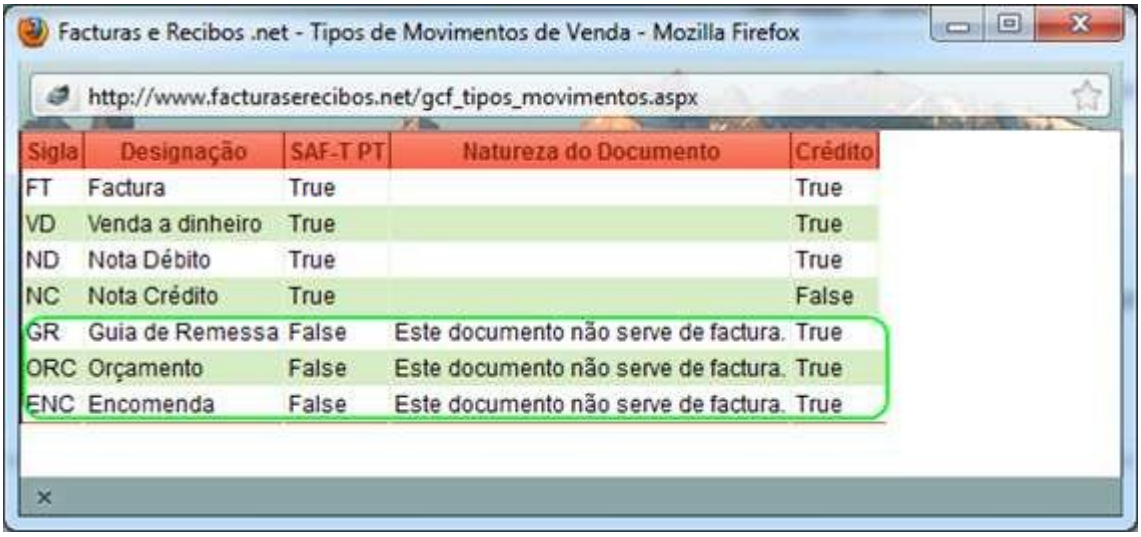
Sigla	Designação	SAF-T PT	Natureza do Documento	Crédito
FT	Factura	True		True
VD	Venda a dinheiro	True		True
ND	Nota Débito	True		True
NC	Nota Crédito	True		False
GR	Guia de Remessa	False	Este documento não serve de factura.	True
ORC	Orçamento	False	Este documento não serve de factura.	True
ENC	Encomenda	False	Este documento não serve de factura.	True

Figura 13 - Lista de tipos de documentos existentes.

Os documentos assinalados com valor True na coluna SAF-T PT são incluídos na exportação do ficheiro SAF-T PT.

Relativamente ao ponto 2.1 e 2.2 do documento *Especificação das Regras Técnicas para Certificação de Software* (6) que passo a citar: *"2.1 Os programas de facturação não podem emitir, para além da factura ou documento equivalente, qualquer outro documento com indicação de bens ou serviços prestados e correspondentes importâncias, susceptível de ser apresentado ao adquirente, como suporte da operação efectuada. 2.2. Todavia, quando por razões do tipo de actividade ou da natureza da operação, forem emitidos documentos de conferência de entrega de mercadoria ou da prestação de serviços, susceptíveis de entrega aos clientes, ficam obrigados às mesmas regras da emissão de facturas, nomeadamente, as previstas no artigo 6.º da Portaria n.º 363/2010, de 23 de Junho."*

Na Figura 14 estão realçados os tipos de documentos que se encontram na situação do ponto 2.2.



Sigla	Designação	SAF-T PT	Natureza do Documento	Crédito
FT	Factura	True		True
VD	Venda a dinheiro	True		True
ND	Nota Débito	True		True
NC	Nota Crédito	True		False
GR	Guia de Remessa	False	Este documento não serve de factura.	True
ORC	Orçamento	False	Este documento não serve de factura.	True
ENC	Encomenda	False	Este documento não serve de factura.	True

Figura 14 - Listagem dos documentos assinalados a verde que não servem de factura.

Na versão demonstração disponível em: http://www.facturaserecibos.net/, poderemos observar que todos os documentos abrangidos pela situação em causa apresentam impressa a expressão no cabeçalho, como demonstra a Figura 15.

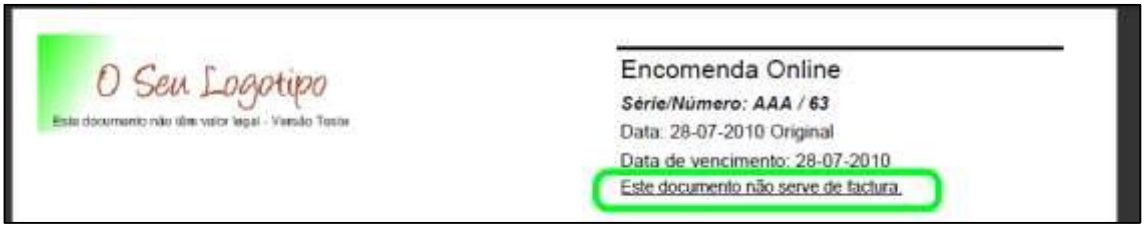


Figura 15 - Exemplo de uso da expressão da natureza do documento.

Relativamente ao ponto 2.4 do documento *Especificação das Regras Técnicas para Certificação de Software* que refere *"2.4. As subsequentes facturas devem conter a identificação dos referidos documentos e ainda constar do SAF-T PT no campo da linha do documento de venda com o índice 4.1.4.14.2 - Referência à encomenda (OrderReferences).* Ao criar um documento de venda, no caso de ser baseado num documento de suporte, por exemplo um orçamento, é necessário utilizar a conversão de documentos para referenciar que as linhas do documento. Na Figura 16 será apresentado o formulário de conversão de um orçamento em Factura, deste modo o programa associa internamente a Factura ao Orçamento.

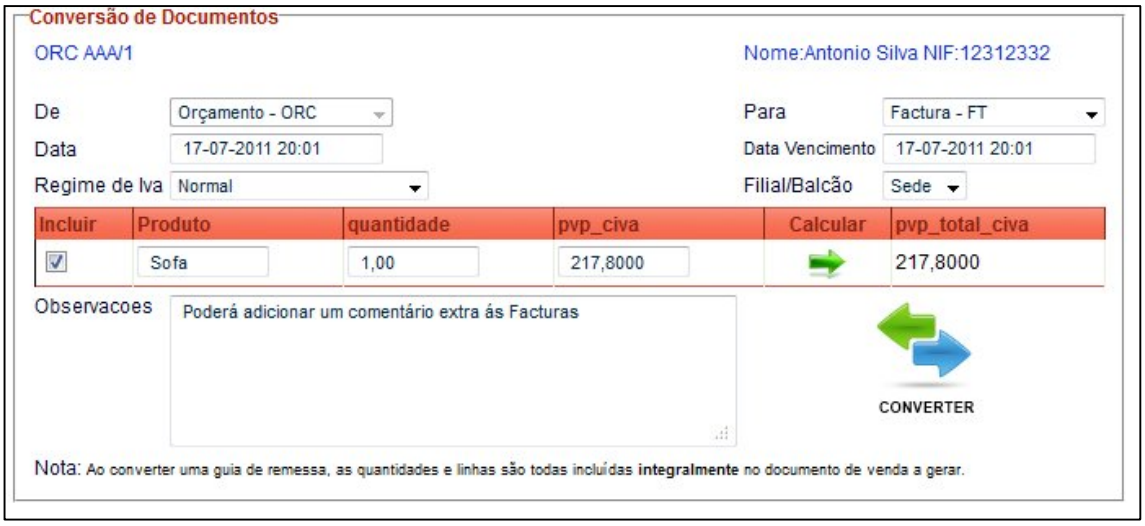


Figura 16 - Exemplo da conversão de um orçamento em factura.

No processo de conversão de documentos é uma maneira rápida, que implementa restrições em termos de escolha do novo documento a criar e o seu tipo, este formulário baseia-se na no esquema de associação de documentos ilustrado na Figura 10.

Relativamente ao ponto 2.5 do documento *Especificação das Regras Técnicas para Certificação de Software* que refere *"2.5. No caso da utilização do programa em modo de formação, os documentos emitidos deverão indicar no cabeçalho os dados identificativos da empresa de software, ao invés dos da empresa cliente e terão ainda de ter impressa a expressão: "Documento emitido para fins de Formação".)....*

Na versão demonstração disponível em: http://www.facturaserecibos.net/, bem como o na Figura 17 poderemos observar que todos os *pdf* gerados apresentam impressa a expressão em causa a vermelho no rodapé dos ficheiros pdf, tendo no cabeçalho os dados identificativos da empresa produtora do software.

Figura 17 - Impressão de um documento em modo formação.

5.4.2 Processo de gravação de uma factura ou talão de venda

Relativamente ao ponto 3.1.1 do documento *Especificação das Regras Técnicas para Certificação de Software* que refere *"3.1.1. No processo de gravação da factura ou talão de venda deverá ser gerada uma assinatura através do algoritmo RSA com base na informação descrita no nº 1 do artigo 6.º da Portaria n.º 363/2010, de 23 de Junho e na chave privada do produtor do programa de facturação. No processo de gravação da factura ou talão de venda deverá ser gerada uma assinatura através do algoritmo RSA com base na informação descrita no nº 1 do artigo 6.º da Portaria n.º 363/2010, de 23 de Junho e na chave privada do produtor do programa de facturação.* Na página de criação de documentos (Movimentos de venda), é possível vislumbrar o detalhe da assinatura caso o documento esteja finalizado, consoante é exemplificado na Figura 6.

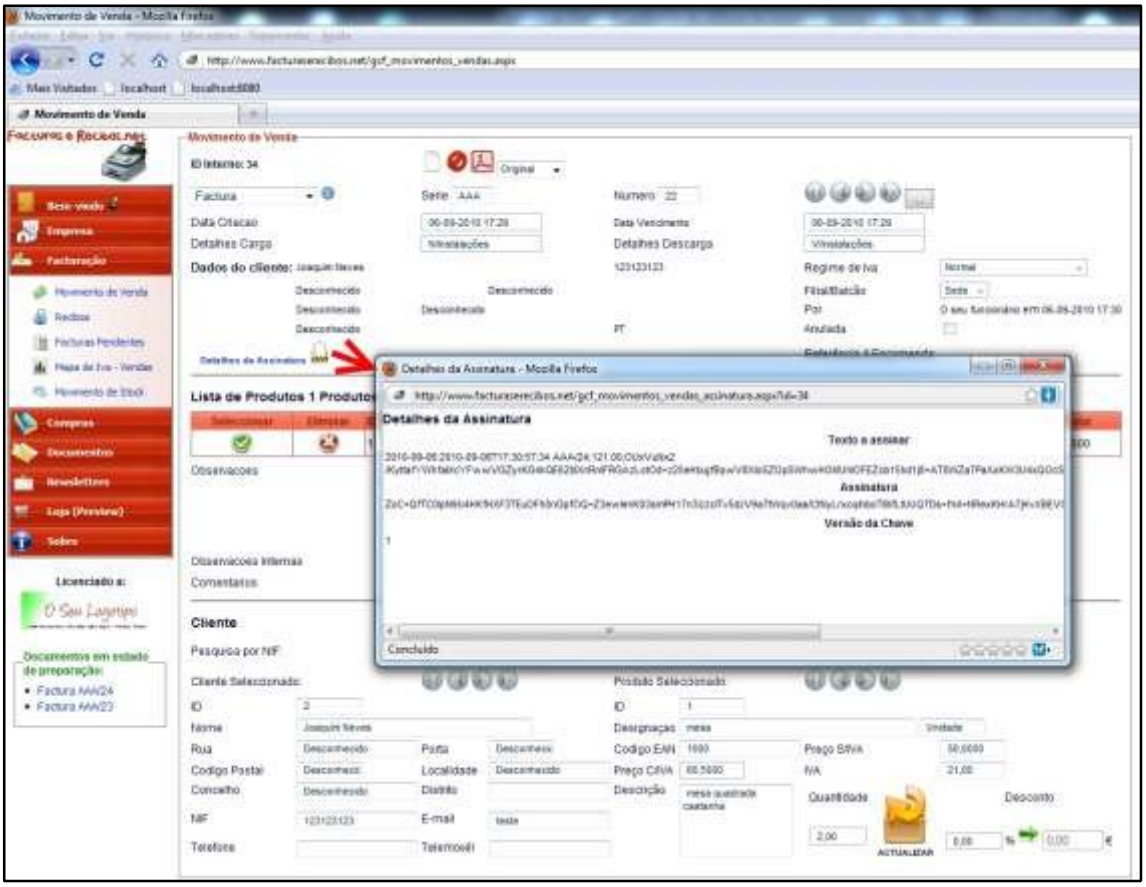


Figura 18 - Assinatura RSA SHA1 num documento finalizado.

Relativamente ao ponto 3.1.2 e 3.1.3 do documento *Especificação das Regras Técnicas para Certificação de Software* que refere *"3.1.2. A assinatura referida no ponto 3.1.1. deverá ser gravada na base de dados com uma associação directa ao registo do documento original, nos termos do número 2 do artigo 6.º da Portaria n.º 363/2010, de 23 de Junho. "3.1.3. Deverá ser gravada adicionalmente a versão (números inteiros sequenciais) da chave privada que foi utilizada para gerar a assinatura do respectivo documento, nos termos do número 2 do artigo 6.º da Portaria n.º 363/2010, de 23 de Junho.* Na Tabela 3, podemos observar que a associação dos campos hash, has_control e id_chave_versao, com a tabela interna do programa, tabela esta com a denominação ou designação "movimentos". Os dois últimos campos referem-se ao id_chave da tabela chaves, com o objectivo de servir como identificação sequencial numérica da versão das chaves.

Relativamente ao ponto 3.1.4 do documento *Especificação das Regras Técnicas para Certificação de Software* que refere *"3.1.4. No caso da gravação de um primeiro documento de uma série/tipo de documento de facturação, ou de um primeiro documento do exercício de cada tipo, o campo referido na alínea e) do artigo 6.º deve ser assumido como não preenchido.* Esta situação encontra-se implementada.

5.4.3 Momento de impressão ou envio electrónico de um documento

No ponto 3.2.1 do documento *Especificação das Regras Técnicas para Certificação de Software* refere *"3.2.1. O documento impresso entregue ao cliente, ou o documento electrónico enviado deve conter impressos obrigatoriamente quatro caracteres da assinatura [Campo 4.1.4.3 – Chave do documento (Hash) do SAF-T PT] correspondentes às posições 1ª, 11ª, 21ª, e 31ª e separado por um "-" (hífen) a expressão "Processado por programa certificado nº <Número do certificado atribuído pela DGCI> em substituição da frase "Processado por computador".*

Na resposta da questão 33 do "FAQs PORTARIA DE CERTIFICAÇÃO DE SOFTWARE", é referido que *"Devem ser impressos os quatro caracteres correspondentes à 1.ª, 11.ª, 21.ª e 31.ª posições da assinatura registada no campo 4.1.4.3 – Hash do SAF T PT, em seguida um hífen "-" e depois o n.º do certificado atribuído pela DGCI, seguido de "/DGCI" (que integra o n.º do certificado, conforme consta da respectiva atribuição)."*

Poderemos observar na Figura 19 que todos os *pdf* gerados apresentam impressa a expressão em causa.

Código	Produto	Preço u. s\iva	Desc.	IVA	Preço u. c\iva	Quantidade	SubTotal c\IVA
1000	Mão de obra	24,59 €	0,00 %	23,00 %	30,25 €	2,00	60,50 €
1001	Aparição	19,68 €	0,00 %	23,00 %	24,20 €	1,00	24,20 €
	VELA DE SERA	2,44 €	0,00 %	23,00 %	3,00 €	3,00	9,00 €
						IVA	17,52 €
						Total S\IVA	76,18 €
						Total C\IVA	93,70 €

COTh-Processado por Programa Certificado nº 418/DGCI. Facturas e Recibos NET versão 5.2011.05.18 http://www.facturaserecibos.net

Observações: Poderá adicionar um comentário extra ás Facturas

Figura 19 - Expressão e extracto da chave nos documentos impressos.

5.4.4 Momento de exportação do ficheiro SAFT-PT

Relativamente ao ponto 3.4.1 do documento *Especificação das Regras Técnicas para Certificação de Software* que refere *"No momento da exportação do SAF-T PT deverá ser exportada para os campos 4.1.4.3 – Chave do documento (Hash) e 4.1.4.4 – Chave de controlo (HashControl) de cada estrutura Invoice (documento de venda – campo 4.1.4) a assinatura e a versão (números inteiros sequenciais) da chave privada respectivas, gravadas previamente na base de dados quando se desencadeou o processo de gravação do documento."* Aquando da exportação saf-t-pt estes campos são incluídos no ficheiro, como é observável na Figura 20.

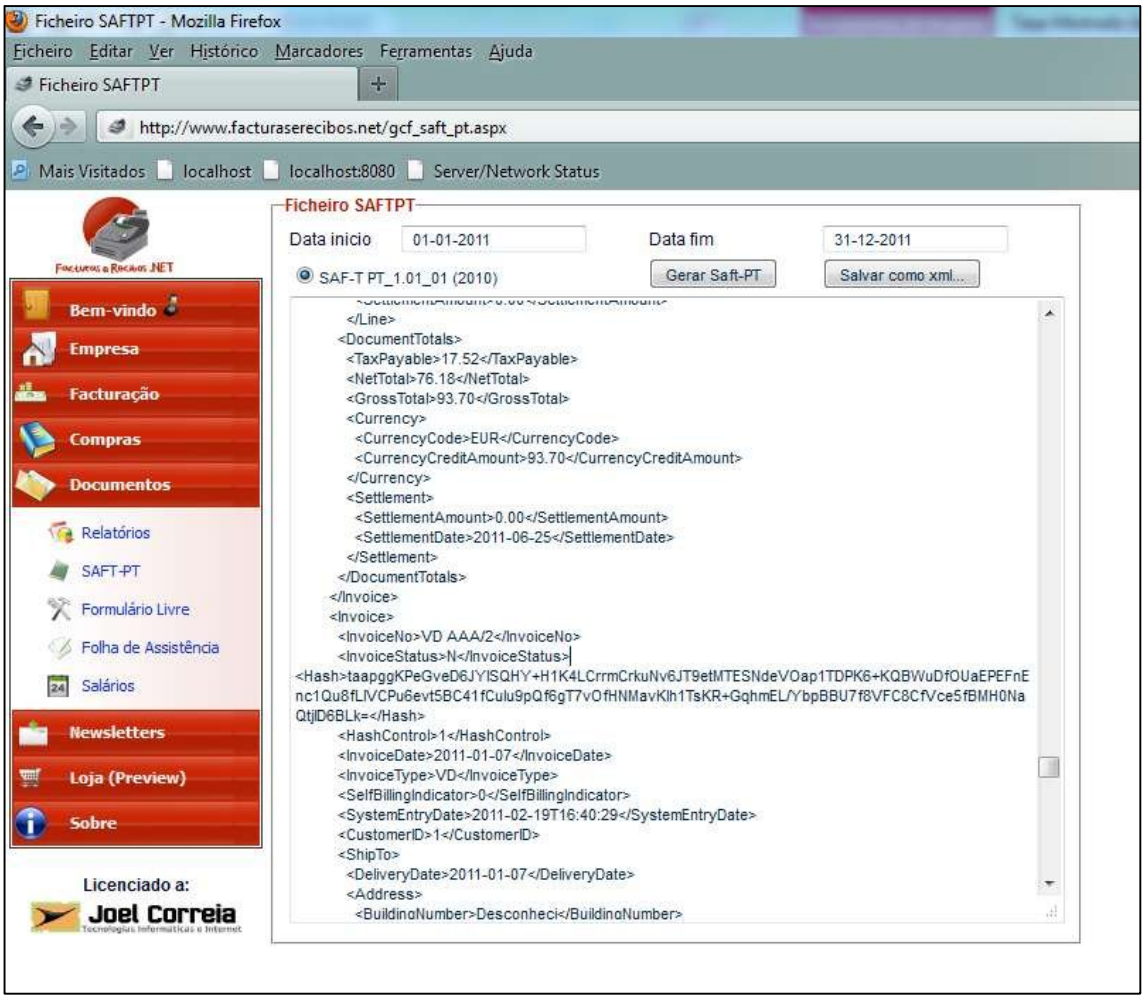


Figura 20 - Exportação do Ficheiro SAF-T-PT.

Existe a possibilidade de visualizar o conteúdo numa caixa de texto ou fazer o download do ficheiro.

5.4.5 Requisitos técnicos relativos ao sistema de identificação

Nos pontos 4.1, 4.2 e 4.3 do documento *Especificação das Regras Técnicas para Certificação de Software* refere, respectivamente, *"Deve ser utilizado o algoritmo RSA (algoritmo de criptografia de dados que usa o sistema de chaves assimétricas, chave pública e chave privada). "* , *"A chave pública a fornecer deve resultar da sua extracção a partir da chave privada, em formato PEM – base 64 e deve ser criado o respectivo ficheiro com a extensão".txt"."* e *"O produtor de software deverá assegurar que a chave privada utilizada para a criação da assinatura que é do seu exclusivo conhecimento, deverá estar devidamente protegida no software."*

As chaves pública e privada encontram-se nas tabelas da base de dados do programa, estão devidamente encriptadas e, consequentemente, protegidas.

No ponto 4.5 do documento *Especificação das Regras Técnicas para Certificação de Software* é apresentado um exemplo da mensagem a assinar, como podemos verificar na Figura 21, a assinatura apresentada é idêntica ao formato requerido, no texto a assinar temos

os detalhes da factura actual: data de emissão, data de alteração, série, número, valor total e assinatura do documento anterior. Este último campo não se aplica à primeira factura.

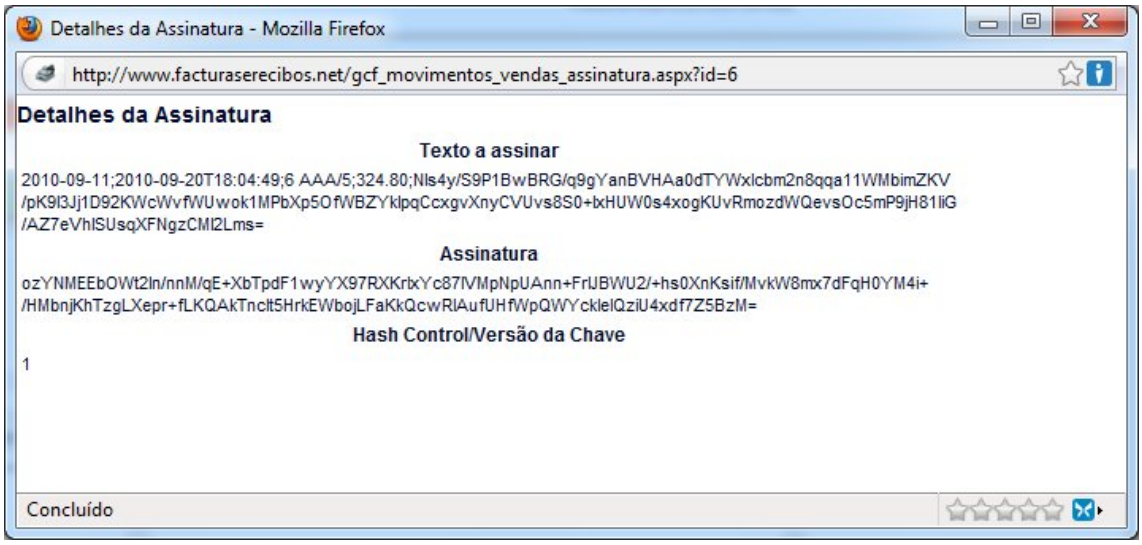


Figura 21 - Exemplo de assinatura RSA SHA1.

Procedeu-se à geração da assinatura conforme o requerido, podemos verificar de entre documentos do mesmo tipo que a assinatura de um documento seguinte inclui a assinatura do documento anterior. De seguida, apresenta-se uma tabela resumo dos campos utilizados para gerar a assinatura e a sua correspondência na base de dados do programa "Facturas e Recibos .NET".

	Tabela da Base de dados	Campo	Descrição
InvoiceDate,	movimentos	data_criacao	
SystemEntryDate	movimentos	data_alteracao	
InvoiceNo:			
Código interno do documento	tipos_movimentos	id_tipo_movimento	
Identificador da série do documento	series	designacao	Está relacionado com a tabela de movimentos através da chave estrangeira id_serie
Número sequencial do documento dentro da série	movimentos	numero	
GrossTotal	movimentos	valor_total_civa	Valor arredondado a duas casas decimais
Hash do registo anterior	movimentos	hash	

Tabela 3 - Correspondência entre campos da base de dados e ficheiro SAF-T-PT.

São guardados em base de dados todos os dados que compõem a assinatura, bem como a própria assinatura.

5.5 Testes de conformidade

Os testes de conformidade decorreram na sede da DGCI em Lisboa, com a presença de dois técnicos que examinaram ao pormenor todo o funcionamento do programa. Desde autenticação no sistema, criação de produtos, geração de facturas e outro tipo de documentos, módulos que o programa pode ter, como por exemplo loja on-line, emissão do ficheiro SAF-T-PT, criação de taxas de iva, verificação de tipos de utilizadores, verificação consistência de valores numéricos inseridos e testes à robustez da interface.

Para além da demonstração prática de todas as funcionalidades do programa, outras questões foram colocadas, nomeadamente:

- Quantos e que tipo de clientes que usam a aplicação?
- Em que sistemas operativos pode ser instalada a aplicação?
- Quem faz as cópias de segurança da base de dados?
- Caso seja a software house, onde são guardados os backups de segurança?

Algumas destas questões podem ser desadequadas no contexto dos testes de conformidade.

6 Questionário

Tendo em vista a obtenção de informação de outras empresas e entidades que também participaram no processo de certificação, pretende-se averiguar sobre as principais dificuldades sentidas no processo de certificação e possíveis soluções. Foi realizado um questionário, no qual se lista na Tabela 4 as questões efetuadas:

Questões	Opções de resposta
1. A certificação de Software dever-se-ia aplicar a todas as aplicações informáticas sem excepção?	Sim, Não
2. Apesar do processo da certificação não ter custos a nível de requisição do processo, este implicou custos de desenvolvimento, cujos valores foram:	<500€ < 1000€ < 2500€ < 5000€ <10000€ >10000€ Não sei/Não respondo
3. Os custos da certificação foram suportados pelos clientes da sua aplicação?	Totalmente Em grande parte Menos de 50% Até 25% Não foram suportados. Não sei/Não respondo
4. O processo da certificação implicou um atraso no desenvolvimento de outras funcionalidades do seu software?	Sim, Não
5. Quantos testes de conformidade necessitaram de realizar?	1,2, mais que 2
6. Qual a principal falha detectada no seu programa?	Processo de geração da factura, Associação de documentos, Anulação de documentos, Texto livre
7. Os testes de conformidade foram uniformes de software para software e empresa para empresa?	Muito uniformes Suficientemente uniformes Pouco uniformes
8. Os testes de conformidade requeriam um formulário de questões previamente fornecido aos requerentes?	Sim, Não
9. A documentação sobre os testes de conformidade foi suficiente para uma boa preparação da aplicação?	Sim, Não
10. Todas as questões foram adequadas ao propósito dos testes de conformidade?	Sim, Não
11. À semelhança de outras áreas (civil, arquitectura, electrónica), seria necessário aos requerentes ter uma pessoa qualificada (Licenciada em Informática) responsável pela certificação?	Sim Não Sem Opinião/Não respondo
12. Melhorias sugeridas no processo da certificação?	Texto livre

Tabela 4 - Perguntas do questionário.

A questão um pretende averiguar a opinião sobre a abrangência da certificação de software de facturação. Na questão dois, pretende-se estimar os custos globais ao nível do país que um processo deste género comporta, a questão três pretende averiguar se se tratou de um encargo, um investimento ou se estes custos foram suportados indirectamente pelo consumidor final. A questão quatro pretende averiguar o impacto negativo em termos de não investimento em outras áreas, que poderiam evoluir a aplicação. As questões cinco, seis, sete,

oito, nove e dez estão relacionadas com os testes de conformidade, uma das fases críticas do processo de certificação. A questão onze visa questionar sobre a relação dos engenheiros informáticos e outras pessoas com qualificações profissionais na área da informática e a regulamentação do exercício da profissão na área da informática.

Através da listagem de programas certificados, disponíveis on-line no site da direção geral de impostos, foram selecionadas aleatoriamente contactos de metade das empresas listadas. Aos contactos conseguidos, foi enviado o endereço do questionário por via correio eletrónico a 224 empresas/programadores, obtiveram-se 29 respostas.

6.1 Estudo Estatístico

O estudo estatístico efetuado vai fornecer uma perspetiva abrangente do processo de certificação. De seguida irá ser feita a analise das respostas obtidas.

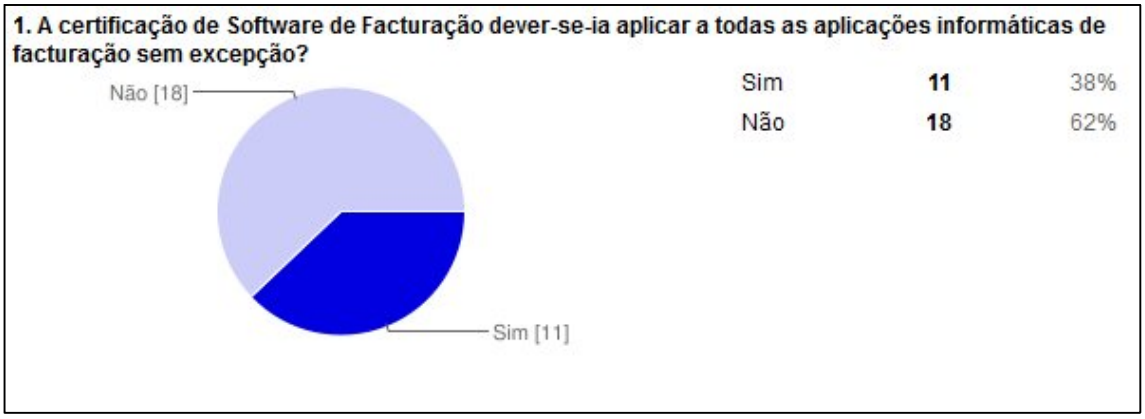


Figura 22 - Gráfico das respostas da questão número um.

Para trinta e oito por cento por inquiridos a certificação de software deveria ser abrangente a todo o software. Mas uma grande percentagem, sessenta e dois por cento, é da opinião que nem todos os softwares deveriam ser sujeitos à certificação.

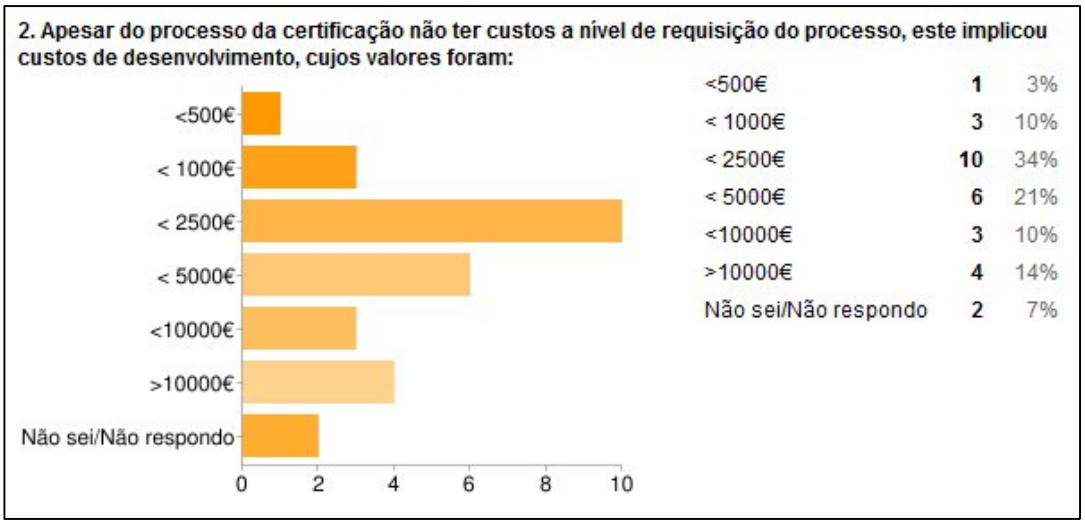


Figura 23 - Gráfico das respostas da questão número dois.

Relativamente a custos inerentes ao processo de faturação, é possível estimar um custo médio de 4907 euros, e considerando que até ao dia vinte e sete de dezembro de dois mil e onze existem 1416 programas na lista de programa certificados, é possível estimar um custo total nacional para as empresas de 6,948 milhões de euros, valor calculado através do valor médio a multiplicar pela quantidade de programas certificados até ao momento: *(500*1+1000*3+2500*10+5000*6+10000*3+11000*4)/27 = 4907 * 1416 = 6 948 312€*

O objetivo da certificação é de combater a fuga ao fisco como é indicado no Diário de notícias pelo Gabinete de Estudos Económicos do Banco de Portugal: "A economia paralela retira anualmente 30,8 mil milhões de euros aos cofres do Estado, representando já 22% do PIB português" (24). Do ponto de vista das empresas pode ser considerado um processo moroso e de custo elevado, o estado pode conseguir travar muitas das situações da economia paralela, mas continua sem conseguir controlar a faturação que não é registada.

Figura 24 - Gráfico das respostas da questão número três.

Embora a certificação não tenha custos diretos de requerimento do processo, os custos de desenvolvimento e outras despesas foram na maior parte suportadas pelo cliente final, provavelmente em valores de upgrade de software. Porém em 28% dos casos existiu um investimento por parte das empresas para suportarem os custos inerentes à certificação.

Figura 25 - Gráfico das respostas da questão número quatro.

Através das respostas à questão quatro, podemos aferir que a certificação implicou um atraso substancial no crescimento funcional das aplicações informáticas de faturação. Pois, oitenta e três por cento dos inquiridos afirmou ter deixado de desenvolver outras funcionalidades na sua aplicação, para a preparar para a certificação.

Figura 26 - Gráfico das respostas da questão número cinco.

Verificamos que em 52% dos casos as aplicações informáticas estavam bem preparadas para os testes de conformidade.

Questão
6. Qual a principal falha detectada no seu programa?
Quantificação das respostas recebidas
• Anulação de documentos (3 respostas); • Problemas na geração do SAF-T-PT (2); • Introdução de linhas com quantidades/valores a negativo nos documentos (2 respostas); • Taxas de IVA, especificamente isenções (2 respostas); • Geração da chave hash/Assinatura digital (2 respostas); • Assinatura digital de documentos com valor inferior a 1€ por causa do 0 á esquerda; • Clientes finais sem código (1 resposta); • Possibilidade de ter desconto financeiro, que teve de ser retirada do software (1 resposta); • A alegada semelhança entre uma proposta/orçamento e uma factura, para além da distintiva designação do documento (1 resposta); • Questões de segurança da informação, em termos de permissões de acesso e de alteração de dados (1 resposta); • Estorno de documentos ou emissão de nota de crédito (1 resposta);

Tabela 5 - Respostas à questão seis.

Das respostas recebidas, a anulação de documentos, a existência da possibilidade de colocar quantidades a negativo o que implica que o valor total do documento seja uma quantidade negativa são das principais falhas detectadas.

Figura 27 - Gráfico das respostas da questão número sete.

Esta questão pretende averiguar o rigor e uniformização dos testes de conformidade, as respostas tiveram percentagens muito semelhantes o que comprova a necessidade de se melhorar este processo, de modo a torná-lo mais uniforme, ou seja igual de empresa para empresa. Na medida em que sejam efetuados os mesmos teste de conformidade, de forma sequencialmente igual e seguindo um plano previamente definido.

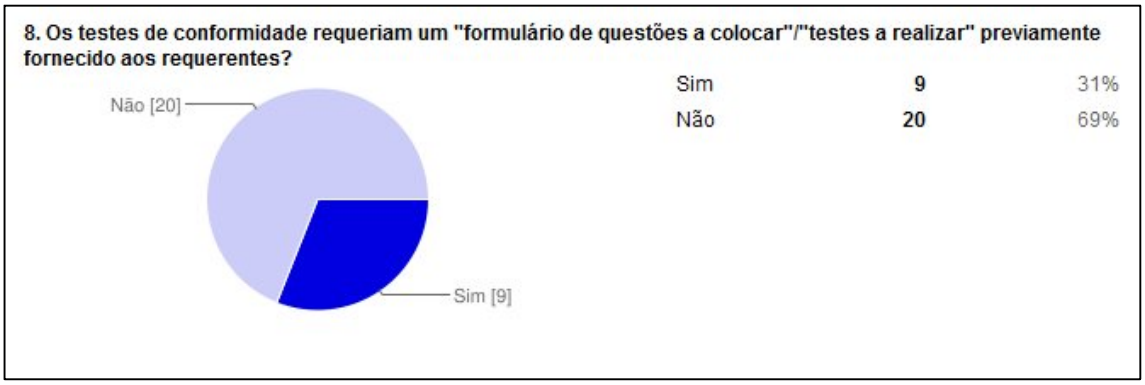


Figura 28 - Gráfico das respostas da questão número oito.

Uma das soluções para a uniformização dos testes de conformidade, seria a criação de um roteiro, ou formulário de questões a colocar, 31% dos inquiridos concordam com esta necessidade.

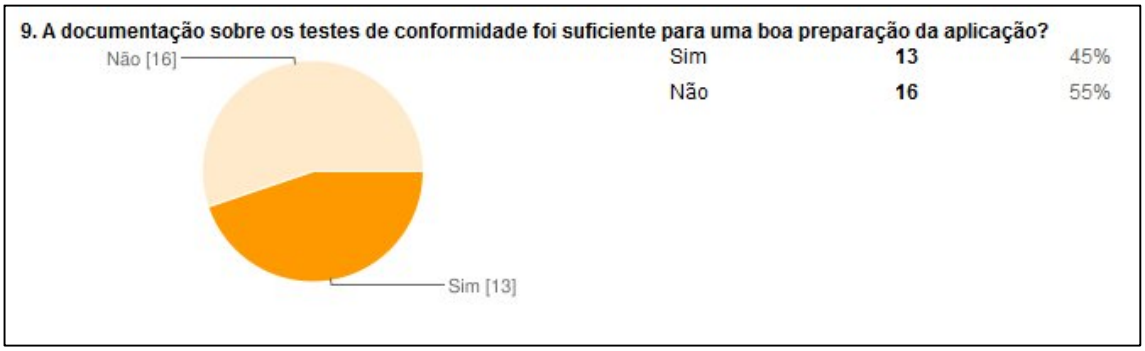


Figura 29 - Gráfico das respostas da questão número nove.

Podemos aferir que a documentação sobre os testes de certificação peca como escassa. De referir a inexistência de artigos ou livros escritos por terceiros que abordem o assunto.

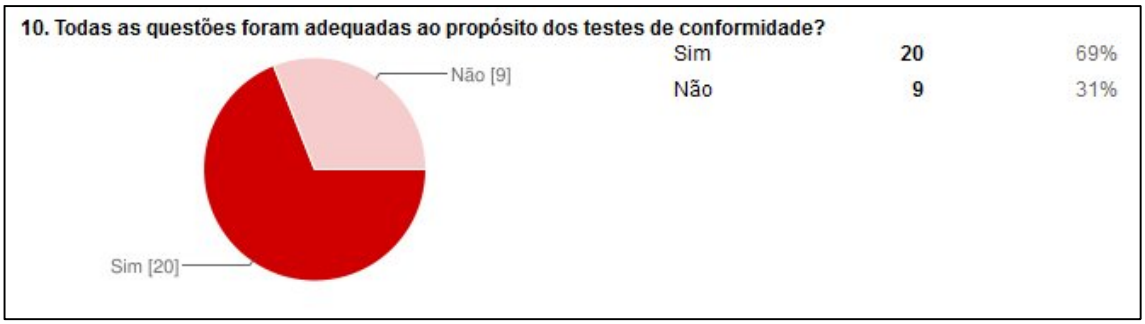


Figura 30 - Gráfico das respostas da questão número dez.

Aparentemente esta questão tem pouca razão de ser, mas constatamos que 31% dos inquiridos foram sujeitos a perguntas desadequadas ao propósito dos testes de conformidade.

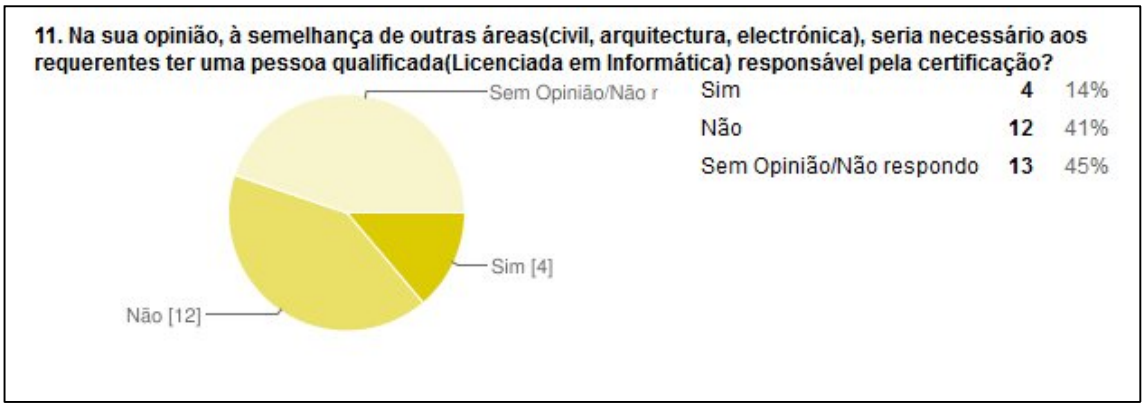


Figura 31 - Gráfico das respostas da questão número onze.

Das respostas obtidas - sem contar com os "Sem Opinião/Não respondo" - das 16 respostas, 25% (4) responderam que é necessário a existência de uma pessoa deviamente credenciada para requerer o processo de certificação, 75% (12) não acham necessário. De uma forma geral, há pouco interesse em legislar, proteger e distinguir os profissionais da área informática. Esta opinião poderá estar ligada á pouca cultura e implementação de leis que regulamentam o sector de desenvolvimento de software e simultaneamente restrinjam o seu desenvolvimento por profissionais oficialmente certificados. Como acontece em muitas outras áreas a ordem dos engenheiros tem um papel crucial na certificação e legalização dos profissionais, nomeadamente na engenharia civil e eletrónica. Na área da informática esse papel é quase inexistente.

Questão
12. Melhorias sugeridas no processo da certificação?
Quantificação das respostas recebidas
• Manual de regras bem definidas e iguais para todos. Elaboração de regras, e conceitos bem definidos a aplicar nos softwares desenvolvidos, para não haver dúvidas, e diferentes tratamentos por parte das diferentes Software Houses. Fornecer aos requerentes previamente um "roteiro", formulário de questões a colocar ou testes a

realizar, assim ficava-se a saber com antecedência quais os testes que iriam ser efectuados. Este facto contribuiria para a igualdade entre programas de facturação, maior rigor no processo e uso da mesma bitola para todos os softwares e respectivas empresas de desenvolvimento, estando as medidas uniformizadas para todas as empresas produtoras de software. (7 respostas)

- Maior rapidez nas respostas, assim como FAQ's mais actualizadas e com melhor documentação. Documentação técnica mais detalhada, com exemplos para cada linguagem de programação. (3 respostas)

- Requerimentos mais explícitos e uniformes. Nomeadamente, na questão da anulação de documentos, quais os documentos que necessitam de assinatura digital, a possibilidade de impressão de documentos, quais os campos que podem ser alterados depois de emitido um documento, criação de registos das alterações após impressão/finalização de documentos, arredondamentos de valores. (5 respostas)

- Melhorias na protecção de dados. (1 resposta)

- Enquadramento numa política de promoção mais ampla, de forma a que um selo de certificação da DGCI fosse mais facilmente reconhecido internacionalmente como garante de conformidade com princípios mais universais que os de caça à fraude que a DGCI colocou nesta iniciativa.(1 resposta)

- Processo de bloqueio de edição do design/layout dos documentos. (1 resposta)

- Flexibilização do local dos testes de conformidade, que apenas se efectua em Lisboa, o que acarreta custos e dispensa de recursos humanos no mínimo por um dia. (1 resposta)

Tabela 6 - Resumo das respostas à questão doze.

De notar que mesmo após a certificação estar concluída e aprovada, muitas dúvidas persistem sobre diversos temas. Não tendo sido explicadas mesmo após a aprovação do software.

Outras questões que surgiram neste questionário, nomeadamente, se o estado deveria obrigar as empresas a usarem um só software fornecido por este, como o sistema básico de facturação/comercial.

Outra conjetura projetada, tem a ver com que a possível obrigação das empresas em comunicar com sistemas diretamente ligados a servidores do Estado. Embora possa parecer uma medida radical e com pontos não exequíveis, em que numa primeira fase o mercado não a aceitaria bem, a entrada em funcionamento dos recibos verdes electrónicos vem a confirmar uma certa tendência futura para a criação de algo que se aproxime da hipotética situação mencionada.

7 Conclusão

O software tem de ter em conta a legislação inerente ao processo de compra e venda, sendo que através dos constrangimentos legais são pensadas as restrições funcionais.

7.1 Funcionalidades desenvolvidas

O momento de criação dos documentos é um dos momentos cruciais. Das alterações efetuadas ao software, uma das características que a criação de documentos teve de ter, foi a existência de um estado de preparação que permite ao utilizador manipular a factura sem a poder imprimir, sendo necessário a finalização da mesma. Só após este processo é que a factura pode ser impressa. Para tal, foi necessário implementar um método de gestão dos números dos documentos, optou-se por manter um número temporário e no momento de finalização do documento de venda este número poderia mudar consoante o número de documentos pendentes.

Relativamente ao método de geração das assinaturas, a escolha recaiu para a Biblioteca nativa da Microsoft em conjunto com a interface de importação do ficheiro PEM. Esta escolha foi efectuada devido aos testes de robustez em que se verificou que nunca ocorreram falhas no algoritmo de codificação, enquanto na biblioteca Bouncy Castle, 1 em 100 tentativas de assinatura não eram efectuadas com sucesso.

Relativamente ao controlo de concorrência entre multiutilizadores, foram efectuados teste com três utilizadores em simultâneo, os testes efectuados demonstraram a eficácia da solução implementada.

A validade do ficheiro SAF-T-PT e das assinaturas foi comprovada utilizando o programa disponibilizado online pela DGCI.

7.2 Reflexão das leis e processo

A desresponsabilização do utilizador é algo que não poderá acontecer. Um software não tem como objectivo principal ser um elemento de policiamento face à actuação do utilizador. Tenta-se que a sua actuação seja condicionada e controlada pelo software. Existem sempre pontos não controláveis, como por exemplo, no caso em que o software permita a criação de cópias de segurança por parte do utilizador e a respectiva reposição das mesmas, esta possibilidade pode ser usada para efectuar cortes na facturação, o utilizador tem a sua cota parte de responsabilidade em efectuar uma utilização consciente.

A possível exclusão do software proprietário ser certificado faz pouco sentido, uma vez que a certificação de software é uma das medidas de combate à fraude e deveria ser abrangente a todo o software, independente de quem o utiliza. Relativamente a esta exclusão

à lei, podem surgir casos de compra dos direitos de software para que não seja necessário a certificação do mesmo. Podendo existir versões de software's que, embora sejam no seu essencial sejam iguais em termos de código fonte, têm proprietários intelectuais diferentes, o que não deixa de ser uma contradição.

7.3 Dificuldades experienciadas

Através das respostas obtidas no questionário, destaca-se as respostas à questão nove, onde se depreende a falta de documentação relativa aos testes de conformidade. Na questão sete, que inquere sobre a uniformidade destes testes, as respostas obtidas foram bastante heterogéneas, o que pode dar a entender a necessidade de implementação estratégias de coerência por parte da entidade que leva a cabo estes testes. Nestes testes dois técnicos averiguam a conformidade da aplicação face à legislação referente aos sujeitos passivos de facturação. Os técnicos podem variar consoante a empresa que requer a certificação, este facto pode contribuir para a não uniformização dos testes no caso de não haver um conjunto de procedimentos uniformes.

De uma forma geral pode dar sensação que se requer que o programa de facturação controle o modo de actuação do utilizador face ao processo de compra e venda. Muitas destas restrições podem por em causa a usabilidade dos programas de facturação. Nem sempre as restrições são claras, tal como o caso de anulação dos documentos, que embora esteja previsto no ficheiro SAF-T-PT, existiram casos em que nos testes de conformidade os técnicos não permitiram a anulação de documentos, trata-se de uma situação pouco explicita e não transversal a todos os programas e a todos os testes de conformidade.

Uma lista de requerimentos ou pontos de verificação seria necessária, porém não se encontra explicitamente percetível. Destes pontos de verificação, poderiam constar os seguintes:

1. Exportação do ficheiro SAF-T-PT;
2. Geração de um número hash por cada transacção;
3. Validação e proteção da chave pública e privada;
4. Restrições em caso de uso do programa no modo de demonstrativo/formativo (Inclusão do nome da empresa produtora ao invés do Cliente);
5. As transacções não puderam ter linhas com valores a negativo;
6. Associação automática de movimentos, como por exemplo, uma encomenda pode ter originado uma factura;
7. Conversão automática de documentos, por exemplo criação de facturas tendo como base uma guia de remessa;

8. Alerta ou obrigatoriedade de emissão das facturas das guias de remessa;

Em suma, esta seria uma bateria de testes que deveria ser seguida à risca, desta forma uniformizando os testes de conformidade por todos os técnicos da Direcção Geral das Finanças.

O software "Facturas e Recibos .NET" obteve a certificação, tendo como número de certificado o 418. Uma versão demonstração do programa está disponível on-line no endereço electrónico: http://www.facturaserecibos.net/.

8 Referências

1. **Project, The OpenSSL.** OpenSSL: The Open Source toolkit for SSL/TLS. [Online] http://www.openssl.org/.

2. **DGCI, Direcção Geral dos Impostos.** SAF T PT (Standard Audit File for Tax purposes) Versão Portuguesa. [Online] http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/NEWS_SAF-T_PT.htm.

3. **Administração, Ministério das Finanças e da.** Portaria n.º 1192/2009. *Diário da Republica.* 2009.

4. **Proiete, Maria.** Obrigatoriedade das facturas e documentos equivalentes. *Contabilidade, Fiscalidade, Finanças, e afins.* [Online] [Citação: 16 de 11 de 2010.] http://www.mariaproiete.com/blogs/financas/fiscalidade/obrigatoriedade-das-facturas-e-documentos-equivalentes/.

5. **Pública, Ministério das Finanças e da Administração.** *Combate à Fraude e Evasão Fiscais 2008.* 2009.

6. **Direcção de Serviços de Planeamento e Coordenação da Inspecção Tributária, DSPCIT.** *Especificação das Regras Técnicas para Certificação de Software Portaria n.º 363/2010, de 23 de Junho.* 2010. 070.05.01.

7. **DGCI, Direcção Geral dos Impostos.** Certificação de Software de Facturação. [Online] http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/CertificacaoSoftware.htm.

8. **Finanças, Ministério das.** Decreto-Lei n.º 198/90. *Diário da República.* 1990.

9. —. Ministério das Finanças, Decreto-Lei nº 147/2003. *Diário da Republica.* I, 2003.

10. **Administração, Ministério das Finanças e da.** Portaria n.º 363/2010, de 23 de Junho, Série I, n.º120. s.l. : Diário da Republica, 2010.

11. **Development, Organisation for Economic Co-operation and.** Guidance Note - Guidance for Developers of Business and Accounting Software Concerning Tax Audit Requirements. [Online] http://www.oecd.org/document/57/0,2340,en_2649_33749_34910329_1_1_1_1,00.html.

12. **Finanças, Ministério das.** *Portaria n.o 321-A/2007.* Ministério das Finanças : s.n., 2007.

13. —. *A Portaria n.º 1192/2009.* s.l. : Ministério das Finanças, 2009.

14. Criptografia. [Online] Emerson Alecrim. [Citação: 23 de 10 de 2010.] http://www.infowester.com/criptografia.php.

15. Criptografia. *Wikipédia.* [Online] Wikipédia. [Citação: 22 de 10 de 2010.] http://pt.wikipedia.org/wiki/Criptografia.

16. **Luis Barbosa, Luis Braghetto, Marcelo Brisqui, Sirlei Silva.** *RSA Criptografia Assimétrica e Assinatura Digital.* Campinas : s.n., 2003.

17. **Wikipédia.** SHA-1. *Wikipédia.* [Online] Wikipédia. [Citação: 12 de 01 de 2011.] http://en.wikipedia.org/wiki/SHA-1.

18. PEM format. *Internet RFC/STD/FYI/BCP Archives.* [Online] http://www.faqs.org/qa/qa-14736.html.

19. Certificates: File Format & Conversion. *A Brief Guide to Certificate Management.* [Online] http://www.bo.infn.it/alice/introgrd/certmgr/node2.html.

20. **Microsoft.** *The Official Microsoft ASP.NET Site.* [Online] Microsoft, 2011. http://www.asp.net/.

21. The Legion of the Bouncy Castle C# Cryptography APIs. [Online] http://www.bouncycastle.org/csharp/.

22. **Boehm, Barry.** *A Spiral Model of Software Development and Enhancement.* s.l. : TRW Defense Systems Group, 1988.

23. **Gallant, Michel I.** RSA Public, Private, and PKCS #8 key parser. *JavaScience Consulting.* [Online] http://www.jensign.com/opensslkey/.

24. **Diário de notícias, Gabinete de Estudos Económicos do Banco de Portugal.** Economia paralela movimenta 31 mil milhões de euros por ano. [Online] http://www.dn.pt/inicio/interior.aspx?content_id=618196.

25. **www.saftpt.com.** Portal Ficheiro Saf-T PT. [Online] http://www.saftpt.com/.

26. *Faqs Portaria De Certificação De Software.* **Direcção de Serviços de Planeamento e Coordenação da Inspecção Tributária, DSPCIT.** 070.05.01.

Anexos

Anexo 1 – Código fonte da classe RsaSha1DotNetCrypto

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Web;
using System.Security.Cryptography;
using System.Text;

namespace RsaSha1Pem
{
    public class RsaSha1DotNetCrypto
    {
        /// <summary>
        /// Sign the data with private key
        /// </summary>
        /// <param name="data">data string</param>
        /// <param name="privateKey">entire private key text from private key PE file.</
    param>
        /// <returns>Base64 signature text</returns>
        public static string Sign(string data, string privateKey)
        {
            //sign
            RSACryptoServiceProvider rsa = Anculus.Core.OpenSslRsaKey.FromPemString
    (privateKey);
            byte[] testData = Encoding.UTF8.GetBytes(data);
            SHA1CryptoServiceProvider sha1 = new SHA1CryptoServiceProvider();
            byte[] signData = rsa.SignData(testData, sha1);
            return Convert.ToBase64String(signData);
        }

        /// <summary>
        /// Verify signature
        /// </summary>
        /// <param name="data">data string</param>
        /// <param name="signature">signature in base64</param>
        /// <param name="publicKey">entire key text from the public key PE file</param>
        /// <returns>verification status</returns>
        public static bool Verify(string data, string signature, string publicKey)
        {
            //verify
            RSACryptoServiceProvider rsa = Anculus.Core.OpenSslRsaKey.FromPemString
    (publicKey);
            byte[] testData = Encoding.UTF8.GetBytes(data);
            SHA1CryptoServiceProvider sha1 = new SHA1CryptoServiceProvider();
            byte[] signatureData = Convert.FromBase64String(signature);
            return rsa.VerifyData(testData, sha1, signatureData);
        }
    }
}
```

Anexo 2 – Código fonte da classe RsaSha1BouncyCrypto

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Web;
using System.Text;

namespace RsaSha1Pem
{
    public class RsaSha1BouncyCrypto
    {
        /// <summary>
        /// Sign the data with private key
        /// </summary>
        /// <param name="data">data string</param>
        /// <param name="privateKey">entire private key text from private key PE file.</param>
        /// <returns>Base64 signature text</returns>
        public static string Sign(string data, string privateKey)
        {
            //sign
            System.IO.TextReader TextReaderPrivateKeyBouncyCastle1 = new System.IO.StringReader(privateKey);
            Org.BouncyCastle.OpenSsl.PemReader PEMReaderBouncyCastle1 = new Org.BouncyCastle.OpenSsl.PemReader(TextReaderPrivateKeyBouncyCastle1);
            Org.BouncyCastle.Crypto.AsymmetricCipherKeyPair keyPair = PEMReaderBouncyCastle1.ReadObject() as Org.BouncyCastle.Crypto.AsymmetricCipherKeyPair;

            byte[] testData = Encoding.UTF8.GetBytes(data);
            //Need to use SHA1WithRSA, to be consistent with Openssl sign command.
            Org.BouncyCastle.Crypto.ISigner sigBouncyCastle1 = Org.BouncyCastle.Security.SignerUtilities.GetSigner("SHA1WithRSA");
            sigBouncyCastle1.Init(true, keyPair.Private);
            sigBouncyCastle1.BlockUpdate(testData, 0, testData.Length);
            byte[] signature = sigBouncyCastle1.GenerateSignature();
            return Convert.ToBase64String(signature);
        }

        /// <summary>
        /// Verify signature
        /// </summary>
        /// <param name="data">data string</param>
        /// <param name="signature">signature in base64</param>
        /// <param name="publicKey">entire key text from the public key PE file</param>
        /// <returns>verification status</returns>
        public static bool Verify(string data, string signature, string publicKey)
        {
            //verify
            string base64pubkeyBouncyCastle1 = publicKey.Trim().Replace("-----BEGIN PUBLIC KEY-----", "").Replace("-----END PUBLIC KEY-----", "");
            Org.BouncyCastle.Crypto.Parameters.RsaKeyParameters pubKey = Org.BouncyCastle.Security.PublicKeyFactory.CreateKey(Convert.FromBase64String(base64pubkeyBouncyCastle1)) as Org.BouncyCastle.Crypto.Parameters.RsaKeyParameters;
            byte[] SignatureToVerifyBouncyCastle1 = Convert.FromBase64String(signature);
            byte[] messageBouncyCastle1 = Encoding.UTF8.GetBytes(data);

            //Need to use SHA1WithRSA, to be consistent with Openssl sign command.
            Org.BouncyCastle.Crypto.ISigner sig_verifyBouncyCastle1 = Org.BouncyCastle.Security.SignerUtilities.GetSigner("SHA1WithRSA");
            sig_verifyBouncyCastle1.Init(false, pubKey);
            sig_verifyBouncyCastle1.BlockUpdate(messageBouncyCastle1, 0, messageBouncyCastle1.Length);
            return sig_verifyBouncyCastle1.VerifySignature(SignatureToVerifyBouncyCastle1);
        }
    }
}
```

Anexo 3 – Diagrama das classes movimentos e chaves