AT autoridade tributária e aduaneira

GABINETE DO SUBDIRETOR-GERAL DA INSPEÇÃO TRIBUTÁRIA

Of.Circulado N.º 50.001/2013 Entrada Geral: N.º Identificação Fiscal (NIF): Sua Ref.ª Técnico:	Exmos. Senhores Subdiretores-Gerais Diretores de Serviços Diretores de Finanças Diretores de Alfândegas Chefes de Equipas Multidisciplinares Chefes dos Serviços de Finanças Coordenadores das Lojas do Cidadão

Assunto: Requisitos técnicos a que se refere a al. e) do artigo 3.º da Portaria n.º 363/2010, de 23 de junho, com a redação dada pela Portaria n.º 22-A/2012, de 24 de janeiro e pela Portaria n.º 160/2013, de 23 de abril.

Nos termos da alínea e) do n.º 3 da Portaria n.º 363/2010, de 23 de junho, com a redação que lhe foi dada pelas portarias n.º 22-A/2012, de 24 de janeiro e n.º 160/2013, de 23 de abril, os programas de faturação e equiparados, adiante designados apenas por programas de faturação, devem ainda observar os demais requisitos técnicos aprovados por despacho do Diretor-Geral da Autoridade Tributária e Aduaneira.

Tendo sido aprovados, por despacho do Diretor-Geral da Autoridade Tributária e Aduaneira, de 2013-07-02, os referidos requisitos, a que devem obedecer todos os programas de faturação, ainda que já certificados, divulgam-se para conhecimento.

1. ASSINATURA DOS DOCUMENTOS EMITIDOS PELOS PROGRAMAS DE FATURAÇÃO

1.1. Os programas informáticos de faturação devem assinar, nos termos dos artigos 6.º e 7.º da Portaria n.º 363/2010, de 23 de junho, os seguintes documentos:

- As faturas e documentos retificativos;
- As guias de transporte, guias de remessa e quaisquer outros documentos que constituam documento de transporte, nos termos do Decreto-Lei n.º 147/2003, de 11 de julho;
- Quaisquer outros documentos, independentemente da sua designação, suscetíveis de apresentação ao cliente para conferência de entrega de mercadorias ou da prestação de serviços, nomeadamente as designadas consultas de mesa.

1.2. Quaisquer outros documentos com eficácia externa emitidos por um programa de faturação, não sujeitos a assinatura, designadamente, orçamentos ou faturas proforma, devem conter de forma evidente a sua natureza e, quando suscetíveis de serem confundidos com uma fatura, conter a expressão “Este documento não serve de fatura”, competindo ao produtor de software criar condições que não permitam alterações de layouts, devendo, caso contrário, estes documentos ser assinados.

Av. Duque d´ Ávila, n.º 71- 7º Piso, LISBOA – 1000-139 Tel: (+351) 213 584 800 Fax: (+351) 213 584 807
Email: sdg-it@at.gov.pt www.portaldasfinancas.gov.pt Centro de Atendimento Telefónico: (+351) 707 206 707

1.3. As faturas e documentos retificativos que tiveram origem noutros documentos emitidos, designadamente, faturas, guias de movimentação de mercadorias ou outros documentos suscetíveis de apresentação ao cliente designadamente as consultas de mesa, devem conter a identificação desses documentos, na estrutura começada com o índice 4.1.4.18.2. – Referência ao documento de origem (OrderReferences).

1.4. As guias de movimentação de mercadorias que tiveram origem noutros documentos emitidos devem conter a identificação desses documentos na estrutura começada com o índice 4.2.3.20.2. – Referência ao documento de origem (OrderReferences).

1.5. No caso de utilização do programa em modo de formação, os documentos assim emitidos deverão, em série específica, indicar sempre, 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", ainda que impressos em papel timbrado do cliente.

1.6. Todos os tipos de documentos deverão ser emitidos cronologicamente em uma ou mais séries (que devem manter-se pelo menos anualmente e que não devem utilizar carateres que violem o esquema de validação ou possam ser interpretados como operadores de XML) devidamente referenciadas e dentro de cada uma numerados sequencialmente. Não pode constar da sequência numérica qualquer outra informação como, por exemplo, o ano ou o número do terminal informático, etc. que, a existir, deverá sempre constar da identificação da série.

1.7. O número do documento deve conter, impresso, um código identificador da(s) série(s) específica de cada um dos estabelecimentos e/ou programa(s), as quais nunca podem ser repetidas no mesmo contribuinte, de modo a identificar univocamente cada documento emitido, mesmo que os documentos sejam emitidos por mais do que um programa de faturação, em consequência, nomeadamente da existência de diversos estabelecimentos.

1.8. Nenhum documento em estado de preparação ou em pré-visualização poderá ser impresso em momento anterior à sua finalização e assinatura, de acordo com os procedimentos elencados nos pontos 2.1. e 2.2.

1.9. A aplicação não pode permitir que num documento já assinado seja alterada qualquer informação fiscalmente relevante, designadamente os elementos referidos nos artigos 36.º e 40.º do Código do IVA, no Decreto-Lei n.º 147/2003, de 11 de julho e nos artigos 6.ºe 7.º da Portaria.

2. PROCESSO DE IDENTIFICAÇÃO (ASSINATURA) DOS DOCUMENTOS E SUBSEQUENTE GRAVAÇÃO NAS BASES DE DADOS

2.1. Processo de identificação de documentos

2.1.1. No processo de identificação de documentos, nomeadamente, fatura ou documento retificativo, documento que acompanhe mercadorias em circulação, valorado ou não, documentos emitidos para conferência, etc., deverá sempre ser gerada uma assinatura através do algoritmo RSA

com base na informação relativa ao documento descrita no n.º 1 do artigo 6.º ou no n.º 2 do artigo 7.º da Portaria n.º 363/2010, de 23 de junho e na chave privada do produtor do programa de faturação.

2.1.2. A assinatura referida no ponto anterior deverá ser gravada na base de dados do programa de faturação (que não pode estar encriptada e deve ser mantida durante o prazo de arquivo legal), com uma associação direta ao registo do documento original, nos termos do n.º 2 do artigo 6.º da Portaria n.º 363/2010, de 23 de junho.

2.1.3. Deverá ser gravada adicionalmente a versão (números inteiros sequenciais) da chave privada que foi utilizada para gerar a assinatura do respetivo documento, nos termos do n .º 2 do artigo 6.º da Portaria n.º 363/2010, de 23 de junho.

2.1.4. A mudança do par de chaves utilizado pelo programa certificado só pode ser realizada pela empresa produtora após comunicação à AT através de uma declaração modelo 24 e do upload da respetiva chave pública.

2.1.5. No caso da gravação de um primeiro documento de uma série/tipo de documento de faturação ou de um primeiro documento do exercício de cada tipo, o campo aplicável (4.1.4.3.; 4.2.3.3. ou 4.3.4.3.) – chave do documento *(Hash)* deve ser assumido como não preenchido.

2.1.6. No caso de documentos de movimentação de mercadorias ou documentos de conferência que não estejam valorados na base de dados, o correspondente campo de valor total [respetivamente 4.2.3.21.3. – Total do documento com impostos (GrossTotal) e 4.3.4.13.3. -. Total do documento com impostos (GrossTotal)], deve ser preenchido com “0.00” (sem aspas) e assim considerado aquando da assinatura.

2.1.7. Caso a emissão do documento seja realizada em moeda estrangeira, o valor a assinar deve ser o contravalor em EUR, uma vez que vai ser este o valor a exportar no ficheiro SAF-T(PT).

2.2. Momento de impressão ou envio eletrónico de um documento

2.2.1. Os documentos suscetíveis de assinatura, só poderão ser impressos depois de devidamente identificados nos termos dos artigos 6.º e 7.º da Portaria 363/2010, de 23 de junho e respeitando o indicado no ponto 2.1.

2.2.2. O documento impresso entregue ao cliente ou o documento eletrónico enviado deve conter impressos obrigatoriamente quatro carateres da assinatura [campos Chave do documento (Hash) das tabelas subordinadas da tabela 4 – Documentos comerciais (SourceDocuments) do SAF-T(PT)] correspondentes às posições 1ª, 11ª, 21ª, e 31ª e separado por um “-“ (hífen) a expressão “Processado por programa certificado n.º <Número do certificado atribuído pela AT>/AT. Exemplo: “AxAx-Processado por programa certificado n.º0000/AT” (sem aspas).

2.2.3. Os documentos referidos no ponto 1. deverão na sua impressão conter a data no formato do SAF-T(PT) – “AAAA-MM-DD” (sem aspas), a série a que o documento pertence e depois a numeração sequencial própria, exclusivamente numérica.

2.2.4. Nas faturas emitidas nos termos dos artigos 36º e 40º do CIVA, entregues a clientes que não facultem a sua identificação fiscal (consumidores finais), deverá nestes documentos ser inutilizada a correspondente linha ou através da expressão "Consumidor final" (sem aspas).

2.2.5. Os documentos impressos pelo programa de faturação não devem conter valores negativos. Quando necessário serão utilizados documentos retificativos de faturas (notas de débito e notas de crédito, nos termos do nº 7 do artigo 29º do CIVA), como documentos de correção de operações de compra e venda, cuja forma, conteúdo e finalidade devem ser respeitados. Os valores negativos só poderão ser impressos nos casos de anulação de registos que já integram a fatura ou para acerto de estimativas nas prestações de serviços continuadas.

2.2.6. A impressão pelo sistema integrador de documentos nele integrados, deverá fazer menção desta qualidade, através da expressão "Cópia do documento original" (sem aspas), sem prejuízo de outras que lhe sejam aplicáveis.

2.2.7. As faturas criadas pelo procedimento indicado no ponto 2.4., deverão conter, quando impressas, a expressão "Cópia do documento original e separada por hífen a expressão referida no ponto 2.4.5.2." (sem aspas).

Exemplo: "Cópia do documento original-FTM abc/00001"

2.2.8. As faturas criadas pelo procedimento indicado no ponto 2.5., deverão conter, quando impressas, a expressão "Cópia do documento original e separada por hífen a expressão referida no ponto 2.5.5.2." (sem aspas).

Exemplo: "Cópia do documento original- FTD 2013A/00099"

2.3. Documentos integrados na base de dados de faturação, originários de outras soluções

2.3.1. Dada a existência de diversas soluções de faturação para colmatar diferentes necessidades dos contribuintes, nomeadamente a faturação em sistemas descentralizados ou em sistemas móveis (as chamadas soluções de mobilidade) devem ser tidas em conta regras com vista à definição das condições de integração de informação entre diferentes sistemas de faturação.

2.3.2. A assinatura referida no ponto 2.1. é, neste caso, da responsabilidade das soluções originais e deve sempre residir nelas (pois só o sistema original conhece a chave privada e tem a capacidade de identificar os carateres impressos na fatura original ou noutro documento emitido).

2.3.3. Uma determinada série/tipo de documento de faturação, de movimentação de mercadorias ou de qualquer outro documento suscetível de ser entregue ao cliente para conferência de entrega de mercadorias ou de prestação de serviços não pode conter documentos com diferentes origens (exemplo: conter documentos criados no sistema e importados de um sistema externo numa mesma série/tipo de documento de faturação).

2.3.4. Assim, o sistema central que realiza a integração deve:

a) Integrar os documentos provenientes de outros sistemas, em séries/tipos de documentos distintas e autónomas das que utiliza para a emissão própria, nas correspondentes tabelas de documentos comerciais (4.1., 4.2. ou 4.3) sendo os documentos integrados entendidos como cópias do documento original, nessas tabelas;

b) Colocar a informação relativa à chave do documento (Hash) igual à que foi gerada no sistema emissor, nas correspondentes tabelas em que é integrado o documento. Isto é, devem ser iguais, no sistema integrador e integrado, respetivamente, o valor do campo 4.1.4.3. para os documentos da tabela 4.1.,o valor do campo 4.2.3.3. para os documentos da tabela 4.2. ou o valor do campo 4.3.4.3 para os documentos da tabela 4.3.;

c) Preencher os campos aplicáveis relativos à origem do documento com o valor "I": o campo 4.1.4.2.5. – Origem do documento (SourceBilling) ou o campo 4.2.3.2.5. –. Origem do documento (SourceBilling), consoante o caso;

d) Preencher o campo 4.1.4.4., o campo 4.2.3.4. ou o campo 4.3.4.4. – Chave de controlo (HashControl), consoante o caso, com o número do certificado com o qual o documento foi assinado no sistema original e a respetiva versão da chave;

e) O formato da informação a registar, nos campos 4.1.4.4., 4.2.3.4. ou 4.3.4.4 – Chave de controlo (HashControl) nos termos da alínea anterior, resultará da concatenação do número do certificado original + um ponto + versão da chave privada utilizada na assinatura original respetivamente dos campos 4.1.4.3., 4.2.3.3 ou 4.3.4.3 – Chave do documento (Hash);

Exemplo: "9999.1", em que "9999" é o número do certificado da aplicação emissora e "1" é a versão da chave utilizada na respetiva assinatura.

f) No caso da informação a integrar provir de programa não certificado, o valor do campo Chave de controlo (*HashControl)* aplicável ao tipo de informação: 4.1.4.4., 4.2.3.4. ou 4.3.4.4., deve ser a menção "não certificado" (sem aspas). Já o valor do campo *(Hash).*respetivo deve ser "0" (zero). Os documentos nestas condições, não devem ser reimpressos pela aplicação integradora.

2.4. Integração de faturas ou documentos retificativos processadas manualmente em impressos emitidos em tipografias autorizadas, nos casos de inoperacionalidade do programa

2.4.1. A integração de faturas ou outros documentos retificativos, processados manualmente deve realizar-se no programa certificado em série específica, de periodicidade anual ou superior e com numeração sequencial própria.

2.4.2. Para este efeito será processada uma nova fatura, que recolha todos os elementos da fatura manual emitida, com observância dos requisitos definidos no artigo 6.º da Portaria 363/2010, isto é, deve assinar o documento e imprimir a respectiva expressão.

2.4.3. Nestas séries de recuperação, a data do documento corresponde à data do documento manual e é de todo o interesse que se criem dois campos distintos, de preenchimento obrigatório, sendo um para a identificação da série manual e o outro para recolher o número manual. Desta forma evitar-se-ão lapsos na recolha deste tipo de documentos designadamente da série.

Podem ser criadas tantas séries, quantas as existentes nos documentos manuais ou apenas uma única série.

2.4.4. Preencher o campo 4.1.4.2.5. – Origem do documento *(SourceBilling)* relativo à origem do documento com o valor "M".

2.4.5. Nestes casos, no campo 4.1.4.4 – Chave de controlo (HashControl) deve ser aposta a seguinte informação:

2.4.5.1. Número da versão da chave privada (1,2, etc.) e separado por um "-" (hífen);

2.4.5.2. Registo sequencial dos seguintes elementos: a sigla constante do campo 4.1.4.7 correspondente ao respetivo tipo de documento, seguida da letra M; um espaço; a série do documento manual; o carater "/"; o número do documento manual.

Exemplo: 1-FTM abc/00001.

2.4.6. Um documento retificativo dum documento manual recolhido na aplicação deve referenciar a série e o nº do documento manual e não a identificação única do documento de venda (InvoiceNo) atribuído pela aplicação ao documento recuperado.

2.4.7. Quando, por opção, houver necessidade de integrar outros tipos de documentos manuais, utilizar-se-ão os campos aplicáveis da tabela que os enquadra, procedendo de maneira idêntica à já referida nos números anteriores.

2.5. Integração de documentos através de duplicados que não integram a cópia de segurança (*backup*), quando houver necessidade de reposição de dados por inoperacionalidade do sistema

2.5.1. Quando ocorrer uma situação de erro ou anomalia do programa, devem ser encerradas as séries em utilização e criadas novas, para prosseguir com a emissão de documentos, após a reposição da última cópia de segurança efetuada.

2.5.2. A integração de documentos emitidos e que não constam da cópia de segurança reposta, deve realizar-se no programa certificado, através dos duplicados desses documentos, em série específica anual e com numeração sequencial própria, iniciada no número 1.

2.5.3. Para este efeito será processado um novo documento do mesmo tipo do duplicado que recolha todos os elementos desse documento emitido, com observância dos requisitos definidos nos artigos 6.º e 7.º da Portaria 363/2010.

2.5.4. Os campos aplicáveis relativos à origem do documento, devem ser preenchidos com o valor "M" respetivamente, o campo 4.1.4.2.5. – Origem do documento *(SourceBilling)* e o campo 4.2.3.2.5. –. Origem do documento *(SourceBilling).*

2.5.5. Nestes casos, no campo 4.1.4.4. – Chave de controlo *(HashControl)* ou no campo 4.2.3.4. Chave de controlo *(HashControl)* deve ser aposta a seguinte informação:

2.5.5.1. Número da versão da chave privada (1,2, etc.) e separado por um "-" (hífen);

2.5.5.2. Registo sequencial dos seguintes elementos: a sigla constante do campo 4.1.4.7 ou do campo 4.2.3.7, conforme aplicável e que deve corresponder ao tipo de documento a recuperar através do duplicado, seguida da letra D; um espaço; a série desse documento; o carater "/"; o número desse documento.

Exemplo: 1-FTD 2013A/00099.

2.5.6. Nestas séries de recuperação de dados, a data do documento corresponde à do duplicado do documento. É de todo o interesse que se crie dois campos distintos, de preenchimento obrigatório, sendo um para a identificação da série do duplicado e o outro para recolher o nº do duplicado. Desta forma evitar-se-á lapsos na recolha deste tipo de documentos designadamente da série. Pode-se criar tantas séries, quantas as existentes nos duplicados dos documentos ou apenas uma única.

2.5.7. Quando, por opção, houver necessidade de integrar outros duplicados de documentos, utilizar-se-ão os campos aplicáveis e os procedimentos dos números anteriores.

2.6. Exportação do ficheiro SAF-T(PT)

2.6.1. O ficheiro XML do SAF-T(PT) deverá respeitar a Portaria n.º 321-A/2007 com a estrutura sintática de dados definida na Portaria n.º 160/2013, de 23 de abril e no respetivo ficheiro de estrutura.

2.6.2. Devem constar deste ficheiro todos os elementos dos índices dos campos definidos como obrigatórios das tabelas aplicáveis ao tipo de ficheiro e, todos aqueles que embora não o sejam tenham valores na aplicação.

2.6.3. Deve ser respeitada a regra de assegurar valores únicos para os elementos indicados nas notas técnicas da estrutura de dados, dentro das tabelas respetivas, de modo a manter a integridade do conteúdo do ficheiro XML de SAF-T(PT). Os elementos referidos nas tabelas de documentos comerciais (4.1 a 4.3) devem existir nas respetivas tabelas mestres (2.2 a 2.5).

2.6.4. O utilizador não poderá ter a faculdade de definir quais os tipos de documentos ou a informação a registar na base de dados que são passíveis de exportação para o ficheiro SAF-T(PT).

2.6.5. O ficheiro XML do SAF-T(PT) deverá conter nos campos das tabelas 4.1 a 4.3, dos documentos comerciais *(SourceDocuments)*: relativos à chave do documento *(Hash)*- campos 4.1.4.3; 4.2.3.3 e 4.3.4.3 – e, nos relativos à chave de controlo *(HashControl)* - campos 4.1.4.4; 4.2.3.4 e 4.3.4.4 - de cada estrutura, respetivamente, a assinatura e a versão (números inteiros sequenciais) da chave privada utilizada, ambas gravadas previamente na base de dados quando se desencadeou o processo de emissão do documento.

2.6.6. Os documentos que eventualmente residam na base de dados de determinada solução de gestão mas que foram originalmente criados num outro sistema devem ser objeto de exportação para o SAF-T(PT) com os campos 4.1.4.3., 4.2.3.3 ou 4.3.4.3 – Chave do documento *(Hash)* e 4.1.4.4., 4.2.3.4. ou 4.3.4.4 – Chave de controlo *(HashControl)*, preenchidos nos termos dos pontos 2.3.2 a 2.3.4 e cumulativamente devem também ser

exportados a partir da solução original, com os referidos campos devidamente preenchidos, em conformidade.

2.6.7. Os valores dos campos 4.1.4.19.3., 4.2.3.21.3. e 4.3.4.13.3 – Total do documento com impostos *(GrossTotal)*, devem ser exportados com o mesmo valor que foi considerado na assinatura, isto é, arredondado a duas casas decimais.

3. REQUISITOS A OBSERVAR PELA APLICAÇÃO

3.1. **A aplicação deve possuir:**

3.1.1. Adequados controlos de acessos devendo obrigar o utilizador a alterar a palavra passe (password) no primeiro acesso (a nova palavra passe não pode ser vazia e o administrador não a pode conhecer ou visualizar). O administrador poderá despoletar o processo de criação de uma nova password, a qual deve ser também alterada, logo que acedida.

3.1.2. Implementada uma política de cópias de segurança de periodicidade obrigatória de forma a minimizar o volume de dados a recuperar em caso de corrupção da base de dados e/ou a manutenção de duas ou mais base de dados simultâneas para que quando uma se corrompa a(s) outra(s) assegure(m) a continuidade da facturação.

3.1.3. Controlo direto ou indireto da base de dados que utiliza e o registo do n.º de reposições de cópias de segurança (*backup*) efetuadas.

3.2. **A aplicação deve assegurar:**

3.2.1. A sequenciação da numeração comparativamente à evolução da data e hora de emissão dos documentos;

3.2.2. A garantia de que não existe mais de que um documento activo (com os campos 4.1.4.2.1., 4.2.3.2.1, ou 4.3.4.2.1 relativos ao estado atual do documento de valor “N”) proveniente da recolha do mesmo documento manual;

3.2.3. O cumprimento dos requisitos elencados no n.º 1 do artigo 9.º da portaria n.º 363/2010, de 23 de junho, quando emite qualquer documento de conferência da prestação de serviços.

3.3. **A aplicação não pode permitir:**

3.3.1. Ser o utilizador a definir quais os tipos de documentos que são assinados e/ou exportáveis para o SAF-T(PT), especialmente, os que foram criados ou modificados por aquele.

3.3.2. O processamento de qualquer cálculo sobre documentos recolhidos ou resultantes de integração de outros sistemas. Assim, se porventura, existir uma incorrecta determinação de imposto, esse erro deve ser evidenciado na base de dados integradora, por resultar de um documento já entregue.

3.3.3. A alteração do NIF, numa ficha de cliente já existente e com documentos emitidos. Só pode permitir a alteração da denominação e da morada desse cliente, se tal vier a acontecer, pois o NIF manter-se-á nesses casos.

3.3.4. A alteração do nome e da morada numa ficha de cliente já existente e com documentos emitidos, mas cujo NIF não foi fornecido (neste âmbito não é considerado o NIF do cliente genérico 999999990), Neste caso poderá ser averbado o NIF em falta e após esse averbamento actuar de acordo com o ponto anterior.

3.3.5. A alteração numa ficha de produto já existente e com documentos emitidos, do campo 2.4.4. – Descrição do produto ou serviço *(ProductDescription)*.

3.3.6. A criação de notas de crédito relativas a documentos anteriormente anulados ou já totalmente retificados.

3.3.7. A anulação de documentos sobre os quais já tenha sido emitido documento retificativo (nota de crédito ou débito) ainda que parcial.

3.3.8. A aceitação de devoluções em documentos de venda ou transmissões em documentos de retificação.

3.4. **A aplicação deve alertar o utilizador:**

3.4.1. Se algum dos campos obrigatórios do SAF-T(PT) não for preenchido pelo utilizador, aquando do processamento de documentos.

Por exemplo: Os dados mestres das fichas de cliente, de fornecedor, de produtos, de tipo e taxas de imposto, ou a indicação do motivo de isenção de imposto.

3.4.2. Quando a emissão do documento possuir data posterior à actual, ou esta é superior à data do sistema. Nesse caso, após essa emissão, não poderá ser emitido um novo documento com a data actual ou anterior, dentro da mesma série.

3.4.3. Caso a data e hora de sistema seja inferior à do último documento emitido (por vezes por questões de manutenção ou quando existe mudanças de mês ou ano estes lapsos sucedem), deve ser pedida a confirmação, antes da emissão, de que a data e hora de sistema se encontra correcta. Esta validação deve ser feita utilizando a data/hora do SystemEntryDate de qualquer tipo de documento emitido, independentemente da sua série.

4. REQUISITOS TÉCNICOS RELATIVOS AO SISTEMA DE IDENTIFICAÇÃO A QUE SE REFERE A ALÍNEA B) DO N.º 3 DA PORTARIA N.º 363/2010, DE 23 DE JUNHO

4.1. Deve ser utilizado o algoritmo RSA (algoritmo de critografia de dados que usa o sistema de chaves assimétricas, chave pública e chave privada).

4.2. A chave pública a fornecer juntamente com a declaração modelo 24 deve resultar da sua extração a partir da chave privada, em formato PEM – base 64 e deve ser criado o respetivo ficheiro com a extensão".txt".

4.3. 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.

4.4. O texto a assinar relativo ao documento deverá conter os dados concatenados no formato indicado nas notas técnicas para cada campo, separados por ";" (Ponto e vírgula).

4.5. **Os documentos emitidos e englobados na tabela 4.1 – Documentos comerciais a clientes (*SalesInvoices)*** referidos no campo 4.1.4.7 – Tipo de documento (InvoiceType), devem utilizar a informação referida no artigo 6.º da Portaria n.º 363/2010, de 23 de Junho, conforme é exemplificado na tabela seguinte:

Campo do SAF-T(PT)	Formato	Dados Exemplo
a) 4.1.4.6 - **InvoiceDate**	AAAA-MM-DD	2013-07-01
b) 4.1.4.11 - **SystemEntryDate**	AAAA-MM-DDTHH:MM:SS	2013-07-01T11:27:08
c) 4.1.4.1 - **InvoiceNo**	Composto pelo código interno do documento, seguido de um espaço, seguido do identificador da série do documento (obrigatória), seguido de uma barra (/) e de um número sequencial do documento dentro da série. **[^]+ [^ / ^]+ / [0-9]+**	FS 001/0009
d) 4.1.4.19.3 - **GrossTotal**	Campo numérico com duas casas decimais, separador decimal "." (ponto) e sem nenhum separador de milhares.	200.00
4.1.4.3 - **Hash** Campo do documento anterior na mesma série, *(**vazio** quando se tratar do primeiro documento da série ou do exercício*)	Base-64	mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/J8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJ9G6nI=

4.6. **Exemplo da mensagem a assinar para os dados anteriores:**

2013-07-01;2013-07-01T11:27:08;FS 001/0009;200.00;mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJG6nI=

4.7. **Os documentos emitidos e englobados na tabela 4.2 – Documentos de movimentação de mercadorias *(MovementOfGoods)*** referidos no campo 4.2.3.7 – Tipo de documento *(MovementType)*, devem utilizar a informação referida na alínea a) do n.º 2 do artigo 7.º da Portaria n.º 363/2010, de 23 de Junho, conforme é exemplificado na tabela seguinte:

Campo do SAF-T(PT)	Formato	Dados Exemplo
a) 4.2.3.6 - **MovementDate**	AAAA-MM-DD	2013-07-02
b) 4.2.3.8 - **SystemEntryDate**	AAAA-MM-DDTHH:MM:SS	2013-07-02T09:37:25
c) 4.2.3.1 - **DocumentNumber**	Composto pelo código interno do documento, seguido de um espaço, seguido do identificador da série do documento (obrigatória), seguido de uma barra (/) e de um número sequencial do documento dentro da série. **[^]+ [^ / ^]+ / [0-9]+**	GR ABC/00021
d) 4.2.3.21.3 - **GrossTotal**	Campo numérico com duas casas decimais, separador decimal "." (ponto) e sem nenhum separador de milhares. Nos casos, como o presente, de não ser valorizado o documento, este campo deve ser preenchido com "0.00" (sem aspas).	0.00
e) 4.2.3.3 - **Hash** Campo do documento anterior na mesma série, *(**vazio** quando se tratar do primeiro documento da série ou do exercício*)	Base-64	mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/J8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJ9G6nI=

4.8. **Exemplo da mensagem a assinar para os dados anteriores:**

2013-07-02;2013-07-02T09:37:25;GR ABC/00021;0.00;mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJG6nI=

4.9. **Os documentos emitidos e englobados na tabela 4.3 – Documentos de conferência de entrega de mercadorias ou da prestação de serviços *(WorkingDocuments)*** referidos no campo 4.3.4.7 – Tipo de documento *(WorkType)*, devem utilizar a informação referida na alínea b) do n.º 2 do artigo 7.º da Portaria n.º 363/2010, de 23 de junho, conforme é exemplificado na tabela seguinte:

Campo do SAF-T(PT)	Formato	Dados Exemplo
a) 4.3.4.6 - **WorktDate**	AAAA-MM-DD	2013-07-03
b) 4.3.4.10 - **SystemEntryDate**	AAAA-MM-DDTHH:MM:SS	2013-07-03T14:25:00
c) 4.3.4.1 - **DocumentNumber**	Composto pelo código interno do documento, seguido de um espaço, seguido do identificador da série do documento (obrigatória), seguido de uma barra (/) e de um número sequencial do documento dentro da série. **[^]+ [^/^]+/[0-9]+**	RC 005/001
d) 4.3.4.13.3 - **GrossTotal**	Campo numérico com duas casas decimais, separador decimal "." (ponto) e sem nenhum separador de milhares.	1500.00
e) 4.3.4.3 - **Hash** Campo do documento anterior na mesma série, *(**vazio** quando se tratar do primeiro documento da série ou do exercício*)	Base-64	mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/J8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJ9G6nI=

4.10. **Exemplo da mensagem a assinar para os dados anteriores:**

2013-07-03;2013-07-03T14:25:00;RC 005/001;1500.00;mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJG6nI=

5. CRIAÇÃO DO PAR DE CHAVES PRIVADA / PÚBLICA

Para exemplificar a criação do par de chaves RSA, foi utilizada a aplicação OpenSSL, que é executada diretamente na linha de comandos com argumentos (Windows / Linux, entre outros), e pode ser obtida em www.openssl.org.

Permite, entre outras funcionalidades, criar chaves RSA, DH e DSA, criar certificados X.509, CSRs e CRLs, assinar digitalmente, criptografar e decriptografar, etc.

Na análise dos exemplos apresentados, deve ter-se em conta que:

a) São meramente ilustrativos, não significando de maneira alguma que o produtor de software tenha ou deva utilizar a aplicação OpenSSL;

b) As linhas de comando respetivas foram preparadas e ensaiadas quer com base em Linux quer em Windows, tendo-se obtido o mesmo resultado final;

c) A utilização do comando ECHO, aplicado na linha de comandos do WIndows/Dos, pode apresentar resultados diferentes dos obtidos em Linux, pelo que não deverá ser utilizado para efeitos de testes;

d) São realizados com o formato PEM.

5.1. Para criar a chave privada

Basta executar o comando OpenSSL com os seguintes argumentos:

openssl genrsa -out ChavePrivada.pem 1024

Onde " ChavePrivada.pem" é o nome do ficheiro que irá conter a chave privada e "1024" é o tamanho em bits.

Como resultado foi obtida, neste caso, a informação de que se apresenta uma parte:

-----BEGIN RSA PRIVATE KEY-----

MIICXQIBAAKBgQCjgbQG27+lNWKdW5SXLFzFgqZu+xFWTkx0Woloo6z1gD5DhllRgQ
5hxitOW0QV1LAGlHVMfZ8PDk9e+N4YJ7cDwW4D+iflyCAEvi4xvKejEGVEInEsnA7act
mg9ORORMHXKqy7mA41P//…..

-----END RSA PRIVATE KEY-----

5.2. Para criar a chave pública com base na chave privada anterior

Basta executar o comando OpenSSL com os seguintes argumentos:

openssl rsa -in ChavePrivada.pem -out ChavePublica.pem -outform PEM –pubout

Onde "ChavePublica.pem" é o ficheiro que contêm a chave pública.

Para fazer o upload da mesma juntamente com a Declaração Mod. 24, basta renomear a sua extensão de ".pem" para ".txt" (sem as aspas).

Como resultado foi obtida, neste caso, a informação seguinte de que se apresenta uma parte:

-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCjgbQG27+lNWKdW5SXLFzFgqZu+xFWTkx0Woloo6z1gD5DhllRgQ5hxitOW0QV1LAGlHVMfZ8PDk9e+N4YJ7cDwW4D+iflyCAEvi4xvKejEGVEInEsnA7actmg9ORO .....

-----END PUBLIC KEY-----

5.3. **Para verificar a chave pública**

Basta executar o comando OpenSSL com os seguintes argumentos:

openssl rsa -in ChavePublica.pem -noout -text -pubin

6. CRIAÇÃO DO CERTIFICADO

6.1. O par de chaves utilizado não requer a emissão de um certificado por parte de uma entidade credenciada. O produtor de software poderá gerar o certificado auto-assinado para efeito da certificação e dele extrair a chave pública para fornecer à AT, com a extensão txt.

6.2. Para a criação do certificado a partir da chave privada, o algoritmo RSA deverá ser utilizado com as seguintes especificações nos parâmetros:

- Formato = x.509
- Charset = UTF-8
- Encoding = Base-64
- Endianess = Little Endian
- OAEP Padding = PKCS1 v1.5 padding
- Tamanho da chave privada = 1024 bits
- Formato do Hash da mensagem = SHA-1

7. EXEMPLO PRÁTICO DE APLICAÇÃO DO MECANISMO DE ASSINATURA A DOCUMENTOS ENGLOBADOS NA TABELA 4.1 – DOCUMENTOS COMERCIAIS A CLIENTES (SALESINVOICES)

7.1. **Criação da ASSINATURA DIGITAL com a chave privada.**

Independentemente da implementação do RSA que for adotada e que melhor se adeque a cada solução, deve ser garantido que as assinaturas contêm 172 bytes, sem quaisquer carateres separadores de linhas.

CAMPOS DO SAF-T(PT)	REGISTO 1	REGISTO 2
4.1.4.6 - InvoiceDate	18-05-2010	18-05-2010
4.1.4.11 - SystemEntryDate	2010-05-18T11:22:19	2010-05-18T15:43:25
4.1.4.1 - InvoiceNo	FAC 001/14	FAC 001/15
4.1.4.19.3 - GrossTotal	3.12	25.62
4.1.4.3 - Hash	Ver 1º registo	Ver 2º registo

Os elementos a assinar (InvoiceDate, SystemEntryDate, InvoiceNo, GrossTotal e Hash) devem ser concatenados apenas com o separador ";" entre cada um dos campos, não devendo conter aspas nem qualquer caráter de fim de linha, quando objeto de encriptação, com vista à obtenção da assinatura.

1º Registo

Tratando-se do primeiro registo, o campo 4.1.4.3 – Hash é preenchido com o hash resultante da aplicação da chave privada anteriormente criada, para assinar digitalmente os campos (InvoiceDate, SystemEntryDate, InvoiceNo e GrossTotal).

O texto a assinar será:

2010-05-18;2010-05-18T11:22:19;FAC 001/14;3.12;

1º Passo:

Guardar a mensagem a assinar

2010-05-18;2010-05-18T11:22:19;FAC 001/14;3.12;

Num ficheiro de texto (que neste exemplo designaremos Registo1.txt), certificando-se que no fim da mensagem não fica qualquer quebra de linha, apenas o ";" sem aspas.

2º Passo:

Assinar a mensagem contida no ficheiro Registo1.txt com o seguinte comando:

openssl dgst -sha1 -sign ChavePrivada.pem -out Registo1.sha1 Registo1.txt

O ficheiro Registo1.sha1 conterá o hash em binário gerado pela aplicação OpenSSL.

3º Passo:

Seguidamente é necessário efetuar o encoding para base 64 do ficheiro Registo1.sha1:

openssl enc -base64 -in Registo1.sha1 -out Registo1.b64 -A

O ficheiro designado por Registo1.b64 é que contém os 172 carateres em ASCII da assinatura que deverão ser transportados para a base de dados e mais tarde exportados para o campo 4.1.4.3 Hash do SAF-T(PT).

O parâmetro –A serve apenas para a aplicação OpenSSL gerar a assinatura numa única linha evitando as quebras de linha adicionais.

Como resultado o ficheiro Registo1.b64conterá a seguinte assinatura:

oso2FoOw4V941CwKTrv6xwzUrOtxBWCwU0yLVAqKwf0CNKZHMETG1XZZC4spRSyby1uDX Bggplogrl8gHnvevA00UEoAvGJo9Fa3DOA0MhZNDa9/rNvu71pp+0zHmN2ra5lWpiHcgmUYxm 5qamLBk49rkgvl7h1myKCYBKqgu60=

A qual deverá ficar registada no campo HASH da tabela anterior e na posição correspondente ao 1º Registo.

2º Registo

Procedendo de forma idêntica, agora com os dados do 2º registo e o hash do registo anterior teríamos como mensagem a assinar no ficheiro Registo2.txt:

2010-05-18;2010-05-18T15:43:25;FAC 001/15;25.62;oso2FoOw4V941CwKTrv6xwzUrOtxBWCwU0yLVAqKwf0CNKZHMETG1X ZZC4spRSyby1uDXBggplogrl8gHnvevA00UEoAvGJo9Fa3DOA0MhZNDa9/rNvu71pp+0 zHmN2ra5lWpiHcgmUYxm5qamLBk49rkgvl7h1myKCYBKqgu60=

Utilizando os procedimentos acima descritos para o 1º registo, passos 1 a 3, criaram-se os ficheiros Registo2.sha1 e Registo2.b64.

Como resultado, este último ficheiro, Registo2.b64 irá conter a assinatura digital do 2º registo:

Y2ogVAC9rcmm9hilZCGGrxjpkZP9NHn5shhp9phBIVWln+Ta2zKf+O+05brA6VU0LULtMQP98 P29q+vcSwVtxSzLDbmmkHMt4l6nQmh91QaOJwPpz2uMqtR3aMkWYPK4Ntc/yfnXpY1cSeUG bQkqAsJOFSidRE4+DibJaC7WMpw=

A qual deverá ficar registada no campo 4.1.4.3 – Hash da tabela anterior e na posição correspondente ao 2º Registo.

7.2. Validação da assinatura digital criada

Para confirmar a validade das assinaturas basta executar o comando:

openssl dgst -sha1 -verify chavepublica.pem -signature registo1.sha1 registo1.txt

8. EFEITOS REVOGATÓRIOS

É revogado o oficio circulado n.º 50000/2012, de 26 de janeiro.

Autoridade Tributária e Aduaneira, em 4 de julho de 2013

O Subdiretor-Geral

(João Ribeiro Elias Durão)