

# MINISTÉRIO DAS FINANÇAS

Despacho n.º 8632/2014, de 3 de Julho

Para cumprimento da alínea e) do artigo 3.º da Portaria n.º 363/2010, de 23 de junho, os programas de faturação e equiparados, ainda que já certificados, adiante designados apenas por programas de faturação, devem observar os seguintes requisitos técnicos.

## **1 - Criação dos documentos emitidos pelos programas de faturação**

1.1 - Os programas informáticos de faturação devem assinar quaisquer documentos emitidos com eficácia externa, com exceção dos recibos, nos termos dos artigos 6.º e 7.º da Portaria n.º 363/2010, de 23 de junho, nomeadamente:

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 documentos que não sejam faturas ou documentos retificativos de fatura, devem conter de forma evidente a sua natureza e, se suscetíveis de apresentação ao cliente, incluindo os que devam constar nas tabelas 4.2, 4.3 e 4.4 do SAF-T (PT), conter a expressão "Este documento não serve de fatura".

1.3 - As faturas, documentos de movimentação de mercadorias, documentos de conferência de entrega de mercadorias ou de prestação de serviços suscetíveis de apresentação ao cliente, que tiveram origem noutros documentos emitidos, designadamente, faturas, guias de movimentação de mercadorias, consultas de mesa ou outros documentos suscetíveis de apresentação ao cliente, devem conter a identificação desses documentos, na estrutura Referência ao documento de origem (OrderReferences) das tabelas 4.1 a 4.3, consoante o caso.

1.4 - Os documentos retificativos de fatura devem conter a identificação do(s) documento(s) retificado(s) na estrutura Referências a faturas (References) da tabela 4.1.

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, identificados através das respetivas designações, deverão ser emitidos cronologicamente em uma ou mais séries, convenientemente referenciadas, de acordo com as necessidades comerciais, devendo ser datados e numerados de forma progressiva e contínua, dentro de cada série, por um período não

inferior a um ano fiscal, sem prejuízo de poderem ser utilizadas por períodos superiores desde que utilizadas até ao final do exercício fiscal que entretanto tenha sido iniciado.

1.7 - Na identificação dos documentos, não devem ser utilizados caracteres que violem o esquema de validação ou possam ser interpretados como operadores de XML. 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.

1.8 - O código identificador da(s) série(s) deve ser específico de cada um dos estabelecimentos e ou programa(s), e nunca pode ser repetido no mesmo contribuinte, para o mesmo tipo de documento, de modo a identificar univocamente cada documento emitido, mesmo que os documentos sejam emitidos por mais do que um programa de faturação.

1.9 - Se por uma questão técnica ou operacional, a utilização de uma série for descontinuada, a aplicação deve inibir a sua utilização, não podendo, de forma alguma, apagar qualquer informação relativa à mesma.

1.10 - 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.

1.11 - 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.º e 7.º da Portaria n.º 363/2010, de 23 de junho.

## **2 - Processo de identificação (assinatura) dos documentos e subsequente gravação nas bases de dados**

2.1 - Processo de assinatura para 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 integral 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 - Em regra, os documentos são assinados tendo em consideração o Hash do último documento emitido da mesma série/tipo. No caso da gravação de um primeiro documento de uma série/tipo de documento de faturação, o campo aplicável Chave do documento (Hash) das tabelas 4.1 a 4.3, deve ser assumido como não preenchido. No caso de utilização de séries plurianuais, no início de cada exercício, o primeiro documento poderá ser assinado tendo em consideração o Hash do último documento emitido da mesma série/tipo, no exercício fiscal anterior.

2.1.6 - O valor a considerar nos campos Total do documento com impostos (GrossTotal) das tabelas 4.2 e 4.3, para a assinatura dos documentos de movimentação de mercadorias ou documentos de conferência é o que constar na base de dados, independentemente do modelo utilizado na sua impressão, valorado ou não. Na ausência de valor na base de dados, o referido campo 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 caracteres da assinatura [campos Chave do documento (Hash) das tabelas subordinadas da tabela 4 - Documentos comerciais (SourceDocuments) do SAF-T(PT)] correspondentes às posições 1.ª, 11.ª,

21.ª, e 31.ª 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.º 0000/AT" (sem aspas), de acordo com as alíneas a) e b) do n.º 3 do artigo 6.º da Portaria n.º 363/2010, de 23 de junho.

2.2.3 - Qualquer documento emitido pela aplicação certificada, impresso ou enviado por via eletrónica, não suscetível de ser assinado nos termos do ponto 2.1, nomeadamente os recibos, deve conter impressos obrigatoriamente a expressão - Emitido por programa certificado n.º «Número do certificado atribuído pela AT»/AT. Exemplo: "Emitido por programa certificado n.º 0000/AT" (sem aspas)

2.2.4 - Os documentos referidos no ponto 1 deverão na sua impressão conter a data no formato "AAAA-MM-DD" ou "DD-MM-AAAA" (sem aspas) e, de acordo com a alínea c) do n.º 3 do artigo 6.º da Portaria n.º 363/2010, de 23 de junho, o código interno do tipo do documento atribuído pela aplicação, a série a que o documento pertence e a numeração sequencial própria, exclusivamente numérica.

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

2.2.6 - 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 n.º 7 do artigo 29.º do CIVA), como documentos de correção de operações de compra e venda, cuja forma, conteúdo e finalidade devem ser respeitados. Os valores negativos apenas poderão ser impressos nos casos de anulação de registos que já integram o documento ou para acerto de estimativas nas prestações de serviços continuadas. O valor negativo nunca poderá ser superior ao valor positivo da mesma rubrica ou serviço em cada fatura. Caso o acerto, por rubrica, seja superior ao valor positivo, estamos perante uma regularização que obriga a emissão da respetiva nota de crédito.

2.2.7 - A menção de franquias, valores de garantia ou retenções na fonte devem constar de campos próprios, desenvolvidos para o efeito na aplicação informática, cuja descrição não seja passível de modificação. Estes montantes não terão qualquer influência nos totais do documento emitido devendo ser referidos após o apuramento do total do documento com impostos (campo GrossTotal das tabelas 4.1 a 4.4). Em circunstância alguma podem ser criados tipos de produto ou serviços ou utilizar a tabela de produtos/serviços (Product) para este fim.

2.2.8 - 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.

2.2.9 - Os documentos criados pelo procedimento indicado no ponto 2.4. deverão conter, quando impressos, a expressão - "Cópia do documento original" e separada por hífen os elementos referidos no ponto 2.4.5.2, com exceção do elemento relativo ao HashControl.

Exemplo: Cópia do documento original - FTM abc/00001

2.2.10 - Os documentos criados pelo procedimento indicado no ponto 2.5., deverão conter, quando impressos, a expressão - "Cópia do documento original" e separada por hífen os elementos referidos no ponto 2.5.5.2, com exceção do elemento relativo ao HashControl.

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

2.2.11 - Os documentos referidos no ponto 1, quando na sua impressão resultar mais do que uma página, devem exibir em todas elas a designação do tipo de documento, a respetiva numeração de acordo com o ponto 2.2.4., os valores acumulados (transportados e a transportar), o respetivo n.º de página e o n.º total de páginas. Os apuramentos globais de base tributável, apuramento de impostos e total do documento, quando existirem, devem constar exclusivamente na última página.

2.2.12 - A aplicação deve garantir a legibilidade na impressão do conteúdo do n.º 3 do artigo 6.º da Portaria n.º 363/2010, de 23 de junho. Por exemplo, estes elementos não devem ser colocados na 1.ª ou última linha ou junto aos limites do documento, de modo a evitar que não sejam impressos por qualquer anomalia da impressora ou na definição da área de impressão.

2.2.13 - Se para a impressão dos documentos referidos no ponto 1 for utilizado papel pré-impresso, a aplicação deve assegurar a impressão de todos os elementos fiscalmente relevantes incluindo as menções obrigatórias, os elementos identificativos do sujeito passivo emitente e a natureza do documento. Não se inclui neste contexto a impressão de logótipos.

2.2.14 - A impressão dos documentos em que a transmissão de bens ou prestação de serviços se encontrem isentos de imposto, deve exibir a expressão legalmente prevista que confere a isenção ou, na sua ausência, o normativo legal aplicável. Caso não conste o motivo de isenção na linha respetiva, deverá utilizar um qualquer tipo de referência que possibilite a associação da linha isenta ao respetivo motivo. O mesmo é válido para associar qualquer taxa de imposto ao respetivo produto/serviço.

2.2.15 - A impressão de uma 2.ª via de um documento deve preservar o seu conteúdo original, ainda que deva conter qualquer expressão que indique não se tratar de um original. Assim, por exemplo, se o domicílio ou denominação de um cliente for alterado na base de dados, a reimpressão de um documento deve respeitar os domicílio e denominação originais.

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.

Nestes termos, a aplicação integradora não deve processar qualquer recálculo ou modificação do conteúdo dos documentos integrados provindos de outros sistemas, respeitando inclusive a identificação única dos documentos (InvoiceNo, DocumentNumber ou PaymentRefNo), com exceção do mencionado nos pontos seguintes.

2.3.2 - A assinatura referida no ponto 2.1. é, neste caso, da responsabilidade das soluções originais (soluções integradas).

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, na séries/tipos de documentos originais, 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 ao campo Chave do documento (Hash) igual à que foi gerada no sistema emissor, nas correspondentes tabelas 4.1 a 4.3 em que é integrado o documento, Isto é, devem ser iguais, no sistema integrador e integrado;
- c) Preencher os campos Origem do documento (SourceBilling) das tabelas 4.1 a 4.3, consoante o caso, com o valor "I" (sem aspas);
- d) Preencher o campo Chave de controlo (HashControl), das tabelas 4.1 a 4.3, 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 Chave de controlo (HashControl) das tabelas 4.1 a 4.3, 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 Chave do documento (Hash) das mencionadas tabelas 4.1 a 4.3;

Exemplo: "9999.1" (sem aspas), 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) das tabelas 4.1 a 4.3, aplicável ao tipo de informação, 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 documentos processados manualmente em impressos emitidos em tipografias autorizadas, nos casos de inoperacionalidade do programa:

2.4.1 - A integração de faturas ou outros documentos rectificativos e documentos de transporte, processados manualmente deve realizar-se no programa certificado em série específica, de periodicidade anual ou superior e com numeração sequencial própria, iniciada no n.º 1.

2.4.2 - Para este efeito será processado um novo documento do mesmo tipo, que recolha todos os elementos do documento manual emitido, com observância dos requisitos definidos no artigo 6.º da Portaria 363/2010, isto é, deve assinar o documento e imprimir a respetiva expressão das alíneas a) e b) do n.º 3 do mesmo artigo.

2.4.3 - Nas séries de recuperação, a data do documento corresponde à data do documento manual sendo de todo o interesse que se criem campos distintos, de preenchimento obrigatório, um para acolher a identificação da série manual e o outro para o número manual, por forma a obviar 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 Origem do documento (SourceBilling) das tabelas 4.1 e 4.2, consoante o caso, com o valor "M" (sem aspas).

2.4.5 - Nestes casos, no campo Chave de controlo (HashControl) das tabelas 4.1 e 4.2, consoante o caso, 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 Tipo do documento (InvoiceType ou MovementType), 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, sendo "abc/00001" a série/número do documento manual.

2.4.6 - Para referenciar um documento manual recolhido na aplicação, deve ser utilizada a série e o n.º do documento manual original, e não a identificação única do documento (InvoiceNo ou DocumentNumber) atribuído pela aplicação ao documento recuperado. (Exemplo: A emissão de uma nota de crédito deve referenciar o número da fatura original, emitida de modo manual.)

2.4.7 - Quando, 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 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 n.º 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 - O campo Origem do documento (SourceBilling) das tabelas 4.1 a 4.2, consoante o caso, deve ser preenchido com o valor "M" (sem aspas).

2.5.5 - Nestes casos, no campo Chave de controlo (HashControl) das tabelas 4.1 e 4.2, consoante o caso, 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 Tipo do documento (InvoiceType ou MovementType conforme aplicável), que deve corresponder ao tipo de documento a recuperar através do duplicado, seguida da letra D; um espaço e a identificação única do documento (InvoiceNo ou DocumentNumber, consoante o caso).

Exemplo: 1-FTD XY 2013A/00099, sendo "XY 2013A/00099" a identificação única do documento integrado.

2.5.6 - Nas séries de recuperação de dados, a data do documento corresponde à do duplicado do documento. É de todo o interesse que se criem campos distintos, de preenchimento obrigatório, para acolher o código interno do tipo de documento, série e n.º do duplicado por forma a evitar lapsos na recolha deste tipo de documentos, designadamente, do código interno do tipo de documento e da série. Poder-se-ão criar tantas séries, quantas as existentes nos duplicados dos documentos, ou apenas uma série única.

2.5.7 - Para referenciar um documento original recolhido na aplicação, deve ser utilizado o código interno do tipo de documento, a série e o n.º do documento original, e não a identificação única do documento (InvoiceNo ou DocumentNumber) atribuído pela aplicação ao documento recuperado.

2.5.8 - Quando, houver necessidade de integrar outros duplicados de outros tipos 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 em vigor e no respetivo esquema de validação.

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), devendo este desiderato ser assegurado pela aplicação informática.

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) e nos relativos à Chave de controlo (HashControl) 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 Chave do documento (Hash) e Chave de controlo (HashControl) das respetivas tabelas 4.1 a 4.3, 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 Total do documento com impostos (GrossTotal) das tabelas 4.1 a 4.3, devem ser exportados com o mesmo valor que foi considerado na assinatura, isto é, arredondado a duas casas decimais.

### **3 - Outros requisitos a observar pela aplicação**

3.1 - A aplicação deve:

3.1.1 - Possuir adequados controlos de acessos, devendo obrigar o utilizador a alterar a palavra passe (password) no primeiro acesso e, posteriormente, sempre que houver necessidade. 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 palavra passe, a qual deve ser também alterada, logo que acedida.

3.1.2 - Ter 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 faturação.

3.1.3 - Controlar direta ou indiretamente a base de dados que utiliza e o registo do n.º de reposições de cópias de segurança (backup) efetuadas, por exemplo, através de sistemas de controlo que validem a base de dados no fecho e arranque da aplicação, de forma a evidenciar eventuais manipulações ou alterações de dados na base de dados, por outra via que não a aplicacional.

3.1.4 - Proteger de forma eficaz a chave privada, incluindo durante o processo de assinatura dos documentos.

3.2 - A aplicação deve assegurar:

3.2.1 - A sequenciação da numeração em função da evolução da data e hora de emissão dos documentos.

3.2.2 - A garantia de que não existe mais de que um documento ativo (com os campos Estado atual do documento - InvoiceStatus, MovementStatus, WorkStatus ou

PaymentStatus - de valor "N") proveniente da recolha do mesmo documento manual ou do procedimento mencionado no ponto 2.5.

3.2.3 - A utilização, para efeito de cálculos, de valor com mais do que 2 casas decimais para evitar erros de arredondamento, motivados por descontos, preços unitários inferiores ao cêntimo, quantidades fracionadas, taxas de câmbio ou pela emissão de documentos em que o preço tem o imposto incluído.

3.2.4 - Nas soluções de mobilidade, a numeração sequencial, bem como a informação relativa à assinatura dos últimos documentos emitidos por série, após estas terem exportado os dados para a aplicação de integração.

3.2.5 - 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.

3.2.6 - A exigibilidade ao utilizador do motivo do não apuramento do imposto, quando tal se verificar.

3.2.7 - O controlo de emissão de notas de crédito parciais, face às quantidades e valores das respetivas faturas a retificar.

3.2.8 - Que os descontos, quando existam, devem situar-se no intervalo entre 0 e 100 %.

3.2.9 - Que a parametrização e desenho dos formulários de impressão dos documentos seja efetuada pelo produtor de software ou, caso seja facultado ao utilizador a possibilidade de criação de novos tipos de documentos, estes sejam validados pelo produtor de software, por exemplo, através de assinatura digital. Em circunstância alguma podem ser utilizados formulários sem a referida validação e respeito pelo descrito no ponto

3.3.1.

3.2.10 - A manutenção da informação relativa a todos os documentos emitidos no seu repositório de dados, nomeadamente os constantes das tabelas existentes na estrutura 4. - Documentos comerciais (SourceDocuments) do ficheiro SAF-T (PT). Deve possuir mecanismos de controlo que, quando atingido o limite da capacidade da base de dados ou do suporte físico da mesma, forcem a produção externa de cópias de arquivo, por forma a garantir a capacidade de exportação do SAF-T (PT) com os requisitos da portaria da certificação e o cumprimento do prazo estabelecido no n.º 1 do artigo 52.º do CIVA.

3.2.11 - Que as telas de visualização (écran) para introdução e exportação de dados, consulta e demais funcionalidades postas ao dispor dos utilizadores, independentemente do seu nível de acesso à aplicação informática, sejam exibidas em língua portuguesa, sem prejuízo de poderem ser multilingues ou que seja assegurada a sua tradução.

3.2.12 - O averbamento da data em que os bens foram colocados à disposição do adquirente ou em que os serviços foram prestados, por forma a permitir o correto preenchimento do campo TaxPointDate.

3.3 - A aplicação não pode permitir:

3.3.1 - Ao utilizador 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. Por exemplo, se existir uma incorreta 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. Apenas poderá ser averbado o NIF em falta, no caso de o campo não estar preenchido, ou estar preenchido com o NIF do cliente genérico "999999990".

3.3.4 - A alteração do nome numa ficha de cliente já existente e com documentos emitidos, mas cujo NIF não foi fornecido. Esta limitação cessa, quando na ficha do cliente for averbado o respetivo NIF.

3.3.5 - A alteração numa ficha de produto já existente e com documentos emitidos, do campo Descrição do produto ou serviço (ProductDescription) constante na tabela 2.4.

3.3.6 - A reutilização de códigos de utilizador (SourceID) após o respetivo utilizador ter procedido à realização de movimentos fiscalmente relevantes.

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

3.3.8 - A anulação de documentos sobre os quais já tenha sido emitido documento retificativo (nota de crédito ou débito) ainda que parcial, sem a prévia anulação do respetivo documento retificativo.

3.3.9 - 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 atual, ou esta é superior à data do sistema. Nesse caso, após essa emissão, não poderá ser emitido um novo documento com a data atual ou anterior, dentro da mesma série.

3.4.3 - Caso a data e hora de sistema seja inferior à do último documento emitido, deve ser pedida a confirmação, antes da emissão, de que a data e hora de sistema se encontra

correta. 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 artigo 3.º da Portaria n.º 363/2010, de 23 de junho**

4.1 - Deve ser utilizado o algoritmo RSA (algoritmo de criptografia 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 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:

(ver documento original)

4.6 - Exemplo da mensagem a assinar para os dados anteriores:

```
2013-07-01;2013-07-01T11:27:08;  
FS001/0009;200.00;mYJEV4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmWmH  
mmGYusfflJjTdsITLX+uujTwzqmL/U5nvt6S9s8iJN3LwkJXsiEpt099e1MET/  
8y3+Y1bn+K+YPJQiVm1QS0fXETSOPo8SwUZdBALt0Vto1VhUZKejACcjEYJG6n1=
```

4.7 - Os documentos emitidos e englobados na tabela 4.2 - Documentos de movimentação de mercadorias (MovementOfGoods) referidos no campo 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:

(ver documento original)

4.8 - Exemplo da mensagem a assinar para os dados anteriores:

```
2013-07-02;2013-07-02T09:37:25;  
GR  
ABC/00021;0.00;mYJEV4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmWmH  
mmGYusfflJjTdsITLX+uujTwzqmL/U5nvt6S9s8iJN3LwkJX  
siEpt099e1MET/8y3+Y1bn+K+YPJQiVm1QS  
0fXETSOPo8SwUZdBA Lt0Vto1VhUZKejACcjEYJG6n1=
```

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 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:

(ver documento original)

4.10 - Exemplo da mensagem a assinar para os dados anteriores:

```
2013-07-03;2013-07-03T14:25:00;  
RC 005/001;1500.00;mYJEV4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3EHmwMhmmGYusff  
lJjTdSITLX  
+uujTwzqML/U5nvt6S9s8ijN3Lwk  
JXsiEpt099e1MET/8y3+Y1bN+K+YPJQivm1QS0fXETsPo8SwUZd  
BALt0vTo1VhUZKejACcjEYJG6n1=
```

## 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](http://www.openssl.org).

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

4.8 - Exemplo da mensagem a assinar para os dados anteriores:

```
2013-07-02;2013-07-02T09:37:25;GR ABC/00021;0.00;  
mYJEV4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3G EHmwMhmmGYusfflJjT  
dSITLX+uujTwzqML/U5nvt6S9s8ijN3LwkJX siEpt099e1MET/8y3+Y1bN+K+  
YPJQivm1QS0fXETsOPo8SwUZdBA  
Lt0vTo1VhUZKejACcjEYJG6n1=
```

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 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:

(ver documento original)

4.10 - Exemplo da mensagem a assinar para os dados anteriores:

2013-07-03;2013-07-03T14:25:00;RC

```
005/001;1500.00;myJEV4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3
EHmwMhmmGYusfflJjTdsITLX+uuJTzwqL/U5nvt6S9s8iJN3Lwk
JXsiEpt099e1MET/8y3+Y1bN+K+YPJQiVm1QS0fXETsPo8SwUZd
BALt0vTo1VhUZKejACcjEYJG6n1=
```

## 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](http://www.openssl.org).

Permite, entre outras funcionalidades, criar chaves RSA, DH e DSA, criar certificados X.509, CSRs e CRLs, assinar digitalmente, criptografar e descriptografar, 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+1NWkdW5SXLfZfgqZu+xFWtkx
0wo1oo6z1gd5Dh11RgQ5hxiTOW0QV1LAG1HVMfZ8Pdk9e+N4YJ
7cDww4D+iFflyCAEvi4xvKejEGVEInEsnA7actmg9OR0rMHXKqy
7mA41P//...
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 contem 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+
1NWkdW5SXLFzFgqZu+xFWTkx0wo1oo6z1gD5Dh11RgQ5hxitow0
QV1LAG1HVMfz8PDK9e+N4YJ7CDww4D+if1yCAEvi4xvKejEG VE
InEsnA7actmg9ORO...
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 e 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 adequa a cada solução deve ser garantido que as assinaturas contêm 172 bytes, sem quaisquer caracteres separadores de linhas.

(ver documento original)

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 carácter de fim de linha, quando objeto de encriptação, com vista à obtenção da assinatura.

## 1.º Registo

Tratando-se do primeiro registo, o campo (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;**

1.º 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.

2.º 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.

3.º 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 caracteres em ASCII da assinatura que deverão ser transportados para a base de dados e mais tarde exportados para o campo (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.b64 conterá a seguinte assinatura:

```
oso2FoOw4V941CwKTrv6xwzUrotxBWCwU0yLVAqKwf0CNKZHM
ETG1XZZC4sprSyby1uDXBggp1ogr18gHnveVA00UEoAVGJo9Fa3DO
A0MhZNDa9/rNvu71pp+0zHmN2ra5IwpiHcgmUYxm5qamLBk49rk
gv17h1myKCYBKqgu60=
```

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

## 2.º Registo

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

```
2010-05-18;2010-05-18T15:25;FAC
```

```
001/15;25.62;oso2FoOw4V941CwKTrv6xwzUrotxBWCwU0yLVAqKwf0CNKZHMETG1XZZC
4sprSyby
1uDXBggp1ogrI8gHnveVA00UE
oAVGJo9Fa3DOA0MhZNDa9/rNvu71pp+0zHmN2ra5IwpiHcgmUY
xm5qamLBk49rkgvI7h1myKCYBKqgu60=
```

Utilizando os procedimentos acima descritos para o 1.º 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 2.º registo:

```
Y2ogvAC9rcmm9hi1zCGGrxjpkZP9NHn5shhp9phBIVwIn+Ta2zKf+
O+05brA6VU0LULtMQP98P29q+vcSwVtxSZLDbmmkHMT4I6nQmh
91Qa0JwPpz2uMqtr3amkwYPK4Ntc/yfnXpY1cSeUGbQkqASJOF
SidRE4+DibJaC7wMpw=
```

A qual deverá ficar registada no campo (Hash) da tabela anterior e na posição correspondente ao 2.º 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 ofício circulado n.º 50001/2013, de 04 de julho.

24 de junho de 2014. - O Diretor-Geral, José A. Azevedo Pereira.