

Of.Circulado N.º: 50 000/2012

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.

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 pela Portaria n.º 22-A/2012, de 24 de janeiro, os 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 meu despacho de 26 de janeiro de 2012, 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 de informáticos de faturação devem assinar, nos termos do artigo 6.º da Portaria n.º 363/2010, de 23 de junho, os seguintes documentos:

- As faturas, documentos equivalentes e talões de venda;
- 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.

1.2. São ainda assinados, nos termos do referido artigo 6.º, 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.

1.3. Quaisquer outros documentos com eficácia externa eventualmente 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 confusão com uma fatura, conter a expressão "Este documento não serve de fatura", competindo ao produtor de software criar condições que não permitam tais alterações de layouts.

1.4. As faturas ou documentos equivalentes que tiveram origem noutros documentos emitidos, designadamente, guias de remessa ou consultas de mesa, devem conter a identificação desses documentos, devendo esta constar ainda do SAF-T(PT) no campo da linha do documento de venda com o índice 4.1.4.14.2 - Referência à encomenda (OrderReferences).

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

- 1.6. Todos os tipos de documentos deverão ser emitidos cronologicamente em uma ou mais séries (pelo menos anuais) devidamente referenciadas e dentro de cada uma numerados sequencialmente.
- 1.7. Se forem emitidas faturas por mais do que um programa de faturação, em consequência, nomeadamente da existência de diversos estabelecimentos, o número do documento deve conter, impresso, um código identificador da série(s) específica de cada um dos estabelecimentos.
- 1.8. Nenhum documento em estado de preparação poderá ser impresso, a menos que seja imediatamente finalizado, 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 no artigo 36.º do Código do IVA, no Decreto-Lei n.º 147/2003, de 11 de julho e no artigo 6.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 equivalente, documento que acompanhe mercadorias em circulação, valorado ou não, talão de venda, etc., 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 faturação.
- 2.1.2. A assinatura referida no ponto anterior deverá ser gravada na base de dados de faturação (que não pode estar encriptada), com uma associação direta ao registo do documento original, nos termos do número 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 número 2 do artigo 6.º da Portaria n.º 363/2010, de 23 de junho.
- 2.1.4. 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 referido na alínea e) do artigo 6.º deve ser assumido como não preenchido.

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 do artigo 6º da Portaria 363/2010, de 23 de junho.
- 2.2.2. O documento impresso entregue ao cliente ou o documento eletrónico 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 AT>/AT” em substituição da frase “Processado por computador”. Exemplo: "AxAx-Processado por programa certificado n.º0000/AT", (sem aspas).
- 2.2.3. Os documentos referidos no ponto 1. deverão também conter a data, série e numeração sequencial própria.
- 2.2.4. Nos talões de venda emitidos nos termos do artigo 40º do CIVA, entregues a clientes que não facultem o seu número de identificação fiscal (consumidores finais), deverá ser

inutilizada a correspondente linha através de um tracejado ou conter a expressão "Consumidor final" (sem aspas).

- 2.2.5. O valor final dos documentos impressos pelo programa de faturação não deve ser negativo. Quando necessário serão utilizados entre outros, notas de débito e notas de crédito (cfr. nº 13 do artigo 29º do CIVA), como documentos de correção de operações de compra e venda, cuja forma, conteúdo e finalidade devem ser respeitados.

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. Assim:

- a) A assinatura referida no ponto 1. é, nestes casos, da responsabilidade da solução original e deve sempre residir no sistema original (só este sistema conhece a chave privada e tem a capacidade de identificar os caracteres impressos na fatura original);
- b) Os documentos provenientes de outros sistemas, que sejam integrados num sistema central (sistema integrador), devem nele ser registados em séries/tipos de documentos de faturação distintas e autónomas das que utiliza, sendo entendidos como cópias do documento original e o respetivo campo 4.1.4.3 – Chave do documento (*Hash*) deve ser igual ao gerado no sistema emissor;
- c) O sistema central integrador deve também preencher o respetivo campo 4.1.4.4 – Chave de controlo (*HashControl*) com o n.º do certificado com o qual o documento foi assinado no sistema original e a versão da chave;
- d) O formato da informação a registar, nos termos da alínea anterior, resultará da concatenação do número do certificado original + um ponto + versão da chave privada utilizada na assinatura original do campo 4.1.4.3. – 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;
- e) Estes documentos quando impressos pelo sistema integrador deverão fazer menção da sua qualidade através da expressão "Cópia do documento original" (sem aspas), sem prejuízo de outras que lhe sejam aplicáveis.

- 2.3.3. Uma determinada série/tipo de documento de faturação não pode conter documentos com diferentes origens (ex.: conter documentos criados no sistema e importados de um sistema externo numa mesma série/tipo de documento de faturação).

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

- 2.4.1. Nos casos previstos no artigo 8.º da Portaria 363/2010, deverão ser observados os seguintes procedimentos:

2.4.1.1. Através do programa, e em série específica, anual, e com numeração sequencial própria, será processada uma nova fatura, que recolha todos os elementos da fatura manual, com observância dos requisitos definidos no artigo 6.º da Portaria 363/2010.

2.4.1.2. No campo 4.1.4.4 – Chave de controlo (*HashControl*) após o número da versão

da chave privada (1,2, etc.) e separado por um "-" (hifen) serão registados:

- a sigla constante do campo 4.1.4.7 - Tipo de documento (InvoiceType) correspondente ao respetivo tipo de documento, seguida da letra M
- um espaço
- a série
- o carácter "/"
- o número do documento manual.

Exemplo: 1-FTM abc/00001.

2.4.2. As faturas criadas por este procedimento deverão conter, quando impressas, a expressão "Cópia do documento original e separada por um hífen a expressão referida no ponto anterior".

Exemplo: "Cópia do documento original-FTM abc/00001" (sem aspas).

2.5. Momento de exportação do ficheiro SAF-T(PT)

2.5.1. 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 respetivas, gravadas previamente na base de dados quando se desencadeou o processo de gravação do documento.

2.5.2. 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 – Chave do documento (Hash) e 4.1.4.4 – Chave de controlo (HashControl) preenchidos nos termos do ponto 2.3.2 alíneas b) a d) e, cumulativamente, devem também ser exportados a partir da solução original, com os referidos campos preenchidos em conformidade.

2.5.3. O valor do campo 4.1.4.15.3 – Total do documento com impostos (GrossTotal) deve ser exportado com o mesmo valor que foi considerado na assinatura (isto é, arredondado a duas casas decimais), de modo a eliminar divergência entre o valor assinado e o exportado, devendo coincidir com o valor impresso no documento emitido.

2.5.4. No caso de guias de transporte ou guias de remessa não valoradas, deverá o campo 4.1.4.15.3 – Total do documento com impostos (GrossTotal) ser preenchido com "0.00" (sem aspas).

3. 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

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

3.2. A chave pública a fornecer 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".

3.3. 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.

3.4. O texto a assinar relativo ao documento deverá conter os seguintes dados concatenados no

referido formato, separados por “;” (Ponto e vírgula) conforme exemplificado na tabela seguinte:

Campo do SAF-T(PT)	Formato	Dados Exemplo
a) 4.1.4.6 - InvoiceDate	AAAA-MM-DD	2010-03-11
b) 4.1.4.9 - SystemEntryDate	AAAA-MM-DDTHH:MM:SS	2010-03-11T11:27:08
c) 4.1.4.1 - InvoiceNo	Composto pelo código interno do documento, seguido de um espaço, seguido do identificador da série do documento, seguido de uma barra (/) e de um número sequencial do documento dentro da série. ([a-zA-Z0-9./_-])+ ([a-zA-Z0-9]*/[0-9]+)	FAC 001/9
d) 4.1.4.15.3 - GrossTotal	Campo numérico com duas casas decimais, separador decimal “.” (ponto) e sem nenhum separador de milhares.	1200.00
e) 4.1.4.3 - Hash Campo do documento anterior na mesma série, (<i>vazio quando se tratar do primeiro documento da série ou do exercício</i>)	Base-64	mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJtD SITLX+uuJTzwqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/J8y3+Y1bN+K+Y PjQivmIQS0fXETsOPo8SwUZdBALt0vTo1VhUZK ejACcjEYJ9G6nl=

3.5. Exemplo da mensagem a assinar para os dados indicados:

3.5.1. 2010-03-11;2010-03-11T11:27:08;FAC
001/9;1200.00;mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJtD
SITLX+uuJTzwqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/8y3+Y1bN+K+YPjQivmIQS0fX
ETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJ9G6nl

4. 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:

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

4.1. 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+INWKdW5SXLfZfGqZu+xFWTKx0Woloo6z1gD5DhIRgQ5hxitOW  
0QV1LAGIHVMfZ8PDK9e+N4YJ7cDwW4D+iflyCAEvi4xvKejEGVEInEsnA7actmg9OROrMHXKqy  
7mA41P//.....
```

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

4.2. 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 contém 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+INWKdW5SXLfZfGqZu+xF  
WTkx0Woloo6z1gD5DhIRgQ5hxitOW0QV1LAGIHVMfZ8PDK9e+N4YJ7cDwW4D+iflyCAEvi4xv  
KejEGVEInEsnA7actmg9ORO .....
```

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

4.3. Para verificar a chave pública

Basta executar o comando OpenSSL com os seguintes argumentos:

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

5. Criação do certificado

- 5.1. 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.
- 5.2. 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

6. EXEMPLO PRÁTICO DE APLICAÇÃO DO MECANISMO DE ASSINATURA

6.1. 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.

CAMPOS DO SAF-T(PT)	REGISTO 1	REGISTO 2
4.1.4.6 - InvoiceDate	18-05-2010	18-05-2010
4.1.4.9 - SystemEntryDate	2010-05-18T11:22:19	2010-05-18T15:43:25
4.1.4.1 - InvoiceNo	FAC 001/14	FAC 001/15
4.1.4.15.3 - 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 carácter 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 – Chave do documento (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 conterà 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 caracteres em ASCII da assinatura que deverão ser transportados para a base de dados e mais tarde exportados para o campo 4.1.4.3 Chave do documento (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:

```
oso2FoOw4V941CwKTrv6xwzUrOtxBWCwU0yLVAqKwf0CNKZHMETG1XZZC4spRSyby1uDXBggplo  
grl8gHnvevA00UEoAvGJo9Fa3DOA0MhZNDa9/rNvu71pp+0zHmN2ra5IWpiHcgmUYxm5qamLBk49rk  
gvl7h1myKCYBKqgu60=
```

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;oso2FoOw4V941CwKTrv6xwzUrOtxBWCwU  
0yLVAqKwf0CNKZHMETG1XZZC4spRSyby1uDXBggplogrl8gHnvevA00UEoAvGJo9Fa3DOA0M  
hZNDa9/rNvu71pp+0zHmN2ra5IWpiHcgmUYxm5qamLBk49rkgl7h1myKCYBKqgu60=
```

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:

```
Y2ogVAC9rcmm9hilZCGGrxjpkZP9NHn5shhp9phBIVWIn+Ta2zKf+O+05brA6VU0LULtMQP98P29q+vc  
SwVtxSzLDbmmkHMT4l6nQmh91QaOJwPpz2uMqtR3aMkWYYPK4Ntc/yfnXpY1cSeUGbQkqAsJOFSidR  
E4+DibJaC7WMPw=
```

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

6.2. 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
```

Autoridade Tributária e Aduaneira, em 26 de janeiro de 2012

O Diretor-Geral da Autoridade Tributária e Aduaneira



(José A. de Azevedo Pereira)