Especificação das Regras Técnicas para Certificação de Software Portaria n.º 363/2010, de 23 de Junho

1. Introdução

1.1. Este documento pretende especificar as regras para a geração da assinatura das facturas de acordo com o estabelecido na alínea b) do artigo 4.º e nos artigos 3.º e 6.º, todos da Portaria n.º 363/2010, de 23 de Junho, que aprova a necessidade de prévia certificação por parte da DGCI dos programas de facturação adoptados pelos sujeitos passivos.

1.2. Pretende-se desta forma:

a) Definir os requisitos técnicos relativos à chave pública que deve ser objecto de disponibilização à DGCI aquando do processo de certificação;

b) Definir os requisitos técnicos relativos ao sistema que permitirá identificar a gravação do registo de facturas, talões de venda e documentos equivalentes, previsto na alínea b) do artigo 3.º e no artigo 6.º, ambos da Portaria n.º 363/2010, de 23 de Junho.

2. Documentos emitidos pelos programas de facturação

2.1. Os programas de facturação não podem emitir, para além da factura ou documento equivalente, qualquer outro documento com indicação de bens ou serviços prestados e correspondentes importâncias, susceptível de ser apresentado ao adquirente, como suporte da operação efectuada.

2.2. Todavia, quando por razões do tipo de actividade ou da natureza da operação, forem emitidos documentos de conferência de entrega de mercadoria ou da prestação de serviços, susceptíveis de entrega aos clientes, ficam obrigados às mesmas regras da emissão de facturas, nomeadamente, as previstas no artigo 6.º da Portaria n.º 363/2010, de 23 de Junho.

2.3. O documento emitido deve conter de forma evidente a sua natureza (por exemplo: guia de remessa) e a expressão “Este documento não serve de factura”.

2.4. As subsequentes facturas devem conter a identificação dos referidos documentos e ainda constar do SAF-T_PT no campo da linha do documento de venda com o índice 4.1.4.14.2 - Referência à encomenda (*OrderReferences*).

2.5. No caso da utilização do programa em modo de formação, os documentos emitidos deverão indicar no cabeçalho os dados identificativos da empresa de software, ao invés dos da empresa cliente e terão ainda de ter impressa a expressão: "Documento emitido para fins de Formação”.

3. Resumo do processo de assinatura de documentos

3.1. **Processo de gravação de uma factura ou talão de venda**

Avª Duque de Ávila, nº 71- 6º, Lisboa - 1000-139
Email: dspcit-dpat@dgci.min-financas.pt
www.portaldasfinancas.gov.
Tel: (+351) 21 358 Fax: (+351) 21 358
Centro de Atendimento Telefónico:707 206 707

3.1.1. No processo de gravação da factura ou talão de venda deverá ser gerada uma assinatura através do algoritmo RSA com base na informação descrita no nº 1 do artigo 6.º da Portaria n.º 363/2010, de 23 de Junho e na chave privada do produtor do programa de facturação.

3.1.2. A assinatura referida no ponto 3.1.1. deverá ser gravada na base de dados com uma associação directa ao registo do documento original, nos termos do número 2 do artigo 6.º da Portaria n.º 363/2010, de 23 de Junho.

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

3.1.4. No caso da gravação de um primeiro documento de uma série/tipo de documento de facturação, ou de um primeiro documento do exercício de cada tipo, o campo referido na alínea e) do artigo 6.º deve ser assumido como não preenchido.

3.2. **Momento de impressão ou envio electrónico de um documento**

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

3.3. **Documentos integrados na base de dados de facturação originários de outras soluções de facturação**

3.3.1. Dada a existência de diversas soluções de facturação para colmatar diferentes necessidades dos contribuintes, nomeadamente a facturação 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 facturação.

3.3.2. Assim:

a) Os documentos que eventualmente residam na base de dados de determinada solução de facturação mas que foram originalmente criados num outro sistema descentralizado devem ser entendidos no sistema central como cópias do documento original, pelo que não devem conter a assinatura referida no ponto 3.1.1;

b) A assinatura referida no ponto 3.1.1. é, nestes casos, da responsabilidade da solução original e deve residir no sistema original (só este sistema conhece a chave privada e tem a capacidade de identificar os caracteres impressos na factura original);

c) Neste caso, a obrigatoriedade de, no processo de gravação da factura ou talão de venda ser gerada uma assinatura e esta ser gravada na base de dados com uma associação directa ao registo do documento original bem como ser também gravada adicionalmente a versão da chave privada que foi utilizada para gerar a assinatura do respectivo documento, é da aplicação original;

d) Os sistemas que integram documentos por si criados e outros originalmente criados noutros sistemas devem clara e inequivocamente dissociá-los entre si, utilizando para o efeito séries/tipos de documentos de facturação distintas e autónomas.

3.3.3. Uma determinada série/tipo de documento de facturação 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 facturação).

3.4. **Momento de exportação do ficheiro SAFT-PT**

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

3.4.2. Os documentos que eventualmente residam na base de dados de determinada solução de gestão mas que foram originalmente criados num outro sistema não devem ser objecto de exportação para o SAF-T_PT devendo ser exportados a partir da solução original.

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 criptografia de dados que usa o sistema de chaves assimétricas, chave pública e chave privada)

4.2. A chave pública a fornecer deve resultar da sua extracção a partir da chave privada, em formato PEM – base 64 e deve ser criado o respectivo ficheiro com a extensão".txt".

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 seguintes dados concatenados no referido formato, separados por ";" (Ponto e vírgula):

Campo (do SAFT-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, vazio quando se tratar do primeiro documento da série ou do exercício)	Base-64	mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/J8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJ9G6nI=

4.5. Exemplo da mensagem a assinar para o documento exemplo indicado:

2010-03-11;2010-03-11T11:27:08;FAC 001/9;1200.00;mYJEv4iGwLcnQbRD7dPs2uD1mX08XjXIKcGg3GEHmwMhmmGYusffIJjTdSITLX+uujTwzqmL/U5nvt6S9s8ijN3LwkJXsiEpt099e1MET/8y3+Y1bN+K+YPJQiVmlQS0fXETsOPo8SwUZdBALt0vTo1VhUZKejACcjEYJG6nI=

5. Exemplo – criação do par de chaves privada / pública

Para exemplificar a criação do par de chaves RSA, foi utilizada a aplicação **OpenSSL,** que é executada directamente 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.

Os exemplos seguintes são realizados com o formato PEM.

5.1. Criação do par de chaves privado / público

5.1.1. Para criar a chave privada

Basta executar o comando openssl com os seguintes argumentos:

cmd> 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 bytes.

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

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

MIICXgIBAAKBgQDWDX9wVqj6ZqNZU1ojwBpyKKkuzHTCmfK39xx/T9vWkqpcV7h3sx++ZOv2KhhNkIe/1I4OCWDPCXRE4g0uIQr0NS29vMlP3aHHayy76+lbBCNVcHFx…..

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

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

Basta executar o comando openssl com os seguintes argumentos:

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

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

Como resultado foi obtida, neste caso, a informação seguinte:

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

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDWDX9wVqj6ZqNZU1ojwBpyK
KkuzHTCmfK39xx/T9vWkqpcV7h3sx++ZOv2KhhNkIe/1I4OCWDPCXRE4g0uIQr0NS29
vMlP3aHHayy76+lbBCNVcHFxM0ggjre1acnD0qUpZ6Vza7F+PpCyuypD2V/pkL1n
X9Z6z5uYyqc0XaSFdwIDAQAB

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

5.2. Geração de certificado a partir da chave privada.

5.2.1. 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 DGCI, com a extensão txt.

5.2.2. 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 bytes
- Formato do Hash da mensagem = SHA-1

6. Exemplo de aplicação com os campos da base de dados requeridos, com a nomenclatura do ficheiro SAF-T_PT

6.1. Criação da ASSINATURA DIGITAL com a chave privada.

	4.1.4.6 InvoiceDate	**4.1.4.9 SystemEntryDate**	**4.1.4.1 InvoiceNo**	**4.1.4.15.3 GrossTotal**	**4.1.4.3 Hash**
Registo 1	2010-05-18	2010-05-18T11:22:19	FAC 001/14	3.12	Ver 1º registo
Registo 2	2010-05-18	2010-05-18T15:43:25	FAC 001/15	25.62	Ver 2º registo

1º 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;** .

Para ver a assinatura digital produzida utilizaríamos, na linha de comandos, o openssl com os seguintes argumentos:

cmd> echo "2010-05-18;2010-05-18T11:22:19;FAC 001/14;3.12; " | openssl dgst -sha1 -sign ChavePrivada.pem | openssl enc -base64

O parâmetro **echo** passa a cadeia de texto ao comando **dgst** que a vai assinar com base na chave privada e com o algoritmo **SHA1**, redireccionando, por sua vez, a saída para o formato **base64.**

Como resultado é produzida a assinatura:

"Am1K5+CP4LDNVDZYvcLYGpnu8/1b+WWkzgoe8sbZhvk6QFzFvNN77Zsq+cHNm52jCVSEDgWLGHgPS1wcT8ZG7w6KgVq+2/VgOU+xKNt0lcC3gouyarZvcZpZclIReDgLh6m3nv8DYYHKAOQc+eCi/BQ4LqUnuJrca+7emgb/kpU="

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:

cmd> echo "2010-05-18; 2010-05-18T15:43:25;FAC001/15;25.62; Am1K5+CP4LDNVDZYvcLYGpnu8/1b+WWkzgoe8sbZhvk6QFzFvNN77Zsq+cHNm52jCVSEDgWLGHgPS1wcT8ZG7w6KgVq+2/VgOU+xKNt0lcC3gouyarZvcZpZclIReDgLh6m3nv8DYYHKAOQc+eCi/BQ4LqUnuJrca+7emgb/kpU=" | openssl dgst -sha1 -sign ChavePrivada.pem | openssl enc -base64

Como resultado é produzida a assinatura digital do 2º registo:

"XRMQW8CTz2WDczHVsieb+0T1WfD3RZV4eKjtpboWggCXg/5JhrQrBJa6CoO10ZYDqOpmn91IMb7lCijkftZTe+HB3NdpshG0TGsbjjZQfbZ1KM/8gHccdE9fgueoPvrWVY59vwiAWkBCFxew/NCabnMiguzy52wQo8o51dmNeWM=",

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