- 1º Aditamento -
Especificação das Regras Técnicas para Certificação de Software
Portaria n.º 363/2010, de 23 de Junho

1. Introdução

1.1. Este documento de aditamento pretende clarificar algumas questões de natureza técnica, relativas ao processo de geração do par de chaves privada e pública, de acordo com o estabelecido no n.º 1 do artigo 6º (utilização do algoritmo RSA, algoritmo de criptografia de dados que usa o sistema de chaves assimétricas, chave pública e chave privada), bem como relativas à assinatura digital 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.

1.2. Pretende-se desta forma:

a) Clarificar alguns aspectos técnicos relativos à chave pública, elemento do par de chaves que deve ser objecto de disponibilização à DGCI aquando do processo de certificação;

b) Clarificar aspectos 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. Geração do par de chaves e processo de assinatura de documentos

2.1. Em aditamento ao constante do documento "Especificação das Regras Técnicas para Certificação de Software - Portaria n.º 363/2010, de 23 de Junho", nomeadamente quanto ao exemplo apresentado no seu ponto 5. "Exemplo - criação do par de chaves privada / pública" deve ter-se em conta:

a) O exemplo apresentado é meramente ilustrativo, não significando de maneira alguma que o produtor de software tenha ou deva utilizar *OpenSSL*.

b) O exemplo apresentado e as linhas de comando respectivas foram preparadas e ensaiadas com base em Linux.

c) O mesmo exemplo, com *OpenSSL*, quando aplicado na linha de comandos do Windows/DOS, apresenta resultados diferentes devido, nomeadamente, ao comportamento do comando "*echo*" do Windows.

d) O comportamento do *OpenSSL,* perante o exemplo apresentado, devolve assinaturas com quebras de linha a cada 64 bytes (introdução do carácter ASCII 10 a cada bloco de 64 bytes).

e) Por este facto, o comprimento da string da assinatura contém 175 bytes, (64 bytes + 1 + 64 + 1 + 44 + 1) em vez dos esperados 172 bytes.

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

f) No caso de se pretender utilizar *OpenSSL*, deve ser utilizado o parâmetro "-A" que, uma vez passado ao comando *OpenSSL*, permite a supressão dos caracteres de "line-feed" (o carácter 10).

Assim, reformulando o exemplo apresentado teríamos:

cmd> echo "2010-05-18;2010-05-18T11:22:19;FAC 001/14;3.12; " | openssl dgst -sha1 -

sign ChavePrivada.pem | openssl enc -base64 -A

permitindo assim a geração de uma assinatura de 172 bytes, em vez de uma de 175 que contém 3 line feeds a cada 64 bytes.

g) O comando "*echo*", também utilizado no exemplo constante do documento de especificação das regras técnicas, tem comportamento diferente no Windows/DOS e em Linux.

h) Em Windows/DOS o comando "*echo*" é cego e entende as aspas como parte da *string* a assinar.

i) Assim, no exemplo, o comando em Windows/DOS **echo "2010-05-18;2010-05-18T11:22:19;FAC 001/14;3.12;"** devolve uma string com as aspas no início e no fim.

j) O mesmo comando em Linux **echo "2010-05-18;2010-05-18T11:22:19;FAC 001/14;3.12;"** devolve uma *string* sem as aspas no início e no fim.

k) O comando "*echo"*, em linha de comando DOS, adiciona também um line feed ao ecoado para écran, o que leva a resultados distintos dos obtidos em Linux, onde é possível através do parâmetro "-N" suprimir o line feed. Em DOS não existe essa possibilidade.

2.2. Em resumo:

2.2.1. 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 objecto de encriptação, com vista à obtenção da assinatura.

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