ORIENTAÇÃO TÉCNICA Nº 01/GNS - IMPIC/2015

Assunto: Utilização de selos de validação cronológica (*timestamps*) nas plataformas eletrónicas de contratação pública

No âmbito das competências atribuídas ao Gabinete Nacional de Segurança (GNS) e ao Instituto dos Mercados Públicos, do Imobiliário e da Construção (IMPIC), nos termos da Lei 96/2015, de 17 de agosto;

No seguimento dos graves problemas que se continuam a verificar com a utilização de selos de validação cronológica (timestamps), por parte das plataformas eletrónicas de contratação pública;

Considerando que a utilização dos selos de validação cronológica (timestamps), por parte das plataformas eletrónicas de contratação pública, deve ser feita de forma universal e transparente para o operador económico (OE);

Considerando ainda que foram ouvidas as Entidades Certificadoras (EC) – DigitalSign e Multicert , visando a normalização da utilização dos serviços de validação cronológica de forma segura, automática e universal, minimizando a necessidade de custódia e proteção de códigos ou outros condicionalismos técnicos, bem como a instalação de software adicional por parte das plataformas, ao mesmo tempo que se cumpra os *standards* e boas práticas em uso, bem como o escrupuloso respeito pela legislação nacional e internacional vigente.

É assim determinado o seguinte:

I - No âmbito da actividade das entidades gestoras de plataformas:

1.º - Cada uma das plataformas deverá implementar os mecanismos necessários para disponibilizar aos OE a possibilidade da parametrização/escolha de um prestador externo de serviços de validação cronológica que sejam emitidos por qualquer entidade de certificação eletrónica, que possua esse mesmo serviço registado, credenciado e publicado na *Trusted — Service Status List (TSL)* emitida pela Autoridade Credenciadora Nacional (Autoridade Nacional de

Segurança) (http://www.gns.gov.pt/trusted -lists.aspx), conforme disposto no n.º 3 do Artigo 43º da Lei 96/2015, de 17 de agosto.

2º A implementação referida no número anterior deve garantir as seguintes parametrizações/características:

a) Estar limitada à introdução dos seguintes dados por parte do OE:
    i. URL do prestador externo de serviços de validação cronológica;
    ii. Identificador único e normalizado;
b) Ser bem visível e de fácil acesso pelo OE;
c) Conservar/memorizar os dados parametrizados pelo OE;
d) Permitir a alteração dos dados parametrizados pelo OE;
e) Facilitar a introdução e edição de dados respeitando as boas práticas da usabilidade e da segurança, não podendo, por isso, entre outras, ser limitada a funcionalidade de copiar e colar.

3.º - O serviço de validação cronológica interoperável é prestado e acedido de acordo com as seguintes regras:

a) Em escrupuloso respeito pelo protocolo IETF - RFC 3161;
b) Acessível através de um canal seguro (HTTPS);
c) Com autenticação forte com recurso a certificado digital de autenticação;
d) O URL para acesso ao serviço de validação cronológica interoperável deve ser complementado com o identificador único, ou seja: https://<URL base>/<identificador>

4.º - Em caso de erro na obtenção de selos temporais, e havendo reclamação do OE, fica a plataforma obrigada a fazer prova técnica do mesmo, comunicando o respetivo resultado ao reclamante num prazo máximo de 2 dias úteis.

5.º - A implementação de todas as ações necessárias para o escrupuloso cumprimento dos pontos anteriores deve ser realizada até **16 de dezembro de 2015**.

6.º - A falta de cumprimento destes procedimentos constitui infração grave nos termos previstos no Artigo 83º da Lei 96/2015, de 17 de agosto, punível com coima entre 10.000€ e 50.000€, nos termos do disposto no Artigo 85º da mesma Lei.

II - No âmbito da actividade das Entidades certificadoras:

7.º - Todos os pacotes de selos temporais disponibilizados pelas ECs para utilização nas plataformas electrónicas (geridos pelas plataformas ou pelos OE) terão um identificador único e normalizado, incluindo o número de identificação fiscal e um identificador:

a) O identificador único normalizado terá um tamanho máximo de 26 carateres alfanuméricos (0-9A-Z);

b) Os 16 carateres iniciais são preenchidos à direita com o número de identificação fiscal, precedido do código internacional de País (Country Code). Caso o tamanho resultante seja inferior aos 16 carateres, deve ser precedido de "0"s (zeros) até completar o tamanho total;

c) Os restantes 10 carateres são preenchidos com um identificador único de pacote. Caso o tamanho resultante seja inferior aos 10 carateres, devem ser preenchidos apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. Exemplo de um identificador único normalizado: 00000PT123123123GHE2Z309IS.

8.º - É da responsabilidade das ECs a definição do identificador único e a informação do mesmo ao OE (diretamente ou através do canal de disponibilização).

9.º - As ECs devem informar as plataformas, dos dados de acesso aos serviços de validação cronológica interoperável, os quais devem ser os seguintes:

a) URL: endereço internet base;

b) OID: o OID da política de validação cronológica aplicável;

10.º - Qualquer alteração à informação descrita no número anterior deve ser informada pelas ECs às plataformas com antecedência nunca inferior a 5 dias úteis.

11.º - O certificado digital de autenticação, referido na alínea c) do nº 3 é fornecido pelas ECs, sem custo, às plataformas, para autenticação de acesso ao serviço de validação cronológica interoperável.

Qualquer esclarecimento sobre esta orientação técnica deve ser solicitado através do seguinte endereço de correio eletrónico: plataformas.eletronicas@gns.gov.pt

01.12.2015

O Diretor do GNS

José Deolindo Torres Sobral

Assinado de forma digital por José Deolindo Torres Sobral
DN: c=PT, o=Presidência do Conselho de Ministros, ou=Gabinete Nacional de Segurança, cn=José Deolindo Torres Sobral
Dados: 2015.12.01 15:10:44 Z

(José Torres Sobral)

O Presidente do Conselho Diretivo do IMPIC, I.P.

Fernando José de Oliveira da Silva

Digitally signed by Fernando José de Oliveira da Silva
DN: c=PT, o=Ministério da Economia, ou=Instituto dos Mercados Públicos do Imobiliário e da Construção IP, cn=Fernando José de Oliveira da Silva
Date: 2015.12.01 14:30:04 Z

(Fernando Oliveira Silva)