



Informação certificada

SOS Digital: Tópico 5

O que fazer com documentos assinados digitalmente ?



Cenário actual

Tendência para considerar AD como uma emulação da assinatura convencional (artº7 do Dec.Lei nº290D/1999, de 2 de Agosto)

acontece que:

- ◆ a informação digital depende de um sistema intermediário para ser criada, processada, acedida e interpretada;
- ◆ AD não é imediatamente perceptível, tornando-se um objecto dependente de outros objectos – hardware e software – com os quais foi produzida;

O que fazer com documentos assinados digitalmente ?

- ◆ O sistema intermediário está sujeito à pressão de um mercado tecnológico muito evolutivo, com um horizonte de obsolescência tecnológica de 7 anos;
- ◆ AD é, por conseguinte, efémera, tornando-se rapidamente obsoleta, ou seja, desatualizada relativamente a novas tecnologias que vão sucedendo àquela em que assinatura foi originalmente produzida: com o passar do tempo deixa de ser processável, tornando-se inacessível e, como tal, incapaz de ser lida e interpretada;

O que fazer para enfrentar o dilema insanável da obsolescência tecnológica ?

Se nada se fizer para evitar a obsolescência, o documento torna-se inacessível, improcessável e, conseqüentemente, inútil. No entanto, se houver intervenção no documento, a AD deixa de certificar o documento intervencionado o qual perde o seu valor probatório.

O que fazer com documentos assinados digitalmente ?

Limitações da AD

- ◆ A constatação técnica de que a preservação, no médio e longo prazo, de documentos com aposição de assinatura digital, sujeitos a migrações periódicas, não garante a inalterabilidade dos documentos;
- ◆ As migrações para outros formatos alteram o código binário do ficheiro da mensagem e os seus valores hash - da versão codificada -, inviabilizando o mecanismo de verificação da assinatura digital;

O que fazer com documentos assinados digitalmente ?



- ◆ Inexistência de medidas legais no ordenamento jurídico português que contemplem a situação da preservação digital de documentos com valor probatório;
- ◆ AD foi pensada para a autenticação imediata , mas não para o médio e longo prazo;
- ◆ A obsolescência do documento original combina com a da AD;
- ◆ AD confere autenticação mas não autenticidade nos termos do artº 370º do Código Civil



Perdem a validade jurídica e probatória ?

Três aspectos do problema

- AEQ baseia a presunção de autenticidade na verificação da inalterabilidade do nível físico do documento;
- Para o documento ser mantido inteligível ao longo do tempo, necessita de ser alterado (migrado, emulado, etc);
- Quando aplicados processos de preservação a AEQ deixa de validar o documento.

Fica claro que a capacidade temporal de certificação da AD é curta, podendo inviabilizar o período de vida operacional, durante o qual os efeitos probatórios têm de estar presentes e activos de forma acutelar os interesses ou direitos instituídos pelo documento.

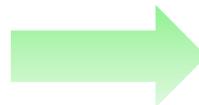


Perdem a validade jurídica e probatória ?

**Não basta
preservar o
documento
electrónico e
AD aplicada**



**É necessário
preservar todos os
documentos
produzidos no
processo de
certificação:
certificados,
revogações mas
também o software
e o hardware
utilizados**



**Estes
documentos
são
igualmente
electrónicos
e devem ser
assinados
com AEQ DL
62/2003**



Perdem a validade jurídica e probatória ?

O que fazer então para não perder a validade jurídica e probatória?



Equacionar soluções de preservação a longo prazo de documentação digital sem prejuízo do seu valor probatório

Como manter documentos assinados inalterados ao longo do tempo ?

O recurso ao *Trusted Archival Service* (Serviço de Arquivo Confiável) parece ser a solução mais viável:

todavia ainda não reconhecida por estar dependente de certas condições, entre outras: da conclusão e aprovação da adaptação a duas normas ISO das duas especificações de requisitos para repositórios digitais: o *TRAC* e o *DRAMBORA*

ISO/DTR 17068 – Information and documentation – Records Management – The Trusted Third Party Repository for Digital Records;

ISO/DIS 16363 – Space data and information transfer systems – Audit and certification of trustworthy digital repositories;

da existência da credenciação de entidades certificadoras de repositórios e do desenvolvimento de uma norma ISO para o efeito: *ISO/DIS 16919 – Space data and information transfer – Requirements for bodies providing audit and certification of candidate trustworthy digital repositories*

Como manter documentos assinados inalterados ao longo do tempo ?

A solução proposta implicaria:

1. a possibilidade de certificar repositórios de acordo com normativos internacionais;
2. a possibilidade de credenciar instituições certificadoras de acordo com normativos internacionais, para adquirirem competências para reconhecimento de repositórios certificados;
3. a aceitação de cópias certificadas como documentos com valor probatório idêntico a “originais” desde que custodiados por um repositório certificado;
4. a regulamentação sobre preservação digital a longo prazo para documentos assinados digitalmente dos TAS – Serviços de Arquivo Confiáveis;
5. a extracção da AD (*striping*) no momento da ingestão do documento no repositório certificado desde que:

Como manter documentos assinados inalterados ao longo do tempo ?

- a) o documento “original” contendo a AD seja mantido ainda que sem preservação associada;
- b) o processo de extracção (antes, durante e após) seja totalmente documentado através da criação de metainformação emitida pelo repositório;
- c) o repositório aplique a sua AD sobre o objecto ingerido.

A solução, no entanto, só será possível, se:

- ◆ forem criados dispositivos legais gerais;
- ◆ for aceite o TAS como método de preservar objectos digitais autenticados;
- ◆ a lei passar a incluir a debilidade do conceito de original em ambiente digital e consequente valorização de cópias certificadas pelos TAS.

Porque é que uma assinatura digital deixa de ter validade ao fim de 3 anos ?

Convém ter presente a distinção entre **AD** e **certificado digital**

Estes dois objectos têm vigências diferenciadas:

- AD tem um prazo de validade variável de acordo com as especificações de cada entidade certificadora, mas que em regra não excede os 5 anos;
- o CD tem um prazo de validade determinado por lei de 20 anos (nº3 do artº12º do Dec.Reg. 25/2004, de 15 de Julho), no entanto, a preservação deste certificado é complexa.

A entidade certificadora tem de assegurar o ciclo evidencial de todos os certificados emitidos por um prazo de 20 anos, ou seja, toda a cadeia de certificação que comporta certificados de ADs e certificados dos certificados.

A obsolescência tecnológica não permite prazos tão dilatados !

Porque é que uma assinatura digital deixa de ter validade ao fim de 3 anos ?

Para resolver a questão da obsolescência tecnológica da AD, a lei portuguesa prevê, de acordo com o Dec. Regulamentar nº 25/2004, de 15 de Julho:

- um **serviço de validação cronológica**, comprovando com a máxima certeza de que AD foi aplicada durante o período de vigência do respectivo certificado (artº 12º);
- a **reassinatura** do documento, ou seja, uma **nova assinatura** que **substitui a caducada** (a) do artº 34º e artº 35º).

Será que estas soluções resolvem ? ...