

AS LEIS DO COMÉRCIO ELECTRÓNICO

*Regime jurídico da
assinatura digital e da factura electrónica
anotado e comentado*

Manuel Lopes Rocha • Marta Felino Rodrigues
Miguel Almeida Andrade • Miguel Pupo Correia
Henrique Carreiro



Manuel Lopes Rocha
Miguel Pupo Correia
Marta Felino Rodrigues
Miguel Almeida Andrade
Henrique José Carreiro

As Leis do Comércio-Electrónico



Edições Centro Atlântico
Portugal/2000

Reservados todos os direitos por Centro Atlântico, Lda.
Qualquer reprodução, incluindo fotocópia, só pode ser feita
com autorização expressa dos editores da obra.

As Leis do Comércio Electrónico

Autor: Manuel Lopes Rocha,
Miguel Pupo Correia,
Marta Felino Rodrigues,
Miguel Almeida Andrade,
Henrique José Carreiro

Colecção: Direito das Novas Tecnologias

Direcção gráfica: Centro Atlântico

Capa: Bárbara Góis Figueira

© Centro Atlântico, Lda., 2000

Av. D. Afonso Henriques, 1462 - 4450 Matosinhos

Tel. 02 - 938 56 28/9 Fax. 02 - 938 56 30

Rua da Misericórdia, 76 - 1200 Lisboa

Tel. 01 - 321 01 95 Fax 01 - 321 01 85

Portugal

geral@centroatlantico.pt

www.centroatlantico.pt

Impressão e acabamento: Inova

1ª edição: Março de 2000

ISBN: 972-8426-25-9

Depósito legal: 147881/00

Marcas registadas: todos os termos mencionados neste livro conhecidos como sendo marcas registadas de produtos e serviços, foram apropriadamente capitalizados. A utilização de um termo neste livro não deve ser encarada como afectando a validade de alguma marca registada de produto ou serviço.

Apesar de terem sido tomadas todas as precauções, podem ter existido falhas humanas na transcrição da legislação. Por essas, ou por quaisquer outras falhas eventualmente existentes neste livro, quer o Editor quer os Autores, não assumem qualquer responsabilidade.

Ao Leitor

ÍNDICE

Ao Leitor	5
Notas Biográficas	9
Decreto-Lei Nº 290-D/99 de 2 de Agosto <i>Decreto-Lei Relativo à Assinatura Digital</i>	11
Capítulo I - Documentos e actos jurídicos electrónicos	21
Capítulo II - Assinaturas digitais	71
Capítulo III - Certificação	77
Secção I - Acesso à actividade de certificação	77
Secção II - Exercício da actividade	127
Secção III - Certificados	141
Capítulo IV - Fiscalização	161
Capítulo V - Disposições finais	171
Decreto-Lei nº 375/99 de 18 de Setembro <i>Decreto-Lei Relativo à Factura Electrónica</i>	183
Apêndices	
Legislação Nacional	211
Legislação Internacional	
União Europeia	249
Estados Unidos da América	269
Alemanha	291
Itália	301
Espanha	313
Abreviaturas	334

Os autores desta obra intervieram em fases distintas do processo legislativo governamental que culminou nos dois diplomas legais que aqui se anotam e comentam. Esta circunstância não lhes confere, como é óbvio, qualquer legitimidade ou tutela sobre dois instrumentos que a prática vem designando de leis do "comércio electrónico". Todavia, os autores deliberaram prolongar a sua colaboração até à elaboração desta obra, por considerarem de alguma utilidade a revelação de parte significativa do seu labor. Contudo, aqui não se trata nem de trabalhos preparatórios, nem de obra definitiva, apenas uma colecção de materiais destacada dos muitos de que os autores se serviram e servem naquele trajecto e no seu trabalho quotidiano. Não tem, por isso, esta obra qualquer conotação oficial ou de leitura única de textos que certamente se verão enriquecidos, quanto à sua exegese, pelas obras que se seguirão e pela acção dos práticos.

Têm também os autores a noção de que estes dois diplomas não esgotam a matéria do comércio electrónico, uma noção vasta, desproporcionada e expansionista que cobre muitas realidades para além destas aqui descritas. Sendo esta uma obra em colaboração, todos os autores participaram na construção do tronco comum da mesma, sendo certo que os comentários com que termina cada artigo, por envolverem uma área de subjectividade e de interpretação pessoal, vão assinados por quem por eles é responsável. Uma vez que estas leis recentemente publicadas "exigem" a publicação de diplomas complementares, os autores certamente regressarão ao tema quando o edifício legal que ora se começou a erguer estiver completado.

Finalmente, os autores orgulham-se do seu contributo parcelar para os diplomas publicados, representando um avanço muito importante na construção deste segmento da Sociedade da Informação, bem como dos laços de muita estima e consideração que estes anos de trabalho foram sedimentando entre eles.

Uma palavra de profundo agradecimento é devida ao Senhor Dr. José António Veloso pela autorização concedida quanto à utilização de estudos seus em algumas páginas deste livro.

Lisboa, Fevereiro de 2000

Decreto-Lei N° 290-D/99 de 2 de Agosto

Decreto-Lei Relativo à Assinatura Digital

A Resolução do Conselho de Ministros n.º. 115/98, de 1 de Setembro, determinou a definição do regime jurídico aplicável aos documentos electrónicos e assinatura digital, como um dos objectivos a alcançar no âmbito da Iniciativa Nacional para o Comércio Electrónico, necessário à plena afirmação do comércio electrónico.

As redes electrónicas abertas, como a Internet, têm assumido uma importância crescente na vida quotidiana dos cidadãos e dos agentes económicos, proporcionando uma teia de relações comerciais globais. Para aproveitar da melhor forma estas oportunidades, urge criar um ambiente seguro para a autenticação electrónica. Na realidade, as comunicações e o comércio electrónicos exigem assinaturas electrónicas e serviços a elas associados que permitam a autenticação electrónica dos dados.

As assinaturas electrónicas possibilitam ao utente de dados enviados electronicamente que verifique a sua origem (autenticação), bem como se os dados foram entretanto alterados (integridade). Em matéria de assinatura electrónica, o presente diploma assenta no modelo tecnológico ora prevalecente: a assinatura digital produzida através de técnicas criptográficas. Como se depreende dos estudos disponíveis sobre tecnologias de assinaturas digitais baseadas na criptografia de chaves públicas, a assinatura digital constitui, neste momento, a técnica mais reconhecida de assinatura electrónica, apresentando o mais elevado grau de segurança para as trocas de dados em redes abertas. E é esta constatação do estado da tecnologia que tem levado as experiências legislativas estrangeiras a privilegiar esta forma de assinatura electrónica.

Contudo, e considerando que em face do constante desenvolvimento tecnológico esta solução de autenticação de dados pode ser, em pouco tempo, tecnicamente ultrapassada pela afirmação de outras formas de assinatura electrónica, o regime previsto no presente diploma poderá vir a ser aplicado a outras modalidades de assinatura electrónica que satisfaçam os requisitos de segurança da assinatura digital.

A verificação da autenticidade e da integridade dos dados, facultada pelas assinaturas electrónicas, em geral, e pela assinatura digital, em particular, não prova necessariamente a identidade do signatário que cria as assinaturas electrónicas. Assim, considera-se necessário, de acordo com a prática tecnicamente recomendada e internacionalmente consagrada, instituir um sistema de confirmação por entidades certificadoras, às quais incumbe assegurar os elevados níveis de segurança do sistema indispensáveis para a criação da desejada confiança no tocante às assinaturas de documentos electrónicos.

Neste contexto, o presente diploma, por um lado, regula o reconhecimento e o valor jurídico dos documentos electrónicos e das assinaturas digitais e, por outro lado, confia o controle da actividade de certificação de assinaturas a uma entidade a designar, e define os poderes e procedimentos desta, bem como as condições de credenciação da actividade e os direitos e os deveres das entidades certificadoras.

Esta actividade de certificação de assinaturas digitais, de harmonia com a orientação consagrada já noutros países da União Europeia, não está sujeita a autorização administrativa prévia. Importa, porém, que o Estado providencie um controle das condições de idoneidade e segurança asseguradas pelas entidades certificadoras, e desse modo ofereça ao público e ao mercado a orientação e a garantia de qualidade que são indispensáveis para a confiança nos novos meios de documentação e assinatura. De harmonia com este desiderato, prevê-se um sistema voluntário de credenciação e fiscalização das entidades certificadoras pela autoridade competente.

Com este diploma dá-se, em Portugal, o primeiro passo no sentido da consagração legal das assinaturas electrónicas acolhendo-se, designadamente, as soluções avançadas no quadro da União Europeia, na proposta de Directiva do Parlamento Europeu e do Conselho, relativa a um quadro legal comunitário para as assinaturas electrónicas. A evolução tecnológica, que nesta matéria é constante, determinará a médio prazo a revisão, adaptação e aprofundamento do regime estabelecido no presente diploma.

Assim:

Nos termos da alínea a) do n.º 1 do artigo 198.º da Constituição, o Governo decreta, para valer como lei geral da República o seguinte:

NOTAS

ENQUADRAMENTO TECNOLÓGICO

A divulgação da Internet e de outras redes de comunicações públicas coloca aos respectivos utentes problemas delicados de confidencialidade dos dados trocados e de garantia de identidades dos intervenientes na comunicação.

Não é certo que, quando se envia uma mensagem de correio electrónico através da Internet, ela não possa ser lida por outrem que não o seu destinatário original. Na realidade, para que tal violação de privacidade suceda nem sequer é preciso que tenha existido à partida qualquer tentativa de interceptação por meios ilícitos: um simples e muito vulgar engano de endereçamento (isto é, um erro ao digitar o endereço do destinatário) poderá enviar a mensagem para a caixa de correio de um terceiro, que terá assim acesso, se nenhuma precaução tiverem sido tomadas, ao respectivo conteúdo.

É, também, muito simples, na Internet, criar mensagens de correio electrónico sob o disfarce de um nome de um terceiro. Não existe assim, qualquer garantia de que o originador de uma mensagem seja quem diz ser. O potencial para abusos e fraudes, caso não sejam tomadas precauções é, deste modo, muito elevado.

Um dos métodos mais comuns nas redes de comunicações para prevenir o acesso indevido a informações e para autenticar um utilizador de forma inequívoca é o recurso a técnicas criptográficas.

A codificação de uma mensagem de correio electrónico, por exemplo, utilizando uma chave de cifragem, torna-a ilegível para toda a gente excepto para o detentor da chave de decifragem.

O método de cifragem mais tradicional e de mais simples aplicação é o chamado de *chave simétrica* ou *chave secreta*. Neste caso, a chave de cifragem e decifragem é uma e a mesma para ambas as operações.

Este método é de implementação simples, mas apresenta algumas desvantagens significativas, que dificultam a sua aplicação prática a sistemas com números elevados de utentes. De entre aquelas, uma das mais dignas de destaque é a complexidade de dar a conhecer as chaves secretas. A necessidade da chave ter que ser conhecida sempre pelo menos por dois intervenientes no sistema, aumenta o risco de falha de segurança na transmissão da chave.

Uma alternativa à criptografia de chave secreta é a chamada *criptografia de chave pública, ou assimétrica*. Nesta, todo o sistema de cifra se baseia num par de chaves (Cf. Artigo 2º):

- Uma *chave pública*, que pode ser distribuída a terceiros.
- Uma *chave privada*, que deve ser apenas do conhecimento do seu titular.

Estas chaves são complementares: se se cifram dados com a chave pública, estes podem apenas ser decifrados com a chave privada, e vice-versa.

Os sistemas de chave pública dependem da relação matemática entre as chaves pública e privada. Não é computacionalmente viável derivar uma a partir do conhecimento da outra.

Exemplo:

Um utilizador (Pedro) pretende enviar a outro (Inês) uma mensagem cifrada. A operação processa-se da seguinte forma:

- O Pedro usa a chave pública da Inês para cifrar a mensagem.
- A Inês usa a sua chave privada para a decifrar.

Com a criptografia de chave pública, a Inês pode distribuir a sua chave pública por forma a que qualquer pessoa possa enviar-lhe documentos cifrados.

Se alguém interceptar as mensagens cifradas, não será capaz de as decifrar uma vez que não possui a chave privada da Inês.

Esta mesma técnica pode ser usada também para *assinar digitalmente* uma mensagem. Uma mensagem cifrada com uma dada chave privada, só pode ser decifrada com recurso à chave pública correspondente. Dado o conhecimento de uma chave pública que pode ser atribuída de forma inequívoca a um determinado utilizador, a utilização dessa chave para decifrar uma mensagem, dá a garantia de que a cifragem foi efectuada com a respectiva chave privada.

Exemplo:

A Inês quer que se saiba que ela cifrou uma dada mensagem:

- Cifra-a usando a sua chave privada.
- Divulga a sua chave pública e a mensagem.
- Uma vez que a mensagem pode ser decifrada com a chave pública da Inês, fica provado que foi cifrada com a sua chave privada, logo que foi a Inês que a cifrou.

O processo de assinatura digital é baseado neste princípio, mas tem alguns passos complementares. Dois conceitos fundamentais e interligados no processo de assinatura digital de uma mensagem são os de *função de "hash"* e de *"digest"* da mensagem.

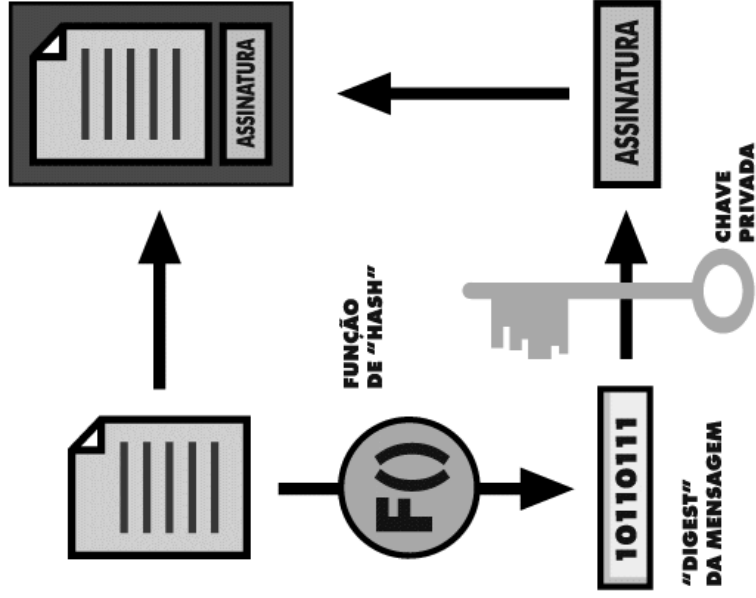
A função de "hash" faz corresponder de uma forma unívoca a uma mensagem uma determinada sequência binária (cadeia de "bits") chamada "digest" de tal forma que a probabilidade de que duas mensagens diferentes dêem origem ao mesmo "digest" seja em termos práticos de zero.

Exemplo:

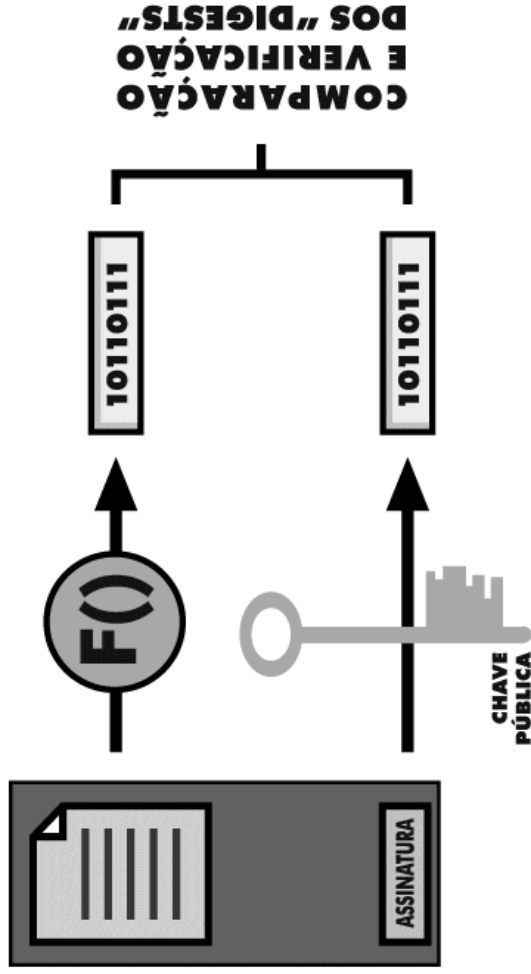
O Pedro pretende enviar uma mensagem assinada digitalmente para a Inês.

- O Pedro utiliza o software presente no seu computador para criar um "digest" (sumário digital) da mensagem, usando uma "função de hash".
- O Pedro encripta então com a sua chave privada, o "digest" criando assim a assinatura digital da mensagem.
- A mensagem e a assinatura então enviadas em conjunto para a Inês.
- Após a recepção da mensagem, a Inês decifra a assinatura com a chave pública do Pedro, revelando assim o "digest" da mensagem.

ASSINATURA



VERIFICAÇÃO



- A aplicação da função de “hash” à mensagem dá origem a um segundo “digest”.
- Se este e o obtido por decifragem da assinatura forem idênticos, é possível garantir que:
 - o conteúdo da mensagem não sofreu qualquer alteração desde que saiu do computador do Pedro.
 - a sua chave privada foi usada para assinar a mensagem, uma vez que a sua chave pública serviu para decifrar a assinatura.

De notar, contudo, que este método de assinatura se baseia no pressuposto que a chave pública é associável de forma inequívoca ao detentor da correspondente chave pública. Mas a chave pública é uma cadeia de bits (um número), e portanto nada a liga intrinsecamente a uma pessoa ou a uma entidade.

Para assegurar que uma chave pública (na realidade, um par de chaves) pode ser associada a um detentor, é necessário um certificado que combine num único documento digital, de forma inseparável, os dados desse detentor e a respectiva chave pública. Esse documento digital é o *certificado digital*, ou *certificado de assinatura* e é emitido e assinado digitalmente por uma *entidade certificadora*.

O formato do certificado, bem como um conjunto de outras importantes regras para a sua publicação e utilização está definido numa norma internacional, denominada X.509 [ISO/IEC 9594-8]¹. A norma indica os princípios básicos que devem ser verificados antes da atribuição do certificado a determinado utente (Cf. também Artigo 25º):

A certificate associates the public key and unique distinguished name of the user it describes. Thus:

- a certification authority shall be satisfied of the identity of a user before creating a certificate for it;*
- a certification authority shall not issue certificates for two users with the same name.*

Uma descrição informal dos campos do certificado (excluindo os campos de extensão), pode ser encontrada na mesma norma.

¹ Ver em <http://www.itu.int>

Specifically, the certificate of a user with distinguished name A and unique identifier UA, produced by the certification authority with name CA and unique identifier UCA, has the following form:

$$CA\langle\langle A \rangle\rangle = CA\{V, SN, AI, CA, UCA, A, UA, Ap, T^A\}$$

where V is the version of the certificate, SN is the serial number of the certificate, AI is the identifier of the algorithm used to sign the certificate, UCA is the optional unique identifier of the CA, UA is the optional unique identifier of the user A, T^A indicates the period of validity of the certificate, and consists of two dates, the first and last on which the certificate is valid. The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate, i.e. publish revocation data. Since T^A is assumed to be changed in periods not less than 24 hours, it is expected that systems would use Coordinated Universal Time as a reference time base. The signature in the certificate can be checked for validity by any user with knowledge of CAp.

Um certificado poderá ter ainda um conjunto de campos de extensão (previstos na norma X.509 Versão 3), que possibilitam a inclusão de informações complementares ou limitações de utilização do certificado (Cf. Artigo 30º).

Versão do Formato do Certificado (Versão 1, 2 ou 3)	
Número de Série do Certificado	
Identificador do Algoritmo de Assinatura (para a Assinatura da Entidade Certificadora)	
Identificação da Entidade Certificadora (segundo a norma X.500) ²	
Período de Validade	Não Antes de
	Não Depois de
Identificação do Titular (segundo a norma X.500)	
Informação Acerca da Chave Pública	Identificador do Algoritmo
	Valor da Chave Pública
Identificador Único da Entidade Certificadora (Opcional) ³	
Identificador Único do Titular (Opcional)	
Extensões (Opcional)	
Assinatura Digital da Entidade Certificadora Relativa ao Presente Certificado	

Tabela 1: O formato de certificado X.509 Versão 3

Um certificado de assinatura tem um tempo de vida limitado, que é delimitado pelas datas de início e fim de validade. Mas para lá do seu termo temporal, um certificado poderá perder ainda a validade devido a um número de razões que poderão ter que ver com questões de segurança (conhecimento não autorizado por terceiros da chave privada do titular do certificado, por exemplo) ou por alterações de designação do titular ou das relações contratuais deste com a entidade certificadora (Cf. Artigo 29º).

A entidade certificadora tem assim a obrigação de manter uma *lista de certificados revogados* (conhecida na norma X.509 como uma *certification revocation list* ou, abreviadamente, *CRL*). Esta lista deverá ser publicamente acessível (por exemplo num determinado endereço Web), por forma a ser facilmente consultável por qualquer utente que

² Ver em <http://www.itu.ch>

³ A certification authority produces the certificate of a user by signing (...) a collection of information, including the user's distinguished name and public key, as well as an optional unique identifier containing additional information about the user. The exact form of the unique identifier contents is unspecified here and left to the certification authority and might be, for example, an object identifier, a certificate, a date, or some other form of certification on the validity of the distinguished name. [X.509]

pretenda fazer a verificação da identidade do titular de um dado certificado (Cf. Artigo 25º).

O âmbito de utilização prática da criptografia de chave pública, dos certificados e das assinaturas digitais é actualmente extremamente vasto. Enumeram-se a seguir algumas das aplicações mais comuns:

1. Securização de correio electrónico: a utilização de encriptação ou de assinaturas digitais permite garantir a confidencialidade ou a autenticidade das mensagens de correio electrónico. De notar, contudo, que se tratam de operações distintas, isto é, por exemplo que a assinatura digital de uma mensagem de correio electrónico não implica a respectiva cifragem.
2. Comunicações seguras na Web: sempre que um "browser" e um servidor Web estabelecem uma comunicação segura, existe uma troca de certificados e um processo de dfragem na origem da comunicação. Esta troca de certificados permite que o "browser" identifique que o servidor Web é o que diz ser (e a recíproca para o servidor relativamente ao "browser").
3. Assinatura digital de ficheiros de programas: para garantir que um programa que é descarregado da Web é disponibilizado por uma entidade digna de confiança e está livre de vírus ou outras aplicações com fins malignos, é comum que estes programas sejam assinados digitalmente. O "browser" que descarrega o programa faz então automaticamente a ligação à entidade certificadora que emitiu o certificado associado à assinatura do programa para se assegurar da identidade do editor deste.
4. Aplicações de pagamentos electrónicos e de banca doméstica: estas aplicações baseiam-se na utilização de certificados como caso particular do exemplo 2., para assegurarem perante o banco ou o servidor Web onde se processa o pagamento, a identidade do titular da conta ou do cartão de crédito. Neste caso, houve em geral um processo prévio em que o banco ou o emissor do cartão de crédito disponibilizou, mediante a presença de meio de identificação adequado, um certificado ao utente, funcionando assim como entidade certificadora.

HJC