

Regulamenta o Decreto-Lei n.º 290-D/99, de 2 de Agosto, que aprova o regime jurídico dos documentos electrónicos e da assinatura digital

Em execução do regime jurídico que disciplina a validade, eficácia e valor probatório dos documentos electrónicos, a assinatura electrónica e a actividade de credenciação das entidades certificadoras estabelecidas em Portugal, constante do Decreto-Lei n.º 290-D/99, de 2 de Agosto, com as alterações que lhe foram introduzidas pelo Decreto-Lei n.º 62/2003, de 3 de Abril, o presente diploma visa aprovar as regras técnicas e de segurança exigíveis às entidades certificadoras que emitem certificados qualificados, regulamentando ainda alguns aspectos específicos relacionados com a credenciação das entidades certificadoras.

Prevê-se que, no exercício da sua actividade, a entidade certificadora utilize processos, sistemas e produtos relacionados com as assinaturas electrónicas de acordo com normas constantes das listas publicadas no Jornal Oficial das Comunidades Europeias, nos termos previstos no n.º 5 do artigo 3.º da Directiva n.º 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de Dezembro, e, na sua falta, com as normas desenvolvidas no âmbito da Iniciativa Europeia de Normalização da Assinatura Electrónica (European Electronic Signature Standardisation Initiative, ou EESSI), para suporte da implementação da Directiva n.º 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de Dezembro, publicadas pelo Instituto Europeu de Normalização para as Telecomunicações (European Telecommunications Standards Institute, ou ETSI), ou pelo Comité Europeu de Normalização (Comité Européen de Normalisation, ou CEN).

Aprovam-se regras precisas relativas aos vários serviços de certificação prestados pela entidade certificadora, como o registo, emissão, distribuição, gestão de revogação e fornecimento de dispositivos seguros de criação de assinaturas e validação cronológica, bem como o respectivo regime de subcontratação.

Prevêem-se ainda normas específicas relativas aos direitos e obrigações da entidade certificadora e dos requerentes e titulares dos certificados e estabelecem-se requisitos operacionais e de gestão, onde se incluem exigências particulares relativas à segurança, política de pessoal, auditorias, cessação da actividade e arquivo de informação. Compreendendo o âmbito de aplicação do diploma todas as entidades certificadoras que emitem certificados qualificados, entidades essas que podem vir a solicitar a credenciação, prevê-se ainda em sede de regulamentação algumas exigências específicas para as entidades credenciadas que se prendem essencialmente com o reforço das garantias exigíveis face ao valor probatório que é conferido às assinaturas electrónicas emitidas por entidades certificadoras credenciadas.

Neste contexto e no âmbito da demonstração dos meios técnicos e humanos exigíveis às entidades certificadoras que solicitem credenciação junto da autoridade credenciadora, é exigida avaliação prévia da conformidade dos processos e dos componentes técnicos que utiliza no exercício da sua actividade de certificação com os requisitos técnicos e de segurança estabelecidos, efectuada por organismos acreditados, ficando sujeita a atribuição de credenciação à apresentação dos respectivos relatórios de avaliação e certificados de conformidade.

Estabelecendo o presente diploma requisitos de natureza essencialmente técnica, sem prejuízo da neutralidade tecnológica assumida pelo regime jurídico consignado no Decreto-Lei n.º 290-D/99, de 2 de Agosto, na sua redacção em vigor, os requisitos técnicos e de segurança ora estabelecidos estão baseados na utilização de criptografia assimétrica (criptografia de chave pública) como suporte das assinaturas electrónicas.

A actual solução de regulamentação de utilização da criptografia de chave pública não prejudica a necessária revisão das normas do presente diploma quando tal apareça justificado pela evolução da tecnologia que venha a verificar-se neste domínio.

Foi ouvida a Autoridade Nacional de Segurança.

Assim:

Ao abrigo do disposto no artigo 39.º do Decreto-Lei n.º 290-D/99, de 2 de Agosto, com a redacção que lhe foi dada pelo Decreto-Lei n.º 62/2003, de 3 de Abril, e nos termos da alínea c) do artigo 199.º da Constituição, o Governo decreta o seguinte:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objecto e âmbito

1 - O presente diploma regulamenta o Decreto-Lei n.º 290-D/99, de 2 de Agosto, com a redacção que lhe foi dada pelo Decreto-Lei n.º 62/2003, de 3 de Abril.

2 - Do presente diploma constam, designadamente, as regras técnicas e de segurança aplicáveis às entidades certificadoras estabelecidas em Portugal na emissão de certificados qualificados destinados ao público.

Artigo 2.º

Normas técnicas

1 - A entidade certificadora utiliza obrigatoriamente, no exercício da sua actividade, processos, sistemas e produtos relacionados com as assinaturas electrónicas em conformidade com o disposto no presente diploma e com normas, especificações e outra documentação técnica, aplicáveis consoante o seu âmbito, tais como:

- a) As constantes das listas publicadas no Jornal Oficial das Comunidades Europeias nos termos previstos no n.º 5 do artigo 3.º da Directiva n.º 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de Dezembro, quando existentes;
- b) As desenvolvidas no âmbito da Iniciativa Europeia de Normalização da Assinatura Electrónica (European Electronic

Signature Standardisation Initiative, ou EESSI), para suporte da implementação da Directiva n.º 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de Dezembro, publicadas pelo Instituto Europeu de Normalização para as Telecomunicações (European Telecommunications Standards Institute, ou ETSI), ou pelo Comité Europeu de Normalização (Comité Européen de Normalisation, ou CEN), em matérias sobre as quais não existam as normas, especificações e outra documentação técnica previstas na alínea anterior;

c) Outras largamente reconhecidas como aplicáveis a produtos de assinatura electrónica.

2 - A autoridade credenciadora publica, em aviso, na 2.ª série do Diário da República, as listas de referências publicadas no Jornal Oficial das Comunidades Europeias das normas a que se refere a alínea a) do número anterior.

3 - As normas a que se referem as alíneas b) e c) do n.º 1 são as aprovadas pela autoridade credenciadora, que publica na 2.ª série do Diário da República as respectivas referências.

4 - As normas previstas no n.º 1, relativas a processos, sistemas e produtos, aplicam-se a:

a) Serviços e processos das entidades certificadoras respeitantes à gestão da infra-estrutura de chave pública, à gestão da segurança da informação e à gestão do ciclo de vida dos certificados qualificados;

b) Sistemas de informação utilizados na emissão e gestão dos certificados qualificados;

c) Módulos criptográficos para operações de assinatura;

d) Aplicações de criação e de verificação de assinaturas;

e) Dispositivos seguros de criação de assinatura;

f) Serviços de validação cronológica.

5 - Sempre que estejam envolvidas matérias classificadas, aplicam-se as regras de credenciação de segurança de matérias classificadas e respectiva credenciação, da competência da Autoridade Nacional de Segurança.

Artigo 3.º

Avaliação da conformidade

1 - A conformidade com o disposto no artigo anterior dos processos, sistemas e produtos relacionados com as assinaturas electrónicas qualificadas é certificada, quando exigido nos termos do presente diploma, por organismos de certificação acreditados de acordo com o disposto no artigo 37.º do Decreto-Lei n.º 290-D/99, de 2 de Agosto.

2 - A avaliação da conformidade dos produtos de assinatura electrónica qualificada é efectuada segundo os critérios comuns para a verificação e avaliação da segurança nas tecnologias da informação (Common Criteria for Information Technology Security Evaluation), ISO/IEC 15408, para os níveis de avaliação de segurança e grau de robustez exigidos nas normas, especificações e outra documentação técnica aplicável nos termos do artigo 2.º

3 - Do certificado de conformidade referente à segurança dos produtos constam, obrigatoriamente:

a) Os requisitos a que a certificação se aplica e em que plataforma foram testados;

b) Os algoritmos e parâmetros utilizados e respectivo prazo de validade;

c) O nível para que os produtos foram testados e o respectivo grau de robustez.

4 - A conformidade das aplicações de criação e verificação de assinaturas e de validação cronológica pode ainda ser demonstrada através de declaração do respectivo fabricante do produto.

5 - A declaração a que se refere o número anterior é emitida de acordo com os documentos orientadores de avaliação de conformidade (EESSI Conformity Assessment Guidance) do CEN, para o produto em causa, e contém a identificação do fabricante, do produto, dos requisitos com os quais garante a conformidade e das disposições da norma relativamente às quais esta se verifica.

Artigo 4.º

Subcontratação

1 - A entidade certificadora é responsável por todos os serviços de certificação prestados por terceiros por ela subcontratados, designadamente os de registo, emissão, distribuição, gestão de revogação, fornecimento de dispositivos seguros de criação de assinaturas e validação cronológica.

2 - A entidade certificadora pode subcontratar a prestação de serviços de certificação e o fornecimento dos respectivos componentes, incluindo o serviço de emissão de certificados, desde que a chave utilizada para gerar os certificados seja sempre identificada como pertencendo à entidade certificadora e que esta assuma e mantenha a inteira responsabilidade pelo cumprimento de todos os requisitos exigidos no presente diploma.

3 - É obrigatoriamente reduzido a escrito o contrato celebrado entre a entidade certificadora e qualquer prestador de serviços, onde se estabelecem as obrigações das partes e se identificam as funções da entidade certificadora prestadas pelo subcontratado.

CAPÍTULO II

Actividade da entidade certificadora

SECÇÃO I

Declaração de práticas e política de certificado

Artigo 5.º

Declaração de práticas de certificação

1 - A entidade certificadora emite uma declaração de práticas de certificação em que constam os procedimentos utilizados para cumprimento dos requisitos identificados nas políticas de certificado, com a qual todos os serviços de certificação prestados terão de estar conformes, contendo, entre outros, os seguintes elementos:

a) Descrição da estrutura de certificação;

b) Descrição da infra-estrutura operacional;

c) Procedimentos de validação da identidade e de outros dados pessoais e profissionais de requerentes e titulares;

d) Procedimentos operacionais;

e) Controlos de segurança física, de processos e de pessoal;

- f) Disposições sobre a emissão, utilização, actualização, renovação, suspensão e revogação dos certificados;
- g) Responsabilidades e obrigações do requerente, do titular, da entidade certificadora e dos destinatários;
- h) Disposições relativas à cessação de actividade;
- i) Método de validação cronológica utilizado;
- j) Período de validade da declaração de práticas de certificação.

2 - A declaração de práticas de certificação é revista periodicamente, pelo menos uma vez por ano, e está permanentemente disponível, por via electrónica, para consulta dos requerentes, titulares e destinatários.

Artigo 6.º

Política de certificado

1 - A entidade certificadora indica em cada certificado, através de um identificador único, a política que estabelece os termos, condições e âmbito de utilização do certificado e os requisitos que a declaração de práticas de certificação está obrigada a conter.

2 - A política de certificado está permanentemente disponível, por via electrónica, para consulta dos requerentes, titulares e destinatários.

SECÇÃO II

Emissão e gestão das chaves

Artigo 7.º

Emissão das chaves da entidade certificadora

Os pares de chaves utilizados pela entidade certificadora na prestação de serviços de certificação são gerados:

- a) Num ambiente fisicamente seguro de acordo com as exigências estabelecidas no plano de segurança previsto no artigo 27.º e por pessoal que cumpra os requisitos estabelecidos no artigo 29.º;
- b) Recorrendo a um algoritmo e comprimento de chave apropriado, de acordo com o disposto no artigo 11.º;
- c) Recorrendo a um dispositivo seguro de criação de assinatura certificado nos termos do artigo 3.º;
- d) Por um mínimo de dois trabalhadores presentes física e conjuntamente no local.

Artigo 8.º

Gestão das chaves da entidade certificadora

1 - As chaves privadas da entidade certificadora são:

- a) Mantidas num dispositivo seguro de criação de assinatura certificado nos termos do artigo 3.º;
- b) Objecto de cópia de segurança, armazenada e reposta por pessoal autorizado e em ambiente físico seguro, de acordo com procedimento descrito no plano de segurança, em condições de protecção igual ou superior às chaves em utilização;
- c) Únicas e confidenciais durante a geração e a transmissão para um dispositivo seguro de criação de assinatura, não podendo ser armazenadas fora desse dispositivo;
- d) Utilizadas dentro de áreas físicas seguras de acordo com o estabelecido no plano de segurança;
- e) Utilizadas dentro do seu período de validade.

2 - A entidade certificadora não pode usar as chaves privadas utilizadas na emissão de certificados e listas de revogação para outra finalidade.

3 - No termo do seu período de validade, a cópia da chave privada é destruída de modo irreversível ou arquivada de forma a não poder ser reutilizada.

4 - Na gestão das suas chaves, é da responsabilidade da entidade certificadora:

- a) Assegurar a integridade e autenticidade das chaves públicas e de qualquer parâmetro a elas associado durante a distribuição, assim como estabelecer um processo que permita autenticar a sua origem;
- b) Manter organizado um arquivo das chaves públicas, após o termo do seu período de validade;
- c) Garantir a segurança e integridade do equipamento criptográfico durante a sua vida útil e assegurar que o mesmo não é acedido ou alterado por pessoal não autorizado;
- d) Garantir que as chaves privadas armazenadas no equipamento criptográfico são destruídas quando da sua retirada de funcionamento;
- e) Assegurar que as operações de gestão das chaves privadas, de manipulação de dispositivos criptográficos e de informação do estado de suspensão e ou revogação são efectuadas por um mínimo de dois trabalhadores em simultâneo.

Artigo 9.º

Emissão das chaves de titulares

A entidade certificadora, na emissão das chaves para titulares, assegura que:

- a) O par de chaves do titular é gerado recorrendo a um algoritmo criptográfico apropriado, de acordo com o disposto no artigo 11.º;
- b) A chave privada entregue ao titular para criação de assinaturas é armazenada de forma segura antes da sua entrega, assegurando-se que a sua integridade não é comprometida;
- c) A chave privada entregue ao titular para criação de assinaturas é distinta da chave entregue para utilização em outras funções;
- d) Não é efectuada cópia de segurança nem de arquivo da chave privada do titular para criação de assinaturas.

Artigo 10.º

Dispositivos seguros de criação de assinaturas

A entidade certificadora, sempre que forneça dispositivos seguros de criação de assinaturas, assegura que:

- a) O dispositivo é preparado, armazenado e distribuído de forma segura e está certificado em conformidade com o disposto no artigo 3.º;
- b) No caso de o dispositivo ter associados dados de activação, estes são fornecidos de forma separada.

Artigo 11.º

Algoritmos criptográficos

Os algoritmos criptográficos utilizados na prestação de serviços de certificação e respectivos parâmetros associados são:

- a) Os constantes das listas publicadas no Jornal Oficial das Comunidades Europeias nos termos previstos no n.º 5 do artigo 3.º da Directiva n.º 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de Dezembro, quando existentes;
- b) Os constantes em especificações técnicas emitidas para algoritmos e parâmetros, de acordo com a alínea b) do n.º 1 do artigo 2.º, quando não tenha sido publicada a lista a que se refere a alínea anterior.

SECÇÃO III

Validação cronológica

Artigo 12.º

Serviço de validação cronológica

1 - A entidade certificadora assegura que a data e a hora da emissão, suspensão e revogação dos certificados possam ser determinadas através de serviços de validação cronológica, que ligam criptograficamente os dados com valores de tempo.

2 - Nos serviços de validação cronológica, garante-se que:

- a) A origem e a validade de cada pedido de validação cronológica são determinadas;
- b) O pedido utiliza um algoritmo criptográfico reconhecido nos termos do artigo 11.º;
- c) A hora utilizada é definida a partir do tempo universal coordenado (UTC) e certificada por um instituto nacional de medida, com incerteza inferior a 100 milissegundos (ms);
- d) Os dados incluídos no pedido são devolvidos sem alteração;
- e) A chave privada utilizada na assinatura da prova de validação cronológica:
 - i) Não é utilizada para outra finalidade;
 - ii) É gerada recorrendo a um algoritmo e comprimento de chave apropriado, reconhecido nos termos do artigo 11.º;
 - iii) É gerada e armazenada num módulo criptográfico, certificado de acordo com o disposto no artigo 3.º;
- f) Em cada prova de validação cronológica são incluídos:
 - i) O valor tempo certificado;
 - ii) Um identificador único;
 - iii) Um indicador único da política de certificação cronológica adoptada;
 - iv) O grau de exactidão do valor tempo utilizado sempre que aquele seja superior ao indicado na política adoptada;
- g) A prova de validação cronológica é assinada criptograficamente antes da devolução da resposta ao pedido;
- h) Não está incluída, na prova de validação cronológica, a identificação da entidade que a solicitou.

3 - Os dados relacionados com a geração e a gestão das chaves utilizadas na validação cronológica, incluindo os dados associados à certificação da hora por um instituto nacional de medida, são registados e arquivados por um período mínimo de 20 anos.

SECÇÃO IV

Certificados qualificados

Artigo 13.º

Pedido

1 - A entidade certificadora assegura que o pedido de emissão de certificado é efectuado por documento electrónico ao qual é aposta uma assinatura electrónica qualificada ou por documento escrito sobre suporte de papel, com assinatura autógrafa, e que o mesmo é requerido em obediência ao disposto nos artigos 14.º e 15.º

2 - A entidade certificadora verifica a identidade do requerente, por meio legalmente reconhecido, verificando, no caso de o pedido ser subscrito para outrem, os poderes bastantes do requerente para a referida subscrição.

Artigo 14.º

Pedido de emissão de certificado para pessoa singular

1 - O pedido de emissão, quando requerido pela pessoa singular a constar como titular do certificado, contém, entre outros, os seguintes elementos:

- a) Nome completo;
- b) Indicação de eventual pseudónimo a constar como titular;
- c) Número do bilhete de identidade, data e entidade emitente ou qualquer outro elemento que permita a identificação inequívoca;
- d) Endereço e outras formas de contacto;
- e) Eventual indicação de uma qualidade específica em função da utilização a que este se destinar;
- f) Indicação quanto ao uso do certificado ser ou não restrito a determinados tipos de utilização, bem como eventuais limites do valor das transacções para as quais o certificado é válido;
- g) Outras informações relativas a poderes de representação, à qualificação profissional ou a outros atributos.

2 - No caso de o pedido de emissão ser requerido por outrem que não a pessoa singular a constar como titular do certificado, o mesmo, para além dos elementos referidos no número anterior, contém, consoante seja requerido por pessoa singular ou colectiva, os seguintes elementos referentes ao requerente:

- a) Nome ou denominação legal;
- b) Número do bilhete de identidade, data e entidade emitente, ou qualquer outro elemento que permita a identificação inequívoca, ou número de pessoa colectiva;
- c) Residência ou sede;
- d) Objecto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;

e) Endereço e outras formas de contacto.

3 - O pedido de inclusão no certificado de dados pessoais da pessoa singular a constar como seu titular terá de ser expressamente autorizado pela própria.

4 - Na situação prevista no n.º 2 do presente artigo, o pedido é ainda acompanhado da declaração da pessoa singular a constar como titular do certificado de que se obriga ao cumprimento das obrigações enquanto titular.

Artigo 15.º

Pedido de emissão de certificado para pessoa colectiva

1 - O pedido de emissão, quando requerido pela pessoa colectiva a constar como titular do certificado, é subscrito pelos seus representantes legais e contém, entre outros, os seguintes elementos:

a) Denominação legal;

b) Número de pessoa colectiva, sede, objecto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;

c) Nome completo, número do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca das pessoas singulares que estatutária ou legalmente a representam;

d) Endereço e outras formas de contacto;

e) Indicação quanto ao uso do certificado ser ou não restrito a determinados tipos de utilização, bem como eventuais limites do valor das transacções para as quais o certificado é válido;

f) Eventual referência a uma qualidade específica, em função da utilização a que o certificado estiver destinado;

g) Outras informações relativas a poderes de representação, à qualificação profissional ou a outros atributos.

2 - No caso de o pedido de emissão ser requerido por outrem que não a pessoa colectiva a constar como titular do certificado, ao mesmo, para além do disposto no número anterior, aplica-se, com as devidas adaptações, o previsto nas alíneas a) a e) do n.º 2 e no n.º 4 do artigo 14.º

Artigo 16.º

Registo

1 - A entidade certificadora recebe o pedido, valida os seus dados e procede ao registo.

2 - Do registo constam:

a) A identificação da entidade que recebeu o pedido;

b) Os dados constantes do pedido;

c) Os documentos de prova que acompanham o pedido;

d) A descrição dos métodos utilizados na verificação do pedido;

e) A identificação do contrato referido no artigo 25.º;

f) Outra informação útil à utilização do certificado.

3 - Os dados do registo não podem ser utilizados para outros fins diferentes dos necessários à utilização do certificado.

4 - A entidade certificadora mantém em arquivo, pelo prazo mínimo de 20 anos, os dados constantes do registo, os documentos que os comprovam e um exemplar do contrato.

Artigo 17.º

Emissão

1 - A entidade certificadora garante que, durante o processo de emissão, os dados de registo do titular são tratados de forma segura e que a chave pública constante do certificado está relacionada com a correspondente chave privada do titular.

2 - A entidade certificadora atribui um identificador único para cada titular, para utilização no certificado.

3 - A entidade certificadora assegura a protecção da confidencialidade e integridade dos dados de registo em todos os procedimentos de emissão.

4 - O termo de validade do certificado não pode ultrapassar o termo de validade dos algoritmos utilizados e respectivos parâmetros.

5 - O termo de validade do certificado complementar não pode ultrapassar o termo de validade do certificado com que esteja relacionado.

6 - A entidade certificadora mantém o registo dos certificados emitidos, desde a data da respectiva emissão e durante o seu período de validade, e conserva-os por um período não inferior a 20 anos a partir da data em que termina aquele prazo.

7 - A entidade certificadora só emite certificado para pessoa colectiva quando está em condições de garantir que a criação da assinatura, através de dispositivo de criação de assinatura, exige a intervenção de pessoas singulares que, estatutária ou legalmente, representam a pessoa colectiva titular desse certificado.

Artigo 18.º

Conteúdo e formato

1 - O certificado qualificado contém, entre outras, as seguintes informações:

a) Nome ou denominação do titular da assinatura e outros elementos necessários para uma identificação inequívoca, ou um pseudónimo claramente identificado como tal;

b) Nome e outros elementos necessários para uma identificação inequívoca das pessoas singulares que estatutária ou legalmente representam o titular, quando este é uma pessoa colectiva;

c) Nome e assinatura electrónica avançada da entidade certificadora, bem como a indicação do país onde se encontra estabelecida;

d) Dados de verificação de assinatura correspondentes aos dados de criação de assinatura do titular;

e) Número de série;

f) Início e termo de validade;

g) Identificadores de algoritmos utilizados na verificação de assinaturas do titular e da entidade certificadora;

- h) Indicação de o uso do certificado ser ou não restrito a determinados tipos de utilização, bem como eventuais limites do valor das transacções para as quais o certificado é válido;
- i) Eventual referência a uma qualidade específica do titular da assinatura, em função da utilização a que o certificado estiver destinado;
- j) Indicação de que é emitido como certificado qualificado;
- l) Outras informações relativas a poderes de representação, à qualificação profissional ou a outros atributos, com a menção de se tratar de informações não confirmadas, se for o caso.

2 - No caso de existir um certificado complementar, é assegurada a sua ligação ao certificado com o qual se relaciona, constando obrigatoriamente do certificado complementar as seguintes informações:

- a) Indicação de que se trata de um certificado complementar;
- b) Referência ao certificado no qual se baseia;
- c) Designação dos algoritmos utilizados na verificação da assinatura da entidade certificadora;
- d) Número de série do certificado complementar;
- e) Identificação da entidade certificadora e país onde se encontra estabelecida;
- f) Outras informações relativas a poderes de representação, à qualificação profissional ou a outros atributos, com a menção de se tratar de informações não confirmadas, se for o caso;
- g) Assinatura electrónica avançada da entidade certificadora.

3 - O formato dos certificados obedece às especificações técnicas emitidas pelo ETSI ou outras equivalentes reconhecidas nos termos do artigo 2.º

4 - A entidade certificadora assegura os mecanismos necessários para que a hierarquia de certificação seja estabelecida e os certificados emitidos possam ser reconhecidos.

Artigo 19.º

Distribuição

A entidade certificadora, na distribuição de certificados, deve utilizar sistemas seguros que permitam a sua conservação e disponibilização para efeitos de verificação, assegurando que:

- a) O certificado é disponibilizado, integralmente, ao titular para quem foi emitido;
- b) O certificado só é publicamente disponibilizado com o consentimento do titular;
- c) São transmitidas ao destinatário as condições a que este se obriga, designadamente de:
 - i) Verificar em cada comunicação ou transacção a validade, suspensão ou revogação do certificado;
 - ii) Verificar se o certificado é utilizado de acordo com as condições emitidas pela entidade certificadora.

Artigo 20.º

Renovação e actualização

Na renovação de certificados ou actualização devida a mudança de atributos do titular, a entidade certificadora deve:

- a) Verificar se toda a informação utilizada para comprovar a identidade e atributos do titular ainda se mantém válida;
- b) Comunicar antecipadamente ao titular todas as alterações dos termos e condições de emissão do certificado;
- c) Assegurar que as chaves de assinatura serão actualizadas antes do fim do seu período de validade e que as chaves públicas com elas relacionadas garantem, pelo menos, o mesmo nível de segurança que ofereciam no certificado inicial;
- d) Garantir que a emissão de um novo certificado, que faça uso da chave pública previamente certificada, só é efectuada se for garantida a segurança criptográfica dessa chave durante o prazo de validade do novo certificado.

Artigo 21.º

Revogação e suspensão

A entidade certificadora utiliza os procedimentos de revogação e suspensão de certificados de acordo com o disposto no artigo 30.º do Decreto-Lei n.º 290-D/99, de 2 de Agosto, e com a sua declaração de práticas de certificação, e assegura:

- a) Que os pedidos e informações relativos a suspensão ou revogação são processados assim que recebidos, não podendo ser superior a vinte e quatro horas o período entre a recepção e a publicitação do seu novo estado;
- b) Que o certificado só é suspenso durante o período de tempo definido no plano de segurança, que não poderá ultrapassar três dias úteis, e que, findo esse período, se a suspensão não for levantada, o certificado é revogado com efeitos a partir da data da suspensão;
- c) Que as alterações no estado de validade de certificados são transmitidas ao titular;
- d) Que um certificado revogado não pode ser reutilizado;
- e) Um serviço permanentemente disponível de actualização do estado de suspensão e revogação de certificados.

SECÇÃO V

Dos direitos e obrigações

Artigo 22.º

Obrigação de informação

No exercício da sua actividade, a entidade certificadora divulga a seguinte informação:

- a) Preço dos serviços a prestar;
- b) Declaração de práticas de certificação;
- c) Termos, condições e âmbito de utilização dos seus certificados;
- d) Um meio de comunicação, permanentemente disponível, através do qual se procede ao pedido de suspensão e ou revogação do certificado;
- e) Indicação de que a informação registada, necessária à utilização do certificado, não é utilizada para outro fim;
- f) Período de tempo durante o qual mantém em arquivo a informação prestada pelo requerente e a referente à

utilização dos respectivos certificados;

g) Indicação de que, em caso de cessação da actividade, a informação referida na alínea anterior é transmitida, nos termos da lei, para outra entidade;

h) Os meios utilizados para resolução de conflitos;

i) Legislação aplicável à actividade de certificação;

j) Número do registo de entidades certificadoras atribuído pela autoridade credenciadora;

l) Data e número da credenciação, se credenciada.

Artigo 23.º

Obrigações do titular

O titular do certificado toma as medidas necessárias a evitar danos a terceiros e a preservar a confidencialidade da informação transmitida e é obrigado a:

a) Utilizar as chaves criptográficas dentro das limitações impostas pela respectiva política de certificado;

b) Garantir o sigilo da chave privada;

c) Utilizar algoritmo e comprimento de chave de acordo com o artigo 11.º, no caso de gerar as suas próprias chaves;

d) Usar um dispositivo seguro de criação de assinatura, se a política de certificado assim o exigir;

e) Gerar as chaves no interior do dispositivo seguro de criação de assinatura, se a política de certificado assim o exigir;

f) Informar de imediato a entidade certificadora em caso de perda de controlo da chave privada, ou de incorrecção ou alteração da informação constante do certificado, durante o período de validade deste.

Artigo 24.º

Obrigações do requerente

1 - As obrigações do requerente em nome próprio são as obrigações do titular referidas no artigo anterior.

2 - Aquele que requer um certificado para outrem é responsável por informar o titular dos termos e condições de utilização dos certificados, bem como das consequências do respectivo incumprimento.

Artigo 25.º

Contrato

1 - O contrato celebrado entre a entidade certificadora e o requerente deve ser reduzido a escrito, em linguagem clara e acessível, num suporte físico duradouro, e subscrito pelas partes com assinatura electrónica qualificada, quando em documento electrónico, ou com assinatura autógrafa, quando em suporte de papel.

2 - As cláusulas do contrato celebrado entre a entidade certificadora e o requerente contêm:

a) As obrigações da entidade certificadora resultantes do disposto nas alíneas a), c), h) e i) do artigo 22.º;

b) As obrigações do requerente referidas no artigo anterior.

3 - O contrato celebrado entre a entidade certificadora e o requerente deve ser registado e arquivado pela entidade certificadora pelo prazo mínimo de 20 anos.

CAPÍTULO III

Requisitos operacionais e de gestão

Artigo 26.º

Implementação da segurança

1 - A entidade certificadora assegura que as instalações, procedimentos, pessoal, equipamentos e produtos obedecem a todas as normas de segurança aplicáveis ao exercício da sua actividade, devendo, designadamente:

a) Ter um plano de segurança implementado de acordo com a norma internacional ISO/IEC 17799;

b) Utilizar sistemas e produtos fiáveis, protegidos contra modificações;

c) Ter um auditor de segurança;

d) Elaborar relatórios de incidentes causados por falhas de segurança ou operação e desencadear atempadamente as respectivas medidas correctivas.

2 - A entidade certificadora assegura que os procedimentos utilizados para garantir os níveis de segurança operacional, física e dos sistemas, de acordo com as normas adoptadas, se encontram documentados, implementados e actualizados, e mantém um inventário de bens com a respectiva classificação, de forma a caracterizar as suas necessidades de protecção.

3 - A Autoridade Nacional de Segurança procede a uma avaliação de segurança da entidade certificadora, antes do início de actividade, sempre que estiverem envolvidas matérias classificadas.

Artigo 27.º

Plano de segurança

1 - O plano de segurança contém, no mínimo:

a) Descrição da estrutura organizacional e funcional e da actividade de certificação;

b) Especificação dos processos de avaliação e de garantia da idoneidade e capacidade técnica do pessoal em funções;

c) Especificação dos requisitos de segurança física, lógica e operacional;

d) Requisitos de disponibilidade da informação, incluindo redundância de sistemas e planos de contingência;

e) Indicação do período de tempo máximo para actualização do estado de revogação e ou suspensão de certificados;

f) Indicação do período de tempo máximo em que um certificado se pode manter no estado de suspensão;

g) Requisitos de protecção da informação, incluindo distinção dos vários níveis de segurança e perfis de acesso implementados;

h) Definição das funções que conferem acesso aos actos e instrumentos de certificação, respectivos requisitos de segurança e perfis de acesso;

i) Descrição dos produtos de assinatura electrónica utilizados e identificação das respectivas certificações de conformidade;

- j) Descrição e avaliação de outros riscos de segurança;
- l) Indicação dos responsáveis pela sua implementação;
- m) Indicação do processo de revisão periódica estabelecido.

2 - No caso de estarem envolvidas matérias classificadas, o plano de segurança deve obter a aprovação da Autoridade Nacional de Segurança.

Artigo 28.º

Plano de contingência

1 - A entidade certificadora, para fazer face à eventual ocorrência de desastres ou incidentes que ponham em causa o funcionamento normal de prestação de serviços de certificação, implementa um plano de contingência que contemple:

- a) A possibilidade de adulteração ou acesso não autorizado às chaves privadas da entidade certificadora;
- b) Um planeamento que assegure a retoma das operações num espaço de tempo previamente definido;
- c) A forma como requerentes, titulares, destinatários e outras entidades certificadoras com as quais exista acordo são informados de qualquer acontecimento que ponha em causa a utilização segura de certificados e do estado de revogação;
- d) A manutenção da integridade e autenticidade da informação relativa ao estado de revogação.

2 - A entidade certificadora assegura que os serviços de distribuição, revogação e estado de revogação de certificados se mantêm permanentemente disponíveis em caso de acidente, bem como procedimentos que permitam a continuação dos serviços em sistemas de recuperação alternativos, e garante que a migração dos sistemas primários para os sistemas de recuperação não põe em risco a segurança dos sistemas.

3 - No caso de estarem envolvidas matérias classificadas, o plano de contingência deve obter a aprovação da Autoridade Nacional de Segurança.

Artigo 29.º

Política de pessoal

1 - A entidade certificadora adopta regras de selecção e contratação do seu pessoal que reforçam e respeitam as disposições de segurança exigidas para o exercício da sua actividade, nomeadamente que:

- a) Para funções de gestão de infra-estruturas de chave pública, emprega pessoal especializado com conhecimentos específicos em tecnologia de assinatura electrónica e com conhecimentos de comportamentos de segurança;
- b) Todo o pessoal que desempenha funções relacionadas com os processos de certificação está livre de conflitos de interesse que possam prejudicar a sua imparcialidade;
- c) As funções relacionadas com os processos de certificação não são desempenhadas por pessoas que se encontram em situação indicadora de inidoneidade;
- d) No âmbito da sua estrutura organizativa contempla, pelo menos, os seguintes cargos e funções necessários à operação dos sistemas:
 - i) Administrador de sistemas: autorizado a instalar, configurar e manter os sistemas, tendo acesso controlado a configurações relacionadas com a segurança;
 - ii) Operador de sistemas: responsável por operar diariamente os sistemas, autorizado a realizar cópias de segurança e reposição de informação;
 - iii) Administrador de segurança: responsável pela gestão e implementação das regras e práticas de segurança;
 - iv) Administrador de registo: responsável pela aprovação da emissão, suspensão e revogação de certificados;
 - v) Auditor de sistemas: autorizado a monitorizar os arquivos de actividade dos sistemas.

2 - Os postos de trabalho ou funções referidos nas subalíneas i), iii) e v) da alínea d) do número anterior não podem ser assegurados pela mesma pessoa.

3 - No caso de conter matéria classificada, a política de pessoal deve obter aprovação por parte da Autoridade Nacional de Segurança.

Artigo 30.º

Auditorias

1 - O auditor de segurança é uma pessoa singular ou colectiva, independente da entidade certificadora, de reconhecida idoneidade, experiência e qualificações comprovadas na área da segurança de informação, na execução de auditorias de segurança e na utilização da norma ISO/IEC 17799, devidamente credenciada pela Autoridade Nacional de Segurança.

2 - A entidade certificadora comprova através do relatório anual de auditoria de segurança, efectuada por auditor de segurança acreditado, que realizou uma avaliação de riscos e identificou e implementou os controlos necessários à segurança da informação.

3 - As auditorias de segurança são efectuadas tendo por base a norma ISO/IEC 17799, devendo o respectivo relatório de auditoria ser enviado à autoridade credenciadora até 31 de Março de cada ano civil.

4 - O auditor de segurança garante que os membros da sua equipa não actuam de forma parcial ou discriminatória e não prestaram serviços de consultoria à entidade certificadora nos últimos três anos nem mantêm com esta qualquer outro acordo ou vínculo contratual.

5 - Em caso de subcontratação, o auditor deve:

- a) Informar previamente a entidade certificadora e obter a concordância desta para a subcontratação;
- b) Garantir a existência de contrato reduzido a escrito no qual estão claramente identificadas as funções subcontratadas e em que se estabelecem as obrigações entre as partes, nomeadamente no que respeita à confidencialidade e à independência de interesses comerciais ou outros, assim como à inexistência de qualquer tipo de vínculo com a entidade certificadora a ser auditada;
- c) Garantir que está apto a comprovar a competência técnica, idoneidade e isenção da entidade subcontratada, bem

como a sua credenciação de segurança pela Autoridade Nacional de Segurança, nos casos legalmente exigíveis, e que esta cumpre o disposto no número anterior;

d) Assumir a completa responsabilidade pelo trabalho subcontratado e pelo relatório final da auditoria.

Artigo 31.º

Cessação da actividade

1 - Em caso de cessação de actividade, a entidade certificadora garante a continuidade da informação relativa a processos de certificação e, em particular, a manutenção do arquivo da informação necessária ao fornecimento de meios de prova em processos judiciais, nos termos do artigo seguinte.

2 - Antes de cessar a sua actividade, a entidade certificadora deve:

a) Comunicar a cessação de actividade nos termos do disposto no n.os 1 e 2 do artigo 27.º do Decreto-Lei n.º 290-D/99, de 2 de Agosto;

b) Comunicar a cessação da actividade à Autoridade Nacional de Segurança para efeitos do cancelamento das credenciações de segurança;

c) Cessar todas as relações contratuais com terceiros autorizados a actuarem em seu nome na execução de funções relativas à emissão de certificados;

d) Destruir ou impedir a utilização, de modo definitivo, das chaves privadas;

e) Garantir que a entidade a quem é transmitida toda a documentação se obriga à sua manutenção durante o período de tempo legalmente exigido.

Artigo 32.º

Arquivo de informação

1 - A documentação referente ao funcionamento dos serviços de certificação, incluindo avarias, situações operacionais especiais e a informação respeitante ao registo, é mantida em ficheiro electrónico e conservada pelo período mínimo de 20 anos.

2 - Para efeitos do disposto no número anterior, a entidade certificadora assegura:

a) A confidencialidade e integridade da informação conservada em arquivo, relativa a certificados qualificados;

b) Que a data e hora precisa de eventos relacionados com a gestão de chaves e de certificados é registada;

c) Que todos os eventos documentados na declaração de práticas de certificação são registados de forma que não permita a sua alteração ou destruição;

d) O arquivo da informação dos eventos relativos a:

i) Registo, incluindo alterações;

ii) Ciclo de vida do par de chaves da entidade certificadora e de todas as chaves de titulares que são geridas pela entidade certificadora;

iii) Ciclo de vida dos certificados qualificados;

iv) Ciclo de vida de chaves geradas por dispositivos seguros fornecidos;

v) Fornecimento de dispositivos seguros de criação de assinatura;

vi) Pedidos relacionados com a revogação de certificados.

3 - A documentação constante do ficheiro electrónico é certificada por meio de assinatura electrónica qualificada com validação cronológica.

4 - A entidade certificadora conserva em ficheiro manual todos os documentos relativos às relações contratuais estabelecidas com os requerentes, comprovativos de identidade e poderes de representação e relações contratuais estabelecidas com subcontratados e os documentos relativos à idoneidade e habilitações profissionais das pessoas que exercem funções relacionadas com serviços de certificação.

5 - A documentação referida no número anterior é guardada, no mínimo, pelo período de 20 anos.

CAPÍTULO IV

Credenciação

Artigo 33.º

Credenciação de entidadesificadoras

1 - As entidadesificadoras que apresentam garantias do cumprimento de todos os requisitos técnicos e de segurança referidos no presente diploma e no Decreto-Lei n.º 290-D/99, de 2 de Agosto, assim como da utilização nas suas operações de certificação de assinaturas electrónicas qualificadas, de processos, sistemas e produtos avaliados e certificados nos termos do artigo 3.º, podem solicitar credenciação, ou a sua renovação, em formulário próprio, disponibilizado pela autoridade credenciadora, instruído com os documentos referidos no artigo 13.º do Decreto-Lei n.º 290-D/99, de 2 de Agosto.

2 - O pedido, quando apresentado em suporte de papel, é entregue directamente ou remetido pelo correio, sob registo, caso o mesmo seja apresentado por via electrónica, em documento electrónico com aposição de assinatura electrónica qualificada. Os documentos destinados à instrução do mesmo são remetidos à autoridade credenciadora no prazo de três dias subsequentes ao envio.

3 - Os documentos referidos no n.º 1 que já tiverem sido apresentados à autoridade credenciadora para efeitos de inscrição no registo das entidadesificadoras e se encontrem dentro do seu prazo de validade poderão ser substituídos por declaração da entidade certificadora onde se declare que os mesmos não sofreram alteração desde a sua apresentação.

4 - O pedido de credenciação, ou de renovação, é ainda instruído com cópias autenticadas, redigidas em português ou acompanhadas de tradução legalizada, dos certificados e relatórios de avaliação de conformidade a que se refere o n.º 1.

Artigo 34.º

Entidadesificadoras credenciadas

As entidades certificadoras credenciadas, além do cumprimento de todas as disposições aplicáveis às entidades certificadoras que emitem certificados qualificados, devem:

- a) Informar os requerentes dos efeitos legais conferidos a uma assinatura electrónica qualificada e da força probatória dos documentos aos quais a mesma tenha sido aposta, assim como sobre a necessidade de voltar a assinar os documentos nos casos em que estes sejam necessários, na forma assinada, por um período de tempo superior à validade dos algoritmos e parâmetros associados utilizados na geração e verificação da assinatura;
- b) Garantir que a referência à credenciação é incluída nos certificados qualificados que emite ou comunicada de outra forma adequada;
- c) Assegurar, dentro do horário de serviço, um prazo máximo de três horas para a actualização das listas de revogação a partir da entrada da respectiva informação, garantindo que fora do horário de serviço são tomadas as medidas adequadas para que um pedido de revogação de um certificado qualificado seja registado por meio de um dispositivo automático que possibilite a suspensão automática e imediata do certificado;
- d) Assegurar que uma interrupção contínua dos serviços de revogação superior a trinta minutos durante o período normal de funcionamento é documentada como avaria.

Artigo 35.º

Segurança dos documentos a longo prazo

A nova assinatura referida na alínea a) do artigo anterior deve ser gerada com os algoritmos e parâmetros associados adequados e incluir as assinaturas anteriores, assim como validação cronológica.

Artigo 36.º

Publicitação

A autoridade credenciadora assegura que se encontra disponível para acesso geral, a qualquer momento, por via electrónica, a informação relativa à identificação das entidades certificadoras credenciadas.

Visto e aprovado em Conselho de Ministros de 12 de Maio de 2003. - José Manuel Durão Barroso - Maria Manuela Dias Ferreira Leite - Maria Teresa Pinto Basto Gouveia - Maria Celeste Ferreira Lopes Cardona - José Luís Fazenda Arnaut Duarte - Maria da Graça Martins da Silva Carvalho.

Promulgado em 22 de Junho de 2004.

Publique-se.

O Presidente da República, JORGE SAMPAIO.

Referendado em 24 de Junho de 2004.

O Primeiro-Ministro, José Manuel Durão Barroso.