



Entidade de Registo da Assembleia da República

Condições Gerais dos Serviços da Entidade de Registo da Assembleia da República

DEVE LER E ACEITAR AS CONDIÇÕES GERAIS REFERENTES AOS SERVIÇOS DA ENTIDADE DE REGISTO DA ASSEMBLEIA DA REPÚBLICA. SE NÃO ACEITAR ESTAS CONDIÇÕES, NÃO DEVE ACEITAR NEM USAR OS CERTIFICADOS ELETRÓNICOS.

1. DEFINIÇÕES

- a) **Assinatura digital:** assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública. A utilização da chave privada permitirá ao titular declarar a autoria do documento eletrónico e a concordância com o seu conteúdo. Por sua vez, o destinatário do documento eletrónico, através da chave pública, poderá verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.
- b) **Certificado Digital (CD):** documento eletrónico que liga os dados de verificação de assinatura digital ao seu titular e confirma a identidade desse titular.
- c) **Certificado Digital Qualificado (CDQ):** certificado que contém indicação de que o certificado é emitido como certificado qualificado, pode conter um atributo específico do titular, restrições ao âmbito de utilização e é emitido por entidade certificadora que reúne os requisitos definidos no artigo 24º do Decreto-Lei n.º 290-D/99, de 2 de Agosto, republicado pelo Decreto-Lei n.º 88/2009, de 9 de Abril, assim como os requisitos constantes do Decreto-Regulamentar n.º 25/2004, de 15 de Julho.
- d) **Chave Privada:** elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se põe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública.
- e) **Chave pública:** elemento do par de chaves assimétricas destinado a ser divulgado pela ERAR, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
- f) **Declaração de Práticas de Certificação (DPC):** documento onde se enunciam as práticas de certificação empregues pela entidade certificadora no processo de gestão de certificados, disponível em <http://pki.multicert.com>.
- g) **Entidade Certificadora:** entidade que cria ou fornece meios para a criação e verificação dos Certificados Digitais (CDs), emite e gere o ciclo de vida dos CDs, assegura a respetiva publicação e presta outros serviços relativos aos certificados digitais.
- h) **Entidade de Registo:** Entidade que presta à MULTICERT os serviços relativos à identificação do Titular, à celebração de contratos de emissão de certificado digital e à gestão de CDs.
- i) **ERAR:** Entidade de Registo da Assembleia da República.
- j) **MULTICERT:** Entidade certificadora, denominada MULTICERT – Serviços de Certificação Eletrónica, S.A, que emite CDQ conforme a sua DPC (Declaração de Práticas de Certificação), credenciada pela Autoridade Nacional de Segurança (<http://www.gns.gov.pt/gns/pt/tsi>), conforme previsto na legislação portuguesa e europeia, estando deste modo habilitada legalmente a emitir todo o tipo de certificados digitais, incluindo os certificados digitais qualificados (certificados digitais de mais elevado grau de segurança/confiança previsto na legislação).
- k) **Política de Certificados (PC):** conjunto de regras que define a aplicabilidade de um CD no contexto de uma determinada comunidade de titulares, disponível em <http://pki.multicert.com>.
- l) **Subscritor:** pessoa singular identificada no Certificado Digital (CD) como honorário do CD, responsável pela sua utilização e que se obriga a respeitar as condições de utilização do certificado digital e as demais condições estabelecidas neste.
- m) **Titular:** o mesmo que subscritor.

2. FUNCIONALIDADES E CONTEÚDO DO CERTIFICADO

O cartão criptográfico entregue ao titular contém dois certificados eletrónicos:

- a) **Certificado digital de autenticação:** permite comprovar a identidade do titular perante os sistemas de informação;
- b) **Certificado digital de assinatura qualificada:** cuja finalidade é a assinatura de documentos eletrónicos, correio eletrónico e transações eletrónicas. A assinatura eletrónica de um documento garante a identidade do assinante, a integridade do documento, ou seja que o seu conteúdo não foi modificado após a aposição da sua assinatura, e o não repúdio, isto é, que o assinante não pode negar a sua autoria. Este certificado cumpre os requisitos legais para ser considerado com força probatória legal, nos termos da lei.

3. OBRIGAÇÕES DO SUBSCRITOR

Ao assumir a titularidade de um Certificado emitido nos termos da Declaração de Práticas de Certificação (“DPC”) e Políticas de Certificados da MULTICERT, que se encontram disponíveis na página eletrónica <http://pki.multicert.com>. Assim, o Titular obriga-se a:

- a) Utilizar o CD exclusivamente nos termos das presentes Condições Gerais, de acordo com o fim a que se destina e no âmbito da respetiva Política de Certificados disponibilizada em <http://pki.multicert.com>;
- b) Verificar os dados pessoais que lhe digam respeito e que se encontrem registados no CD e comunicar à ERAR todas as inexactidões e ou possíveis alterações que possam ocorrer;
- c) Garantir que a chave privada/cartão é mantida sob seu controlo e que são tomadas as medidas suficientes para impedir a sua utilização não autorizada durante o período de validade da mesma, garantindo, para a realização desta tarefa, os adequados mecanismos de segurança física, procedimental e técnica, assumindo total e exclusiva responsabilidade pelas consequências de qualquer falha em tomar tais precauções;

- d) Não divulgar, nem facultar a terceiros, os parâmetros e procedimentos de identificação da referida chave privada, nomeadamente o PIN;
- e) Requerer à ERAR a imediata suspensão e/ou revogação de um CD, sempre que haja suspeitas de quebra de confidencialidade da chave privada, perda ou roubo, seguindo o processo disponibilizado pela ERAR;
- f) Utilizar a chave privada e o Certificado por sua conta e risco, assumindo total responsabilidade pelo conteúdo de quaisquer transmissões, mensagens ou contratos adotados ou assinados utilizando um Certificado emitido pela MULTICERT;
- g) Ressarcir integralmente a MULTICERT pelas perdas que advenham de falhas na proteção da segurança e integridade do seu cartão criptográfico e respetivo conteúdo, ou de qualquer quebra, resultante da não observância ou não cumprimento dos termos e condições da DPC;
- h) Aceitar e autorizar a ERAR a comunicar a terceiros os seus dados pessoais, incluindo o seu nome e morada, se esta comunicação for razoavelmente necessária por força de algum imperativo legal ou regulamentar, bem como para cumprimento de qualquer requerimento de autoridade judicial ou administrativa, bem como para qualquer outro fim lícito, nos termos do artigo 6.º da Lei n.º 67/98, de 26 de Outubro.

Considera-se ainda que o titular é,

- a) Civil e criminalmente responsável pela prática de quaisquer atos que violem as presentes Condições Gerais e, em especial, pelos atos de utilização da chave privada correspondente ao CD, que tenham sido praticados por si;
- b) Responsável pelos atos praticados por qualquer pessoa que use a chave privada correspondente ao seu CD.

3. OBRIGAÇÕES DA ERAR

Ao assumir a titularidade de um Certificado emitido, o titular fica ciente de que a ERAR assume que, desde que o Certificado não expire ou seja revogado:

- a) Não há deturpações dos factos conhecidos no Certificado;
- b) A informação necessária à emissão dos certificados (incluindo o endereço eletrónico) não foi nem será utilizada para qualquer propósito ilícito, cumprindo as normas legais referentes aos dados pessoais sendo que os dados recolhidos destinam-se à emissão do CD e ao cumprimento dos demais deveres legais a que a ERAR se encontra obrigada, não sendo utilizados para quaisquer outros fins diferentes dos referidos;
- c) Garante o sigilo e a confidencialidade de todos os dados pessoais cujo conhecimento não se destine a divulgação pública, designadamente, os relativos à chave privada, ou outros cuja confidencialidade venha a ser imposta por via legal ou regulamentar;
- d) Não existem erros de dados de transcrição no Certificado relativos à informação fornecida pelo Titular, aquando da inscrição;
- e) O Certificado cumpre com todos os requisitos legais e regulamentares;
- f) O Titular pode pedir que sejam retificados, completados, esclarecidos, atualizados ou suprimidos os seus dados pessoais que estejam incorretos, incompletos, desatualizados, ou cuja recolha, utilização, comunicação ou conservação sejam proibidas;
- g) Mantém atualizados os dados pessoais do Titular que lhe forem transmitidos, procedendo à sua atualização sempre que necessário e tomando as medidas adequadas para assegurar que sejam apagados, ou retificados, os dados inexatos ou incompletos;
- h) Publicará a chave pública e o Certificado do titular no diretório de autenticação (Active Directory) no qual os sistemas informáticos estão integrados;
- i) Os seus serviços de revogação e a utilização de um Repositório estão conformes com a DPC em todos os aspetos materiais.

Desde o momento de criação do cartão criptográfico, o titular é a única pessoa a conhecer qualquer frase de confirmação, PIN e *software* ou *hardware* de proteção do seu conteúdo, incluindo a sua chave privada, e nenhuma pessoa não autorizada teve ou terá acesso à mesma.

4. EXPIRAÇÃO DO CERTIFICADO

Os Certificados expiram ao fim de quatro anos e meio após a sua emissão ou no final da Legislatura Parlamentar no caso do titular se tratar de um Deputado.

5. REVOGAÇÃO DO CERTIFICADO DIGITAL

O titular deve solicitar, com urgência à ERAR, a revogação do Certificado quando ocorram alguma das seguintes situações:

- a) Roubo, suspeita de roubo perda ou inoperacionalidade do cartão criptográfico;
- b) Revelação, modificação, ou suspeita de comprometimento das chaves privadas do titular;
- c) Uso indevido ou abusivo deliberado de chaves e certificados, ou a falta de observância ou contravenção dos requisitos operacionais contidos no termo de Aceitação das condições de uso dos certificados pessoais, DPC ou da Política de Certificados;
- d) Convicção razoável de que um dado fundamental relativo ao certificado é falso ou pode ter sido falsificado.

A revogação deve ser feita por formulário próprio através da Intranet da Assembleia da República.

A ERAR reserva-se o direito de revogar o Certificado quando:

- a) Suspeite que a chave privada ou o Certificado do Titular possam estar comprometidos, ou tal comprometimento esteja provado;
- b) A revogação lhe seja devidamente requerida em conformidade com o disposto na DPC;
- c) Sempre que o Titular se desvincule da Assembleia da República

6. RENOVAÇÃO DO CERTIFICADO DIGITAL

Os Certificados emitidos pela MULTICERT não são renováveis. As renovações serão consideradas novas emissões.