Declaração de Divulgação de Princípios da EC CC

Políticas (POL#20)

Nível de Acesso: Público

Versão: 5.0

Data: Mar 204

IRN – Instituto dos Registos e Notariado, I.P.
Av. D. João II, Lote 1.08.01, Edifício H, Parque das Nações 1990-097 Lisboa, Portugal
Telefone: +351 217 985 500 e-mail: geral@irn.mj.pt

Identificador do Documento: POL#20

Palavras-chave: PKI CC, Cartão de Cidadão, Divulgação de Princípios

Tipologia Documental: Políticas

Título: Declaração de Divulgação de Princípios da EC CC

Nível de acesso: Público

Autor: IRN - Instituto dos Registos e Notariado, I.P.

Data: Mar 204

Versão atual: 5.0

Validade do Documento: 2 (dois) anos após a sua aprovação.

Histórico de Versões

Versão	Data	Detalhes
1.0	29/06/2012	Versão inicial.
2.0	03/07/2018	Versão aprovada após revisão eIDAS.
3.0	Jan 2020	Versão aprovada após revisão anual.
4.0	Jan 2022	Revisão. Inclusão da entrega do CC ao domicílio.
5.0	**Mar 2024**	**Revisão no âmbito do Novo CC**

Documentos Relacionados

Documento	Autor	Descrição
Política de Certificados da EC do Cartão de Cidadão (POL#22)	IRN	Descreve a Política de Certificados da EC do Cartão de Cidadão, identificando os perfis de certificado e LCR emitidos, assim como a resposta OCSP.
Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão (POL#23)	IRN	Descreve a Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão, identificando os perfis de certificado e LCR emitidos, assim como a resposta OCSP.
Política de Certificados da EC de Autenticação do Cartão de Cidadão (POL#24)	IRN	Descreve a Política de Certificados da EC de Autenticação do Cartão de Cidadão, identificando os perfis de certificado e LCR emitidos, assim como a resposta OCSP.
Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão (POL#29)	IRN	Descreve os procedimentos e práticas utilizados pela EC de Autenticação do Cartão de Cidadão para suportar a sua atividade de emissão de certificados.
Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão (POL#28)	IRN	Descreve os procedimentos e práticas utilizados pela EC de Assinatura Digital Qualificada do Cartão de Cidadão para suportar a sua atividade de emissão de certificados qualificados.
Declaração de Práticas de Certificação da EC do Cartão de Cidadão (POL#27)	IRN	Descreve os procedimentos e práticas utilizados pela EC do Cartão de Cidadão para suportar a sua atividade de emissão de certificados.

Estado do documento

Este é um documento controlado e aprovado pelo IRN.

Embora este documento possa ser impresso, a versão eletrónica assinada digitalmente pelo(s) elemento(s) do Grupo de Gestão, é a cópia controlada. Qualquer cópia impressa deste documento não é controlada.

Sendo um documento **controlado** e de **acesso público**, este documento pode ser arquivado em unidades locais ou de rede, assim como ser acedido diretamente no repositório da PKI do Cartão de Cidadão em https://pki2.cartaodecidadao.pt/.

Índice

1 Introdução

Este documento resume (mas não substitui), de forma simples e acessível, as características descritas nas Políticas de Certificado (POL#22, POL#23 e POL#24) e Declaração de Políticas de Certificação da Infraestrutura de chave pública da Entidade de Certificação (POL#27, POL#28 e POL#29), disponíveis em http://pki.cartaodecidadao/ e http://pki2.cartaodecidadao.pt/. É elaborado tendo em conta as especificações técnicas indicadas no anexo A da norma ETSI 319 411-1[1].

A infraestrutura da Entidade de Certificação do Cartão de Cidadão (ou Entidade de Certificação do Cidadão) fornece uma hierarquia de confiança, que promove a segurança eletrónica do Cidadão no seu relacionamento com o Estado. A Entidade de Certificação do Cidadão estabelece uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação, através dos seguintes certificados eletrónicos incluídos no Cartão de Cidadão:

- Certificado qualificado de assinatura eletrónica, emitido por prestador qualificado de serviço de confiança (IRN - Instituto dos Registos e Notariado, I.P.), conforme regulamento eIDAS[2];
- Certificado avançado de autenticação, emitido por prestador qualificado de serviço de confiança (IRN - Instituto dos Registos e Notariado, I.P.), pré-notificado a 30/05/2018 (de acordo com o regulamento eIDAS) como meio/sistema de identificação eletrónica com nível de garantia "elevado" e, publicado no Jornal Oficial da União Europeia a 28/02/2019.

A hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Eletrónica do Estado Português (SCEE[3]).

A Declaração de Divulgação de Princípios da Entidade de Certificação do Cidadão não constitui uma Política de Certificados sob a qual se regem os certificados emitidos pela mesma. Para este efeito devem ser consultadas as Políticas de Certificados e Declaração de Práticas de Certificação disponíveis em https://pki2.cartaodecidadao.pt/.

1.1 Público-Alvo

O público-alvo deste documento são os titulares, e terceiras partes de confiança, de certificados qualificados de assinatura eletrónica incluídos no Cartão de Cidadão, emitidos na hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão.

[1] ETSI 319 411-1: *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirement.* V1.2.2.
[2] Regulamento eIDAS: Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.
[3] https://www.scee.gov.pt/

2 Contactos da Entidade de Certificação do Cartão de Cidadão

O contacto principal da Entidade de Certificação do Cartão de Cidadão é o seguinte:

Nome	**IRN I.P. - Departamento de Identificação Civil** **MINISTÉRIO DA JUSTIÇA**
Morada	Civil Campus de Justiça. Avenida D. João II, 1.08.01, Edifício J - 4º e 5º piso. 1990-097 Lisboa
Correio eletrónico	cartaodecidadao@irn.mj.pt
Telefone	924 138 459

Caso necessite de revogar o(s) certificado(s) eletrónico(s) incluído(s) no Cartão de Cidadão, tal processo implica o cancelamento do Cartão de Cidadão. O pedido de cancelamento do Cartão de Cidadão pode ser efetuado de quatro formas alternativas (informação retirada do sítio https://eportugal.gov.pt/servicos/cancelar-o-cartao-de-cidadao, à data de aprovação da versão mais recente deste documento, devendo ser consultado o sítio para informação mais atualizada):

- Presencial, nos balcões do Instituto dos Registos e do Notariado, nas Lojas de Cidadão, nas Lojas RIAC (nos Açores) ou nos postos consulares portugueses, se estiver fora de Portugal;
- Telefone, através da Linha Cartão de Cidadão – (+351) 210 990 111 – ; ou
- *Online* sem autenticação, desde que reúna as seguintes condições:
    - Tenha conhecimento do número completo do Cartão de Cidadão (dígitos e letras),
    - Tenha conhecimento do código de cancelamento constante da carta PIN enviada na ativação do Cartão de Cidadão;
    - Tenha fornecido o contacto de *e-mail* ou de telemóvel, no âmbito do pedido relativo ao Cartão de Cidadão a cancelar;
- *Online* com autenticação, desde que reúna as seguintes condições:
    - Tenha aderido à Chave Móvel Digital[4] e esteja na posse do PIN de autenticação da mesma;
    - Tenha conhecimento do número completo do Cartão de Cidadão (dígitos e letras),
    - Tenha conhecimento do código de cancelamento constante da carta PIN enviada na ativação do Cartão de Cidadão.

O pedido de cancelamento de Cartão de Cidadão, no caso de menores de 16 anos de idade ou nas situações de interdição ou inabilitação por anomalia psíquica, é efetuado por quem, nos

[4] https://www.autenticacao.gov.pt/web/guest/a-chave-movel-digital

termos da lei, exerce as responsabilidades parentais, a tutela ou a curatela. Nestas situações, a autenticação é sempre efetuada através de Cartão de Cidadão ou de Chave Móvel Digital, estando o cancelamento dependente da introdução do número do cartão de cidadão e do código de cancelamento constante da carta PIN do cartão a cancelar.

Os motivos para a revogação de um certificado encontram-se definidos nos artigos 18.º e 33.º da Lei n.º 7/2007 de 5 de fevereiro, na redação dada pela Lei 32/2017, de 1 de junho.

3 Tipos de certificados, procedimentos de validação e utilização

Na hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão são emitidos os seguintes tipos de certificados eletrónicos para o cidadão:

- Certificado qualificado de assinatura eletrónica – Este certificado qualificado é emitido por prestador qualificado de serviço de confiança (IRN - Instituto dos Registos e Notariado, I.P.), conforme regulamento eIDAS[2], de acordo com o perfil de certificado identificado no documento "Política de Certificado de Assinatura Digital Qualificada[5]". Esta política de certificado é representada no certificado qualificado através de um número único designado de "identificador de objeto" (OID): 2.16.620.1.1.1.2.4.1.0.1.1. O certificado qualificado de assinatura eletrónica é um meio legalmente aceite para assinar documentos eletrónicos, garante a integridade dos conteúdos assinados, autenticidade da sua assinatura e não repúdio, não podendo negar que assinou determinado conteúdo.
- Certificado avançado de autenticação – Este certificado avançado é emitido por prestador qualificado de serviço de confiança (IRN - Instituto dos Registos e Notariado, I.P.), conforme regulamento eIDAS[2], de acordo com o perfil de certificado identificado no documento "Política de Certificado de Autenticação[5]". Esta política de certificado é representada no certificado avançado através de um número único designado de "identificador de objeto" (OID): 2.16.620.1.1.1.2.4.2.0.1.1. O certificado avançado de autenticação é um meio/sistema de identificação eletrónica com nível de garantia "elevado", publicado no Jornal Oficial da União Europeia a 28/02/2019, permitindo a identificação do cidadão perante sistemas e serviços *online*.

Estes certificados constam no Cartão de Cidadão, podendo verificar-se o seu estado de validade através do serviço OCSP (*Online Certificate Status Protocol*) e/ou da consulta das LRC (Listas de Revogação de Certificados), ambos identificados no próprio certificado.

[5] Documento disponibilizado no sítio https://pki.cartaodecidadao.pt/.

4 Limites de confiança

O certificado qualificado de assinatura eletrónica tem como objetivo a sua utilização em qualquer aplicação/sítio/serviço para efeitos de assinatura digital qualificada, enquanto que o certificado avançado de autenticação tem como objetivo a sua utilização em qualquer aplicação/sítio/serviço para efeitos de autenticação do seu titular.

O Cidadão (pessoa singular) é o titular do certificado e encontra-se devidamente identificado pelo nome único (*distinguished name* do "*Subject*") no próprio certificado.

Na utilização do certificado e da chave pública, o titular deve garantir o cumprimento das seguintes condições:

a) Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados;

b) Ser responsável pela sua correta utilização;

c) Ler e entender os termos e condições descritos nas políticas e práticas de certificação;

d) Verificar os certificados (validação de cadeias de confiança) e Listas de Revogação de Certificados tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;

e) Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

4.1 Arquivo de informação de registo

A informação de registo e emissão dos certificados é guardada durante um prazo de 20 anos, de acordo com a alínea r) do artigo 24.° do Decreto-lei n.° 290-D/99, na redação atual.

Os dados pessoais recolhidos para a emissão dos certificados são os dados que constam no próprio certificado, nomeadamente: nome, número de identificação civil e, data de nascimento do cidadão.

5 Responsabilidades do titular do certificado

Os certificados identificados na secção 3 (e respetiva chave privada) só podem ser utilizados para o fim a que estes se destinam (conforme estabelecido no campo do certificado "*keyUsage*") e, sempre com propósitos legais. A sua utilização apenas é permitida:

a) A quem estiver designado no campo "*Subject*" do certificado (titular do certificado);

b) Enquanto o certificado se mantiver válido e não estiver na Lista de Revogação de Certificados da Entidade de Certificação.

Os certificados identificados na secção 3 (e respetiva chave privada) consideram-se aceites pelo titular:

- Certificado qualificado de assinatura eletrónica – no ato de levantamento (ou receção) do Cartão de Cidadão;
- Certificado avançado de autenticação – no ato de levantamento (ou receção) do Cartão de Cidadão.

O titular do certificado tem obrigação de:

- Fornecer informação correta e completa;
- Ativar o certificado qualificado de assinatura eletrónica, antes da sua utilização;
- Utilizar os certificados (e respetiva chave privada) apenas para os fins a que se destinam (cf. secção 3);
- Garantir que a chave privada apenas é utilizada pelo titular do certificado, pelo que se deve abster de partilhar o Cartão de Cidadão e de divulgar os PIN de acesso às chaves privadas;
- Utilizar a chave privada para funções criptográficas, apenas em dispositivo criptográfico seguro (vulgarmente designado por leitor de cartões).

O titular do certificado tem de iniciar o processo de revogação do certificado (tal processo implica o cancelamento do Cartão de Cidadão), sem qualquer atraso razoável, sempre que uma das seguintes situações ocorra antes do final do período de validade do certificado (idêntico ao período de validade do Cartão de Cidadão):

- O Cartão de Cidadão tenha sido perdido ou roubado;
- O controlo sobre a chave privada tenha sido perdido ou potencialmente comprometido (por exemplo, pela divulgação da carta PIN enviada na ativação do Cartão de Cidadão, ou outra razão);
- Imprecisão ou alteração dos dados do titular constantes no certificado.

A partir do momento em que ocorra uma das situações identificadas para início do processo de revogação do certificado, o titular tem de interromper imediata e permanentemente o uso da respetiva chave privada.

No caso de ser informado que o certificado ou algum certificado na hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão foi revogado ou comprometido, o titular tem de deixar de utilizar a respetiva chave privada.

6 Verificação do estado do certificado por terceiras partes

Terceiras partes que confiam nos certificados emitidos na hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão são responsáveis por:

- Verificar o estado do certificado (ativo, suspenso ou revogado) no momento da sua utilização, através dos mecanismos OCSP e/ou LRC identificados no certificado, e aceitá-lo apenas se estiver dentro do seu período de validade e no estado ativo;
- Aceitar o certificado apenas quando é utilizado para o fim a que se destina (conforme estabelecido no campo do certificado "*keyUsage*");
- Ter em atenção limitações na utilização do certificado, indicadas no próprio certificado ou nas políticas do certificado em causa;
- Ter em atenção outras precauções identificadas em normas, acordos internacionais, legislação ou outros.

A aceitação do certificado é da responsabilidade exclusiva da parte confiante.

7 Limitação de responsabilidades

A Entidade de Certificação do Cartão de Cidadão:

- Responde pelos prejuízos que cause aos titulares ou a terceiros pela falta ou atraso na inclusão no serviço de consulta sobre a vigência dos certificados, da revogação ou suspensão dum certificado, uma vez que tenha conhecimento dele;
- Só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando não tenha consignado no certificado, de forma clara reconhecida por terceiros o limite quanto ao possível uso.
- A responsabilidade da administração / gestão da Entidade de Certificação do Cartão de Cidadão assenta sobre base objetiva e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços;
- Não responde se o destinatário dos documentos assinados eletronicamente não os validar e tiver em conta as restrições que figuram no certificado quanto às suas possíveis utilizações;
- Não se responsabiliza pelo uso indevido dos certificados digitais;
- Não se responsabiliza por qualquer utilização dos certificados digitais que não conste na Declaração de Práticas de Certificação ou na Política de Certificados;
- Não assume qualquer responsabilidade no caso de perca ou prejuízo:
    - Dos serviços que presta, em caso de guerra, desastres naturais ou qualquer outro caso de força maior;
    - Ocasionados pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Política de Certificados e correspondente Declaração de Práticas de Certificação:
    - Ocasionado pelo uso indevido ou fraudulento dos certificados ou LRC.

Adicionalmente,

- A utilização dos certificados digitais é da exclusiva responsabilidade do seu titular;
- No âmbito do Cartão de Cidadão, a proteção das chaves privada/pública é da exclusiva responsabilidade do Cidadão.

8 Acordos aplicáveis, Declaração de Práticas de Certificação e Políticas de Certificação

É aplicável a:

- "Política de Certificados da EC do Cartão de Cidadão",
- "Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão",
- "Política de Certificados da EC de Autenticação do Cartão de Cidadão",
- "Declaração de Práticas de Certificação da EC do Cartão de Cidadão",
- "Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão",
- "Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão".

Estes documentos encontram-se disponíveis em https://pki2.cartaodecidadao.pt/.

9 Política de privacidade

A Entidade de Certificação do Cartão de Cidadão tem medidas implementadas que garantem a privacidade dos dados pessoais, de acordo com a legislação portuguesa, garantindo que a informação do titular, constante nos respetivos certificados digitais, não se encontra publicada, sendo processada de acordo com a "Política de Certificação do Sistema de Certificação Eletrónica do Estado"[6].

[6] Disponível no repositório https://www.scee.gov.pt/rep/.

10 Indemnizações

De acordo com a legislação em vigor.

11 Legislação aplicável e resolução de conflitos

É aplicável a Lei Portuguesa e os Regulamentos da EU, nomeadamente:

- Lei n.º 19-A/2024, de 7 de fevereiro. Alteração às Leis 7/2007, de 5 de fevereiro, que cria o cartão de cidadão e rege a sua emissão e utilização, 37/2014, de 26 de junho, que estabelece um sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na Internet da Administração Pública denominado Chave Móvel Digital, e 13/99, de 22 de março, que estabelece o novo regime jurídico do recenseamento eleitoral, e ao Decreto-Lei n.º 135/99, de 22 de abril, que define os princípios gerais de ação a que devem obedecer os serviços e organismos da Administração Pública na sua atuação face ao cidadão;
- Regulamento (UE) 1157/2019 visa reforçar a segurança dos bilhetes de identidade dos cidadãos e dos títulos de residência emitidos aos cidadãos da União e seus familiares.
- Regulamento (UE) Nº 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE;
- Lei nº7/2007 de 5 de fevereiro – Cria o cartão de cidadão e rege a sua emissão e utilização;
- Lei nº91/2015 de 12 de agosto – Primeira alteração à Lei nº7/2007, de 5 de fevereiro, que cria o cartão de cidadão e rege a sua emissão e utilização;
- Lei nº32/2017 de 1 de junho – Segunda alteração à Lei nº7/2007, de 5 de fevereiro, que cria o cartão de cidadão e rege a sua emissão e utilização, primeira alteração à Lei nº37/2014, de 26 de junho, que estabelece um sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na *Internet* da Administração Pública denominado Chave Móvel Digital, e sétima alteração ao Decreto-Lei nº83/2000, de 11 de maio, que aprova o regime legal da concessão e emissão de passaportes;
- Lei nº61/2021 de 19 de agosto – Terceira alteração à Lei nº7/2007, de 5 de fevereiro, que cria o cartão de cidadão e rege a sua emissão e utilização. Procede à republicação da Lei n.º 7/2007, de 5 de fevereiro;
- Portaria nº285/2017 – Relativo à regulamentação das formas de entrega do Cartão de Cidadão e dos respetivos códigos;
- Portaria nº286/2017 – Relativo aos requisitos técnicos e de segurança a observar na captação da imagem facial e das impressões digitais do titular do pedido e ainda das medidas concretas de inclusão de cidadãos com necessidades especiais na sociedade da informação;
- Portaria nº287/2017 – Relativo aos mecanismos técnicos de acesso e leitura de dados constantes do circuito integrado; o seu prazo de validade; as circunstâncias em que o Portal do Cidadão pode receber os pedidos de renovação do Cartão de Cidadão; as condições do seu cancelamento pela via telefónica e eletrónica; a fixação do montante devido pelo IRN à AMA, pela sua função de supervisão do Cartão de Cidadão e dos serviços que lhe estão associados, bem como as regras relativas à conservação do ficheiro com o código pessoal para o seu desbloqueio;
- Portaria nº291/2017 – Define as taxas devidas pela prestação dos serviços associados ao cartão de cidadão e pela emissão do cartão de cidadão provisório, bem como as situações de redução, isenção ou gratuidade daquelas;

- Portaria n.º 190-B/2019 – Primeira alteração à Portaria n.º 287/2017, de 28 de setembro, que procede à regulamentação dos mecanismos técnicos de acesso e leitura dos dados constantes de circuito integrado do cartão de cidadão, do prazo geral de validade do cartão de cidadão, dos casos e os termos em que o Portal do Cidadão funciona como serviço de receção de pedidos de renovação de cartão de cidadão, do sistema de cancelamento do cartão de cidadão pela via telefónica e eletrónica, do montante devido pelo Instituto dos Registos e Notariado, I. P. (IRN), à Agência de Modernização Administrativa, I. P. (AMA), pelo exercício das suas competências, previstas no artigo 23.º da Lei n.º 7/2007, de 5 de fevereiro, alterada pelas Leis n.os 91/2015, de 12 de agosto, e 32/2017, de 1 de junho, e das regras relativas à conservação do ficheiro com o código pessoal de desbloqueio (PUK) do cartão de cidadão;
- Decreto-Lei n.º 10-A/2020 – Estabelece medidas excecionais e temporárias relativas à situação epidemiológica do novo Coronavírus - COVID 19;
- Resolução do Conselho de Ministros nº41/2018 – Define orientações técnicas para a Administração Pública, recomendando-as ao setor empresarial do Estado, em matéria de arquitetura de segurança de redes e sistemas de informação e procedimentos a adotar de modo a cumprir as normas RGPD;
- Decreto-Lei nº290-D/99 de 2 de agosto – Aprova o regime jurídico dos documentos eletrónicos e da assinatura digital (em todos os pontos que não forem contrariados pelo Regulamento (UE) nº910/2014);
- Decreto-Lei nº62/2003 de 3 de abril – Altera o Decreto-Lei nº290-D/99, de 2 de agosto;
- Decreto-Lei nº165/2004 de 6 de julho – Altera o artigo 29º do Decreto-Lei nº290-D/99, de 2 de agosto, na redação que lhe foi dada pelo Decreto-Lei nº62/2003, de 3 de abril;
- Lei nº41/2004 de 18 de agosto – Transpõe para a ordem jurídica nacional a Diretiva nº2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas;
- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados);
- Lei n.º 58/2019 de 8 de agosto – Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;
- Regulamento (UE) nº611/2013 da Comissão, de 24 de jungo de 2013, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE;
- Lei nº5/2004 de 10 de fevereiro – Lei das Comunicações Eletrónicas;
- Decisão da Autoridade Nacional de Comunicações (ANCOM), aprovada por deliberação do respetivo Conselho de Administração, de 12 de dezembro de 2013, relativa às exigências de comunicação e divulgação ao público de violações de segurança ou perdas de integridade ocorridas em redes e serviços de comunicações;
- Lei nº109/2009 de 15 de setembro – Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro nº2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

11.1 Resolução de conflitos

Em caso de litígio o titular do certificado pode recorrer a uma Entidade de Resolução Alternativa de Litígios de consumo. A Lista oficial de tais Entidades está disponível no Portal do Consumidor em www.consumidor.gov.pt.

Sem prejuízo da possibilidade de recurso prévio à mediação, caso não seja obtido acordo entre as partes no âmbito de tal procedimento, qualquer uma das partes poderá recorrer à via judicial, ficando desde já fixado como foro competente para o efeito a Comarca de Lisboa.

12 Repositório e auditorias

Toda a informação referente à Entidade de Certificação do Cartão de Cidadão encontra-se disponível publicamente no repositório acessível em https://pki.cartaodecidadao.pt.

Todas as intervenções realizadas à Entidade de Certificação do Cartão de Cidadão são devidamente auditadas por auditores internos. A Entidade de Certificação do Cartão de Cidadão é auditada por um Organismo de Avaliação da Conformidade (devidamente registado no Organismo Nacional de Acreditação), o qual emite um Relatório de Conformidade (CAR[7]) que é disponibilizado à Entidade Supervisora, para avaliar a continuidade de disponibilização de serviços de confiança, conforme regulamento eIDAS[2].

12.1 Certificações

O prestador qualificado de serviço de confiança (IRN - Instituto dos Registos e Notariado, I.P.) está certificado para a emissão dos certificados qualificados de assinatura eletrónica, conforme regulamento eIDAS[2], podendo tal ser verificado na *eIDAS Trusted List* em em https://webgate.ec.europa.eu/tl-browser/#/tl/PT/1.

O prestador qualificado de serviço de confiança (IRN - Instituto dos Registos e Notariado, I.P.) emite o certificado avançado de autenticação, reconhecido como meio/sistema de identificação eletrónica com nível de garantia "elevado", conforme publicado no Jornal Oficial da União Europeia a 28/02/2019.

[7] *Conformity Assessment Report*

Aprovação

Aprovado pelo Grupo de Gestão.

Assinado por: **DIOGO DE CAMPOS MONTEIRO BRÁS**
Num. de Identificação: 10295504
Data: 2024.03.01 13:39:24+00'00'

Assinado por: **RICARDO JOÃO CORREIA VIEIRA**
Num. de Identificação: 13004962
Data: 2024.05.06 15:13:54+01'00'