

IDENTIFICAÇÃO ELETRÓNICA SEGURA DO ESTADO

Ceger.
CENTRO DE GESTÃO
DA REDE INFORMÁTICA
DO GOVERNO



O que é um Certificado Digital?

Um certificado digital poderá atuar um pouco à semelhança de um documento de identidade.

O Certificado Digital associa uma chave criptográfica a uma identidade, de tal forma que esta fique ligada aos documentos electrónicos sobre os quais se aplica o dito certificado.

Um certificado digital é um ficheiro eletrónico que contém diversos dados, como os dados do titular e a sua chave pública e que, por sua vez, é assinado por uma entidade certificadora.

Para que serve um Certificado Digital?

Pode utilizar-se um para:

Autenticar a identidade de um titular de forma eletrónica perante terceiros ou serviços e aplicações.



Assinar digitalmente, de forma que se garanta a integridade dos dados e a sua procedência.



Cifrar dados para que só o destinatário de um determinado documento ou ficheiro possa aceder ao seu conteúdo.



A utilização de certificados digitais garante:

Autenticação das partes - a identidade do emissor e do recetor da informação.

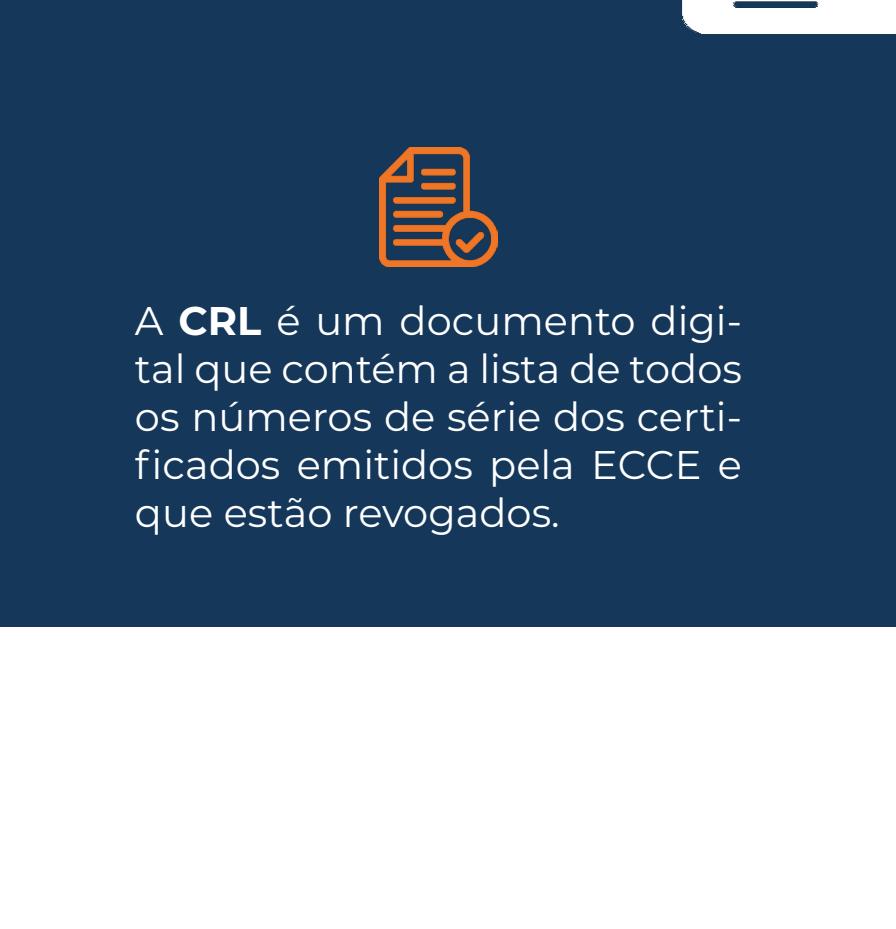


Integridade - a informação não foi manipulada.

Confidencialidade - só o emissor e recetor conseguem ver a informação.

Não-repúdio - o titular de uma mensagem não pode negar que efetivamente assinou.

Que elementos contém um Certificado Digital?



A IDENTIDADE DO TITULAR



A CHAVE PÚBLICA DO TITULAR



A ASSINATURA DA ENTIDADE CERTIFICADORA



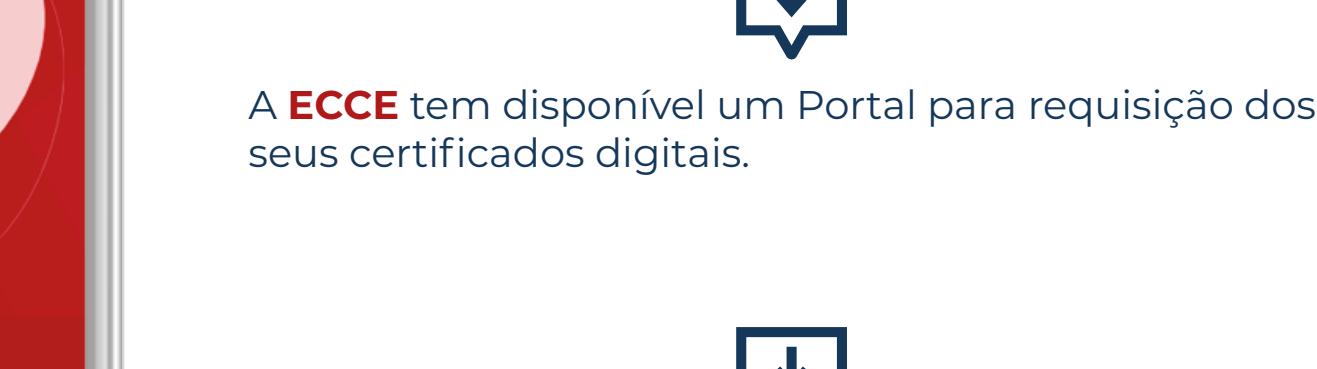
DADOS PRÓPRIOS DO CERTIFICADO



A IDENTIDADE DA ENTIDADE CERTIFICADORA QUE O EMITIU

Como consultar a validade de um Certificado Digital?

Podemos consultar a validade de um Certificado Digital descarregando as **Listas de Certificados Revogados** (CRL's) ou através do serviço de **Protocolo de Status de Certificado Online** (OCSP).



Muitas das aplicações que estão preparadas para a utilização de certificação digital (Office, Adobe, Mail, etc), verificam automaticamente a validade de um certificado através da consulta das CRL's ou do serviço OCSP.



A **CRL** é um documento digital que contém a lista de todos os números de série dos certificados emitidos pela ECCE e que estão revogados.



O **OCSP** é um protocolo e padrão de Internet usado para obter o status de revogação de um certificado digital.

Todas as entidades e organismos da Administração Direta, Indireta e Autónoma do Estado podem adquirir um Certificado Digital através dos serviços da **Entidade Certificadora Comum do Estado** (ECCE).



A **ECCE** tem disponível um Portal para requisição dos seus certificados digitais.



No Portal da **ECCE** pode aceder aos seus pedidos de certificados e cartões e efetuar a sua gestão de forma mais prática, célere e simples.

WWW.ECCE.GOV.PT

