PKI DISCLOSURE STATEMENT

Entidade Certificadora Comum do Estado - ECCE

Nível de Acesso: Documento Público
Versão: 6.0
Data: 2023.04.10
OID: 2.16.620.1.1.1.2.3.2.6

APROVAÇÃO E ASSINATURA

Aprovo o documento e a sua entrada em vigor com a aposição da minha assinatura.

O Diretor do Centro de Gestão da Rede Informática do Governo,

DN: c=PT, title=Diretor, ou=CEGER, o=Centro de Gestão da Rede Informática do Governo, sn=Pereira, givenName=José Louro, cn=José Louro Pereira
Dados: 2023.10.20 12:26:12 +01'00'

(José Manuel Louro Pereira)

CONTROLO DO DOCUMENTO

VERSÃO	DATA	AUTOR	INFORMAÇÕES
1.0	24/08/2017	João Reis Silva	Versão Inicial do documento no âmbito do Regulamento eIDAS.
2.0	18/12/2018	João Reis Silva	Revisão anual e adoção de novo *template* de documento ECCE.
3.0	16/01/2020	Rui Jorge Silva	Revisão anual sem alterações significativas.
4.0	25/02/2021	Rui Jorge Silva	Revisão anual. Foi adicionada uma referência à Política de Privacidade.
5.0	05/05/2022	Rui Jorge Silva	Revisão anual sem alterações significativas.
6.0	10/04/2023	Rui Jorge Silva	Revisão anual sem alterações significativas.

Índice

1. INFORMAÇÕES DE CONTATO DA AUTORIDADE DE CERTIFICAÇÃO

Entidade Certificadora Comum do Estado (ECCE)

Centro de Gestão da Rede Informática do Governo (CEGER)

Campus APP

Avenida João XXI, n.º 63

1000-300 Lisboa

Portugal

Presença na internet: https://www.ecce.gov.pt/

Correio eletrónico: certificacao@ecce.gov.pt

2. TIPO DE CERTIFICADO, PRÁTICAS DE VALIDAÇÃO E UTILIZAÇÃO

2.1 Tipo de Certificado

Esta declaração aplica-se apenas aos serviços de certificação qualificados fornecidos pela ECCE. Os certificados qualificados de chave pública são emitidos pela entidade de certificação qualificada da ECCE nos serviços de certificação qualificados da ECCE. O perfil e qualquer outra limitação do certificado de chave pública certificada emitido pela ECCE são compatíveis com o ETSI EN 319 411-2-v2.2.2.

2.2 Procedimento de Validação

O Certificado qualificado é emitido para uma pessoa após a verificação da sua identidade. A verificação da pessoa pode ser realizada por uma autoridade de registo ou por outra pessoa que esteja autorizada a confirmar a identidade do detentor do certificado. A pessoa, solicitando a emissão de um certificado qualificado, deve ser identificada pelo documento de identidade nacional. No caso de pessoas associadas ou agindo em nome de uma organização, é necessária a autorização do assinante (o signatário) para agir e usar o certificado em nome da organização ou, em alternativa, o registo oficial ou do registo comercial dos poderes conferidos.

2.3 Utilização

Os certificados qualificados emitidos pela ECCE só podem ser utilizados de acordo com o Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho, relativo aos serviços eletrónicos de identificação e confiança para transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.

3. LIMITES DE CONFIANÇA

Não aplicável, no âmbito do SCEE, de acordo com a Política de Certificação e legislação nacional.

4. OBRIGAÇÕES DOS SUBSCRITORES

Ao solicitar a emissão do certificado e aceitar o contrato de assinante, o subscritor concorda em entrar no sistema de certificação de acordo com as condições estabelecidas no contrato e Declaração de Práticas de Certificação dos Serviços de Certificação Qualificados da ECCE.

O assinante compromete-se a:

→Cumprir as regras do acordo celebrado com a ECCE;

→ Indicar dados verdadeiros no pedido submetido à ECCE;

→ Apresentar os documentos exigidos que confirmem as informações incluídas no pedido de certificação;

→ Informar imediatamente a ECCE sobre quaisquer erros, defeitos ou alterações no certificado;

→ Aplicar o seu próprio par de chaves e as chaves públicas de outros utilizadores de serviços de certificação apenas para os propósitos indicados na Declaração de Práticas de Certificação e que o mesmo tome todas as medidas razoáveis para manter a confidencialidade e proteja de forma adequada a chave privada, incluindo:

- Controlar o acesso a dispositivos que contenham sua chave privada;
- Informar imediatamente a ECCE quando uma chave privada foi ou há uma razão para suspeitar fortemente que está comprometida;

- Não criar qualquer assinatura eletrónica com sua chave privada se o período de validade do certificado tiver expirado, o certificado tiver sido revogado ou suspenso;

- Controlar o acesso ao *software* e dispositivos nos quais as chaves ou credenciais são armazenadas;

- Providenciar que as chaves privadas estão inacessíveis para outras pessoas;

- Iniciar um procedimento de revogação em caso de violação de segurança ou violação de segurança suspeita da sua chave privada;

- Providenciar que o certificado qualificado e a chave privada correspondente apenas são utilizados para os fins indicados no certificado e de acordo com os objetivos e restrições indicados neste documento.

5. OBRIGAÇÃO DE CONTROLO DO ESTADO DO CERTIFICADO PELAS PARTES DE CONFIANÇA

Uma parte confiável, usando os serviços ECCE, pode ser qualquer entidade que aceite a assinatura eletrónica qualificada com base na validade da conexão entre a identidade do assinante e sua chave pública, confirmada pelas autoridades de certificação ECCE.

Uma parte confiante está comprometida a:

→ Verificar se uma assinatura eletrónica foi criada por meio de uma chave privada correspondente a uma chave pública definida no certificado do assinante, emitido pela ECCE;

→ Verificar se uma mensagem/documento assinado ou um certificado não foram modificados após a assinatura;

→ Realizar operações criptográficas com precisão e correção, utilizando o *software* e dispositivos cujo nível de segurança atende ao nível de sensibilidade do certificado em processamento e ao nível de confiança dos certificados aplicados;

→ Considerar que a assinatura eletrónica ou o certificado sejam inválidos se, por meio de *software* e dispositivos aplicados, não é possível indicar se a assinatura eletrónica ou o certificado são válidos ou se o resultado da verificação é negativo;

→ Confiar apenas nesses certificados qualificados que são usados de acordo com o propósito declarado e são apropriados para intervalos de aplicabilidade especificados

pela parte confiável, sendo o respetivo estado verificado com base nas listas de revogação de certificados ou no serviço OCSP, ambos disponibilizados pela ECCE.

6. GARANTIA LIMITADA E RENÚNCIA/LIMITAÇÕES DE RESPONSABILIDADE

A ECCE não assume qualquer responsabilidade pelas ações de terceiros, assinantes e outras partes não associadas à ECCE. Em particular ECCE não assume a responsabilidade de:

→ Danos decorrentes de catástrofes naturais, tais como: fogo, inundação, tempestade, outras situações como guerra, ataque terrorista, epidemia e outros desastres naturais ou desastres causados por pessoas;

→ Danos decorrentes da instalação e uso de aplicativos e dispositivos usados para gerar e manusear chaves criptográficas, criptografia, criação de assinatura eletrónica que não esteja incluída na lista de aplicativos autorizados;

→ Danos decorrentes do uso inadequado de certificados emitidos, como seja o uso de um certificado revogado, inválido ou suspenso;

→ Armazenamento de dados falsos nas bases de dados da ECCE e sua publicação em lista de certificado público emitida para o assinante, no caso deste ter declarando tais dados falsos.

7. ACORDOS APLICÁVEIS, DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO E POLÍTICA DE CERTIFICADO

A ECCE publica no repositório https://www.ecce.gov.pt os seguintes documentos:

→ Política de Certificação;

→ Declaração de Práticas de Certificação dos Serviços Qualificados.

8. POLITICA DE PRIVACIDADE

Os dados do assinante são processados pela ECCE, de acordo com a legislação aplicável para proteção de dados pessoais em vigor.

Para mais detalhes, deverá ser consultada a Política de Privacidade da ECCE, disponível em: https://www.ecce.gov.pt/repositorio/politica-de-privacidade.

9. POLÍTICA DE REEMBOLSO

A ECCE esforça-se para garantir o mais alto nível de qualidade de seus serviços. O reembolso não é aplicável aos serviços prestados pela ECCE.

10. LEIS APLICÁVEIS, RECLAMAÇÕES E RESOLUÇÃO DE DISPUTAS

A operação da ECCE baseia-se nas regras gerais estabelecidas na Declaração de Práticas de Certificação e está de acordo com a legislação em vigor na República Portuguesa e nos atos supranacionais aplicáveis. Eventuais disputas relacionadas com os serviços qualificados da ECCE serão submetidas ao foro de tribunal administrativo de acordo com o estipulado.

11. AUTORIDADE DE CERTIFICADO E LICENÇAS DE REPOSIÇÃO, MARCAS DE CONFIANÇA E AUDITORIA

As auditorias que verificam a consistência na ECCE com os regulamentos, preceitos legais e boas práticas, são realizadas pelo menos uma vez por ano, por entidade externa acreditada para o efeito.

12. IDENTIFICAÇÃO DESTE DOCUMENTO

Este documento foi registado na ECCE e foi-lhe atribuído o *Object Identifier* (OID) 2.16.620.1.1.1.2.3.2.6.

13. PONTOS DE REGISTO E PONTOS DE CONFIRMAÇÃO DA IDENTIDADE

Os pontos de registo e verificação da identidade estão disponíveis em https://www.ecce.gov.pt.

FIM DO DOCUMENTO