PKI DISCLOSURE STATEMENT

Entidade Certificadora Comum do Estado – ECCE

SISTEMA DE CERTIFICAÇÃO ELETRÓNICA DO ESTADO (SCEE)

INFRAESTRUTURA DE CHAVES PÚBLICAS

OID: 2.16.620.1.1.1.2.3.2.1

2017.08.24

Documento Público

CONTROLO DE VERSÕES

Data	Versão	Autor da Alteração	Descrição da Alteração
2017/08/24	1.0	João Reis Silva (Coordenador DQS)	Versão Inicial do documento no âmbito do Regulamento eIDAS

APROVAÇÃO E ASSINATURA

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

O Diretor do Centro de Gestão da Rede Informática do Governo

Tito Carlos Soares Vieira

Digitally signed by Tito Carlos Soares Vieira
DN: c=PT, o=Centro de Gestão da Rede Informática do Governo, cn=Tito Carlos Soares Vieira
Date: 2017.11.20 22:48:21 Z

Tito Carlos Soares Vieira

CONTEÚDO

1. INFORMAÇÕES DE CONTATO DA AUTORIDADE DE CERTIFICADO

Entidade Certificadora Comum do Estado (ECCE)

Centro de Gestão da Rede Informática do Governo (CEGER)

Rua Almeida Brandão Nº 7

1200-602 Lisboa

Portugal

Site: https://www.ecce.gov.pt/

Email: certificacao@ecce.gov.pt

2. TIPO DE CERTIFICADO, PRÁTICAS DE VALIDAÇÃO E USO

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.

PROCEDIMENTO DE VALIDAÇÃO

Certificado qualificado é emitido para uma pessoa após a verificação da sua identidade. A verificação da pessoa pode ser realizada por uma autoridade de registro 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 identificado 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 o, em alternativa, o registo oficial ou do registo comercial dos poderes conferidos.

Uso

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 de 2014, sobre serviços eletrônicos de identificação e confiança para transações eletrônicas no mercado interno e que revoga a Diretiva 1999/93 / CE.

3. LIMITES DE CONFIANÇA

Não aplicável, no âmbito da SCEE, de acordo com o P.Cert e a legislação nacional.

4. OBRIGAÇÕES DOS SUBSCRITORES

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

O assinante comprometeu-se a:

- cumprir as regras do acordo celebrado com a ECCE;

- indicar dados verdadeiros no pedido submetidas 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 seu próprio par de chaves e as chaves públicas de outros usuários de serviços de certificação apenas para os propósitos indicados na Declaração de Prática de Certificação e que o mesmo tome todas as medidas razoáveis para

manter a confidencialidade e proteja de forma adequada a chave particular, incluindo:

- controlar do 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 será comprometida;

- não criar qualquer assinatura eletrônica 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 no 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 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 eletrônica 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 eletrônica 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 o nível de confiança dos certificados aplicados;

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

- Confiar apenas esses certificados qualificados que são usados de acordo com o propósito declarado e são apropriados para intervalos de aplicabilidade que foram especificados pela parte confiável e o estado foi verificado com base nas listas de revogação de certificados válidas ou no serviço OCSP 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 eletrônica que não esteja incluída na lista de aplicativos autorizados;

- danos decorrentes do uso inadequado de certificados emitidos, tais como 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 do assinante ter declarando tais dados como falsos.

7. ACORDOS APLICÁVEIS, DECLARAÇÃO DE PRÁTICA DE CERTIFICAÇÃO, POLÍTICA DE CERTIFICADO

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

- Política de Certificação dos Serviços de Certificação Qualificados da ECCE;

- Declaração de Prática de Certificação dos Serviços de Certificação Qualificada da ECCE.

8. POLÍTICA DE PRIVACIDADE

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

9. POLÍTICA DE REEMBOLSO

O ECCE esforça-se para garantir o mais alto nível de qualidade de seus serviços. O reembolso não é aplicável aos serviços prestados pela ECCE, de acordo com o estabelecido na DPCert da ECCE e na PCert do SCEE.

10. LEIS APLICÁVEIS, RECLAMAÇÕES E RESOLUÇÃO DE DISPUTAS

A operação do ECCE baseia-se nas regras gerais estabelecidas na Declaração de Prática 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 submetidos ao foro de tribunal administrativo de acordo com o estabelecido na PCert do SCEE e DPCert da ECCE.

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

Auditorias que verificam a consistência com os regulamentos e preceitos legais, em particular a consistência com a DPCert da ECCE e a PCert do SCEE é realizada pelo menos uma vez por ano.

12. IDENTIFICAÇÃO DESTE DOCUMENTO

Este documento foi registrado com ECCE e foi atribuído um Object Identifier (OID): 2.16.620.1.1.1.2.3.2.1

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