PKI DISCLOSURE STATEMENT

Entidade Certificadora Comum do Estado - ECCE

Access Level: Public Document
Version: 6.0
Date: 2023.04.10
OID: 2.16.620.1.1.1.2.3.7.6

APPROVAL AND SIGNATURE

I approve this document and its entry into force upon signature.

The Director of 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 12:25:37 +01'00'

(José Manuel Louro Pereira)

DOCUMENT CONTROL

VERSION	DATE	AUTHOR	DESCRIPTION
1.0	2017/08/24	João Reis Silva	Initial Version of the document under the Regulation eIDAS
2.0	2018/12/18	João Reis Silva	Annual revision with insertion of new document template
3.0	2020/01/16	Rui Jorge Silva	Annual review with no major changes
4.0	2021/02/25	Rui Jorge Silva	Annual review. A reference to the Privacy Policy has been added.
5.0	2022/05/04	Rui Jorge Silva	Annual review with no major changes.
6.0	2023-04-10	Rui Jorge Silva	Annual review with no major changes.

Contents

1. CERTIFICATE AUTHORITY CONTACT INFORMATION

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

Portugal

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

Email: certificacao@ecce.gov.pt

2. CERTIFICATE TYPE, VALIDATION PROCEDURES AND USAGE

2.1 Certificate Type

This statement applies only to qualified certification services provided by ECCE. Public key qualified certificates are issued by the qualified certification authority of ECCE within the ECCE qualified certification services. Profile and any other limitation of certified public key certificate issued by the ECCE are compliant with the ETSI EN 319 411-2-v2.2.2.

2.2 Validation Procedure

The Qualified certificate is issued to an individual after verification of their identity. Verification of the individual may be conducted by a registration authority or by other person who is authorized to confirm identity of the certificate holder. The individual, requesting issuance of a qualified certificate, shall be identified by his national identity document. In case of individuals associated or acting on behalf of an organization, the authorization of the subscriber (the signatory) to act and to use the certificate on behalf of the organization is required or the official government or trade register record of the powers is required.

2.3 Usage

The Qualified certificates issued by ECCE may be used only in accordance with Regulation (EU) n. º 910/2014, of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

3. RELIANCE LIMITS

Not applicable, in the scope of ECCE, in accordance with the certification policy and Portuguese legislation.

4. OBLIGATIONS OF SUBSCRIBERS

By applying for the certificate issuance and entering the subscriber agreement, the subscriber agrees to enter the certification system pursuant to the conditions stated in Certification Practice for Qualified Certification Services of ECCE.

Subscriber is committed to:

→ Comply with the rules of the agreement made with ECCE;

→ State true data in applications submitted to the ECCE;

→ Submit or present of required documents confirming the information included in a certification request;

→ Immediately inform ECCE about any errors, defects, or changes in the certificate;

→ Apply his own key pair and the public keys of other certification services users only for the purposes stated in the Certification Practice Statement and to take all reasonable measures to keep confidential, and properly protect at all times the private key, including:

● Control of the access to devices containing his private key;

● Immediately inform ECCE when a private key has been or there is a reason to strongly suspect it would be compromised;

● Do not create any electronic signature with its private key if the validity period of certificate has expired and certificate has been revoked or suspended;

● Control the access to this software, media, and devices on which the keys or passwords are stored;

● Make his private keys inaccessible to other persons;

● Start a procedure of revocation in the case of security violation or security violation suspicion of his private key;

● Apply qualified certificates and the corresponding private key only for the purpose stated in the certificate and in accordance with the aims and restrictions stated in this document.

5. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES

A relying party, using ECCE services, can be any entity who accept the qualified electronic signature relying on validity of the connection between subscriber's identity and his public key confirmed by ECCE certification authorities.

A relying party is committed to:

→ Verify that an electronic signature has been created by means of a private key corresponding to a public key set in the subscriber's certificate issued by ECCE;

→ Verify that a signed message/document or a certificate have not been modified after being signed;

→ Conduct cryptographic operations accurately and correctly, using the software and devices whose security level complies with the sensitivity level of the certificate being processed and the trust level of applied certificates;

→ Consider the electronic signature or the certificate to be invalid if by means of applied software and devices it is not possible to state if the electronic signature or the certificate are valid or if the verification result is negative;

→ Trust only these qualified certificates that are used in accordance with the declared purpose and are appropriate for applicability ranges that were specified by the relying party, and the status was verified based on the valid Certificate Revocation Lists or OCSP service available at ECCE.

6. LIMITED WARRANTY & DISCLAIMER/ LIMITATION OF LIABILITY

The ECCE does not take any responsibility for the actions of third parties, subscribers and other parties not associated with ECCE. In particular ECCE does not bear responsibility for:

→ Damages arising from forces of nature: fire, flood, gale, other situations such as war, terrorist attack, epidemic, and other natural disasters or disasters caused by people;

→ Damages arising from the installation and usage of applications and devices used for generating and managing cryptographic keys, encryption, creating of an electronic signature that are not included in the authorized applications list;

→ Damages arising from inappropriate usage of issued certificates like the use of a revoked, invalidated, or suspended certificate;

→ Storage of false data in ECCE database and their publication in a public certificate key issued to the subscriber in the case of subscriber's stating such false data.

7. APPLICABLE AGREEMENTS, CERTIFICATION PRACTICE STATEMENT, CERTIFICATE POLICY

The ECCE publishes at the repository https://www.ecce.gov.pt the following documents:

→ Certification Policy;

→ Qualified Services Certification Practice Statement.

8. PRIVACY POLICY

The Subscriber data is processed by ECCE, in accordance with the applicable legislation for personal data protection in force.

For further details, please refer to the ECCE Privacy Policy, available at: https://www.ecce.gov.pt/repositorio/politica-de-privacidade.

9. REFUND POLICY

The ECCE makes efforts to secure the highest level of quality of its services. The refund is not applicable, in the scope of ECCE.

10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

The operation of ECCE is based on the general rules stated in the Certification Practice Statement and it is in accordance with the legal acts in force in the Republic of Portugal and the applicable supranational acts. Disputes related to ECCE qualified services will be submitted to the Administrative Court in accordance with the stipulated.

11. CERTIFICATE AUTHORITY AND REPOSITORY LICENCES, TRUST MARKS, AND AUDIT

The audits that verify consistency in the ECCE with the regulations, legal and good practices, are conducted at least once a year by an accredited external entity for this purpose.

12. IDENTIFICATION OF THIS DOCUMENT

This document has been registered within ECCE and has been assigned the Object Identifier (OID) 2.16.620.1.1.1.2.3.7.6.

13. REGISTRATION POINTS, POINTS OF THE IDENTITY CONFIRMATION

The points of registration and identity verification can be found at https://www.ecce.gov.pt.

END OF DOCUMENT