



PKI DISCLOSURE STATEMENT

Entidade Certificadora Comum do Estado – ECCE

SISTEMA DE CERTIFICAÇÃO ELETRÓNICA DO ESTADO (SCEE)
INFRAESTRUTURA DE CHAVES PÚBLICAS

OID: 2.16.620.1.1.1.2.3.7.1

2017.08.24

Public Document



VERSION CONTROL

Date	Version	Author of change	Description of change
2017/08/24	1.0	João Reis Silva (Coordinator DQS)	Initial Version of the document under the Regulation eIDAS

APPROVAL AND SIGNATURE

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

Tito Carlos Soares Vieira

(Director of Government Computer Network Management Center)



CONTENTS

1.	CERTIFICATE AUTHORITY CONTACT INFORMATION	4
2.	CERTIFICATE TYPE, VALIDATION PROCEDURES AND USAGE	4
	Certificate type	4
	Validation procedure	4
	Usage	5
3.	RELIANCE LIMITS	5
4.	OBLIGATIONS OF SUBSCRIBERS	5
5.	CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES	6
6.	LIMITED WARRANTY & DISCLAIMER/ LIMITATION OF LIABILITY	7
7.	APPLICABLE AGREEMENTS, CERTIFICATION PRACTICE STATEMENT, CERTIFICATE POLICY..	7
8.	PRIVACY POLICY.....	8
9.	REFUND POLICY.....	8
10.	APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION.....	8
11.	CERTIFICATE AUTHORITY AND REPOSITORY LICENCES, TRUST MARKS AND AUDIT.....	8
12.	IDENTIFICATION OF THIS DOCUMENT	8
13.	REGISTRATION POINTS, POINTS OF THE IDENTITY CONFIRMATION	9



1. CERTIFICATE AUTHORITY CONTACT INFORMATION

Entidade Certificadora Comum do Estado (ECCE)

Centro de Gestão da Rede Informática do Governo (CEGER)

Rua Almeida Brandão N° 7

1200-602 Lisboa

Portugal

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

Email: certificacao@ecce.gov.pt

2. CERTIFICATE TYPE, VALIDATION PROCEDURES AND USAGE

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.

VALIDATION PROCEDURE

Qualified certificate is issued to an individual after verification of their identity. Verification of the individual may be carried out 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.



USAGE

Qualified certificates issued by ECCE may be used only in accordance with REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF 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 to the PCert of SCEE 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 Practice Statement 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 certificate 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;
- carry out 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

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

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



- Certification Policy of SCEE;
- Certification Practice Statement of ECCE.

8. PRIVACY POLICY

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

9. REFUND POLICY

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

10. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

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 to the PCert of SCEE and Certification Practice Statement of ECCE.

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

Audits checking the consistency with procedural and legal regulations particularly the consistency with Certification Practice Statement and Certification Policy is carried out at least once a year.

12. IDENTIFICATION OF THIS DOCUMENT

This document has been registered with ECCE and has been assigned an Object Identifier (OID) of: 2.16.620.1.1.1.2.3.7.1



13. REGISTRATION POINTS, POINTS OF THE IDENTITY CONFIRMATION

The points of registration and identity verification can be find on <https://www.ecce.gov.pt>.

END OF DOCUMENT