# PKI Disclosure Statement

**Effective Date: 12 February 2024**

**Version 1.8**

## Document History

| Version | Date | Author | Reason for Change |
|---|---|---|---|
| **0.1** | 05/06/2018 | Paris Erotokritou | Initial version |
| **1.0** | 26/07/2018 | Paris Erotokritou | Initial publication |
| **1.1** | 26/06/2019 | Paris Erotokritou | Minor changes regarding Appendix A, chapter 4 |
| **1.2** | 31/03/2020 | Paris Erotokritou | Minor change regarding chapter 8 |
| **1.3** | 15/07/2020 | Paris Erotokritou | Minor Changes regarding chapter 5 |
| **1.4** | 08/03/2021 | Paris Erotokritou | CP/CPS has been included in section 8 for the issuance of certificates under JCC Root CA |
| **1.5** | 19/07/2021 | Paris Erotokritou | Changes in chapter 4, 8 and 13 due to National Electronic Identity (eID) |
| **1.6** | 08/06/2022 | Paris Erotokritou | Revised Date |
| **1.7** | 31/10/2022 | Paris Erotokritou | Changes regarding the inclusion of Qualified short-term certificates & Remote eSeals |
| **1.8** | 12/02/2024 | Paris Erotokritou | Changes regarding the inclusion of Advanced Electronic Seals |

## Document Approvals

| Version | Date | Approved By |
|---|---|---|
| **0.1** | 07/06/2018 | Andreas Savva |
| **0.1** | 08/06/2018 | Nicodemos Damianou |
| **1.0** | 26/07/2018 | Steering Committee |
| **1.1** | 26/06/2019 | Nicodemos Damianou |
| **1.2** | 31/03/2020 | QTSP Policy Management |
| **1.3** | 15/05/2020 | QTSP Policy Management |
| **1.4** | 08/08/2021 | QTSP Policy Management |
| **1.5** | 20/07/2021 | QTSP Policy Management |
| **1.6** | 08/06/2022 | Andreas Savva |

| | | |
|---|---|---|
| **1.7** | 31/10/2022 | QTSP Policy Management |
| **1.8** | 12/02/2024 | QTSP Policy Management |

### Document Distribution List

| Version | Date | Role/Name |
|---|---|---|
| **0.1** | 08/06/2018 | All QTSP Staff |
| **1.0** | 26/07/2018 | All QTSP Staff |
| **1.1** | 26/06/2019 | All QTSP Staff |
| **1.2** | 01/04/2020 | All QTSP Staff |
| **1.3** | 20/07/2020 | All QTSP Staff |
| **1.4** | 02/06/2021 | All QTSP Staff |
| **1.5** | 20/07/2021 | All QTSP Staff |
| **1.6** | 08/06/2022 | All QTSP Staff |
| **1.7** | 31/10/2022 | All QTSP Staff |
| **1.8** | 12/02/2024 | All QTSP Staff |

# Contents

## 1. Overview

This document aims at providing the Subscriber and Relying Parties of Qualified Certificates with a quick recap concerning the information available in JCC Payment Systems' Certificate Practice Statements (CPSs) and Terms and Conditions.

*This document does not substitute or replace the Terms and Conditions nor the CPSs, it just summarizes the key points for the benefit of the Subscribers and Relying Parties*

## 2. Contact info

JCC Payment Systems Ltd

Qualified Trust Service Provider
1 Stadiou Street
2571 Industrial Area Nisou
Cyprus

Web: http://www.jcc.com.cy
E-mail: trust-policies@jcc.com.cy

Telephone: (+357) 22 868 500
Fax: (+357) 22 868 591

## 3. Obligations of Subscriber

The certificate subscriber has the obligations set forth in the CPSs and the Terms & Conditions. In particular, but not limited , the subscriber has the following obligations:

- Provide the CA with precise and true information in the certificate request
- Use the certificate only in the ways and for the purposes provided for in the CPSs;
- Shall protect and ensure the safety of his/her local QSCD and the environment that this is used
- Shall protect and ensure the safety of his/her authentication credentials in case of the remote QSCD and the environment that this is used
- Shall protect and ensure the safety of the private key in case of non-QSCD and the environment that this is used
- Not to leave the local QSCD exposed and place it in a secure location
- Not to leave the private key exposed in case of non-QSCD and place it in a secure location
- Not to leave the authentication credentials of the remote QSCD exposed
- Treat the local QSCD as any object containing private and confidential data
- Treat authentication credentials as private and confidential data

- In the event of a confirmed compromise of any of their own private keys or other reasons such as change of OTP generation device (e.g mobile phone), immediately contact JCC Payment Systems (Ref. 2 – Contact Info)
- Not to continue using the private key if the Certificate has been revoked, expired or the CA has been compromised

## 4. Revocation

A Subscriber can revoke his/her certificate by:

- Online by logging to JCC Portal https://trust.jcc.com.cy/aqs-portal/

Also, a Subscriber requesting revocation or a successor who wishes to request revocation in case of a deceased Subscriber (natural person) provided that is legally eligible, can send his/her request via e-mail or call:

*Working days (08:00-14:30):*

- e-mail at revocation@jcc.com.cy
- Call (+357) 22 868 500

*24 x 7 Service:*

- Call (+357) 22 868 500

JCC Payment Systems will promptly initiate revocation of the certificate. The Revocation form can be found at https://pki.jcc.com.cy/repository

A Cypriot Citizen can revoke his/her Electronic Identity (eID) by:

- Online by logging to JCC Portal https://trust.jcc.com.cy/aqs-portal/ and using his eID
- By visiting one of the Service Providers service areas and signing a revocation request form

## 5. Certificates types, validation procedures and usage

- Qualified certificate to natural person for eSignature. Qualified Certificates for Electronic Signatures issued to Natural Person are either Long-term or Short-term. A Long-Term Certificate is valid for 1 to 3 years and a Short-Term Certificate (SLC) is valid up to 24 hours.
- Qualified certificate to natural person associated with legal person for eSignature,
- Qualified certificate to legal person for eSeal,
- Authentication certificate to natural person

Advanced certificate to legal person for eSeal (without the use of a QSCD)JCC Payment Systems issues all above types of Qualified Certificates on both local QSCD as well as remote QSCD, except Authentication Certificates for the purpose of eID and Short-term Qualified certificates which are only provided on a remote QSCD.

Validation procedures comply with the latest version of the Validation Plans.

Certificates shall be used as prescribed by the CPS and Terms and Conditions only. Any different usage is forbidden.

JCC CA Certificates are issued according to the certificate policies mentioned in CPS section 1.2.

## 6. Certificate status checking obligations of Relying parties

Relying Parties shall check the status of Certificates on which they wish to rely. A way of checking the status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely.

Alternatively, Relying Parties may check the Certificate status by using the relevant OCSP URL published in JCC repository(https://pki.jcc.com.cy/repository).

## 7. Reliance Limits

Audit logs are retained on-site for no less than two (2) months. Physical or digital archive records regarding Certificate applications, registration information and requests or applications for suspension, termination of suspension and revocation are retained for at least seven (7) years after the expiry of the relevant Certificate.

## 8. Applicable Agreements, CP, CPS

Relevant agreements, policies and practice statements for use of Certificates are:

- JCC Payment Systems Certificate Policy
- Certification Practice Statement for authentication certificates and for EU Qualified certificates for electronic signatures & electronic seals (This CPS concerns the certificates issued under JCC Root CA)
- Certification Practice Statement for Cyprus National Electronic Identity (eID) (This CPS concerns the eIDs issued under JCC Root CA)
- Certificate and OCSP Profiles for authentication certificates and for EU Qualified Certificates for Electronic Signatures & Electronic Seals.

Current versions of all applicable documents are publicly available in the JCC Payment Systems repository https://pki.jcc.com.cy/repository

## 9. Refund Policy

JCC Payment Systems makes efforts to secure the highest level of quality of its services.

The exercise of the right to refund shall be made by a written request by the Subscriber to JCC Payment Systems, by sending an email to trust-sales@jcc.com.cy. JCC Payment Systems will handle the refund requests based on applicable law.

## 10.Privacy Policy

JCC Payment Systems process personal data in accordance to the applicable data protection legislation in force. For further details, please refer to JCC Payment Systems Privacy Statement https://pki.jcc.com.cy/repository.

## 11.Repository Licenses, Trust Marks and Audit

JCC Payment Systems Ltd is a Qualified Trust Service Provider and is granted the qualified status by a supervisory body and is listed in the EU Trusted List for Trust Service Providers, following the submission of a conformity assessment report by an accredited Conformity Assessment Body.
JCC Payment Systems Trust Services for authentication certificates and for EU Qualified certificates for electronic signatures & electronic seals are register as a Qualified Trust Service Provider in the EU Member States trusted list as defined in Regulation (EU) No 910/2014 which include information related to the qualified trust service providers which are supervised by the competent Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in the Regulation. The Cyprus Trusted List is available at the following URL:

http://www.mcw.gov.cy/mcw/dec/dec.nsf/All/146E36DA8D517E04C22576A10040DE5E?Opendocument

The prerequisite requirement of this registration is in compliance with applicable regulations and standards.

The Conformity Assessment Body is accredited in accordance with Regulation (EC) No 765/2008 as competent to carry out conformity assessment of the Qualified Trust Service Provider and qualified Trust Services it provides.

## 12. Limited warranty and Disclaimer, Limitation of liability

For warranty and liability limitations, please refer to the Terms and Conditions published on the JCC Payment Systems website at https://pki.jcc.com.cy/repository

## 13. Applicable Law, Complaints, Dispute Resolution

JCC Payment Systems ensures compliance with the legal requirements to meet all applicable statutory requirements for protecting records from loss, destruction and falsification, and the requirements of the following:

- eIDAS - 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;
- Governing Law & decrees for Cyprus National Electronic Identity

- Personal Data laws and EU Regulations;
- Related European Standards:

1. ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
2. ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
3. ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates;

Any disputes related to the Trust Services provided by JCC Payment Systems shall be governed by the laws of Cyprus. The Subscriber must notify JCC Payment Systems of any dispute, claim or complaint, not later than thirty (30) calendar days after the detection of the basis of the claim, unless otherwise provided by law.

If the dispute is not resolved within sixty (60) days after the initial notice, then a party may seek legal resolution. Courts of Cyprus, shall have exclusive jurisdiction and venue for hearing and resolving any dispute.

## Appendix A. Table of Acronyms and definitions

**Table of Acronyms**

| Term | Definition |
|---|---|
| **CA** | Certification Authority |
| **CP** | Certificate Policy |
| **CPS** | Certification Practice Statement |
| **CRL** | Certificate Revocation List |
| **OCSP** | Online Certificate Status Protocol |
| **OTP** | One-Time Password |
| **QSCD** | Qualified Electronic Signature Creation Device |

**Definitions**

| Term | Definition |
|---|---|
| **JCC PAYMENT SYSTEMS Repository** | JCC PAYMENT SYSTEMS's database of Certificates and other relevant JCC PAYMENT SYSTEMS information accessible on-line. |
| **Authentication** | Unique identification of a natural person by checking his/her alleged<br>identity |
| **Certificate** | Public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it |
| **Certificate Applicant** | An individual or organization that requests the issuance of a Certificate by a CA. |
| **Certificate Application** | A request from a Certificate to a CA for the issuance of a Certificate. |
| **Certificate Chain** | An ordered list of Certificates containing a Subscriber Certificate and CA Certificates, which terminates in a root Certificate. |

| Term | Definition |
|---|---|
| **Certificate Policy (CP)** | Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements |
| **Certificate Revocation List (CRL)** | Signed list indicating a set of certificates that have been revoked by the certificate issuer |
| **Certificate Signing Request (CSR)** | A message conveying a request to have a Certificate issued. |
| **Certification Authority (CA)** | An entity authorized to create and assign certificates |
| **Certification Practice Statement (CPS)** | Statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates |
| **Electronic Signature**, authentication | Data in electronic form which are attached to or logically associated with other electronic data and which is used by the signatory to sign. |
| **Electronic seal** | Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity. |
| **Local QSCD** | USB token or smart card type of QSCD |
| **Online Certificate Status Protocol (OCSP)** | A protocol for providing Relying Parties with real-time Certificate status information. |
| **Practice Statement** | A statement of the practices that a TSP employs in providing a Trust Service. |
| **Private key** | The key of a key pair that is kept secret by the holder of the key pair, and that is used to create a qualified certificate or to decrypt electronic records or files that were encrypted with the corresponding public key |
| **Public Key** | The key of a key pair that may be publicly disclosed by the holder of corresponding private key and that is used by Relying Party to verify |

| Term | Definition |
|---|---|
| | a qualified certificate created with the holder’s corresponding private key and/or to encrypt messages so that they can be decrypted only with the holder’s corresponding private key. |
| **Qualified electronic seal** | Is an advanced electronic seal that is created by a qualified electronic seal creation device and is based on a qualified certificate for electronic seals. |
| **Qualified electronic Signature** | An advanced electronic signature that is created by a qualified electronic signature creation device, and is based on a qualified certificate for electronic signatures; |
| **Qualified Certificate** | Qualified Certificate is a Certificate issued by a CA which has been accredited and supervised by authorities designated by an EU member state and meets the requirements of eIDAS. Qualified Certificates for Electronic Signatures are either Long-term or Short-term. A Long-Term Certificate is valid for 1 to 3 years and a Short-Term Certificate is valid up to 24 hours. |
| **Qualified signature creation device (QSCD)** | A device that is responsible for qualifying digital signatures by using specific hardware and software that ensures that the signatory only has control of their private key. Qualified electronic signature or seal creation devices meet the requirements of eIDAS. |
| **Qualified Trust Service Provider** | A trust service provider who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body. |
| **Relying Party** | An individual or organization that acts in reliance on a certificate. |
| **Remote QSCD** | Server based HSM that is used for central generation and usage of Subscriber private keys. |
| **Revocation** | Permanent termination of the certificate's validity before the expiry date indicated in the certificate |
| **Subscriber** | An entity subscribing with Trust Service Provider who is legally bound to any Subscriber obligations. |

| Term | Definition |
|---|---|
| **Supervisory Body** | The authority which is designated by member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS in the territory of that member state. |
| **Trust Service** | Electronic service for:<br>creation, verification, and validation of digital signatures, authentication and related certificates;<br>creation, verification, and validation of time-stamps and related certificates;<br>registered delivery and related certificates;<br>creation, verification and validation of certificates for website authentication; or<br>preservation of digital signatures, authentication or certificates related to those services. |
| **Trust Service Provider** | An entity that provides one or more Trust Services. |