General Terms and Conditions for Use of Certificates

Effective Date: 26 July 2018

Version 1.0

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

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

Document Distribution List

Department	Role/Name	Date

Definitions and Acronyms

Term/Acronym	Definition
Authentication	Unique identification of a person by checking his/her alleged identity.
CA	Certificate Authority: A part of JCC Payment Systems structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature.
Certificate	Public Key, together with additional information, laid down in the Certificate Profile rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it.
CP	Symantec Certificate Policy for qualified certificates.
CPS	Certification Practice Statement.
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.
OCSP	Online Certificate Status Protocol.
OID	An identifier used to uniquely name an object.
PIN code	Activation code for the Qualified Certificates for Electronic Signatures and for Electronic Seals.
Private Key	The key of a key pair that is assumed to be kept in secret by the holder of the key pair, and that is used to create electronic signatures and/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 the corresponding Private Key and that is used by Relying Parties to verify electronic signatures 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 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 Electronic Signature	Advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a Qualified Certificate for electronic signatures.
Qualified Electronic Seal	Advanced electronic seal that is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.
QSCD	A Secure Signature Creation Device that meets the requirements laid down in eIDAS Regulation.
Relying Party	Entity that relies on the information contained within a Certificate.
Qualified trust service	A trust service, as defined in eIDAS, that meets the applicable requirements laid down in this Regulation.
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.
JCC Payment Systems	A trust service provider.
Subject	The subject can be: a) a natural person; b) a natural person identified in association with a legal person; c) a legal person (that can be an Organization or a unit or a department identified in

	association with an Organization);
Subscriber	An entity subscribing with Trust Service Provider who is legally bound to any Subscriber obligations.
General Terms and Conditions for Use of Qualified Certificates	Present document that sets forth the terms and conditions under which a natural or legal person acts as a Subscriber and/or as a Subject or as a Relying Party and JCC Payment Systems provides the corresponding Trust Services.

1. General Terms

Present General Terms and Conditions describe main policies and practices followed by JCC Payment Systems and provided in CP and CPS, that are also described in a supplemental and simplified way in the PKI Disclosure Statement (PDS), for authentication certificates and for EU Qualified certificates for electronic signatures & electronic seals.

1.1 The Terms and Conditions govern Subscribers' use of the Certificates and constitute a legally binding contract between Subscriber and JCC Payment Systems.

1.2 The Subscriber has to be familiar with and accept the Terms and Conditions.

1.3 JCC Payment Systems has the right to amend the Terms and Conditions at any time should JCC Payment Systems have a justified need for such amendments. Information on the amendments will be published on the website. https://pki.jcc.com.cy/repository.

1.4 The Subscriber can apply for:

1.4.1 EU Qualified Certificate for Electronic Signatures only personally, except in case the Subscriber is a legal person and the Subject is a natural person associated with the legal person.

1.4.2 EU Qualified Certificate for Electronic Seals through the natural person representing the legal person to whom the Qualified Certificate for the Qualified Electronic Seal is provided.

1.4.3 Authentication Certificate for natural person

2. Certificate Acceptance

2.1 Upon submitting an application for a Certificate, the Subscriber confirms that he/she is familiar with and accepts the Terms and Conditions.

The following conduct constitutes Certificate acceptance for authentication certificates and for EU Qualified certificates for electronic signatures & electronic seals::

- Failure of the Subscriber to object to the Certificate or its content within 24 hours from downloading it constitutes Certificate acceptance.

2.2 If the Certificate re-keying is performed the Subscriber confirms that he/she has read and agrees to the Terms and Conditions.

2.3 Certificate Type, Usage and Certification Procedure

Certificate Type	Usage	Certification Policy Applied and Published
For Qualified Electronic Signatures compliant with eIDAS.	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign	JCC Payment Systems Certification Practice Statement for authentication certificates and for EU Qualified certificates for electronic signatures & electronic seals published https://pki.jcc.com.cy/repository ETSI EN 319 411-2 Policy: QCP-n-qscd
For Qualified Electronic Seals compliant with eIDAS.	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.	JCC Payment Systems Certification Practice Statement for EU Qualified certificates for authentication certificates and for EU Qualified certificates for electronic signatures & electronic seals published https://pki.jcc.com.cy/repository ETSI EN 319 411-2 Policy: QCP-l-qscd
For Authentication	Data in electronic form which is attached to or logically associated	JCC Payment Systems Certification Practice Statement for authentication certificates and for

	with other data in electronic form and which is used by the Subscriber to authenticate himself	EU Qualified certificates for electronic signatures & electronic seals published https://pki.jcc.com.cy/repository ETSI EN 319 411-1

3. Prohibitions of use

3.1 The use of the Subscriber´s Certificates is prohibited for any of the following purposes:

3.1.1 unlawful activity (including cyber-attacks and attempt to infringe the Certificate);
3.1.2 issuance of new Certificates and information regarding Certificate validity;
3.1.3 enabling other parties to use the Subscriber's Private Key;
3.1.4 enabling the Certificate issued for electronic signing to be used in an automated way;
3.1.5 using the Certificate issued for electronic signing for signing documents which can bring about unwanted consequences (including signing such documents for testing purposes).
3.1.6 enabling the Authentication Certificate to create Qualified Electronic Signatures compliant with eIDAS.

4. Reliance Limits

4.1 Certificates become valid as of the date specified in the Certificate.
4.2 The validity of the Certificate expires on the date of expiry indicated in the Certificate or if the Certificate is revoked.
4.3 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.

5. Subscriber's Rights and Obligations

5.1 The Subscriber has the right to submit an application for issuing a Certificate
5.2 The Subscriber is obligated to:

5.2.1 accept the Terms and Conditions;
5.2.2 adhere to the requirements provided by JCC Payment Systems;
5.2.3 submit accurate, true and complete information in relation to the issuance of the Certificate;
5.2.4 not to continue with the Certificate issuance procedure, if the Subscriber is not legally eligible to do so, and/or if he/she is not an adult;
5.2.5 ensure that the credentials under which he gets access to the Private Key is used under his/her control and exercise reasonable care to avoid unauthorized use of it;
5.2.6 use his/her Private Key and Certificate in accordance with Terms and Conditions, including applicable agreements set out in Section 9, and the laws of Cyprus and European Union;
5.2.7 notify JCC Payment Systems of the correct details during a reasonable time, in case of a change in his/her personal details or of the legal person's details and of the identity of the natural person representing it or of any inaccuracy to the Certificate content;
5.2.8 immediately inform JCC Payment Systems of a possibility of unauthorized use of his/her Private Key or if his/her Private Key has been lost, stolen, potentially compromised or if control over his/her Private Key has been lost due to a compromise of activation data (e.g. username, password, OTP code, PIN code) or other reasons such as change of OTP generation device (e.g. mobile phone) and immediately revoke his/her Certificate;
5.2.9 not to continue using the private key if the Certificate has been revoked, expired or the CA has been compromised;

6. JCC Payment Systems Rights and Obligations

JCC Payment Systems is obligated to:
6.1 supply certification service in accordance with the applicable agreements set out in Section 9 and the relevant legislation;
6.2 keep account of the certificates issued by it and of their validity;
6.3 provide security with its internal security procedures;
6.4 provide the possibility to check the validity of certificates 24 hours a day;
6.5 ensure that the certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of JCC Payment Systems;
6.6 ensure that the subscriber certification keys used in the supply of the certification service are activated on the basis of subscriber sole control;

6.7 keep records related to the Certificate applications submitted, the relative Certification Authority's event logs, as well as the Certificates, safely for seven (7) years after the revocation or expiration day of the Certificate;

7. Certificate Status Checking Obligations of Relying Parties

7.1 A Relying Party studies the risks and liabilities related to acceptance of the Certificate. The risks and liabilities have been set out in the CPS and the CP. A Relying Part acknowledges that he/she has access to sufficient information to ensure that he/she can make an informed decision as to the extent to which he/she will chose to rely on the information in a Qualified Certificate. A RELYING PARTY IS RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON THE INFORMATION IN A QUALIFIED CERTIFICATE.

7.2 A Relying Party acknowledges and agrees that his/her use of JCC Payment Systems Repository and his/her reliance on any Qualified Certificate shall be governed by JCC Payment Systems applicable CPS as amended from time to time. The applicable CPS is published on the Internet in the Repository at https://pki.jcc.com.cy/repository and is available via e-mail by sending a request to: trust-policies@jcc.com.cy. Amendments to the applicable CPS are also posted in JCC Payment Systems Repository at https://pki.jcc.com.cy/repository.

7.3 A Relying Party shall verify the validity of the Certificate using current revocation status information prior to relying on a Signature, Authentication or Seal. In the case that not enough evidence is enclosed to the authentication certificates or EU Qualified certificates for electronic signatures or electronic seals, with regard to the validity of the Certificate a method by which the relying party may check Certificate status is by consulting the most recent Certificate Revocation List from the Certification Authority that issued the digital certificate on which you wish to rely.

7.4 A Relying Party follows the limitations stated within the Certificate and makes sure that the transaction to be accepted corresponds to the CPS and CP. Generally: Certificates shall be used only to the extent use is consistent with applicable law. Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

7.5 JCC Payment Systems ensures the availability of Certificate Status Services 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0.5% annually.

7.6 JCC Payment Systems offers OCSP service for checking Certificate status. Service is accessible over HTTP protocol.

7.7 A Relying Party verifies the validity of the Certificate by checking Certificates validity against OCSP. JCC Payment Systems offers OCSP with following checking availability:

- An OCSP service is free of charge and publicly accessible at http://ocsp.jcc.com.cy
- The URL of the OCSP service is included in the certificate on the Authority Information Access (AIA) field in accordance with the Certificate Profile.

8. Limited Warranty and Disclaimer/Limitation of Liability.

8.1 The Subscriber and Subject are solely responsible for the maintenance of his/her Private Key and credentials that allows access to it.

8.2 The Subscriber and Subject are solely and fully responsible for any consequences of using their Certificates both during and after the validity of the Certificates.

8.3 The Subscriber and Subject are solely liable for any damage caused due to failure or undue performance of their obligations specified in the Terms and Conditions and/or the laws of Cyprus and European Union.

8.4 The Subscriber and Subject are aware that Electronic Signatures, Electronic Seals and Authentication given on the basis of expired or revoked Certificates are invalid.

8.5 JCC Payment Systems ensures that:

- the certification service is provided in accordance with CPS, CP and the relevant legislation of European Union;
- the CA certification keys are protected by hardware security modules (HSM) according to CPS
- The Subscriber certification Keys on a Remote QSCD are protected by hardware security modules (HSM) and are under sole control of JCC Payments Systems;
- the certification keys used to provide the certification service are activated on the basis of shared control;
- it has compulsory insurance contracts covering all JCC Payment Systems trust services to ensure compensation for damages caused by JCC Payment Systems breach of obligations;
- it informs all Subscribers and Subjects before JCC Payment Systems terminates service of Certificates and maintains the documentation related to the terminated service of Certificates and

information needed according to the process set out in CPS.

8.6 JCC Payment Systems is not liable for the secrecy of the Private Keys of the Subjects when residing on a Local QSCD; any misuse of the Certificates or inadequate checks of the Certificates or for the wrong decisions of a Relying Party or any consequences due to error or omission in Certificate validation checks; the non-performance of its obligations if such non-performance is due to faults or security problems of the Supervisory Body, the data protection supervision authority, Trusted List or any other public authority; the failure to perform if such failure is occasioned by force majeure.

8.7 AS STATED IN THE CPS, JCC PAYMENT SYSTEMS PROVIDES LIMITED WARRANTIES AND DISCLAIMS ALL OTHER WARANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, LIMITS LIABILITY, AND EXCLUDES ALL LIABILITY FOR ANY LOSS OF PROFITS, LOSS OF DATA, OR OTHER INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE, NONPERFORMANCE, OR UNAVAILABILITY OF CERTIFICATES, ELECTRONIC SIGNATURES, ELECTRONIC SEALS, AUTHENTICATION OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED HEREIN, EVEN IF JCC PAYMENT SYSTEMS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL THE AGGREGATE LIABILITY OF JCC PAYMENT SYSTEMS S.A. TO ALL PARTIES (INCLUDING YOU) EXCEED THE APPLICABLE LIABILITY CAP FOR SUCH QUALIFIED CERTIFICATE SET FORTH, BELOW. THE COMBINED AGGREGATE LIABILITY OF JCC PAYMENT SYSTEMS TO ANY AND ALL PERSONS CONCERNING A SPECIFIC CERTIFICATE SHALL BE LIMITED TO AN AMOUNT NOT TO EXCEED ONE THOUSAND (1.000,00) EUROS FOR THE AGGREGATE OF ALL CERTIFICATES AND TRANSACTIONS RELATED TO SUCH CERTIFICATE.

8.8 SUBCRIBERS, SUBJECTS AND RELYING PARTIES ARE HEREBY NOTIFIED OF THE POSSIBILITY OF THEFT OR OTHER FORM OF COMPROMISE OF A PRIVATE KEY CORRESPONDING TO A PUBLIC KEY CONTAINED IN A CERTIFICATE, WHICH MAY OR MAY NOT BE DETECTED, AND OF THE POSSIBILITY OF USE OF A STOLEN OR COMPROMISED KEY TO FORGE A SIGNATURE OR SEAL TO A DOCUMENT OR ATTEMPT OF AUTHENTICATION.

9. Applicable Agreements, Policies, CP, CPS.

Relevant agreements, policies and practice statements related to Terms and Conditions for use of Certificates are:

9.1 Symantec Certificate Policy, published at https://pki.jcc.com.cy/repository;

9.2 JCC Payment Systems Certification Practice Statement, for authentication certificates and for EU Qualified certificates for electronic signatures & electronic seals published at: https://pki.jcc.com.cy/repository;

9.3 Certificate and OCSP Profiles for EU Qualified Certificates for Electronic Signatures, Electronic Seals and for Authentication Certificates, published at: https://pki.jcc.com.cy/repository

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

10. Privacy Policy and Confidentiality

10.1 JCC Payment Systems follows the Privacy Policy, and all Cyprus and European Union legal acts, when handling personal information and logging information.

10.2 All information that has become known while providing services and that is not intended for disclosure (e.g. information that had been known to JCC Payment Systems because of operating and providing Trust Services) is confidential. The Subscriber has the right to obtain information from JCC Payment Systems about him/her pursuant to the law.

10.3 JCC Payment Systems secures confidential information and information intended for internal use from compromise and refrains from disclosing it to third parties (except information contained in the certificates which are necessary for the provision of the related trust services to the authorized Qualified Trust Service Provider Sub-Contractor) by implementing security controls.

10.4 JCC Payment Systems has the right to disclose information about the Subscriber or Subject to a third party who pursuant to relevant laws and legal acts is entitled to receive such information and provided that such disclosure is lawful according to EU and national data protection legislation.

10.5 Additionally, non-personalized statistical data about JCC Payment Systems services is considered public information. JCC Payment Systems may publish non-personalized statistical data about its services.

11. Refund Policy

11.1 In case of sale of the Certificate directly through JCC Payment Systems, the Subscriber has the right, under Article 8 § 1 of L. 133(I)/2013 as amended, to withdraw from the sales contract without stating the reasons within an exclusive time limit of fourteen (14) calendar days from the date of purchase. The exercise of this right shall be made in writing by the Subscriber to JCC Payment Systems, sending an email to trust-sales@jcc.com.cy.

After that period, the right of withdrawal expires and JCC Payment Systems has no further obligation for the above cause.
11.2 Subject to section11.1 JCC Payment Systems handles refund case-by-case.

12. Applicable law, complaints and dispute resolution.
12.1 Any disputes related to the trust services provided under these terms shall be governed in all respects by and construed in accordance with the laws of Cyprus excluding its conflict of laws rules, and European Union as the location where JCC Payment Systems is registered as a CA. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.
12.2 To the extent permitted by law, before any dispute resolution mechanism may be invoked with respect to a dispute involving any aspect of JCC Payment Systems Trust Services, the Subscriber or other party must notify JCC Payment Systems, and any other party to the dispute of any 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. All parties agree that the courts of Cyprus, shall have exclusive jurisdiction and venue for hearing and resolving any dispute regarding the interpretation and execution of these terms and the provision of JCC Payment Systems services.
12.3 The Subscriber or other party can submit their claim or complaint on the following email: trust-policies@jcc.com.cy.
12.4 All dispute requests should be sent to contact information stated in these Terms and Conditions.

13. JCC Payment Systems and Repository Licenses, Trust Marks and Audit
13.1 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.
13.2 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.
13.3 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.

14. Contact Information.
14.1 Qualified Trust Service Provider
JCC Payment Systems Ltd
Office: 1 Stadiou Str., 2571 Nisou Ind. Area, Nicosia, Cyprus
Tel: +357 22 868 500
Fax: +357 22 868 591
E-mail: trust-policies@jcc.com.cy
Web: http://www.jcc.com.cy

14.2 Requests for certificate revocation are accepted via phone, email and self-service web portal.
14.3 Website Information and contact details of the self-service web portal is available at:
https://trust.jcc.com.cy/ and https://pki.jcc.com.cy/repository.

15. Validity of Terms and Conditions
If any provision of these Terms and Conditions, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder (and the application of the invalid or unenforceable provision to other persons or circumstances) shall not be affected by such finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the parties.