JCC Payment Systems Ltd.

Certificate Policy for authentication certificates and for EU Qualified certificates for electronic signatures & electronic seals

Effective Date: 03 June 2024

Version 1.2

Document History

Version	Date	Author	Reason for Change
1.0	20/07/2021	Paris Erotokritou	Initial version
1.1	03/06/2023	Paris Erotokritou	Review, No changes
1.2	03/06/2024	Fani Efstathiou	Review, No changes

Document Approvals

Version	Date	Approved By
1.0	20/07/2021	QTSP Policy Management
1.1	03/06/2023	QTSP Policy Management
1.2	03/06/2024	QTSP Policy Management

Document Distribution List

Version	Date	Role/Name
1.0	20/07/2021	All QTSP Staff
1.1	03/06/2023	All QTSP Staff
1.2	03/06/2024	All QTSP Staff

JCC Payment Systems Ltd Certificate Policy for authentication certificates and for EU Qualified Certificates for electronic signatures & electronic seals

Trademark Notices

JCC Payment Systems is the registered mark of JCC Payment Systems Ltd. Other names may be trademarks of their respective owners.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of JCC Payment Systems Ltd.

Notwithstanding the above, permission is granted to reproduce and distribute this JCC Payment Systems Ltd Certification Practice Statement on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to JCC Payment Systems Ltd.

Requests for any other permission to reproduce this JCC Payment Systems Ltd Certification Practices Statement (as well as requests for copies from JCC Payment Systems Ltd.) must be

addressed to JCC Payment Systems Ltd, Stadiou 1, 2571 Nisou, , CYPRUS, Telephone: (+357) 22 868 500, Fax: (+357) 22 868 591, , e-mail: trust-policies@jcc.com.cy

Table of Contents

1. INTRODUCTION 10
1.1 Overview 10
1.2 Document name and Identification 12
1.3 PKI Participants 13
1.3.1 Certification Authorities 13
1.3.2 Registration Authorities 14
1.3.3 Local Registration Authorities 15
1.3.4 Subscribers 15
1.3.5 Relying Parties 16
1.3.6 Other Participants 16
1.4 Certificate Usage 16
1.4.2 Prohibited Certificate Uses 17
1.5 Policy Administration 17
1.5.1 Organization Administering the Document 17
1.5.2 Contact Person 17
1.5.3 Person Determining CP Suitability for the Policy 18
QTSP Policy Officer and JCC Management jointly determine the suitability and applicability of this CP 18
1.5.4 CP Approval Procedure 18
1.6 Definitions and Acronyms 18
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 18
2.1 Repositories 18
2.2 Publication of Certificate Information 19
2.2.1 Publication and Notification Policies 19
2.2.2 Items not published in the Certificate Policy 19
2.3 Time or Frequency of Publication 19
2.4 Access Controls on Repositories 19
3. IDENTIFICATION AND AUTHENTICATION 21
3.1 Naming 21
3.1.1 Type of Names 21
3.1.2 Need for Names to be Meaningful 21
3.1.3 Anonymity or Pseudonymity of Subscribers 21
3.1.4 Rules for Interpreting Various Name Forms 21
3.1.5 Uniqueness of Names 21
3.1.6 Recognition, Authentication, and Role of Trademarks 21
3.2 Initial Identity Validation 22
3.2.1 Method to Prove Possession of Private Key 22
3.2.2 Authentication of Organization identity 22
3.2.3 Authentication of Individual Identity 22
3.2.4 Non-Verified Subscriber information 23
3.2.5 Validation of Authority 23
3.2.6 Criteria for Interoperation 23
3.3 Identification and Authentication for Re-key Requests 23
3.3.1 Identification and Authentication for Routine Re-key 23
3.3.2 Identification and Authentication for Re-key After Revocation 24
3.4 Identification and Authentication for Revocation Request 24

4. CERTIFICATE LIFE-CYCLE OPERATIONAL 25
4.1 Certificate Application 25
4.1.1 Who Can Submit a Certificate Application? 25
4.1.2 Enrollment Process and Responsibilities 25
4.2 Certificate Application Processing 25
4.2.1 Performing Identification and Authentication Functions 25
4.2.2 Approval or Rejection of Certificate Applications 25
4.2.3 Time to Process Certificate Applications 26
4.3 Certificate Issuance 26
4.3.1 CA Actions during Certificate Issuance 26
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate 26
4.4 Certificate Acceptance 26
4.4.1 Conduct Constituting Certificate Acceptance 26
4.4.2 Publication of the Certificate by the CA 27
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 27
4.5 Key Pair and Certificate Usage 27
4.5.1 Subscriber Private Key and Certificate Usage 27
4.5.2 Relying Party Public Key and Certificate Usage 27
4.6 Certificate Renewal 28
4.7 Certificate Re-Key 28
4.7.1 Circumstances for Certificate Re-Key 28
4.7.2 Who May Request Certification of a New Public Key 28
4.7.3 Processing Certificate Re-Keying Requests 28
4.7.4 Notification of New Certificate Issuance to Subscriber 28
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 29
4.7.6 Publication of the Re-Keyed Certificate by the CA 29
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 29
4.8 Certificate Modification 29
4.8.1 Circumstances for Certificate Modification 29
4.8.2 Who May Request Certificate Modification 29
4.8.3 Processing Certificate Modification Requests 29
4.8.4 Notification of New Certificate Issuance to Subscriber 29
4.8.5 Conduct Constituting Acceptance of Modified Certificate 29
4.8.6 Publication of the Modified Certificate by the CA 29
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 29
4.9 Certificate Revocation and Suspension 30
4.9.1 Circumstances for Revocation 30
4.9.2 Who Can Request Revocation 31
4.9.3 Procedure for Revocation Request 32
4.9.4 Revocation Request Grace Period 32
4.9.5 Time within Which CA Must Process the Revocation Request 32
4.9.6 Revocation Checking Requirements for Relying Parties 32
4.9.7 CRL Issuance Frequency 33
4.9.8 Maximum Latency for CRLs 33
4.9.9 On-Line Revocation/Status Checking Availability 33
4.9.10 On-Line Revocation Checking Requirements 33
4.9.11 Other Forms of Revocation Advertisements Available 33
4.9.12 Special Requirements regarding Key Compromise 33

4.9.13 Circumstances for Suspension 33
4.9.14 Who Can Request Suspension 34
4.9.15 Procedure for Suspension Request 34
4.9.16 Limits on Suspension Period 34
4.10 Certificate Status Services 34
4.10.1 Operational Characteristics 34
Certificate status information is available via CRL and OCSP responder. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period. OCSP information for subscriber Certificates is updated as per section 34
4.10.2 Service Availability 34
4.10.3 Optional Features 34
4.11 End of Subscription 34
4.12 Key Escrow and Recovery 34
4.12.1 Key Escrow and Recovery Policy and Practices 34
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 34
5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS 36
5.1 Physical Controls 36
5.1.1 Site Location and Construction 36
5.1.2 Physical Access 36
5.1.3 Power and Air Conditioning 37
5.1.4 Water Exposures 37
5.1.5 Fire Prevention and Protection 37
5.1.6 Media Storage 37
5.1.7 Waste Disposal 38
5.1.8 Off-Site Backup 38
5.1.9 External RA Systems 38
5.2 Procedural Controls 38
5.2.1 Trusted Roles 38
5.2.2 Number of Persons Required per Task 39
5.2.3 Identification and Authentication for Each Role 39
5.2.4 Roles Requiring Separation of Duties 40
5.3 Personnel Controls 40
5.3.1 Qualifications, Experience, and Clearance Requirements 40
5.3.2 Background Check Procedures 40
5.3.3 Training Requirements 41
5.3.4 Retraining Frequency and Requirements 41
5.3.5 Job Rotation Frequency and Sequence 42
5.3.6 Sanctions for Unauthorized Actions 42
5.3.7 Independent Contractor Requirements 42
5.3.8 Documentation Supplied to Personnel 42
5.4 Audit Logging Procedures 42
5.4.1 Types of Events Recorded 42
5.4.2 Frequency of Processing Log 44
5.4.3 Retention Period for Audit Log 44
5.4.4 Protection of Audit Log 44
5.4.5 Audit Log Backup Procedures 44
5.4.6 Audit Collection System (Internal vs. External) 44

5.4.7 Notification to Event-Causing Subject 44
5.4.8 Vulnerability Assessments 45
5.5 Records Archival 45
5.5.1 Types of Records Archived 45
5.5.2 Retention Period for Archive 45
5.5.3 Protection of Archive 45
5.5.4 Archive Backup Procedures 45
5.5.5 Requirements for Time-Stamping of Records 45
5.5.6 Archive Collection System (Internal or External) 45
5.5.7 Procedures to Obtain and Verify Archive Information 46
5.6 Key Changeover 46
5.7 Compromise and Disaster Recovery 46
5.7.1 Incident and Compromise Handling Procedures 46
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 46
5.7.3 Entity Private Key Compromise Procedures 47
5.7.4 Business Continuity Capabilities after a Disaster 47
5.8 CA or RA Termination 48
6. TECHNICAL SECURITY CONTROLS 50
6.1 Key Pair Generation and Installation 50
6.1.1 Key Pair Generation 50
6.1.2 Private Key Delivery to Subscriber 50
6.1.3 Public Key Delivery to Certificate Issuer 50
6.1.4 CA Public Key Delivery to Relying Parties 50
6.1.5 Key Sizes 51
6.1.6 Public Key Parameters Generation and Quality Checking 51
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 51
6.2 Private Key Protection and Cryptographic Module Engineering Controls 51
6.2.1 Cryptographic Module Standards and Controls 51
6.2.2 Private Key (m out of n) Multi-Person Control 52
6.2.3 Private Key Escrow 52
6.2.4 Private Key Backup 52
6.2.5 Private Key Archival 52
6.2.6 Private Key Transfer Into or From a Cryptographic Module 53
6.2.7 Private Key Storage on Cryptographic Module 53
6.2.8 Method of Activating Private Key 53
6.2.9 Method of Deactivating Private Key 54
6.2.10 Method of Destroying Private Key 54
6.2.11 Cryptographic Module Rating 54
6.3 Other Aspects of Key Pair Management 54
6.3.1 Public Key Archival 54
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 54
6.4 Activation Data 55
6.4.1 Activation Data Generation and Installation 55
6.4.2 Activation Data Protection 55
6.4.3 Other Aspects of Activation Data 56
6.5 Computer Security Controls 56
6.5.1 Specific Computer Security Technical Requirements 56
6.5.2 Computer Security Rating 57

6.6 Life Cycle Technical Controls 57
6.6.1 System Development Controls 57
6.6.2 Security Management Controls 58
6.6.3 Life Cycle Security Controls 58
6.7 Network Security Controls 58
6.8 Time-Stamping 59
7. CERTIFICATE, CRL, AND OCSP PROFILES 60
7.1 Certificate Profile 60
7.1.1 Version Number 60
7.1.2 Certificate Extensions 60
7.1.3 Algorithm Object Identifiers 68
7.1.4 Name Forms 68
7.1.5 Name Constraints 70
7.1.6 Certificate Policy Object Identifier 71
7.1.7 Usage of Policy Constraints Extension 71
7.1.8 Policy Qualifiers Syntax and Semantics 71
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 71
7.2 CRL Profile 71
7.2.1 Version number 71
7.2.2 CRL and CRL Entry Extensions 71
7.3 OCSP Profile 72
7.3.1 Version Number 72
7.3.2 OCSP Extensions 72
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 73
8.1 Frequency and Circumstances of Assessment 73
8.2 Identity/Qualifications of Assessor 73
8.3 Assessor's Relationship to Assessed Entity 73
8.4 Topics Covered by Assessment 73
8.5 Actions Taken as a Result of Deficiency 74
8.6 Communications of Results 74
8.7 Self-audits 75
9. OTHER BUSINESS AND LEGAL MATTERS 76
9.1 Fees 76
9.1.1 Certificate Issuance or Renewal Fees 76
9.1.2 Certificate Access Fees 76
9.1.3 Revocation or Status Information Access Fees 76
9.1.4 Fees for Other Services 76
9.1.5 Refund Policy 76
9.2 Financial Responsibility 77
9.2.1 Insurance Coverage 77
9.2.2 Other Assets 77
9.2.3 Insurance or Warranty Coverage for End-Entities 77
9.3 Confidentiality of Business Information 77
9.3.1 Scope of Confidential Information 77
9.3.2 Information Not Within the Scope of Confidential Information 77
9.3.3 Responsibility to Protect Confidential Information 77
9.4 Privacy of Personal Information 78
9.4.1 Privacy Plan 78

9.4.2 Information Treated as Private....78
9.4.3 Information Not Deemed Private....78
9.4.4 Responsibility to Protect Private Information....78
9.4.5 Notice and Consent to Use Private Information....78
9.4.6 Disclosure Pursuant to Judicial or Administrative Process....78
9.4.7 Disclosure upon Owner's Request....78
9.4.8 Other Information Disclosure Circumstances....79
9.5 Intellectual Property rights....79
9.5.1 Property Rights in Certificates and Revocation Information....79
9.5.2 Property Rights in the CP....79
9.5.3 Property Rights in Names....79
9.5.4 Property Rights in Keys and Key Material....79
9.5.5 Violation of Property Rights....80
9.6 Representations and Warranties....80
9.6.1 CA Representations and Warranties....80
9.6.2 RA Representations and Warranties....81
9.6.3 Subscriber Representations and Warranties....81
9.6.4 Relying Party Representations and Warranties....82
9.6.5 Representations and Warranties of Other Participants....82
9.7 Disclaimers of Warranties....82
9.8 Limitations of Liability....83
9.9 Indemnities....83
9.9.1 Indemnification by Subscribers....83
9.9.2 Indemnification by Relying Parties....83
9.10 Term and Termination....84
9.10.1 Term....84
9.10.2 Termination....84
9.10.3 Effect of Termination and Survival....84
9.11 Individual Notices and Communications with Participants....84
9.12 Amendments....84
9.12.1 Procedure for Amendment....84
9.12.2 Notification Mechanism and Period....85
9.12.3 Circumstances under Which OID Must be changed....85
9.13 Dispute Resolution Provisions....85
9.13.1 Disputes among JCC, Affiliates, and Customers....85
9.13.2 Disputes with Subscribers or Relying Parties....86
9.14 Governing Law....86
9.15 Compliance with Applicable Law....86
9.16 Miscellaneous Provisions....86
9.16.1 Entire Agreement....86
9.16.2 Assignment....87
9.16.3 Severability....87
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)....87
9.16.5 Force Majeure....87
9.1 Other Provisions....87
Appendix A. Table of Acronyms and definitions....88
Table of Acronyms....88
Definitions....88

1. INTRODUCTION

This document is the JCC Payment Systems Ltd Certificate Policy ("CP") for authentication certificates and for EU Qualified certificates for electronic signatures & electronic seals. It states the procedural and operational requirements that JCC Payment Systems Trusted Service Provider (TSP) adhere in order to provide authentication certificates and EU Qualified certificates for electronic signatures & electronic seals, in accordance but not limited to Articles 19, 24, 28, 38 and 45 of Regulation (EU) N° 910/2014 [eIDAS].

This document establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates and providing associated trust services. These requirements apply to all Certificate Authorities (CAs), Registration Authorities (RAs), Processing Centers, Affiliates, Subscribers, Relying Parties, and other PKI entities that interoperate with JCC's PKI.

This CP describes how JCC Payment Systems meets these requirements in accordance with Regulation (EU) N° 910/2014 and describes the procedural and operational requirements that JCC Payment Systems adhere for:

- Securely managing the related infrastructure that supports JCC's PKI, and
- Issuing, managing, revoking and renewing of EU Qualified Certificates as defined in Regulation (EU) N° 910/2014
- Issuing, managing, revoking and renewing of Authentication certificates & EU Qualified Certificates for Electronic Signature for Cyprus National Electronic Identity (eID)

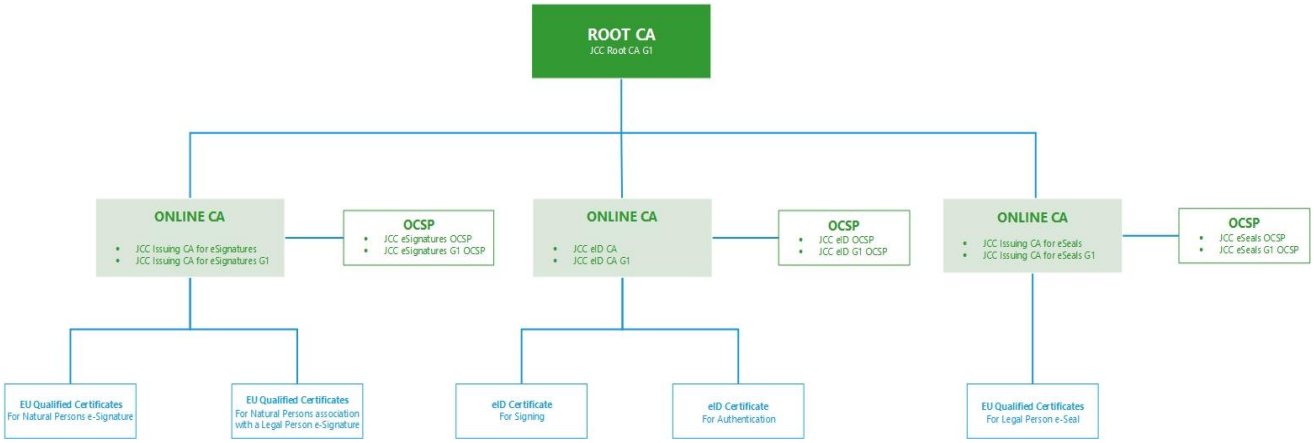
This CP conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction.

1.1 *Management may make exceptions to this Certification Practice Statement on a case-by-case basis to mitigate material, imminent impacts to customers, partners, relying parties, and/or others within the certificate ecosystem where practical workarounds do not exist. Any such management exceptions are documented, tracked, and reported as part of the audit process.* Overview

This CP describes the defines the procedural and operational requirements identified by Regulation (EU) N° 910/2014 that JCC Payment Systems adhere to for issuing, maintenance and lifecycle management of authentication certificates and EU Qualified certificates for electronic signatures & electronic seals.
These practices and procedures are compliant with ETSI EN 319 411-2 Policy: QCP-n-qscd for EU Qualified Certificates for electronic signatures and Policy: QCP-l-qscd for EU Qualified

Certificates for electronic seals and with ETSI EN 319 411-1 Policy: extended Normalized Certificate Policy (NCP+) for all types of certificates.

JCC Payment Systems is currently using the following certificate chain:



This CP is specifically applicable to JCC Payment Systems Issuing CAs, who issue:

- EU Qualified Certificates for electronic signatures
- EU Qualified Certificates for electronic seals
- Authentication certificates for authentication

Private CAs or services provided by JCC Payment Systems to other Organizations are also within the scope of this CP. The practices relating to services provided by other Organizations are beyond the scope of this CP.

JCC Payment Systems publishes this CP in order to comply with the specific policy requirements of the applicable legislation, or other industry standards and requirements.

The CP is only one of a set of documents relevant to JCC Payment Systems Trust Services. These other documents include:

- Ancillary confidential security and operational documents[3] that supplement the CP by providing more detailed requirements, such as:
  - Key Ceremony Reference Guide, which presents detailed CA key management operational requirements.
  - The JCC Payment Systems Physical and Environmental Security Policy which sets forth security principles governing JCC Payment Systems infrastructure,
  - The JCC Payment Systems Information Security Policy that states the requirements for Information System infrastructure in order to operate securely and according to relative legislative and contractual requirements.

[3] Although these documents are not publicly available their specifications are included in JCC Payment Systems Conformity Assessment Report for Trust Service Providers issuing EU Qualified certificates and may be made available to customer under special agreement,

  - JCC Payment Systems Key Management Policy, which presents detailed key management operational requirements.
- Certification Practice Statement for EU Qualified certificates for electronic signatures & electronic seals
- Certification Practice Statement for Cyprus National Electronic Identity
- General Terms and Conditions imposed by JCC Payment Systems. These General Terms and Conditions bind Customers, Subscribers and Relying Parties of JCC Payment Systems. Among other things, the General Terms and conditions cover a broad range of commercial terms and JCC Payment Systems Trust Services specific terms.

In many instances, the CP refers to these ancillary documents for specific, detailed practices implementing JCC Payment Systems Policies where including the specifics in the CP could compromise the security of JCC Payment Systems' CA.

1.2 Document name and Identification

JCC CA Certificates are issued according to the following certificate policies:

1.3.6.1.4.1.56511	Identification Number (OID) of JCC Payment Systems, registered to IANA
1.3.6.1.4.1.56511.1	Trust Service Provider
1.3.6.1.4.1.56511.1.1	Trust Services Certificate Policy (CP)
1.3.6.1.4.1.56511.1.1.1	Certification Practice Statement (CPS) for EU Qualified Certificates for Electronic Signatures and Electronic Seals
1.3.6.1.4.1.56511.1.1.2	Certification Practice Statement (CPS) for Cyprus National Electronic Identity (eID)
1.3.6.1.4.1.56511.1.1.1.0	Qualified Signature certificate QCP-n-qscd (0.4.0.194112.1.2)
s1.3.6.1.4.1.56511.1.1.1.1	Qualfied Seal certificate QCP-l-qscd (0.4.0.194112.1.3)
1.3.6.1.4.1.56511.1.1.2.1	eID Signature certificate QCP-n-qscd (0.4.0.194112.1.2)
1.3.6.1.4.1.56511.1.1.2.2	eID Authentication certificate NCP+ (0.4.0.2042.1.2)

The applicable and current CP (OID) shall be inserted by reference within each and every Certificate Policy ruled by the JCC Payment Systems CP.
Certificate Policy Object Identifiers are used in accordance with Section 7.1.

1.3 PKI Participants

1.3.1 Certification Authorities

The authority trusted by the users of the certification services (i.e. subscribers as well as relying parties) to create and assign certificates, is called the CA. The CA has overall responsibility for the provision of the certification services.

JCC Payment Systems is currently using the following certificate hierarchy:
List of Root CAs

A/A	Subject Distinguished Name	Certificate SHA-256 Fingerprint
1	CN=JCC Root CA G1 O = JCC PAYMENT SYSTEMS LTD C = CY	B55650C17CBCF1D4F8A38F0C0A58F434495941077A93E762D6C9E69D87A04351

List of Issuing Cas

A/A	Subject Distinguished Name	Certificate SHA-256 Fingerprint
1	CN = JCC Issuing CA for eSignatures 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD C = CY	0cf19de62187d68a51a8d0defd42f71ff73841300109c6647e7a05533bb8b3fa
2	CN = JCC Issuing CA for eSeals 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD C = CY	8522c10f0820633961bcf64f8d0eca32821d1a892ba6edc9cd469c265dd4f534
3	CN = JCC Issuing CA for eSignatures G1 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD C = CY	8404181ebd08f48d07066ae7fdaacdd1fda1567da6ea1cc208ceae9f64727458
4	CN = JCC Issuing CA for eSeals G1 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD	17e473dc97721a8fddd4668c3c9e4e328a653f2a508a0819c5b2aa0dacfa0662

	C = CY	
5	CN = JCC eID CA 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD C = CY	8653a6b2ec8aa847706c2d4048b58861cafaedca333b2c145e96111e966f8740
6	CN = JCC eID CA G1 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD C = CY	c23d300b481fce5440098e78edcdd9ff01e501471683b6ead8d9d893c18ee04e

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and validation of Subscribers and Subjects for issuing Certificates, initiates or passes along revocation requests for Certificates, and approves applications for re-keying certificates on behalf of the CA. JCC Payment Systems acts as an RA for all Certificates it issues.

JCC Payment Systems has the authority to enter into a contractual relationship with one or more third parties, in order to outsource part of RA responsibilities, especially regarding the validation of the Subscriber and Subject. In this case, the third party constitutes a Local Registration Authority (LRA). LRA performs its responsibilities in full compliance with this CP, the applicable CPS, the respective Validation plans and the terms of the LRA Agreement signed between LRA and JCC Payment Systems.

JCC Payment Systems trains LRA's authorized employees on validation process and security procedures, prior starting LRA's related operations. Thereafter, JCC Payment Systems re-trains yearly LRA's authorized employees.

JCC Payment Systems performs yearly audits to the LRA operations and procedures in order to ensure compliance with this CP, the applicable CPS, the Validation Plans and the LRA Agreement.

Third parties, who enter into a contractual relationship with JCC Payment Systems, may operate their own RA and authorize the issuance of certificates by a JCC Payment Systems CA. In this case, the third party becomes a RA and performs its responsibilities in full compliance with this CP, the applicable CPS, the respective Validation plans and the terms of the RA Agreement signed between RA and JCC Payment Systems.

Validation of domain portion of the email address cannot be delegated to a third party and is only validated by the RA of the Issuer CA.

1.3.3 Local Registration Authorities

A Local Registration Authority is an entity that performs the identification and validation of Subscribers and Subjects and the initial examination of their respective documents for the issuance, re-keying and revocation of Certificates. The relationship between LRA and RA is described in the LRA's contract agreement and includes, but not limited, the following:

- Full details of LRA's authorized employees, that will perform LRA's duties and activities;
- LRA's obligation to receive yearly training of LRA's authorized employees from JCC Payment Systems regarding LRA's duties and activities and to accept yearly audits by JCC Payment Systems regarding LRA operations and procedures;
- LRA's authorized employee's obligation to use credentials issued by JCC Payment Systems RA to ensure secure communications between both parties;
- LRA's obligation to process Subscribers' applications exclusively through LRA's authorized employees

Local Registration Authority passes all Subscriber's applications or requests accompanied by the related documents to the Registration Authority for approval or rejection of Certificate issuance, re-keying or revocation.

JCC Payment Systems also acts as an LRA for all the identification and validation of Subscribers and Subjects.

1.3.4 Subscribers

Two different terms are used in this CP to distinguish between these two roles: "Subscriber", is the entity which contracts with JCC Payment Systems for the issuance of credentials and; "Subject", is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the individual that is authenticated when the credential is presented.

Subscriber means a natural or legal person to whom JCC Payment Systems provides the Trust Services according to this CP and the CPS.

The subject means:

- a natural person
- a natural person who is identified in association with a legal person
- a legal person

The Subscriber may or may not be the Subject of a certificate. The link between the Subscriber and the Subject is one of the following:

- To request a certificate for natural person the Subscriber is:
    a) the natural person itself;
    b) a natural person mandated to represent the Subject; or
    c) any entity with which the natural person is associated.
- To request a certificate for legal person the Subscriber is:

a) any entity as allowed under the relevant legal system to represent the legal person; or
b) a legal representative of a legal person subscribing for its subsidiaries or units or departments.

1.3.5 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature authentication issued under the CA. A Relying party may, or may not also be a Subscriber.

1.3.6 Other Participants

Not applicable.

1.4 Certificate Usage

A digital Certificate is formatted data that cryptographically binds an identified Subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Qualified Certificates for electronic signatures are normally used by individuals to sign and encrypt e-mail and for authentication purposes, provided that the usage is not otherwise prohibited by law, by this CP, by any applicable CPS under which the certificate has been issued and any agreements with Subscribers. Qualified Certificates for electronic seals are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate are authenticated. A Qualified Certificate for electronic seal is normally used to ensure the integrity and the origin of that data to which it is linked, or for other purposes, provided that the usage is not otherwise prohibited by law, by this CP and any agreements with Subscribers.

1.4.1. Appropriate Certificate Usages

1.4.1.1 Certificates Issued for electronic signature

Certificates are compliant with NCP+ and QCP-n-qscd.
Certificates issued under these requirements are aimed to support qualified electronic signatures with the use of a Qualified Signature Creation Device (QSCD) such as defined in article 3 (12) of the Regulation (EU) N° 910/2014 [i.1].

1.4.1.2 Certificates Issued for authentication

Certificates are compliant with NCP+.
Certificates issued under these requirements are aimed to support authentication with the use of a Qualified Signature Creation Device (QSCD).
The Authentication Certificate cannot be used to create Qualified Electronic Signatures compliant with eIDAS.

1.4.1.3 Certificates Issued for electronic seals

Certificates are compliant with NCP+ and QCP-l-qscd.
Certificates issued under these requirements are aimed to support qualified electronic seals with the use of a Qualified Seal Creation Device (QSCD) such as defined in article 3 (27) of the Regulation (EU) N° 910/2014 [i.1].

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the Certificate was verified as reasonably correct when the Certificate issued.
Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.
Usage of Certificates that are issued by JCC Payment Systems, other than to support applications identified in Section 1.4.1 of the present CP is prohibited.

CA Certificates may not be used for any functions except CA functions. In addition, Subscriber Certificates shall not be used as CA Certificates.

Relying Parties shall use the JCC Payment Systems Certificate Policy OIDs as identified in the Certificate to appropriately accept or reject a Certificate usage.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP and the relevant documents referenced herein are maintained by the QTSP Policy Officer and JCC Management, which can be contacted at:
JCC Payment Systems Ltd
1 Stadiou Street
2571 Industrial Area Nisou
Cyprus

1.5.2 Contact Person

QTSP Policy Officer
JCC Payment Systems Ltd
1 Stadiou Street
2571 Industrial Area Nisou
Cyprus

Telephone: (+357) 22 868 500
Fax: (+357) 22 868 591
trust-policies@jcc.com.cy

1.5.2.1 Revocation Contact Person

For Certificate revocation requests, refer to paragraph 4.9.3.

1.5.3 Person Determining CP Suitability for the Policy

QTSP Policy Officer and JCC Management jointly determine the suitability and applicability of this CP.

1.5.4 CP Approval Procedure

Subsequent amendments to this CP are performed by the QTSP Policy Officer under JCC Management approval. The revised edition of the CP and any other QTSP technical and operational document must be approved by the QTSP Policy Management which is consisted by the QTSP Manager, Information Security & Risk Management Manager, Chief Operating Officer or Chief Executive Officer. QTSP Policy Management will decide whether the document needs to be approved by the ISSC. Amendments are either in the form of a document containing an amended form of the CP or an update notice. Amended versions or updates shall be linked to the JCC Payment Systems Repository located at: https://pki.jcc.com.cy/repository

Updates supersede any designated or conflicting provisions of the referenced version of the CP. The QTSP Policy Officer shall determine whether changes to the CP require any changes in the Certificate policy object identifiers of the Certificate policies.

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

JCC Payment Systems as an Issuer CA shall publishes all publicly trusted CA Certificates, issued to and from the Issuer CA, revocation data for issued digital Certificates, CP, CPS, Privacy Statement and Terms & Conditions. JCC Payment Systems shall ensure that its root Certificate and the revocation data for issued Certificates are regularly available through an online repository. Upon revocation of a Subscriber's Certificate, JCC Payment Systems publishes notice of such revocation in the repository. JCC Payment Systems issues Certificate Revocation Lists (CRLs) and provides OCSP services pursuant to the provisions of this CP.

JCC Payment Systems shall ensure that its repository is available 24 hours a day, 7 days a week, with a minimum of 99,00% availability overall per year with a scheduled down-time that does not exceed 0,5% annually.

Upon system failure, service or other factors which are not under the control of JCC Payment Systems, JCC Payment Systems shall apply best endeavours to ensure that this information service is not unavailable for longer than above time.

2.2 Publication of Certificate Information

JCC Payment Systems maintains a web-based repository in a public data communications network (https://pki.jcc.com.cy/repository) that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. JCC Payment Systems provides Relying Parties with information on how to find the appropriate repository to check Certificate status and how to find the right OCSP responder.

JCC Payment Systems publishes in its public information repository at least the following information:

- Overview of the certification hierarchy
- Certification Practice Statements
- Certification Policies
- Certificates, including root and issuing CAs
- Certificate Profiles
- General Terms and Conditions for use of Certificates
- Certificate Revocation Lists link

2.2.1 Publication and Notification Policies

This JCC Payment Systems CP is published in JCC Payment Systems public information repository.
JCC Payment Systems CP along with the enforcement dates is published no less than 30 days prior taking effect.

2.2.2 Items not published in the Certificate Policy

Refer to Section 9.3.1 of this CP.

2.3 Time or Frequency of Publication

Refer to section 2.2.1 of current CP for updates to this CP. Updates to Subscriber and Relying Party General Terms and Conditions are published as necessary. Certificate status information is published in accordance with the provisions of this CP.

2.4 Access Controls on Repositories

Information published in the repository portion of the JCC Payment Systems web site is publicly-accessible information. Read only access to such information is unrestricted. JCC Payment Systems has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries according to the applicable JCC Payment Systems security policies. JCC Payment Systems makes its repository

publicly available in a read only manner, and specifically at the link https://pki.jcc.com.cy/repository.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Naming in certificates are as specified in Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7] and the appropriate part of ETSI EN 319 412

3.1.1 Type of Names

Type of names assigned to the CA and to the Subscriber is described in the relevant Certificate Profile documentation publish in JCC Payment Systems repository

JCC Payment Systems CA and Subscriber Certificates contain X.501 Distinguished Names in the Issuer and Subject fields.

3.1.2 Need for Names to be Meaningful

Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate.
JCC Payment Systems CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

Not allowed.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

JCC Payment Systems ensures that Subject Distinguished Names (DN) of Subscriber are unique within the domain of a specific CA through automated components of the Subscriber enrollment process. The uniqueness of the Distinguished Name for electronic signatures and authentication is ensured by the Serial Number attribute value in the Subject field of the certificate. For electronic seals is ensured by the Organizational Identifier attribute value in the Subject field of the certificate.
The process to ensure that the values put in the serialNumber attribute are unique, is based on the uniqueness of each subscriber's certificate application entry within the application.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. JCC Payment Systems, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate or otherwise resolve any dispute

concerning the ownership of any domain name, trade name, trademark, or service mark. JCC Payment Systems is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

JCC Payment Systems may use the following methods described in this Section to ascertain the identity of a Subscriber. JCC Payment Systems may refuse to issue a Certificate at its sole discretion if identity validation is not successful.

Identity validation is part of the process of the certificate application certificate issuance and device provisioning.

3.2.1 Method to Prove Possession of Private Key

The key generation process is ensured by this CP in compliance with the ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 technical standards.
The Certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration or another JCC Payment Systems approved method.

3.2.2 Authentication of Organization identity

The Issuer CA or an RA shall verify an individual's identity in accordance with the process established in the applicable CPS section 3.2.2.

If the request is for a Certificate that asserts an organizational affiliation between a human

3.2.3 subscriber and an organization, JCC Payment Systems shall obtain documentation from the organization that recognizes the affiliation. Authentication of Individual Identity

JCC Payment Systems as an Issuer CA or the RA shall verify an individual's identity in accordance with the process established in the applicable CPS section 3.2.3 by obtaining and verifying proof of the individual's identity.
In case the individual requesting the Certificate is an RA or LRA's authorized employee, the identity validation of this very individual must not be conducted by herself/himself and must involve one of her/his RA/LRA peers.

3.2.3.1 Domain Email validation

JCC Payment Systems verifies a Subscriber's right to use or control an email address to be contained in a Certificate that will have the "Secure Email" EKU by sending an approval email message to the email address to be included in the Certificate and by sending a unique

Random Value by SMS to the mobile number provided in the signed application form by the Subscriber.

3.2.4 Non-Verified Subscriber information

Non-verified subscriber information includes:

- Organization Unit (OU) attributes
- Any other information designated as non-verified in the Certificate

3.2.5 Validation of Authority

Whenever a natural person's name is associated with a legal person's name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the legal person JCC Payment Systems RA:

- Determines that the legal person exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the legal person, and
- Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the legal person, the employment with the legal person of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the legal person.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. JCC Payment Systems generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey").
Please refer to Sections 3.2.2 and 3.2.3 of this CP.

In addition, all documents required can be sent electronically digitally signed by an existing EU Qualified Certificate for electronic signatures. The validation of electronically signed registration documents is performed automatically using the adobe acrobat application.

3.3.1 Identification and Authentication for Routine Re-key

Not applicable

3.3.2 Identification and Authentication for Re-key After Revocation

Refer to Sections 3.2.2 and 3.2.3 of this CP.

3.4 Identification and Authentication for Revocation Request

RA authenticates all revocation requests.
Prior to the revocation of a Certificate, RA verifies that the revocation has been requested by the Certificate's Subscriber.

Acceptable procedures for authenticating the revocation requests of a Subscriber are established in the applicable CPS section 3.4..

JCC Payment Systems RA Administrators are entitled to request the revocation of Certificates. JCC Payment Systems authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

Application for EU Qualified Certificates may be submitted by a natural or legal person, and for Authentication Certificates by natural person, who in both cases is the Subscriber of the Certificate, provided that is legally eligible. Applicants are responsible for any data that the Applicant or any authorized person by the Applicant supplies to JCC Payment Systems.

4.1.2 Enrollment Process and Responsibilities

JCC Payment Systems as Issuer CA is responsible for ensuring that the identity of each Applicant is verified in accordance with this CP and the applicable CPS prior to the issuance of any Certificate type per the applicable legal agreements. Applicants are responsible for submitting sufficient information and documentation for the Issuer CA or the RA to perform the required verification of identity prior to issuing a Certificate.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

JCC Payment Systems performs identification and authentication of all required Subscriber information in terms of Section 3.2.
JCC Payment Systems performs identification and authentication of all required Subscriber information either a) by physical presence, or b) by using a method equivalent to physical presence in accordance with Section 3.2.
If an LRA/RA assists in the verification, the LRA/RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to JCC Payment Systems. After verification is complete, JCC Payment Systems evaluates the information and decides whether or not to issue the Certificate. As part of this evaluation, JCC Payment Systems RA may check the Certificate against an internal database of previously revoked Certificates and rejected certificate requests to identify suspicious certificate requests.

4.2.2 Approval or Rejection of Certificate Applications

JCC Payment Systems approves an application for a certificate only if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2
- Payment has been received.

JCC Payment Systems rejects a certificate application if:

- Identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or

- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received, or
- JCC Payment Systems believes that issuing a certificate to the Subscriber may bring JCC Payment Systems into disrepute.

In case of a Local QSCD, upon certificate application rejection, Subscriber has the right either to return the QSCD in accordance to Section 9.1.5 or to keep it for future usage under his own full responsibilities.

In case JCC Payment Systems rejects a certificate application related to a Remote QSCD, the relevant Subscriber account is not created and no other actions are needed from Subscriber.

4.2.3 Time to Process Certificate Applications

JCC Payment Systems begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant General Terms and Conditions, CP, the applicable CPS or other agreement. A certificate application remains active until rejected.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by JCC Payment Systems. JCC Payment Systems creates and issues to a Certificate Subscriber a Certificate based on the information in a Certificate Application, following the approval of such Certificate Application.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

JCC Payment Systems notifies Subscribers that the Certificates have been created, and provides Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates are made available to Subscribers, by informing them via an e-mail message.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

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

4.4.2 Publication of the Certificate by the CA

JCC Payment Systems does not publish the Certificates it issues in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs and LRAs may receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the private key corresponding to the public key in the Certificate is only permitted once the Subscriber has agreed to the General Terms and Conditions, accepted the Certificate. The Certificate shall be used lawfully in accordance with JCC Payment Systems General Terms and Conditions and the relevant CPS. Certificate use must be consistent with the KeyUsage field extensions included in the Certificate. Certificate key usage is of type B as specified in clause 4.3.2 of ETSI EN 319 412-2.

Subscribers shall maintain their private keys under their sole control, protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber shall not archive the Subscriber Private Key.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to JCC Payment Systems General Terms and Conditions as a condition of relying on the Certificate.

Reliance on a Certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:

- The appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CP and the relevant CPS. JCC Payment Systems is not responsible for assessing the appropriateness of the use of a Certificate.
- That the certificate is being used in accordance with the Key Usage field extensions included in the certificate.
- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature or authentication performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely

at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 Certificate Renewal

Not applicable.

4.7 Certificate Re-Key

Certificate rekey is the application for the issuance of a new certificate that certifies a new public key.

4.7.1 Circumstances for Certificate Re-Key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

Only the Subscriber may request Certificate re-keying.

4.7.3 Processing Certificate Re-Keying Requests

Re-keying procedures ensure that the Subscriber seeking to re-key a Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

The Subscriber submits a re-keying application to JCC Payment Systems' RA or to an LRA's authorized employee and JCC Payment Systems' RA or the LRA's authorized employee, reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements, as described in Section 3.3.1.

Other than this procedure or another JCC Payment Systems approved procedure, the requirements for the authentication of an original Certificate Application shall be used for re-keying an end-user Subscriber Certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

JCC Payment Systems does not publish the Re-Keyed Certificates it issues in a publicly accessible repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs and LRAs may receive notification of the issuance of Certificates they approve.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key).

It is not possible to modify a certificate, the certificate shall be revoked and a new corrected one issued.

Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1.

4.8.3 Processing Certificate Modification Requests

JCC Payment Systems performs identification and authentication of all required Subscriber information in terms of Section 3.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, all revocation requests are authenticated as per Section 3.4.

Revocation of certificates is performed according to the following sections.

4.9.1 Circumstances for Revocation

The JCC Payment Systems General Terms and Conditions provide the obligation and/or right of the Subscriber to request revocation of a Certificate. Only in the circumstances listed below, will a Subscriber Certificate be revoked by JCC Payment Systems (or by the Subscriber) and published on a CRL.

A Subscriber Certificate is revoked if:

- JCC Payment Systems or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key. In case a compromise is reported by a third party JCC Payment Systems requires respective confirmation from the Subscriber;
- JCC Payment Systems has reason to believe that the Subscriber has breached a material obligation, representation, or warranty under the applicable General Terms and Conditions for Use of Certificates;
- JCC Payment Systems has reason to believe that the Certificate was issued in a manner not materially in accordance with the requirements of this CP and the procedures stated in the relevant CPS , was issued to a person other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person named as the Subject of such Certificate;
- JCC Payment Systems is aware of changes which impact the validity of the certificate;
- the used cryptography is no longer ensuring the binding between the Subject and the public key;
- JCC Payment Systems has reason to believe that a material fact in the Certificate Application is false;
- JCC Payment Systems determines that a material prerequisite to Certificate issuance was neither satisfied nor waived;
- Subscriber loses the legal eligibility, is declared in absence or death, is dissolved or declared bankrupted, taking into consideration that each certificate is non-transferable in any case;
- Subscriber loses ability to use the local QSCD or mobile device required to access a remote QSCD;
- In case the Subject of the Certificate is a natural person associated with the Subscriber-legal person and the Subscriber requires the revocation;
- A final court judgment requires the relevant revocation or cancellation
- The private key of the CA has been compromised;

- The Supervisory Body requests the revocation according to the law;
- The Subscriber identity has not been successfully re-verified ;
- The Subscriber has not submitted payment, when due;
- The continued use of that certificate is harmful to JCC Payment Systems.

When considering whether Certificate usage is harmful to JCC Payment Systems, JCC Payment Systems considers, among other things, the following:

- The nature and number of complaints received;
- The identity of the complainant(s);
- Relevant legislation in force;
- Responses to the alleged harmful use from the Subscriber.

JCC Payment Systems may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

JCC Payment Systems General Terms and Conditions for Use of Certificates require Subscribers to immediately notify JCC Payment Systems of a known or suspected compromise of its private key.

After the approval of a revocation request by the CA, the revoked certificate cannot be re-entered into force.

A CA Certificate is revoked if, among others:

- The private key of the CA has been compromised
- A final court judgment requires the relevant revocation or cancellation
- The Supervisory Body requests the revocation according to the law

4.9.2 Who Can Request Revocation

Request for revocation of a Certificate may be submitted by:

- a natural or legal person, or their legal representatives, who is the Subscriber of the Certificate, or a successor who wishes to request revocation in case of a deceased Subscriber (natural person), provided that is legally eligible
- a competent court
- the Supervisor Body
- RA or LRA
- CA

4.9.3 Procedure for Revocation Request

4.9.3.1 Procedure for Requesting the revocation of a CA

In case of CA's certificate revocation request, the procedure described in Section 4.9.3.1 of the relevant CPS shall apply.

4.9.3.2. Procedure for Requesting the Revocation of a Subscriber Certificate

To request revocation, the procedure described in Section 4.9.3.2 of the relevant CPS shall apply.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

4.9.5 Time within Which CA Must Process the Revocation Request

JCC Payment Systems takes commercially reasonable steps to process revocation requests without delay and in any case the maximum delay from the time JCC Payment Systems receives a revocation request in accordance with the procedure described in Section 4.9.3.1 of the relevant CPS and the actual change of its status information being available to all relying parties shall be at most 24 hours. If though the revocation request cannot be confirmed within 24 hours, then the status need not be changed.

Right after the approval of a revocation request, the CA informs, where possible, the Subscriber and the Subject of the certificate for the revocation via e-mail for this event.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate 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 meet this requirement by checking Certificate status using the JCC Payment Systems web-based repository or by using OCSP. CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository or OCSP responder to check for revocation status.
Due to the numerous and varying locations for CRL repositories, relying parties are advised to access CRLs using the URL(s) embedded in a certificate’s CRL Distribution Points extension.
The proper OCSP responder for a given certificate is placed in its Authority Information Access extension.

Revocation status information shall be made available beyond the validity period of the certificate.

4.9.7 CRL Issuance Frequency

CRLs for Subscriber Certificates are issued at least once per day. CRLs for CA Certificates are issued at least annually, but also whenever a CA Certificate is revoked.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation. This is generally done automatically within minutes of generation.

4.9.9 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository and OCSP. In addition to publishing CRLs, JCC Payment Systems provides Certificate status information through query functions in the JCC Payment Systems repository.
Certificate status information is available at the JCC Payment Systems repository at: https://pki.jcc.com.cy/repository
The maximum delay between the confirmation of the revocation of a certificate to become effective and the actual change of the status information of this certificate being made available to relying parties is at most 60 minutes. If though the revocation request requires revocation in advance (e.g. Subject's planned cessation from his/her duties at a certain date), then the scheduled date may be considered as the confirmation time.

4.9.10 On-Line Revocation Checking Requirements

A relying party must check the status of a certificate on which he/she/it wishes to rely. If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the JCC Payment Systems repository or by requesting Certificate status using the applicable OCSP responder.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements regarding Key Compromise

JCC Payment Systems uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or have reason to believe, that there has been a Compromise of the private key of one of its own CAs.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status information is available via CRL and OCSP responder. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period. OCSP information for subscriber Certificates is updated as per section

4.10.2 Service Availability

JCC Payment Systems shall ensure that its Certificate Status Services are available 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.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

A Subscriber may end a subscription for a JCC Payment Systems Certificate by:

- Allowing the Certificate to expire without re-keying that Certificate,
- Revoking the Certificate before expiration without replacing it

4.12 Key Escrow and Recovery

Not applicable.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

JCC Payment Systems has implemented the JCC Payment Systems Physical and Environmental Security Policy, which supports the security requirements of this CP. Compliance with these policies is included in JCC Payment Systems audit requirements described in section 8. JCC Payment Systems Physical and Environmental Security Policy contains sensitive security information and is only available upon agreement with JCC Payment Systems. An overview of the requirements is described below.

JCC Payment Systems outsources CA operation to ADACOM SA
who is a QTSP registered in Greece and listed in EU Trusted List. All facility, management and operations controls related to JCC Payment Systems CA and described below are provided by ADACOM SA.

5.1.1 Site Location and Construction

JCC Payment Systems QTSP operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

JCC Payment Systems also maintains Disaster Recovery facility for its QTSP operations. JCC Payment Systems Disaster Recovery facility is protected by multiple tiers of physical security comparable to those of JCC Payment Systems primary facility.

5.1.2 Physical Access

JCC Payment Systems CA systems are protected by seven (7) tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Some tiers enforce individual access control through the concurrent use of proximity cards and biometrics (two factor authentication). Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.

The physical security system includes tiers for CA key management security which serves to protect both online and offline storage of CA Cryptographic Signing Unit (CSUs) and keying material. Areas used to create and store cryptographic material enforce dual control, each through the concurrent use of proximity cards and biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance

with ADACOM's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

JCC Payment Systems RA dedicated workspace is protected using physical access controls making them accessible only to appropriately authorized individuals. Access to the RA area requires the use of an access card and PIN. Usage of the access cards is logged by an access control system.

Access cards log review as well as CCTV footage is monitored real time by the 24x7 guard as well as periodic reviews performed by the Fraud & Safety department. In addition, RA workspace is protected by PIR and alarm locking of the area. JCC Payment Systems securely stores all paper containing sensitive plain-text information related to its RA operations in a secure space.

JCC Payment Systems securely stores the Cryptographic Signing Units (CSU) used to generate and store the Subscribers Private Keys for remote signature and authentication. The room used for key storage and key generation activities is classified as a high security area with multiple tiers of security and a number of security features in place.

5.1.3 Power and Air Conditioning

All secure facilities are equipped with primary and backup:

- Power systems to ensure continuous, uninterrupted access to electric power and
- Heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

All secure facilities are equipped with monitoring systems to detect excess moisture and to minimize the impact of water exposure

5.1.5 Fire Prevention and Protection

All secure facilities are equipped with fire suppression mechanisms to prevent and extinguish fires or other damaging exposure to flame or smoke.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information related to JCC Payment Systems QTSP operations is stored in a secure off-site/alternate storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance to the manufacturers' guidance prior to disposal.

5.1.8 Off-Site Backup

JCC Payment Systems performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using the JCC Payment Systems Disaster Recovery facility

Off-site backup copies of CA Private Keys and activation data are stored for disaster recovery purposes in a physically secure manner using the ADACOM Disaster Recovery facility.

5.1.9 External RA Systems

All physical control requirements under Section 5.1 apply equally to any external RA system.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees that have access to or control authentication or cryptographic operations that may materially affect:

- The validation of information in Certificate Applications;
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, re-key requests, or enrollment information;
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- The handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- RA and LRA personnel,
- Key Management personnel,
- Security personnel,
- System administration personnel, and
- Executives that are designated to manage infrastructural trustworthiness.

JCC Payment Systems considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CP and the relevant CPS. The functions and duties performed by persons in trusted

roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations.

5.2.2 Number of Persons Required per Task

JCC Payment Systems has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to any cryptographic device. Access to cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to any of the devices. Persons with physical access to modules do not hold “Secret Shares” and vice versa.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through an HR process based on check of well-recognized forms of identification (e.g., passports or identification cards). Identity is further confirmed through the background checking procedures in Section 5.3.2.

JCC Payment Systems ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- Issued access devices and granted access to the required facilities;
- Issued electronic credentials to access and perform specific functions on JCC Payment Systems QTSP Systems or other IT systems.

JCC Payment Systems has implemented an access control system, which identifies authorities and registers all the JCC Payment Systems information system users in a trustworthy manner.

User accounts are created for personnel in specific roles that need access to the system in question. All users must log in with dedicated account, and administrative commands are only available with explicit permission and auditing of the execution. File system permissions and other features available in the operating system security model are used to prevent any other use.

User accounts are locked as soon as possible when the role change dictates. Access rules are audited annually.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include, but are not limited to:

- The validation and handling of information in Certificate Applications;
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, or re-keying requests, or enrollment information;
- The generation, issuing or destruction of a CA certificate;
- The access to the Remote QSCD

To accomplish this separation of duties, JCC Payment Systems designates individuals to the trusted roles, restricting an employee from assuming multiple roles, and thus preventing an employee from having more than one identity.

5.3 Personnel Controls

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.1 Qualifications, Experience, and Clearance Requirements

JCC Payment Systems requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities, as specified in the employment contract, job description and Roles and Responsibilities documents, competently and satisfactorily as well as proof of any government clearances, if any, necessary to perform certification services under government contracts, before they perform any operational or security functions.

The employment contracts signed by the employees of JCC Payment Systems provide for the following obligations:

- To maintain the secrecy of confidential information that has come to their knowledge in the course of their performance,
- To prevent them from holding business interests in a company, which may affect their judgment in the supply of the service and - to ensure that they have not been punished for a willful crime.
- All personnel in Trusted Roles are free from any interests that may affect their impartiality regarding JCC Payment Systems operations.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, JCC Payment Systems conducts background checks which include the following:

- Verification of identity

- Check of previous employment and professional reference (if available);
- Confirmation of the highest or most relevant educational degree obtained;

Attestation that employees satisfy the knowledge, skills, reliability and experienceTo the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, JCC Payment Systems will utilize a substitute investigative technique permitted by law that provides substantially similar information.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable professional references, and
- Certain criminal convictions

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable laws.

5.3.3 Training Requirements

JCC Payment Systems provides its personnel involved with PKI operations with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. JCC Payment Systems maintains records of such training. JCC Payment Systems periodically reviews and enhances its training programs as necessary.

JCC Payment Systems training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- Security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

JCC Payment Systems provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

JCC Payment Systems re-trains yearly RA and LRA's authorized employees.

5.3.5 Job Rotation Frequency and Sequence

No rotation used.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for employees and agents failing to comply with this CP and the applicable CPS, unauthorized actions or other violations of JCC Payment Systems policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to JCC Payment Systems employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in Section 5.3.2 are permitted access to JCC Payment Systems secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8 Documentation Supplied to Personnel

JCC Payment Systems provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily, including a copy of this CP and other technical and operational documentation needed to maintain the integrity of JCC Payment Systems' CA operations. Employees are also given access to information on internal systems and security documentation, identity verification procedures and other relevant information.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

JCC Payment Systems ensures that all relevant information concerning the operation of JCC Payment Systems Trust Services is recorded for providing evidence for the purpose of legal proceedings. This information includes the archive records that are required for proving the validity of the Trust Service operation.

The following significant events are manually or automatically recorded:

- CA certificate and key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction

  - Changes to CA details or keys
  - Cryptographic device life cycle management events.
- Subscriber certificate and key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Certificate Applications, issuance, re-key, and revocation
  - Successful or unsuccessful processing of requests
  - Changes to certificate creation policies
  - Generation and issuance of Certificates and CRLs.
- Trusted Employee Events, including:
  - Logon and logoff attempts
  - Attempts to create, remove, set passwords or change the system privileges of any privileged users
  - Personnel changes.
- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - Start-up and shutdown of systems and applications
  - Possession of activation data for CA private key operations
  - System configuration changes and maintenance
  - PKI and security system actions performed
  - Security sensitive files or records read, written or deleted
  - Security policy settings changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activity
  - Remote QSCD facility access entry/exit.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Kind of entry.

JCC Payment Systems RA and LRA log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant
- Record of unique identification data, numbers, or a combination thereof (e.g., Certificate Applicant's identification card number) of identification documents, if applicable. Storage location of copies of applications and identification documents for Certificates
- Any specific choices in the Certificate Application
- Identity of entity accepting the application and in case of EU Qualified e-Seals identity of the natural person representing the legal person to whom the EU Qualified Certificate for the electronic seal is provided
- Method used to validate identification documents, if any
- Name of receiving CA or submitting RA and LRA, if applicable.

5.4.2 Frequency of Processing Log

The QTSP systems are continuously monitored to provide real time alerts of significant security and operational events for review by designated system security personnel. Monthly reviews of the audit logs include verifying that the logs have not been tampered with and thoroughly investigating any alerts or irregularities detected in the logs. Actions taken based on audit log reviews are also documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.

Physical or digital archive records about certificate applications, registration information and requests or applications for revocation are retained for at least seven (7) years after any certificate based on these records ceases to be valid.

In case of JCC Payment Systems CA termination, audit logs and archive records are retained and accessible until abovementioned term for retention in accordance with Section 5.8.

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

Incremental or differential backups of audit logs are created daily and full backups are performed weekly.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by personnel in Trusted Roles.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event, unless such notice is compulsory according to the law.

Should the records concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons who have a legal right of access.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Vulnerability Assessments are performed and reviewed annually in order to identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. JCC Payment Systems also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that it has in place to control such risks. The Vulnerability Assessment and Risk Assessment are an input to JCC Payment Systems' annual conformity assessment audit. Monthly Vulnerability Assessments will be an input into JCC Payment Systems annual audit.

5.5 Records Archival

5.5.1 Types of Records Archived

Records been archived:

- All audit data collected in terms of Section 5.4
- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information

5.5.2 Retention Period for Archive

The retention period for archive is described in Section 5.4.3.

5.5.3 Protection of Archive

All archives are protected so that only authorized Trusted Persons are able to obtain access to the archives. The archives are protected against unauthorized viewing, modification, deletion, or other tampering by storage within a trustworthy system. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CP.

5.5.4 Archive Backup Procedures

An incremental or differential back up of electronic archives is performed on a daily basis and a full backup is performed on a weekly basis.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries contain time and date information. Such time information need not to be cryptographic-based.

5.5.6 Archive Collection System (Internal or External)

Archive information is collected internally by ADACOM for CA operations and by JCC Payment Systems for the rest QTSP related operations.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

Should the records concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons who have a legal right of access.

5.6 Key Changeover

JCC Payment Systems CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CP and the relevant CPS. JCC Payment Systems CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs are generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

Prior to the expiration of the CA Certificate for a Superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities within the Superior CA's hierarchy from the old Superior CA key pair to new CA key pair(s). JCC Payment Systems CA key changeover process requires that:

- A Superior CA ceases to issue new Subordinate CA Certificates no later than 60 days before the point in time ("Stop Issuance Date") where the remaining lifetime of the Superior CA key pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by Subordinate CAs in the Superior CA's hierarchy.
- Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the "Stop Issuance Date," Certificates will be signed with a new CA key pair.

The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backups of the QTSP information are kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys are generated and maintained in accordance with Section 6.2.4 of this CP.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

In the event of the corruption of computing resources, software, and/or data, internal or from any external third party, such an occurrence is reported to JCC Payment Systems Security and

JCC Payment Systems incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, JCC Payment Systems key compromise or disaster recovery procedures will be enacted.

5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of a JCC Payment Systems CA, JCC Payment Systems follows the plan of actions as described within Incident Management policy.

If CA Certificate revocation is required, the following procedures are performed by ADACOM SA:

- The Certificate's revoked status is communicated to Relying Parties through the JCC Payment Systems repository in accordance with Section 4.9.9,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected Participants, and
- The CA will generate a new key pair in accordance with Section 5.6, except where the CA is being terminated in accordance with Section 5.8.

Paragraph 5.7.3 is also applicable in case of PKI algorithm compromise.

5.7.4 Business Continuity Capabilities after a Disaster

JCC Payment Systems maintains a Business Continuity Plan (BCP) in order to establish procedures to recover the JCC Payment Systems critical business functions following a disaster.

The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
    - Notification/Activation phase to detect and assess damage and activate the plan.
    - Recovery phase to restore temporary IT operations and recover damage done to the original system.
- Identify the activities, resources, and procedures needed to carry out JCC Payment Systems QTSP functions during prolonged interruptions to normal operations.
- Assign responsibilities to designated JCC Payment Systems personnel and provide guidance for recovering JCC Payment Systems procedures during prolonged periods of interruption to normal operations.
- Ensure coordination with other JCC Payment Systems staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

JCC Payment Systems has the capability to restore or recover essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate revocation,

- Publication of revocation information.

JCC Payment Systems maintains redundant hardware and backups of its CA and infrastructure system software at its Disaster Recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with Section 6.2.4.

5.8 CA or RA Termination

The CA is terminated:

- with a decision of the JCC Payment Systems Management;
- with a decision of the authority exercising supervision over the supply of the service;
- with a judicial decision;
- Upon the liquidation or termination of the operations of JCC Payment Systems.

JCC Payment Systems ensures that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation of JCC Payment Systems services, and in particular, it ensures the continued maintenance of information required to verify the correctness of Trust Services.

In the event that it is necessary for a JCC Payment Systems CA, to cease operation, JCC Payment Systems makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, JCC Payment Systems will activate the documented "JCC Payment Systems Termination Plan" to minimize disruption to Customers, Subscribers, and Relying Parties. This termination plan may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by JCC Payment Systems,
- The preservation of the CA's archives and records for the time periods required in this CP and the applicable CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- Refunding (if necessary) Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key, including backup key, and the hardware tokens containing such private key,
- Provisions needed for the transition of the CA's services to a successor CA where possible,
- Provision notice to relevant authorities such as supervisory bodies,

- Transfer of obligations to a reliable party for maintaining all information necessary to provide evidence of the Trust Services operation for a reasonable period, unless it can be demonstrated that JCC Payment Systems does not hold such information,
- The submission of the JCC Payment Systems CA's archives and records to another contracting Certification Service Provider for Certificates, for the time periods required by the law.

Upon termination of CA's operations, or termination of RA's services, for any reason, any contracts assigning part of the TSP responsibilities to third parties shall expire automatically. To this end, third parties shall secure the transfer of the records and documents related to the assigned responsibilities, according to applicable law.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

For the JCC Payment Systems CAs, the generation of keys, their storage and subsequent use, is performed by ADACOM S.A., using cryptographic modules that meet the requirements of FIPS 140-2 level 3. CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using trustworthy systems and processes that provide for the security and required cryptographic strength for the generated keys.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's Guide.The activities performed in each CA key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by ADACOM S.A. and JCC Payment Systems.

Generation of end-user Subject key pairs is generally performed by the Subject. The Subject uses a QSCD certified cryptographic module compliant with eIDAS Regulation requirements.

For Certificates on a remote QSCD, the generation of keys, their storage and subsequent use, is performed by JCC Payment Systems using exclusively devices certified specifically in accordance with the applicable requirements per Article 30.3 of the eIDAS and, thus included in the list of qualified devices maintained by the European Commission in compliance with Articles 30, 31 and 39 of eIDAS.

6.1.2 Private Key Delivery to Subscriber

When Subject key pairs are generated on QSCD by the Subject, private key delivery to the Subject is not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

Subject submit their public key to JCC Payment Systems for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Transport Layer Security (TLS).

6.1.4 CA Public Key Delivery to Relying Parties

JCC Payment Systems makes the Root and Issuing CA Certificates available to Subscribers and Relying Parties through its repository.

JCC Payment Systems generally provides its own full certificate chain (including the issuing CA and any CAs in the chain) to the Subscriber upon Certificate issuance.

Subscribers, during the certificate pick-up process, automatically download and install into their computer, the intermediate and issuing CA's public keys. In any case if a user needs to verify and/or download the public key of the CA, he can do so by accessing the JCC Payment Systems repository https://pki.jcc.com.cy/repository.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The JCC Payment Systems Standard for minimum key sizes is the use of key pair equivalent in strength to 4096 bit RSA for CAs and 2048 bit RSA for Subscriber certificates

Currently, JCC Payment Systems generates and uses at least the following minimum key sizes, signature algorithms, and hash algorithms for signing Certificates, CRLs, and certificate status server responses:

- RSA keys whose modulus size in bits is divisible by 8, and is at least 2048;
- Digest algorithms: SHA-256, SHA-384, or SHA-512.

6.1.6 Public Key Parameters Generation and Quality Checking

The quality of Public Keys is guaranteed by using secure random number generation and on-board generation of Public Keys. Key Pairs are generated using secure algorithms and parameters based on current research and industry standards following the recommendations of ETSI TS 119 312.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Refer to Section 7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

JCC Payment Systems has implemented a combination of physical, logical, and procedural controls to ensure the security of JCC Payment Systems private keys. Subscribers are also required to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

For CA key pair generation and CA private key storage, JCC Payment Systems uses hardware cryptographic modules operated and provided by ADACOM SA that are certified at or meet the requirements of FIPS 140-2 Level 3.

Subscriber Private Keys are generated on QSCD compliant to eIDAS Regulation requirements. JCC monitors QSCD certification status at least once a year, until the end of the validity period of certificates linked to these QSCDs.

In case of a modification of the certification status of the QSCD, JCC will:

- Stop the issuance of certificates on these devices
- Revoke any non-expired certificates whose keys reside on these devices.

6.2.2 Private Key (m out of n) Multi-Person Control

JCC Payment Systems follows the ADACOM SA technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. These mechanisms use "Secret Sharing" to split the activation data needed to make use of a CA private key into separate parts called "Secret Shares" which are held by trained and trusted individuals called "Shareholders." A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is three (3). It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CP.

No Multi-Person control is applied to Subscriber Private Keys.

6.2.3 Private Key Escrow

JCC Payment Systems CA and Subscribers private keys are not escrowed.

6.2.4 Private Key Backup

Backup copies of CA private keys are performed by ADACOM SA and backup copies of Subscriber private keys generated and stored by a Remote QSCD are performed by JCC Payment Systems, for standard recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for private key storage meet the requirements of this CP.

Modules containing onsite backup copies of private keys are subject to the requirements of this CP. Modules containing disaster recovery copies of private keys are subject to the requirements of this CP.

In case of a local QSCD, the Subscriber Private Keys cannot be extracted or backup or restored from the QSCD.

6.2.5 Private Key Archival

Upon expiration of a JCC Payment Systems CA Certificate, the key pair associated with the certificate is securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CP. These CA key pairs are not used for any

signing events after their expiration date of the corresponding CA Certificate, unless the CA Certificate has been renewed in terms of this CP.

The Subscriber Private Keys cannot be extracted or restored from the QSCD and are not archived.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

ADACOM SA generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, ADACOM SA makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

JCC Payment Systems generates Subscriber key pairs on the hardware cryptographic modules in which the keys will be used. In addition, JCC Payment Systems makes copies of such Subscriber key pairs for high availability and disaster recovery purposes. Where Subscriber key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

Private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8 Method of Activating Private Key

All JCC Payment Systems Subscribers shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

Activation data generation is described in Section 6.4.1

The Subscriber Private Keys on Local QSCD are protected by PIN codes. The rules are defined in section 6.2.8 of the relevant CPS.

The Subscriber Private Keys on Remote QSCD are protected by username, password and authorization through mobile application using passcode or biometrics. The rules are defined in section 6.2.8 of the relevant CPS.

The CA's private key shall be activated by a threshold number of Shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline. Similarly, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA's private key. Once the private key is activated, it shall be active only for one time.

6.2.9 Method of Deactivating Private Key

Power off of the cryptographic module that hosts the JCC Payment Systems CA private keys deactivates the keys

Subscriber private keys will be deactivated after each operation, upon logging off their end point, or upon removal of the Local QSCD from the end point or upon logging off of the Remote QSCD. In all cases, Subscribers have an obligation to adequately protect their private key(s) in accordance with this CP and the CPS.

6.2.10 Method of Destroying Private Key

Where required, JCC Payment Systems destroys CA and Subscriber private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. JCC Payment Systems utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of private keys. When performed, key destruction activities are witnessed.

The Subscriber Private Keys of a Local QSCD can be destroyed by physically destroying or damaging the QSCD.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

JCC Payment Systems Subscriber Certificates are backed up and archived as part of JCC Payment Systems routine backup procedures.

All the Subscriber Public Keys are kept in database of JCC Payment Systems and ADACOM SA and may be archived for at least seven (7) years after expiration of the CA that has issued the certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that they may continue to be used for signature verification. The maximum Operational Periods for JCC Payment Systems Certificates issued on or after the effective date of this CP are set forth in the following table below.

Certificate Issued By:	Validity Period
PCA Root CA	Normally up to 30 years

Certificate Issued By:	Validity Period
JCC PAYMENT SYSTEMS Issuing CA	Normally up to 8 years
Subscriber Certificates	Normally up to 3 years

In addition, JCC Payment Systems CAs stop issuing new Certificates at an appropriate date (60 days plus maximum validity period of issued Certificates) prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates. The lifetime of Subscriber's certificates will not exceed the lifetime of the CA's signing
certificate.

Subscribers shall cease all use of their key pairs after their usage periods have expired.

If an algorithm or the appropriate key length offers no sufficient security during the validity period of the certificate, the concerned certificate will be revoked and a new certificate application will be initiated. The applicability of cryptographic algorithms and parameters is constantly supervised by the JCC Payment Systems management.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used to protect HSM containing JCC Payment Systems CA private keys are generated in accordance with the requirements of Section 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

Activation data used (PINs) to protect Local QSCD containing Subject's private keys are generated in accordance with the user manual of the QSCD.

- Where key pairs are generated by the Subject, pre-defined activation data must be changed immediately before the key generation.

Activation data used (username, password and authorization through mobile application using passcode or biometrics)to protect Remote QSCD containing Subject's private keys are generated in accordance with the compliance requirements of the QSCD.
JCC Payment Systems will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

6.4.2 Activation Data Protection

JCC Payment Systems Key Custodians are required to safeguard Remote QSCD Secret Shares and sign an agreement acknowledging their responsibilities.

The Subscriber shall memorize the activation credentials (PIN, username, password, authorization through mobile application using passcode or biometrics) and not share them with anyone else.

JCC Payment Systems enforces multi-factor authentication for all accounts capable of causing certificate issuance or performing Registration Authority or delegated third party functions, or implement technical controls operated by the CA to restrict certificate issuance through the account to a limited set of pre-approved domains or email addresses.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

To the extent activation data for private keys are transmitted, Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.3.2 Activation Data Destruction

Activation data for CA private keys are decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in section 5.5.2 lapse, JCC Payment Systems destroys activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

JCC Payment Systems performs all QTSP functions using trustworthy systems that meet the requirements of ADACOM ISMS and JCC Payment Systems ISMS.

6.5.1 Specific Computer Security Technical Requirements

JCC Payment Systems ensures that the systems maintaining QTSP Services and data files are trustworthy systems secure from unauthorized access. In addition, JCC Payment Systems limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

JCC Payment Systems production network is logically separated from other components. This separation prevents network access except through defined application processes. JCC Payment Systems uses firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

All critical software components are installed and updated from trusted sources only. There are also internal procedures to protect the integrity of certification service components against viruses, malicious and unauthorized software.

JCC Payment Systems personnel are authenticated before using critical applications related to the services. User accounts are created for personnel in specific roles that need access to the system in question. File system permissions and other features available in the operating

system security model are used to prevent any other use. User accounts are removed as soon as possible when the role change dictates. Access rules are audited annually.

JCC Payment Systems requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. JCC Payment Systems requires that passwords be changed on a periodic basis.

Direct access to JCC Payment Systems databases supporting JCC Payment Systems QTSP Operations is limited to Trusted Persons having a valid business reason for such access.

The JCC Payment Systems certification services system components are managed in accordance with defined change management procedures. These procedures include system testing in an isolated test environment and the requirement that change must be approved by the Security Officer. The approval is documented for further reference.

All media containing production environment software and data, audit, archive, or backup information are stored within JCC Payment Systems with appropriate physical and logical access controls. Media containing Sensitive Information are securely disposed of when no longer required.

Incident response and vulnerability management procedures are documented in an internal document. Monitoring system detects and alarms of abnormal system activities that indicate potential security violation, including intrusion into the network.

Paper documents and materials with Sensitive Information are shredded before disposal. Media used to collect or transmit Sensitive Information are rendered unreadable before disposal.

RAs must ensure that the systems maintaining software and data files are trustworthy systems, secure from unauthorized access and logically separated from other components. RAs must use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

New versions of software are developed and implemented by JCC Payment Systems in accordance to change management procedure.

New or updated software, when first loaded provides a method to verify that the software on the system originated from trust source, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

JCC Payment Systems has mechanisms and/or policies in place to control and monitor the configuration of its CA systems.
JCC Payment Systems follows the network security guidelines of section 7.8 of ETSI EN 319 401. Upon installation and periodically thereafter, JCC Payment Systems validates the integrity of its CA systems.
Only the software directly used for performing the tasks is used in the information system.

6.6.3 Life Cycle Security Controls

JCC Payment Systems policies and assets are reviewed at planned intervals, or when significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

The configurations of the systems of JCC Payment Systems are checked at least annually for changes that violate the JCC Payment Systems security policies. The Security Officer approves changes that have an impact on the level of security provided.

JCC Payment Systems has procedures for ensuring that security patches are applied to the certification system within a reasonable time period after they become available, but not later than six months following the availability of the security patch. The reasons for not applying any security patches will be documented.

JCC Payment Systems manages the registration of information assets and classifies all information assets into security classes according to the results of the regular security analysis consistent with the risk assessment.

6.7 Network Security Controls

All CA and RA functions are using networks secured in accordance with ADACOM ISMS, JCC Payment Systems ISMS and to prevent unauthorized access and other malicious activity. JCC Payment Systems ensures all communications of sensitive information is protected through the use of encryption and digital signatures.

The security level of the internal network and external connections is constantly monitored to prevent all access to protocols and services not required for the operation of the Trust Services.

JCC Payment Systems performs a vulnerability assessment periodically on public and private IP addresses. Also, penetration tests are performed on the certification systems annually or upon major changes.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries contain time and date information. The system time on JCC Payment Systems' computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every one hour.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Certificate profile is in accordance with the X.509 version 3, the IETF RFC 5280 and clause 6.6.1 of ETSI EN 319 411-1.

7.1.1 Version Number

All Certificates are X.509 version 3 Certificates.

7.1.2 Certificate Extensions

Every issued certificate includes extensions as they are defined for X.509v3 Certificates.

JCC Payment Systems' Technically Constrained Issuing CA Certificates include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Issuing CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId does not appear in the EKU extension of JCC Payment Systems trusted certificates.

Below is a list of extensions used by JCC Payment Systems for each type of certificate.

7.1.2.1 For Root Cas

Standard Extension	***Field***	***Value***
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.56511.1.1**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/repository
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the Root Certificate.*

7.1.2.2 For Issuing CAs for electronic signatures (*JCC Issuing CA for eSignatures*)

Standard Extension	***Field***	***Value***
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**

	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.56511.1.1.1**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.jcc.com.cy/ca/root.crl**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://pki.jcc.com.cy/certs/root.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Subject Alternative Name	Directory Address	CN=PRIVATE-4096-8

7.1.2.3 For Issuing CAs for electronic seals (*JCC Issuing CA for eSeals*)

Standard Extension	***Field***	***Value***
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.56511.1.1.1)**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.jcc.com.cy/ca/root.crl**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://pki.jcc.com.cy/certs/root.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Subject Alternative Name	Directory Address	*CN=PRIVATE-4096-9*

7.1.2.4 For Issuing CAs for eID (*JCC eID CA*)

Standard Extension	*Field*	*Value*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	1.3.6.1.4.1.56511.1.1.2
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://crl.jcc.com.cy/ca/root.crl
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://pki.jcc.com.cy/certs/root.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Subject Alternative Name	Directory Address	CN=PRIVATE-4096-10

7.1.2.5 For Issuing CAs for electronic signatures (*JCC Issuing CA for eSignatures G1*)

Standard Extension	*Field*	*Value*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.56511.1.1.1**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/repository
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://crl.jcc.com.cy/ca/root.crl
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**

Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://pki.jcc.com.cy/certs/root.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.6 For Issuing CAs for electronic seals (*JCC Issuing CA for eSeals G1*)

Standard Extension	*Field*	*Value*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.56511.1.1.1)**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/repository
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://crl.jcc.com.cy/ca/root.crl
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://pki.jcc.com.cy/certs/root.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.7 For Issuing CAs for eID (*JCC eID CA G1*)

Standard Extension	*Field*	*Value*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	1.3.6.1.4.1.56511.1.1.2
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/repository
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://crl.jcc.com.cy/ca/root.crl

Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://pki.jcc.com.cy/certs/root.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.8 For Natural Person electronic signatures

Standard Extension	*Field*	*Value*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1**
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1.0**
	Cert Policy ID	**0.4.0.194112.1.2**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://pki.jcc.com.cy/crl/eSignature/LatestCRL.crl or http://crl.jcc.com.cy/crl/eSignature-G1/LatestCRL.crl
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location	https://pki.jcc.com.cy/repository/PDS/
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	http://ocsp.jcc.com.cy **or** http://ocsp2.jcc.com.cy
	Access Method	**1.3.6.1.5.5.7.48.2**

	Access Location	https://pki.jcc.com.cy/certs/ca-esign.crt **or** https://pki.jcc.com.cy/certs/ca-esign-g1.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.9 For Natural Person in association with a Legal Person electronic signatures

Standard Extension	***Field***	***Value***
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1**
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1.0**
	Cert Policy ID	**0.4.0.194112.1.2**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://pki.jcc.com.cy/crl/eSignature/LatestCRL.crl or http://crl.jcc.com.cy/crl/eSignature-G1/LatestCRL.crl
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location	https://pki.jcc.com.cy/repository/PDS/
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	http://ocsp.jcc.com.cy **or** http://ocsp2.jcc.com.cy
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	https://pki.jcc.com.cy/certs/ca-esign.crt **or** https://pki.jcc.com.cy/certs/ca-esign-g1.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.10 For Legal Person electronic seals

Standard Extension	*Field*	*Value*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1**
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1.1**
	Cert Policy ID	**0.4.0.194112.1.3**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://pki.jcc.com.cy/crl/eSeal/LatestCRL.crl **or** http://pki.jcc.com.cy/crl/eSeal-G1/LatestCRL.crl
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location	https://pki.jcc.com.cy/repository/PDS/
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEseal	**0.4.0.1862.1.6.2**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	http://ocsp.jcc.com.cy **or** http://ocsp2.jcc.com.cy
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://pki.jcc.com.cy/certs/ca-eseal.crt or http://pki.jcc.com.cy/certs/ca-eseal-g1.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.11 For eID electronic signatures

Standard Extension	*Field*	*Value*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**

	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.2**
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.2.1**
	Cert Policy ID	**0.4.0.194112.1.2**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://pki.jcc.com.cy/crl/eID/LatestCRL.crl or http://pki.jcc.com.cy/crl/eID-G1/LatestCRL.crl
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location	https://pki.jcc.com.cy/repository/PDS/
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	http://ocsp.jcc.com.cy or http://ocsp2.jcc.com.cy
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://pki.jcc.com.cy/certs/ca-eid.crt or http://pki.jcc.com.cy/certs/ca-eid--g1.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.12 For eID authentication

Standard Extension	*Field*	*Value*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.2**

	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.2.2**
	Cert Policy ID	**0.4.0.2042.1.2**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://pki.jcc.com.cy/crl/eID/LatestCRL.crl or http://pki.jcc.com.cy/crl/eID-G1/LatestCRL.crl
Key Usage	Digital Signature	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	http://ocsp.jcc.com.cy or http://ocsp2.jcc.com.cy
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://pki.jcc.com.cy/certs/ca-eid.crt or http://pki.jcc.com.cy/certs/ca-eid--g1.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.3 Algorithm Object Identifiers

The signature algorithms follow the specifications described in sections 6.1.5 and 6.1.6. All algorithms used for CAs and Subscriber follow current research and industry standards to deliver reasonable security for the intended purposes they are being used.

7.1.4 Name Forms

Each Certificate includes a unique serial number that is never reused
The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuer CA to support name chaining as specified in RFC 5280, section 4.1.2.4.

7.1.4.1 For Natural Person electronic signatures

Field	Value	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surename in UTF8 format according to RFC5280*
	serialNumber	*Random code as specified in clause 5.1.3 of ETSI EN 319 412-1*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	

Signature Algorithm	**Sha256withRSAEncryption**

7.1.4.2 For Natural Person in association with a Legal Person electronic signatures

Field	Value	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surename in UTF8 format according to RFC5280*
	serialNumber	*Random code as specified in clause 5.1.3 of ETSI EN 319 412-1*
	Organization	*Issuer organization name who made subscriber identification.*
	Organizational Unit	*Issuer organization unit name (optional)*
	OrganizationIdentifier	*Legal Entity's Identification Number from a national trade register with the following semantics: "**NTR**CY-123456789".* *Legal Entity's Tax Identification Number with the following semantics: "**VAT**CY-123456789"*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.3 For Legal Person electronic seals

Field	Value	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
	Common Name	*Legal Person's name*
Subject DN	Organization	*Issuer organization name who made subscriber identification.*
	Organizational Unit	*Issuer organization unit name (optional)*
	OrganizationIdentifier	*Legal Entity's Identification Number from a national trade register with the following semantics: "**NTR**CY-123456789".*
		*Legal Entity's Tax Identification Number with the following semantics: "**VAT**CY-123456789"*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	

Signature Algorithm	**Sha256withRSAEncryption**

7.1.4.4 For eID Signature certificate

Field	Value	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surename in UTF8 format according to RFC5280*
	serialNumber	*Personal Identification Card with the following semantics: "IDCCY-0000123456787"*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.5 For eID Authentication certificate

Field	Value	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surename in UTF8 format according to RFC5280*
	serialNumber	*Personal Identification Card with the following semantics: "IDCCY-0000123456787"*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.5 Name Constraints

JCC Payment Systems may include name constraints in the nameConstraints field when appropriate.
If an Issuing CA Certificate includes the extended key usage "id-kp-emailProtection" it is treated as technically constrained and audited as described in section 8.

7.1.6 Certificate Policy Object Identifier

According to each certificate type, the following recognized OIDs can be added in the certificatePolicies extension:

- **QCP-n-qscd**: 0.4.0.194112.1.2 as described in ETSI EN 319 411-2
- **QCP-l-qscd**: 0.4.0.194112.1.3 as described in ETSI EN 319 411-2
  NCP+: 0.4.0.2042.1.2 as described in ETSI EN 319 411-1

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

The policy qualifier is the URI which points to the published JCC Payment Systems CPS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

CRL profile is in accordance with the X.509 version 2 and the IETF RFC 5280.

7.2.1 Version number

JCC Payment Systems issues version 2 CRLs that contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name	JCC Issuing CA SubjectDN
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date
Signature	The signature algorithm MUST follow the requirements described in sections 6.1.5 and 6.1.6

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer

Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation
ExpiredCertsOnCRL	This CRL extension field indicates that the CRL includes revocation notices for expired certificates

7.3 OCSP Profile

7.3.1 Version Number

JCC's OCSP responders conform to version 1 of RFC 6960.

7.3.2 OCSP Extensions

Standard Extension	*Field*	*Value*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	1.3.6.1.4.1.56511.1.1.1
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	**https://pki.jcc.com.cy/cps**
Key Usage	Digital Signature	**Set**
OCSP No Revocation Checking	ocsp-nocheck	**Set**
Enhanced Key Usage	OCSP Signing	**Set**
Subject Alternative Name	Directory Address	CN=OCSP2048-1-28 (eSignatures) CN=OCSP2048-1-29 (eSeals)
Subject Key Identifier	RFC822 Name	*This field contains the ID of the Certificate Holder's key.*

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The conformity of information system, policies and practices, facilities, personnel, and assets of JCC Payment Systems are assessed by a conformity assessment body pursuant to the eIDAS regulation, the corresponding legislation and standards, or whenever a major change is made to Trust Service operations, based on ETSI standards listed in Section 9.15.

In addition to compliance audits, JCC Payment Systems is entitled to perform other reviews and investigations to ensure the trustworthiness of JCC Payment Systems Certification Services. JCC Payment Systems is entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm.

JCC Payment Systems is entitled to perform second party audits to contractors that are under a relationship with JCC Payment Systems to operate as Registration Authorities (RA) or Local Registration Authorities (LRAs).

8.1 Frequency and Circumstances of Assessment

JCC Payment Systems Compliance Audits are conducted at least annually. Audits are conducted over unbroken sequences of audit periods with each period no longer than one-year duration.

8.2 Identity/Qualifications of Assessor

JCC Payment Systems CA compliance audits are performed by:

- Internal Auditors;
- A conformity assessment body which is accredited in accordance with Regulation EC no 765/2008 and EN 319 403, the ETSI standards and the Baseline Requirements (section 8.2);
- The Supervisory Body.

8.3 Assessor's Relationship to Assessed Entity

The auditor of the conformity assessment body shall be independent from JCC Payment Systems and JCC Payment Systems assessed systems.

The internal auditor shall not audit his/her own areas of responsibility.

8.4 Topics Covered by Assessment

The conformity assessment covers the conformity of JCC Payment Systems information system, policies and practices, facilities, personnel, and assets with eIDAS regulation, respective legislation and standards. Conformity assessment body audits the parts of information system used to provide Trust Services.

The areas of activity subject to internal auditing are the following:

- Quality of service;
- Security of service;
- Security of operations and procedures;
- Protection of the data of Subscribers and security policy, performance of work procedures and contractual obligations, as well as compliance with the CP and service-based Policies and Practice statements.

The Conformity Assessment Body and the Internal Auditor also audit these parts of the information system, policies and practices, facilities, personnel, and the assets of sub-contractors that are related to providing JCC Payment Systems Trust Services (e.g. including LRAs).

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of JCC Payment Systems operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by JCC Payment Systems management with input from the auditor. JCC Payment Systems QTSP Policy Officer is responsible for developing and implementing a corrective action plan. If JCC Payment Systems determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the Trust Services, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, JCC Payment Systems QTSP Policy Officer will evaluate the significance of such issues and determine the appropriate course of action.

Additionally, in the event of a result of the assessment by the Conformity Assessment Body, showing deficiency, the Supervisory Body requires JCC Payment Systems to remedy any failure to fulfil requirements within a time limit (if applicable) set by the Supervisory Body. JCC Payment Systems makes efforts to stay compliant and fulfil all requirements of the deficiency on time. JCC Payment Systems QTSP Policy Officer is responsible to implement a corrective action plan. JCC Payment Systems evaluates the significances of deficiencies and prioritizes appropriate actions to be taken at least during the time limit declared by Supervisory Body or reasonable period of time.

Where personal data protection rules appear to have been breached, the Supervisory Body shall inform the data protection authority of the results of the compliance audit.

8.6 Communications of Results

Audit conclusions or certificate(s) for trust service(s), which are based on audit results of the conformity assessment body conducted pursuant to the eIDAS regulation, corresponding legislation and standards, may be published on JCC Payment Systems repository https://pki.jcc.com.cy/repository.

In addition, JCC Payment Systems submits the resulting conformity assessment report to the Supervisory Body within at period of three (3) working days of receiving it. JCC Payment Systems submits the audit conclusions or certificate(s) for trust service(s) to maintainers of the Browsers Root Programs in which JCC Payment Systems is participating and other interested parties.

Results of the internal audits of JCC Payment Systems operations may be released at the discretion of JCC Payment Systems Management.

8.7 Self-audits

JCC Payment Systems performs regular internal audits in order to ascertain compliance as per Section 8.4.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

JCC Payment Systems charges Subscribers for the issuance, management, and re-key of Certificates.

9.1.2 Certificate Access Fees

JCC Payment Systems does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

JCC Payment Systems does not charge a fee as a condition of OCSP services and making the CRLs required by this CP and the relevant CPS available in a repository or otherwise available to Relying Parties. JCC Payment Systems does not permit access to revocation information or certificate status information in their repositories by third parties that provide products or services that utilize such Certificate status information without JCC Payment Systems prior express written consent.

9.1.4 Fees for Other Services

JCC Payment Systems does not charge a fee for access to this CP. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with JCC Payment Systems.

9.1.5 Refund Policy

9.1.5.1 Distant sales

In case the sale of the Certificate is effected via the internet or a phone call 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 Subsequently, and following communication, JCC Payment Systems is obliged to repay the money corresponding to the value of the sales contract to the Subscriber. Refund payment is effected with the same method as initial payment and the Subscriber is not entitled to use the Certificate. After that period, the right of withdrawal expires and JCC Payment Systems has no further obligation for the above cause.

9.1.5.2 Other cases

Subject to Section 9.1.5.1 JCC Payment Systems handles refund case-by-case.
To request a refund Subscriber should send a written application to JCC Payment Systems. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

JCC Payment Systems maintains a commercially reasonable level of civil liability insurance coverage for errors and omissions through an errors and omissions insurance program with an insurance carrier.

9.2.2 Other Assets

JCC Payment Systems has sufficient financial resources to maintain its operations and perform its duties, and is reasonably able to bear the risk of liability to Subscribers and Relying Parties. Proof of financial resources is not made publicly available.

9.2.3 Insurance or Warranty Coverage for End-Entities

See Section 9.2.1 of this CP.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

All information that has become known while providing services and that is not intended for publication (e.g. information that had been known to JCC Payment Systems because of operating and providing Trust Services) is confidential. Subscriber has a right to get information from JCC Payment Systems about him/herself according to the applicable laws.

9.3.2 Information Not Within the Scope of Confidential Information

Any information not listed as confidential or intended for internal use is public information. Information considered public in JCC Payment Systems is listed in section 2.2 of this CP.

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

9.3.3 Responsibility to Protect Confidential Information

JCC Payment Systems secures confidential information and information intended for internal use from compromise and disclosure to third parties by implementing different security controls.

Disclosure or forwarding of confidential information to a third party is permitted only with the written consent of the legal possessor of the information on the basis of a court order or in other cases provided by law.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

JCC Payment Systems has implemented a privacy policy which is located at: https://pki.jcc.com.cy/repository in compliance with the applicable laws.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private.

9.4.3 Information Not Deemed Private

Subject to applicable laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

JCC Payment Systems secures private information from compromise and disclosure to third parties and complies with all applicable privacy laws.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CP, the applicable Privacy Policy or by agreement, private information are not used without the consent of the party to whom that information applies, in accordance with applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

JCC Payment Systems shall be entitled to disclose Confidential Information if, in good faith, JCC Payment Systems believes that:

- Disclosure is necessary in response to subpoenas and search warrants.
- Disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Disclosure upon Owner's Request

JCC Payment Systems privacy policy contains provisions relating to the disclosure of private Information to the person disclosing it to JCC Payment Systems. This section is subject to applicable privacy laws.

9.4.8 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property rights

The allocation of Intellectual Property Rights among JCC Payment Systems Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such JCC Payment Systems Participants. The following subsections apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. JCC Payment Systems grants permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the General Terms and Conditions for Use of Certificates referenced in the Certificate. JCC Payment Systems grants permission to use revocation information to perform Relying Party functions subject to the applicable General Terms and Conditions for Use of Certificates, or any other applicable agreements.

9.5.2 Property Rights in the CP

Subscribers acknowledge that JCC Payment Systems retains all Intellectual Property Rights in and to this CP.

9.5.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and Subscribers are property of the CAs and Subscribers that are the respective Subjects of these Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, JCC Payment Systems' Root public keys and the Root Certificates containing them, including all PRCA public keys and self-signed Certificates, are the property of JCC Payment Systems. Finally, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of those shares or the CA from JCC Payment Systems.

9.5.5 Violation of Property Rights

JCC Payment Systems does not knowingly violate the intellectual property rights of any third party

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

JCC Payment Systems CA warrants that:

- Provides its services consistent with the requirements and the procedures defined in this CP, the applicable CPS and related documents;
- Complies with eIDAS regulation and related legal acts defined in this CP and related documents;
- Publishes its CP, CPS and related documents and guarantees their availability in a public data communications network;
- Publishes and meet its claims in terms and conditions for subscribers and guarantees their availability and access in a public data communications network;
- Maintains confidentiality of the information which has come to its knowledge in the course of supplying the service and is not subject to publication;
- Keeps account of the Trust Service Tokens issued by it and their validity and ensure possibility to check the validity of certificates;
- Ensures the access to the private keys on the Remote QSCD to the authorized Subject of the keys;
- Ensures the proper management and compliance of the Remote QSCD
- Informs the Supervisory Body of any changes to a public key used for the provision Trust Services;
- Without undue delay but in any event within 24 hours after having become aware of it, notify the Supervisory Body and, where applicable, other relevant bodies as national CERT or Data Inspectorate, of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein;
- Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the Trusted Service has been provided, notify the natural or legal person of the breach of security or loss of integrity without undue delay;
- Preserves all the documentation, records and logs related to Trust Services according to Sections 5.4 and 5.5;
- Ensures a conformity assessment according to requirements and present the conclusion of conformity assessment body to the Supervisory Body to ensure continual status of Trust Services in the Trusted List;
- Has the financial stability and resources required to operate in conformity with this CP;
- Publishes the terms of the compulsory insurance policy and the conclusion of conformity assessment body in a public data communications network;
- Provides access to its services for persons with disabilities where feasible;

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate;
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate;
- Revocation services and use of a repository conform to this CP in all material aspects.

JCC Payment Systems General Terms and Conditions for Use of Certificates may include additional representations and warranties.

9.6.2 RA Representations and Warranties

JCC Payment Systems RA warrants that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate;
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application;
- Their Certificates meet all material requirements of this CP; and
- Revocation services (when applicable) and use of a repository conform to this CP in all material aspects.

JCC Payment Systems General Terms and Conditions for Use of Certificates may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each EU Qualified e-Signature or e-Seal created using the private key corresponding to the public key listed in the EU Qualified Certificate, is the EU Qualified e-Signature or e-Seal of the Subscriber and the EU Qualified Certificate has been accepted and is operational (not expired or revoked) at the time the EU Qualified e-Signature or e-Seal is created;
- Each authentication performed using the private key corresponding to the public key listed in the Authentication Certificate, is the authentication of the subscriber and the authentication certificate has been accepted and is operational (not expired or revoked) at the time authentication is created;
- The credentials (PIN, username, password, authorization through mobile application using passcode or biometrics) accessing the private key are protected and that no unauthorized person has ever had access to them;
- EU Qualified e-Signature or e-Seal, or Authentication are only created by a QSCD device;

- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true, and the Subscriber is aware of the fact that JCC Payment Systems may refuse to provide the service if the Subscriber has intentionally presented false, incorrect or incomplete information in the application for the service;
- The Subscriber observes the requirements provided by JCC Payment Systems in this CP, the applicable CPS and the related documents;
- All information supplied by the Subscriber and contained in the Certificate is true and in the event of a change in the data submitted, Subscriber shall notify the correct data in accordance with the rules established by this CP, the applicable CPS and the related documents;
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CP;
- The Subscriber is not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise;
- The Subscriber shall notify JCC Payment Systems without any reasonable delay, if Subject's private key or control to it has been lost, stolen, potentially compromised.

JCC Payment Systems General Terms and Conditions for Use of Certificates may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

JCC Payment Systems General Terms and Conditions for Use of Certificates require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP.

JCC Payment Systems General Terms and Conditions for Use of Certificates may include additional representations and warranties of Relying Parties.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, General Terms and Conditions for Use of Certificates disclaim JCC Payment Systems possible warranties, including any warranty of merchantability or fitness for a particular purpose.

JCC Payment Systems is not liable for:

- The secrecy of the credentials (PIN, username, password, authorization through mobile application using passcode or biometrics) that have access to the private keys of the

Subjects, possible misuse of the certificates or inadequate checks of the certificates or for the wrong decisions of a Relying Party or any consequences due to errors or omission in Trust Service 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;
- Non-fulfilment of the obligations arising from this CP, the applicable CPS and the related documents if such non-fulfilment is occasioned by Force Majeure.

9.8 Limitations of Liability

JCC Payment Systems General Terms and Conditions for Use of Certificates limit JCC Payment Systems liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include the liability cap of one thousand Euros (1,000.00 €) limiting JCC Payment Systems damages concerning a Certificate.

The liability (and/or limitation thereof) of Subscribers and Relying Parties is as set forth in the JCC Payment Systems General Terms and Conditions for Use of Certificates**.**

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers are required to indemnify JCC Payment Systems for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

JCC Payment Systems General Terms and Conditions for Use of Certificates may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, JCC Payment Systems General Terms and Conditions for Use of Certificates requires Relying Parties to indemnify JCC Payment Systems for:

- The Relying Party's failure to perform the obligations of a Relying Party,

- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

JCC Payment Systems General Terms and Conditions for Use of Certificates may include additional indemnity obligations.

9.10 Term and Termination

9.10.1 Term

The CP becomes effective at least 30 days upon publication in the JCC Payment Systems repository.

9.10.2 Termination

This CP as amended from time to time remains in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CP, JCC Payment Systems Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, JCC Payment Systems Participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

Section 1.5.1 provides all the available means of communication.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this CP are made by the JCC Payment Systems QTSP Policy Officer. Amendments are either in the form of a document containing an amended form of the CP or an update. Amended versions or updates are linked to JCC Payment Systems repository located at: https://pki.jcc.com.cy/repository. Updates supersede any designated or conflicting provisions of the referenced version of the CP. The QTSP Policy Officer shall determine whether changes to the CP require a change in the Certificate policy object identifiers of the Certificate policies.

9.12.2 Notification Mechanism and Period

JCC Payment Systems QTSP Policy Officer reserves the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The QTSP Policy Officer decision to designate amendments as material or non-material shall be within the QTSP Policy Officer sole discretion.

Proposed amendments to the CP are linked to JCC Payment Systems Repository located at: https://pki.jcc.com.cy/repository.

Notwithstanding anything in the CP to the contrary, if the QTSP Policy Officer believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of the TSP or any portion of it, JCC Payment Systems management and the QTSP Policy Officer shall be is entitled to make such amendments by publication in the JCC Payment Systems repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, JCC Payment Systems provides notice to of such amendments to JCC Payment Systems Participants.
At a minimum JCC Payment Systems management and the QTSP Policy Officer will update this CP annually.

Amendments which do not change the meaning of this CP, such as spelling corrections, translation activities and contact details updates are documented in the Versions and Changes section of the present document. In this case the fractional part of the document version number is enlarged.

In case of substantial changes, the new CP version is clearly distinguishable from the previous ones and the serial number is enlarged by one.

9.12.3 Circumstances under Which OID Must be changed

If the QTSP Policy Officer, determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment contains new object identifiers for the Certificate policies. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among JCC, Affiliates, and Customers

Disputes among JCC Payment Systems Participants are resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with Subscribers or Relying Parties

JCC Payment Systems General Terms and Conditions for Use of Certificates contain a dispute resolution clause. Disputes involving JCC Payment Systems require an initial negotiation period of sixty (60) days followed by litigation in the courts of Cyprus.

9.14 Governing Law

The law of Cyprus governs the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Cyprus. This choice of law is made to ensure uniform procedures and interpretation for all JCC Payment Systems Participants, no matter where they are located.

This governing law provision applies only to this CP. Agreements incorporating the CP by reference may have their own governing law provisions, provided that this section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

9.15 Compliance with Applicable Law

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;
- Personal Data laws and EU Regulations, such as Regulation (EU) 2016/679 (GDPR) –;
- Related European Standards:
    a. ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
    b. ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
    c. 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;

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable.

9.16.2 Assignment

Any entities operating under this CP may not assign their rights or obligations without the prior written consent of JCC Payment Systems. Unless specified otherwise in a contract with a party, JCC Payment Systems does not provide notice of assignment.

9.16.3 Severability

In the event that a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP shall remain valid.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

JCC Payment Systems may claim indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. JCC Payment Systems failure to enforce a provision of this CP does not waive JCC Payment Systems right to enforce the same provision later or right to enforce any other provision of this CP. To be effective, waivers must be in writing and signed by JCC Payment Systems.

9.16.5 Force Majeure

Non-fulfilment of the obligations arising from the CP and/or related documents is not considered a violation if such non-fulfilment is occasioned by Force Majeure. None of the parties shall claim damage or any other compensation from the other parties for delays or non-fulfilment of this CP and/or related documents caused by Force Majeure.

9.17 Other Provisions

JCC Payment Systems incorporates by reference, through its CA Certificates, the relevant CPS and General Terms and Conditions applicable to each Certificate it issues. This incorporation by reference is further described in the applicable CA Certificate Profile.

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.
CSR	Certificate Signing Request
FIPS	United State Federal Information Processing Standards.
LRA	Local Registration Authority
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol.
OID	Object Identifier, a unique object identification code
PCA	Primary Certification Authority.
PDS	PKI Disclosure Statement
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
QSCD	Qualified Electronic Signature Creation Device
RA	Registration Authority.
RFC	Request for comment.
SSL	Secure Sockets Layer.
TSP	Trust Service Provider

Definitions

Term	Definition
JCC PAYMENT SYSTEMS Repository	JCC PAYMENT SYSTEMS's database of Certificates and other relevant JCC PAYMENT SYSTEMS information accessible on-line.
Administrator	A Trusted Person within the organization that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Advanced electronic seal	An electronic seal that meets the following requirements: it is uniquely linked to the creator of the seal; it is capable of identifying the creator of the seal;

Term	Definition
	it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.
Advanced electronic signature	An electronic signature that meets the following requirements it is uniquely linked to the signatory; it is capable of identifying the signatory; it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
Authentication	Unique identification of a natural person by checking his/her alleged identity
Authentication Certificate	A Certificate which is intended for Authentication.
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.
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
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use

Term	Definition
	the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke the Subscriber's Certificate.
Compliance Audit	A periodic audit that a Processing Center, Service Center or Managed PKI Customer undergoes to determine its conformance with standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Domain Name	The label assigned to a node in the Domain Name System
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.
Electronic Signature	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.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Local QSCD	USB token or smart card type of QSCD
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only adjudication by

Term	Definition
	a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature, authentication verified with reference to a STN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Offline CA	PCAs Issuing Root CAs and other designated CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
OTP	One Time Password
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10 developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12 developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
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
Primary Certification Authority (PCA)	A CA that acts as a root CA and issues Certificates to CAs subordinate to it.
Processing Center	The JCC PAYMENT SYSTEMS site that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates.
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 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.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.

Term	Definition
	The JCC Payment Systems PKI consists of systems that collaborate to provide and implement the JCC Payment Systems PKI.
QTSP Policy Officer	The person within JCC PAYMENT SYSTEMS responsible for promulgating this policy.
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 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.
Registration Authority (RA)	An entity approved by a CA that is responsible for identification and authentication of subjects of certificates. Additionally an RA can assist in the certificate application process or revocation process or both.
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
Root CA	Certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s).
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications

Term	Definition
	Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Subordinate CA	Certification authority who's Certificate is signed by the Root CA, or another Subordinate CA. A subordinate CA normally either issues end user certificates or other subordinate CA certificates.
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.
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: creation, verification, and validation of digital signatures, authentication and related certificates; creation, verification, and validation of time-stamps and related certificates; registered delivery and related certificates; creation, verification and validation of certificates for website authentication; or preservation of digital signatures, authentication or certificates related to those services.
Trust Service Provider	An entity that provides one or more Trust Services.
Trusted Person	An employee, contractor, or consultant of an entity, responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.
Trusted Position	The positions within JCC PAYMENT SYSTEMS that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.

Term	Definition
General Terms and Conditions for Use of Certificates	A binding document setting forth the terms and conditions under which an a natural or legal person acts as a Subscriber or as a Relying Party and JCC PAYMENT SYSTEMS provides the corresponding Trust Services.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date.