



PACI
Certification Practice
Statement
Version 1.1

02 May 2013



1	INTRODUCTION	1
1.1	Overview	2
1.2	Document name and identification.....	3
1.3	PKI participants.....	3
1.3.1	Certification Authorities	3
1.3.2	Registration Authorities.....	3
1.3.3	Subscribers.....	3
1.3.4	Relying Parties.....	3
1.3.5	Other participants.....	4
1.4	Certificate usage	4
1.4.1	Appropriate certificate uses	4
1.4.1.1	Card ID certificate	4
1.4.1.2	Authentication & Signing certificate	4
1.4.2	Prohibited certificate uses	4
1.5	Policy administration.....	5
1.5.1	Organization administering the document.....	5
1.5.2	Contact person.....	5
1.5.3	Person determining CPS suitability for the policy	5
1.5.4	CPS approval procedures.....	5
1.6	Definitions and acronyms.....	5
1.6.1.	Acronyms	5
1.6.2	Definitions.....	5
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	8
2.1	Repositories.....	8
2.2	Publication of certification information	8



2.3	Time or frequency of publication	8
2.4	Access controls on repositories	8
3	IDENTIFICATION AND AUTHENTICATION	9
3.1	Naming	9
3.1.1	Types of names	9
3.1.2	Need for names to be meaningful	9
3.1.3	Anonymity or pseudonymity of subscribers	9
3.1.4	Rules for interpreting various name forms.....	9
3.1.5	Uniqueness of names.....	10
3.1.6	Recognition, authentication, and role of trademarks	10
3.2	Initial identity validation.....	10
3.2.1	Method to prove possession of private key	10
3.2.2	Authentication of organization identity	10
3.2.3	Authentication of individual identity	10
3.2.4	Non-verified subscriber information	10
3.2.5	Validation of authority.....	11
3.2.6	Criteria for interoperation	11
3.3	Identification and authentication for re-key requests	11
3.3.1	Identification and authentication for routine re-key.....	11
3.3.2	Identification and authentication for re-key after revocation	11
3.4	Identification and authentication for revocation request.....	11
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	12
4.1	Certificate Application.....	12
4.1.1	Who can submit a certificate application	12
4.1.2	Enrollment process and responsibilities	12
4.2	Certificate application processing	13



4.2.1	Performing identification and authentication functions	13
4.2.2	Approval or rejection of certificate applications	13
4.2.3	Time to process certificate applications	13
4.3	Certificate issuance.....	14
4.3.1	CA actions during certificate issuance	14
4.3.2	Notification to subscriber by the CA of issuance of certificate	14
4.4	Certificate acceptance	14
4.4.1	Conduct constituting certificate acceptance	14
4.4.2	Publication of the certificate by the CA	14
4.4.3	Notification of certificate issuance by the CA to other entities	14
4.5	Key pair and certificate usage	14
4.5.1	Subscriber private key and certificate usage	14
4.5.2	Relying party public key and certificate usage	15
4.6	Certificate renewal	15
4.6.1	Circumstance for certificate renewal.....	15
4.6.2	Who may request renewal	15
4.6.3	Processing certificate renewal requests	15
4.6.4	Notification of new certificate issuance to subscriber	15
4.6.5	Conduct constituting acceptance of a renewal certificate	16
4.6.6	Publication of the renewal certificate by the CA	16
4.6.7	Notification of certificate issuance by the CA to other entities	16
4.7	Certificate re-key	16
4.7.1	Circumstance for certificate re-key	16
4.7.2	Who may request certification of a new public key	16
4.7.3	Processing certificate re-keying requests	16
4.7.4	Notification of new certificate issuance to subscriber	17



4.7.5	Conduct constituting acceptance of a re-keyed certificate	17
4.7.6	Publication of the re-keyed certificate by the CA.....	17
4.7.7	Notification of certificate issuance by the CA to other entities	17
4.8	Certificate modification	17
4.8.1	Circumstance for certificate modification	17
4.8.2	Who may request certificate modification.....	17
4.8.3	Processing certificate modification requests.....	17
4.8.4	Notification of new certificate issuance to subscriber	17
4.8.5	Conduct constituting acceptance of modified certificate	18
4.8.6	Publication of the modified certificate by the CA.....	18
4.8.7	Notification of certificate issuance by the CA to other entities	18
4.9	Certificate revocation and suspension	18
4.9.1	Circumstances for revocation	18
4.9.2	Who can request revocation	18
4.9.3	Procedure for revocation request	18
4.9.4	Revocation request grace period.....	19
4.9.5	Time within which CA must process the revocation request	19
4.9.6	Revocation checking requirement for relying parties	19
4.9.7	CRL issuance frequency	19
4.9.8	Maximum latency for CRLs	19
4.9.9	On-line revocation/status checking availability.....	20
4.9.10	On-line revocation checking requirements	20
4.9.11	Other forms of revocation advertisements available.....	20
4.9.12	Special requirements re CA key compromise.....	20
4.9.13	Circumstances for suspension	20
4.9.14	Who can request suspension.....	20



4.9.15	Procedure for suspension request.....	20
4.9.16	Limits on suspension period	20
4.10	Certificate status services.....	21
4.10.1	Operational characteristics.....	21
4.10.2	Service availability.....	21
4.10.3	Optional features	21
4.11	End of subscription.....	21
4.12	Key escrow and recovery.....	21
4.12.1	Key escrow and recovery policy and practices	21
4.12.2	Session key encapsulation and recovery policy and practices	21
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	23
5.1	Physical controls	23
5.1.1	Site location and construction	23
5.1.2	Physical access	23
5.1.3	Power and air conditioning.....	23
5.1.4	Water exposures.....	23
5.1.5	Fire prevention and protection.....	24
5.1.6	Media storage	24
5.1.7	Waste disposal	24
5.1.8	Off-site backup.....	24
5.2	Procedural controls	24
5.2.1	Trusted roles	24
5.2.2	Number of persons required per task	25
5.2.3	Identification and authentication for each role.....	25
5.2.4	Roles requiring separation of duties.....	25
5.3	Personnel controls.....	26



5.3.1	Qualifications, experience, and clearance requirements	26
5.3.2	Background check procedures.....	26
5.3.3	Training requirements	26
5.3.4	Retraining frequency and requirements.....	26
5.3.5	Job rotation frequency and sequence	26
5.3.6	Sanctions for unauthorized actions	26
5.3.7	Independent contractor requirements.....	26
5.3.8	Documentation supplied to personnel	27
5.4	Audit logging procedures	27
5.4.1	Types of events recorded	27
5.4.2	Frequency of processing log	27
5.4.3	Retention period for audit log	27
5.4.4	Protection of audit log	28
5.4.5	Audit log backup procedures	28
5.4.6	Audit collection system (internal vs. external)	28
5.4.7	Notification to event-causing subject.....	28
5.4.8	Vulnerability assessments.....	28
5.5	Records archival.....	28
5.5.1	Types of records archived.....	28
5.5.2	Retention period for archive.....	28
5.5.3	Protection of archive	28
5.5.4	Archive backup procedures	29
5.5.5	Requirements for time-stamping of records	29
5.5.6	Archive collection system (internal or external).....	29
5.5.7	Procedures to obtain and verify archive information	29
5.6	Key changeover	29



5.7	Compromise and disaster recovery.....	29
5.7.1	Incident and compromise handling procedures.....	29
5.7.2	Computing resources, software, and/or data are corrupted	30
5.7.3	Entity private key compromise procedures.....	30
5.7.4	Business continuity capabilities after a disaster	30
5.8	CA or RA termination.....	30
6	TECHNICAL SECURITY CONTROLS	31
6.1	Key pair generation and installation	31
6.1.1	Key pair generation.....	31
6.1.2	Private key delivery to subscriber.....	31
6.1.3	Public key delivery to certificate issuer	31
6.1.4	CA public key delivery to relying parties.....	31
6.1.5	Key sizes.....	31
6.1.6	Public key parameters generation and quality checking.....	32
6.1.7	Key usage purposes (as per X.509 v3 key usage field).....	32
6.2	Private Key Protection and Cryptographic Module Engineering Controls	32
6.2.1	Cryptographic module standards and controls	32
6.2.2	Private key (m out of n) multi-person control	32
6.2.3	Private key escrow	32
6.2.4	Private key backup.....	32
6.2.5	Private key archival	33
6.2.6	Private key transfer into or from a cryptographic module.....	33
6.2.7	Private key storage on cryptographic module.....	33
6.2.8	Method of activating private key.....	33
6.2.9	Method of deactivating private key.....	33
6.2.10	Method of destroying private key	33



6.2.11	Cryptographic Module Rating	33
6.3	Other aspects of key pair management	33
6.3.1	Public key archival.....	33
6.3.2	Certificate operational periods and key pair usage periods.....	34
6.4	Activation data	34
6.4.1	Activation data generation and installation	34
6.4.2	Activation data protection.....	34
6.4.3	Other aspects of activation data.....	34
6.5	Computer security controls	34
6.5.1	Specific computer security technical requirements	34
6.5.2	Computer security rating.....	35
6.6	Life cycle technical controls.....	35
6.6.1	System development controls	35
6.6.2	Security management controls.....	35
6.6.3	Life cycle security controls.....	35
6.7	Network security controls	35
6.8	Time-stamping.....	35
7	CERTIFICATE, CRL, AND OCSP PROFILES	36
7.1	Certificate profile.....	36
7.1.1	Version number(s)	36
7.1.2	Certificate extensions	36
7.1.3	Algorithm object identifiers.....	36
7.1.4	Name forms	37
7.1.5	Name constraints.....	37
7.1.6	Certificate policy object identifier	37
7.1.7	Usage of Policy Constraints extension.....	37



7.1.8	Policy qualifiers syntax and semantics.....	37
7.1.9	Processing semantics for the critical Certificate Policies extension	37
7.2	CRL profile.....	37
7.2.1	Version number(s)	38
7.2.2	CRL and CRL entry extensions.....	38
7.3	OCSP profile.....	38
7.3.1	Version number(s).....	38
7.3.2	OCSP extensions.....	38
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	39
8.1	Frequency or circumstances of assessment.....	39
8.2	Identity/qualifications of assessor.....	39
8.3	Assessor's relationship to assessed entity.....	39
8.4	Topics covered by assessment	39
8.5	Actions taken as a result of deficiency	39
8.6	Communication of results	39
9	OTHER BUSINESS AND LEGAL MATTERS.....	40
9.1	Fees.....	40
9.1.1	Certificate issuance or renewal fees.....	40
9.1.2	Certificate access fees.....	40
9.1.3	Revocation or status information access fees	40
9.1.4	Fees for other services.....	40
9.1.5	Refund policy	40
9.2	Financial responsibility	40
9.2.1	Insurance coverage	40
9.2.2	Other assets	40
9.2.3	Insurance or warranty coverage for end-entities.....	41



9.3	Confidentiality of business information	41
9.3.1	Scope of confidential information	41
9.3.2	Information not within the scope of confidential information	41
9.3.3	Responsibility to protect confidential information	41
9.4	Privacy of personal information	41
9.4.1	Privacy plan.....	41
9.4.2	Information treated as private	41
9.4.3	Information not deemed private	41
9.4.4	Responsibility to protect private information	42
9.4.5	Notice and consent to use private information.....	42
9.4.6	Disclosure pursuant to judicial or administrative process.....	42
9.4.7	Other information disclosure circumstances.....	42
9.5	Intellectual property rights.....	42
9.6	Representations and warranties	42
9.6.1	CA representations and warranties	42
9.6.2	RA representations and warranties	42
9.6.3	Subscriber representations and warranties	43
9.6.4	Relying party representations and warranties	43
9.6.5	Representations and warranties of other participants	43
9.7	Disclaimers of warranties	43
9.8	Limitations of liability	43
9.9	Indemnities.....	43
9.10	Term and termination	43
9.10.1	Term.....	43
9.10.2	Termination	43
9.10.3	Effect of termination and survival	44



9.11	Individual notices and communications with participants.....	44
9.12	Amendments	44
9.12.1	Procedure for amendment	44
9.12.2	Notification mechanism and period	44
9.12.3	Circumstances under which OID must be changed	44
9.13	Dispute resolution provisions.....	44
9.14	Governing law.....	44
9.15	Compliance with applicable law	44
9.16	Miscellaneous provisions	45



Revision History

REVISION HISTORY					
Revision	Description of Change	Author	Reviewed By	Approved By	Effective Date
1.0	Document Creation	Nasser Al Otaibi Tareeq Al Rashed	Mansour Al Methen	Musaed Al Asousi	1/5/2009
1.1	Adding Corporate individual certificate category	Alaa Eldin Mahmoud Aly	Nasser Al Otaibi	Tareeq Al Rashed	2/5/2013



1 INTRODUCTION

The Public Authority for Civil Information (PACI) is the Kuwait governmental body responsible for issuing the Civil ID Card for all Kuwait residents, Kuwaiti or non Kuwaiti. The Civil ID Card has the resident Unique ID number that will be used in all his transactions and other information. The Civil ID Card is issued on a Smart Card to enable the digital use of its data and enable the e-Identity to facilitate all e-Use. PACI will use the Civil ID Card to deploy Kuwait PKI.

PACI mission statement

“Government organizations in Kuwait should be able to transact Communications & Business among themselves with a Trust by securing all credentials. Some Organizations might have a high need for data integrity and data confidentiality. This will be achieved by use of PKI through a Smartcard to be used for authentication and non-repudiation.”

PACI, as the issuer of the Civil ID card, have an automated process using a Card Management System to issue Civil ID card (Civil ID Card Issuance System), the system is directly linked to the centralized information database. The certificate life-cycle is integrated with the Civil ID Card Issuance System, administration interface enable administrators to do the full control over the certificate life-cycle, from the Civil ID Card Issuance System like: enrollment, approval, suspension and revocation of certificates.

This document describes the policies and practices that govern the PKI environment. It sets the business, and technical requirements for approving, issuing, managing, using, revoking, and renewing, Kuwaiti resident different digital certificates types issued by PACI CAs.

1.1 Overview

PACI root Certification Authority (CA) “PACI Policy CA” issued PACI online Certification Authority (CA) “PACI ID Issuance CA”. PACI online CA “PACI ID Issuance CA” is responsible for issuing Certificates to Card Holders. The Registration Authority (RA) responsibility will be PACI responsibility.

The PKI environment will have the following categories of Digital Certificates:

- 1- Digital certificates issued to the public individuals by “PACI ID Issuance CA”, these include the following types:

- a. Card ID certificate – Currently being issued to each smart civil ID card.

The Card ID certificate will be used to authenticate and validate the Civil ID Card itself.

- b. Authentication & Signing certificate – Currently being issued upon end user request and agreement

The Authentication & Signing certificate will be used to prove the identity of the Card Holder and also enable Electronic Signature.

- c. Encryption certificate



- 2- Digital certificates issued to specific group individuals by designated CAs, these certificates will be issued to natural persons only. It can be considered as “Corporate Individual certificate”.

1.2 Document name and identification

This document “PACI CPS Version 1.0” is for The Public Authority for Civil Information (PACI) of Kuwait.

1.3 PKI participants

1.3.1 Certification Authorities

Certification Authorities (CA) are responsible for issuing and distributing certificates to Subscribers. PACI online CA “PACI ID Issuance CA” is responsible for issuing Certificates to Subscribers.

1.3.2 Registration Authorities

The Registration Authority (RA) performs identification and authentication of certificate applicants for Subscribers certificates, initiates or passes along revocation requests for certificates for Subscribers certificates, and approves applications for replacement or renewal (re-keying) certificates on behalf of PACI CA. PACI act as an RA for the certificates its issues.

Card ID certificate is issued automatically with every issued Civil ID Card with no authentication. The issuance is associated with Civil ID Card issuance process with no Card Holder control over the certificate.

1.3.3 Subscribers

Civil ID Card (physical card) is considered a Subscriber by itself for the Card ID certificate use and purposes.

Also, Subscriber is the Civil ID Card Holder, or other equivalent Smart Card, as the natural person holding the card for which his identification and authentication have been performed by PACI staff while receiving certificate applications with full control over the Authentication & Signature certificate.

1.3.4 Relying Parties

All e-services parties included but not limited to: e-government services and portals, financial and commercial institutes & organizations that services depend on the issued digital certificates and also individuals who will receive the certificate.



1.3.5 Other participants

Not applicable.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

1.4.1.1 Card ID certificate

The Card ID certificate will be used to authenticate the card itself and its validity.

The certificate will not be controlled by the Card Holder but will be used by the systems and applications for its purposes.

1.4.1.2 Authentication & Signing certificate

The Authentication & Signing certificate will be used to:

- Prove the Card Holder identities to systems and applications and other parties.
- Sign electronic files like emails and documents.

The certificate will be controlled and used by the Card Holder personally.

1.4.1.3 Corporate Individual certificate

The Corporate Individual certificate will be used for one or more of the following:

- Prove the Card Holder identity to systems and applications and other parties.
- Means of representation for a company or organization.
- Sign electronic files like emails and documents.
- Encrypt transitory electronic communication/emails.

The certificate will be controlled and used by the Card Holder personally.

1.4.2 Prohibited certificate uses

As the PACI CA issued the certificates for intended purposes, so certificates may not be used for purposes other than those stated. In general, certificates may not be used for any Law prohibited use.



1.5 Policy administration

1.5.1 Organization administering the document

The Public Authority for Civil Information (PACI)

Ministries Zone, Sixth Ring Road,

South Surra, Kuwait.

Tel: 00965-1844447

Email: info@paci.gov.kw

Web: www.paci.gov.kw

1.5.2 Contact person

CPS Administrator:

PKI-CPS@paci.gov.kw

1.5.3 Person determining CPS suitability for the policy

PACI CP & CPS designated committee determine the suitability of this document.

1.5.4 CPS approval procedures

It's the responsibility of PACI CP & CPS designated committee to set the approval procedure and also any needed amendments.

1.6 Definitions and acronyms

1.6.1. Acronyms

CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
FIPS	United State Federal Information Processing Standards.
OCSP	Online Certificate Status Protocol.
PACI	The Public Authority for Civil Information.
PKI	Public Key Infrastructure.
RA	Registration Authority.

1.6.2 Definitions

Card Holder	Person holding the Civil ID card or Smart Card.
Card ID	Civil ID card unique identification number.



Card Management System	A solution of software products that enables organizations to securely manage the identity credential (Smart Card) within a single, integrated, workflow driven platform.
Card PIN	Pin used to authorize the use of private key.
Certificate or Digital Certificate	A computer file with the Subscriber information, Subscriber's public key, Certificate's start and end validity dates, Certificate serial number, CA information, and is digitally signed by the CA.
Certificate Application	A request from a Subscriber to a CA for the issuance of a Certificate.
Certificate Policies	A document stating the certificate policies.
Certificate Revocation List	An electronic file that has been generated, signed and published by the CA to disclose the revoked certificates to the public.
Certification Authority	An entity authorized to issue, manage, revoke, and renew Certificates.
Certification Practice Statement	A statement of the practices that an organization do in approving or rejecting Certificate requests and issuing, managing, and revoking Certificates.
Civil ID Card	The Civil ID Card has the Kuwaiti resident Unique ID number and issued by PACI.
Civil ID Card Issuance System	An automated process using a Card Management System to issue Civil ID card linked directly to the centralized information database
Electronic Signature	Electronic data affixed to other electronic data or having logical association with electronic data and used to authenticate identification.
On-line Certificate Status Protocol	A protocol for providing Relying Parties with real-time Certificate status information.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
Public Key Infrastructure	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.



Registration Authority	An entity approved by a CA to assist Subscribers in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Smart Card	A card with embedded integrated circuits which can process data.
Subject Distinguished Name	A unique Subscriber information consent his unique identity.
Subscriber	A person request and hold a Certificate.
Unique ID number	A unique number assigned to each Kuwaiti resident.



2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 *Repositories*

Certificate information is publicly published in PACI CA repositories. In case of revoking a certificate its revocation information is added to the CRLs. In Addition, Online Certificate Status Protocol (OCSP) services will be supported to designated requesters for real-time Certificate status check.

2.2 *Publication of certification information*

PACI CA prepares, maintains and publishes necessary repositories containing certificate information that its CAs manage. PACI ensures that accurate and up-to-date data kept in the repository. PACI CA is responsible for issuing Certificate Revocation Lists (CRLs) with revoked certificates information. In case of revoking a certificate, its information is published in the appropriate CRLs. In Addition, Online Certificate Status Protocol (OCSP) services will be provided upon approving designated requests for real-time Certificate status check.

2.3 *Time or frequency of publication*

Certificate and on-line certificate status are constantly published. Periodical certificate revocation lists are updated every hour.

2.4 *Access controls on repositories*

Repositories will be publicly accessible repositories. Read only access to such information is unrestricted. All necessary measures to ensure authenticity of the published information are implemented.



3 IDENTIFICATION AND AUTHENTICATION

PACI, as the Kuwait Civil ID Card issuer, authenticates the identification of the Civil ID Card applicant. The same personal authentication methods will apply on certificates requests except for Card ID certificate as it will be issued with each new Civil ID Card automatically.

3.1 Naming

All certificates use X.501 distinguished names. All Subscriber certificate information will be automatically added from previously authenticated information stored in PACI Civil ID Cards database as per PACI Civil ID Card name rules.

3.1.1 Types of names

For the Card ID certificate, mandatory fields:

- Civil ID
- Card serial number
- Document number
- Application use

For Authentication & Signing certificate, mandatory fields:

- Full Latin name
- Civil ID
- Full name in Arabic
- Email
- Title
- Application use

3.1.2 Need for names to be meaningful

Name will match the name appear in Civil ID Card. Name rules for PACI Civil ID Cards will apply.

3.1.3 Anonymity or pseudonymity of subscribers

Not allowed.

3.1.4 Rules for interpreting various name forms

Not applicable.



3.1.5 Uniqueness of names

Subject Distinguished Name of Certificate will be unique. To ensure the uniqueness the Subscriber Civil ID unique number is mandatory to include.

3.1.6 Recognition, authentication, and role of trademarks

Not applicable.

3.2 *Initial identity validation*

Identity validation will be face to face at PACI designated sites.

3.2.1 Method to prove possession of private key

PACI CA, in general, will generate the private and public key pair on behalf of the Subscriber on the Civil ID Card or equivalent Smart Card (for non-Civil ID Card holders) using a secure and controlled Civil ID Card Issuance System.

For Card ID certificate, PACI CA will generate Private and Public key pair on the Civil ID Card automatically with no Subscriber control.

For Authentication & Signing certificate and other certificates, Private Key use will be controlled by Card PIN. Card and Card Pin possession is the prove of Private Key possession.

3.2.2 Authentication of organization identity

Organization Identity is proved by presenting organization official documents authenticated by relevant governmental agency stamp.

3.2.3 Authentication of individual identity

Card ID certificate does not require identity check.

PACI CA requires physical presence to request Authentication & Signing certificate. Personal authentication and validating identity is confirmed via two PACI staff.

Subscriber information will be automatically entered from PACI Civil ID Card database; no manual data entry will be required.

For Corporate Individual certificates, The company/organization owns the CA is responsible for validating the identity of the end user, his relation to the organization and requesting the certificate only after the successful validation and using correct information.

3.2.4 Non-verified subscriber information

Not applicable.



3.2.5 Validation of authority

Approval letter with official stamp from the organization is required to add organization name and job title to the Subscriber certificate.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

Re-keying for the Subscriber certificate requires that a new key pair is generated to replace the existing Key Pair. Re-Key is required for the Subscriber to obtain a new certificate for “replace” and “renewal” request.

3.3.1 Identification and authentication for routine re-key

Subscriber must show in person and proof of identity is validated by PACI staff to request routine re-keying (certificate renewal).

As Card ID certificate is requested automatically via the Civil ID Card system so identification and authentication for routine re-key is not required.

3.3.2 Identification and authentication for re-key after revocation

Subscriber must show in person and proof of identity is validated by PACI staff to request re-keying after revocation (certificate replace).

As Card ID certificate is requested automatically via the Civil ID Card system so identification and authentication for re-key after revocation is not required.

3.4 Identification and authentication for revocation request

Subscriber must show in person and proof of identity is validated by PACI staff to request revocation. If the subscriber cannot submit revocation request in person, so after validating the requester identity, certificate will be “suspended”.

All Card certificates are revoked automatically via the Civil ID Card Issuance System when the Civil ID Card is revoked for any reason, so no separate revoke requests are required. PACI will configure the Civil ID Card Issuance System to revoke all card valid certificates, automatically, when revoking the Civil ID Card with no Subscriber request. The CA will send to the Subscriber a revoke notification.



4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

PACI Generate its CAs according to its CA hierarchy needs, CAs Life-cycle is maintained by PACI qualified key management team.

Certificates of the Registration Authorities that will serve as the registration centers are created to Civil ID Card automated issuance systems (Civil ID Card Issuance System) that carries out administration actions automatically. Certificates Life-cycle is maintained by PACI qualified administration team.

PACI, as the issuer of the Civil ID card, have an automated process, Civil ID Card Issuance System, to issue Civil ID card, the system is directly linked to the centralized information database. The certificate life-cycle control is integrated with the Civil ID Card Issuance System, administration interface enable administrators to do the full control over the certificate life-cycle, like:

- Enrollment, using the stored information in the central database.
- Approval, after applying the required authentication and validation and confirm legal eligibility.
- Suspension, if subscriber cannot request revocation personally.
- Revocation, when subscriber request revocation personally, or other auto revocation cases occur.

Once an Authentication & Signing certificate is issued on the Civil ID Card, the card holder is requested to enter a new Pin in a secure way e.g. using secure PINPad. The Card Pin is required to enable Authentication & Signing certificate Private Key use.

The following section describes the Subscriber certificate Life-cycle.

4.1 *Certificate Application*

4.1.1 Who can submit a certificate application

- Subscribers who want to obtain an Authentication & Signing certificate.
- Subscriber legal representative who present a legally recognized representation document.

PACI staff members who receive Subscribers' requests will request their own certificate from their supervisory level.

Card ID certificate do not need a requestor as it is an automated procedure with the Civil ID Card issuance.

4.1.2 Enrollment process and responsibilities

- Subscriber or his legal representative will have to fill and manually sign the Authentication & Signing "Certificate Application".
- PACI staff will validate the Subscriber proof of identity or the legal representative identity and the legally recognized representation document before accepting the application.



- Subscriber must pass PACI “Eligibility Check” done automatically by the system which confirms that Subscriber is legally eligible to enroll for an Authentication & Signing certificate like: age check, free from court restriction order, and other conditions. The conditions will be set by PACI “Certificates Eligibility Committee” and reside and executed on the centralized information database.
- PACI staff cannot accept their own “Certificate Application”. Supervisory level is required to accept, review and authenticate PACI staff “Certificate Application”.
- All relevant documents will be attached to “Certificate Application” and stored in the Subscriber file.

After completing the above requirements, the Civil ID Card Issuance System will initiate an automated process to enroll for the Certificate Application on behalf of the Subscriber.

Card ID certificate do not need enrollment request as it is part of Civil ID Card issuance processes.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

- Two PACI staff members will process the Subscriber “Certificate Application”.
- PACI staff will validate the Subscriber proof of identity or the legal representative identity and the legally recognized representation document.
- The authentication action shall be made face to face at PACI designated sites.
- Subscriber must present acceptable approval letter with official stamp from his organization to add organization name and job title to his certificate.

No authentication shall be made when processing applications for Card ID certificate.

4.2.2 Approval or rejection of certificate applications

The certificate application is approved if:

- Successfully passing the identification & authentication and document checks; and
- Successfully passing “Eligibility Check” done by the system.

Card ID certificate is approved automatically.

4.2.3 Time to process certificate applications

PACI CA will process and complete the certificate application within a reasonable time of receipt a fully qualified Certificate Application.



4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

After successfully completing the administrative checks for the certificate application, a Certificate is created and issued following the approval of a Certificate Application automatically by the Civil ID Card Issuance System.

A Card Pin is generated, printed, and securely enveloped to enable Private Key use.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Once the Certificate is generated, PACI CA system will notify the Subscriber by an e-mail or an official letter or other messaging system, like Mobile SMS when available.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Any of the following conducts constitutes the Subscriber certificate acceptance:

- Subscriber sign for receiving the Card Pin.
- Failing to promptly request Certificate Revocation after receiving the Issuance notification.
- Using the certificate for the first time.

4.4.2 Publication of the certificate by the CA

Certificates are published in a publicly accessible repository.

4.4.3 Notification of certificate issuance by the CA to other entities

Not applicable.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscriber is responsible for:

- The use of the Private Key.
- Ensuring security of the Private Key.
- Prevent the use of the Private Key by others than himself.
- The security of the Card Pin.
- Report the lost, disclosed, compromise of the Private Key and / or Card Pin to the CA immediately.



- Using the certificate in their intended purposes in accordance with the Law and other regulatory actions.

4.5.2 Relying party public key and certificate usage

Relying Party is responsible for:

- Checking the validity of certificates and corresponding information.
- Check the use of a Certificate as set in the Certificate intended purpose.
- Check the Certificate Status through the appropriate CRL and also of all its CA chain.

4.6 Certificate renewal

Technically, the term “Certificate Renewal” means issuing a new Certificate using the same Subscriber information and using existing Subscriber Key Pairs.

Technically, the term “Re-Key” means issuing a new Certificate using the same Subscriber information or updated, changed information and requires generating a new Key Pairs.

Publicly known and commonly used, the term “Certificate Renewal” describe Issuing a new Certificate focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated or not.

PACI CA does not support “Certificate Renewal” from the technical prospective. A new Key Pair is always required.

To match the technical definition and keep this document standard consistency and also meet the publicly known term, “Certificate Renewal” will be referred to “Certificate Re-Key”, section 4.7 of this document.

4.6.1 Circumstance for certificate renewal

Same as section 4.7.1 of this document.

4.6.2 Who may request renewal

Same as section 4.7.2 of this document.

4.6.3 Processing certificate renewal requests

Same as section 4.7.3 of this document.

4.6.4 Notification of new certificate issuance to subscriber

Same as section 4.7.4 of this document.



4.6.5 Conduct constituting acceptance of a renewal certificate

Same as section 4.7.5 of this document.

4.6.6 Publication of the renewal certificate by the CA

Same as section 4.7.6 of this document.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

Certificate Re-Key commonly known as Certificate Renewal requires a new Key Pair to be generated to replace the current Key Pair. For the consistency, whenever Certificate Renewal is mentioned please refer to Certificate Re-Key.

PACI internal regulations are to issue a new Civil ID Card at the time of the card expiration. As the Subscriber certificates reside on Civil ID Card and the certificates validation is the same as the Civil ID Card validation, so whenever a Civil ID Card is renewed the associated Card ID certificate is renewed automatically with an automated integrated process between the Civil ID Card Issuance System and the certificate issuance system.

4.7.1 Circumstance for certificate re-key

Card ID certificate is automatically Re-Keyed (Certificate Renewal) with Civil ID Card renew processes.

Subscriber Certificate will be renewed with explicit request form the Subscriber. The renewal is subject to all Certificate Application, section 4.1 of this document.

4.7.2 Who may request certification of a new public key

Card ID certificate is automatically renewed with Civil ID Card renew processes.

Subscriber Certificate will be renewed with explicit request form the Subscriber or his legal representative. The renewal is subject to all Certificate Application, section 4.1 of this document.

4.7.3 Processing certificate re-keying requests

Procedures are the same as the initial certificate issuance described in section 4.2 of this document.



4.7.4 Notification of new certificate issuance to subscriber

Once the Certificate is generated, PACI CA system will notify the Subscriber by an e-mail or an official letter or other messaging system, like Mobile SMS when available.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Any of the following conducts constitutes certificate acceptance:

- Subscriber sign for receiving the New Card' Card Pin.
- Failing to promptly request Certificate Revocation after receiving the Issuance Notification.
- Using the certificate for the first time.

4.7.6 Publication of the re-keyed certificate by the CA

Certificates are published in a publicly accessible repository.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 *Certificate modification*

Modification to any issued certificate is not allowed. Whenever the Subscriber information need to be changed, old certificate shall be revoked and a new application shall be filed for a new certificate with new information subject to all Certificate Application, section 4.1 of this document.

4.8.1 Circumstance for certificate modification

Not applicable.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable.



4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

If any of the following circumstances occurs, but not limited to, the certificate must be revoked:

- The Subscriber show in person at PACI designated sites and request Certificate Revocation.
- Certificate information need to be changed or updated.
- Subscriber link to an organization is terminated while organization information is in the certificate.
- Subscriber legal status is changed and became not eligible legally for any reason.
- The private key has been lost, stolen or compromised.
- Subscriber death notification reaches PACI.
- PACI internal Certificate Application audit result that certificate information is inaccurate or false.

4.9.2 Who can request revocation

- The subscriber himself or his legal representative.
- Civil ID Card Issuance System will request Card ID certificate automatically as part of revoking the Civil ID Card itself when Civil ID Card is revoked for any reason.
- An organization legal representative when the Subscriber link to the organization is terminated.
- An official legal authority request when revocation is required.

4.9.3 Procedure for revocation request

All Card certificates are revoked automatically via the Civil ID Card Issuance System when the Civil ID Card is revoked for any reason, so no separate revoke requests are required.

For the Authentication & Signing certificate:

- Subscriber or his legal representative fill and manually sign the "Certificate Revocation" at PACI designated sites.
- PACI staff will validate the Subscriber proof of identity or the legal representative identity and the legally recognized representation document before accepting the request.



- PACI staff will complete and initiate the certificate revocation.

Alternative method:

- Subscriber can request his Certificate Revocation by calling PACI call center.
- Validating the caller identity is required before accepting the request.
- After initial Subscriber identity validation the certificate status is changed to “suspended”.
- Suspended Certificates will be included in the CRL list.

Suspended Certificate is revoked when:

- Subscriber or his legal representative fill and manually sign the “Certificate Revocation” at PACI designated sites.
- PACI staff will validate the Subscriber proof of identity or the legal representative identity and the legally recognized representation document.
- PACI staff will complete and initiate the certificate revocation.

When certificate is revoked before the end of its life, Subscriber can request a replacement “Certificate Replacement” the same procedure of the new Certificate Application.

4.9.4 Revocation request grace period

Subscriber must request revocation as soon as its reason occurs.

4.9.5 Time within which CA must process the revocation request

Validated & authenticated revocation request is executed immediately. Automated revocation processes are executed immediately.

4.9.6 Revocation checking requirement for relying parties

Relying Parties must check the certificate status. Relying Parties will use publicly available CRL to verify the certificate status. Online Certificate Status Protocol (OCSP) services will be provided upon approving designated requests for real-time Certificate status check.

4.9.7 CRL issuance frequency

CRLs are issued every hour with 24 hours validity.

4.9.8 Maximum latency for CRLs

CRLs are posted to the repository automatically within minutes of generation.



4.9.9 On-line revocation/status checking availability

Web-base certificate status query will be available through PACI web site at:

<http://www.paci.gov.kw>.

4.9.10 On-line revocation checking requirements

Relaying parties can use online certificate status check to check the certificate status when needed.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements re CA key compromise

Public notice will be advertised as soon as PACI CAs key compromise is discovered.

4.9.13 Circumstances for suspension

- Subscriber cannot show in person to request Certificate revocation at PACI designated sites.
- PACI internal Certificate Application audit result that certificate information is incomplete.

4.9.14 Who can request suspension

- Subscriber requests his Certificate Revocation.
- PACI internal Certificate Application audit committee.

4.9.15 Procedure for suspension request

- The Subscriber notifies PACI with the request "Certificate Revocation", not in person.
- Validating the caller identity is required before accepting the request.
- After initial Subscriber identity validation the certificate status is changed to "suspended" by the administrator.
- Suspended Certificates will be included in the CRL list automatically.
- Requester is informed to show in person to confirm "Certificate Revocation".

4.9.16 Limits on suspension period

- Remotely reported revocation which result suspension will last until the Subscriber show in person at PACI designated sites to either confirm revocation or deny revocation.



In case of confirm revocation the certificate will be permanently revoked by the administrator, else if deny revocation then the administrator will change the certificate status to be removed from CRL at the first CRL update.

- PACI internal Certificate Application audit committee suspension will be changed by the administrator as soon as the Subscriber complete his Certificate Application, else certificate will be revoked permanently.

4.10 Certificate status services

4.10.1 Operational characteristics

Certificates status is publicly available via CRL web-base, LDAP directory and OCSP responder (when configured).

4.10.2 Service availability

Service is available 24/7. Redundant systems will be available and monitored to ensure 24/7 availability.

4.10.3 Optional features

Online Certificate Status Protocol (OCSP) services will be provided upon approving designated requests and complete technical requirements for real-time Certificate status check.

4.11 End of subscription

- Subscription ends upon the expiry of the certificate without Subscriber explicit renewal request.
- Subscription ends upon revoking the certificate without Subscriber explicit new certificate request.

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*

5.1.1 Site location and construction

- PACI center is located in a controlled & physically protected location.
- Site construction includes reinforced walls and ceiling to ensure penetration resistance.
- Doors are strong enough to resist forceful entry.
- Emergency exit doors opened from the inside only.
- Doors alarms installed.
- Card reader and biometric reader are installed to control doors open.
- Multi Security areas have been identified and construction security measures increased.
- Sensitive locations are camera monitored with guard supervision 24/7.
- Guards and guard's stations are located in various areas of the location 24/7.

5.1.2 Physical access

- Physical access to areas within PACI center is restricted & controlled.
- All doors are always closed.
- Access is logged.
- Designated access rights are implemented.
- Dual access required for higher security areas.
- Visitors are escorted.
- Maintenance and service personnel are escorted and supervised.

5.1.3 Power and air conditioning

PACI center is supported by uninterrupted power supplies and generators which will immediately be enabled in cases of power interruption to ensure a continuous supply of power. Maintenance for standby power units is regularly performed and monitored.

Air conditioning always available to control temperature and humidity. Also proper ventilation systems are available.

5.1.4 Water exposures

PACI center is protected against floods and water exposures.



5.1.5 Fire prevention and protection

PACI center is equipped with smoke and heat detectors. Different fire extinguishing systems exist, utilizing different materials suitable for systems & staff.

5.1.6 Media storage

All media containing production software and data, audit, archive, or backup information is stored in a secure storage with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage.

5.1.7 Waste disposal

All sensitive information on documents and different medias shall be destroyed before disposal. Cryptographic modules are re-set according to the manufacturer's instructions.

5.1.8 Off-site backup

PACI keeps the backups of critical systems & data and crypto equipments in secure off-site for business continuity purposes.

5.2 Procedural controls

5.2.1 Trusted roles

Trusted roles related to all certification business processes are identified, include but are not limited to:

Management:

Senior managers & line managers technically and administratively responsible for conduct PACI certification services as planned. Responsible for planning, managing and controlling technical and administrative functioning of relevant units where customer services and basic certification processes as well as all support functions such as archival and facility security are carried out.

Key Management:

Responsible for CAs generation and life-cycle, security, maintenance, backup and crypto HW activations.

Authorized Personnel for Registration and Customer Services:

Staff responsible for routine certification services such as customer services, document control, and registration processes relating to certificate application, renewal and revocation.

Information Security Management System Personnel:



Responsible for ensuring information security in business processes under PACI certification services, execution of security principles and related procedures.

System and Network Administrators:

Employees responsible for installing, configuring, backing up of all systems software and hardware components used in certification processes.

Certificate Production Center Officers:

Responsible for daily certificate production maintenance, support, and backing and ensure service availability who have special access control privileges over certificate production systems.

Auditors:

Responsible for auditing certificate production processes and all related documents.

Security Personnel:

Serving as security supervisors over security personnel at the building entry and critical units who are responsible of physical security of the entire facilities.

5.2.2 Number of persons required per task

PACI applies control procedures to ensure separation of duties according to job responsibilities and tasks. The most sensitive tasks require multiple trusted persons.

5.2.3 Identification and authentication for each role

- Employees are issued access devices and granted access rights to their work areas.
- Employees are issued electronic credentials to access and perform specific functions on the system.

5.2.4 Roles requiring separation of duties

Duties have been separated to prevent a single person of performing a start-to-end work process. Also to prevent security risks by preventing one person from being able to overcome security barriers.

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

- Validation of information in Certificate Applications;
- Approving issuance of Certificates.
- Creating CA;
- Activating CA on production systems.
- Grant access to systems location;
- Performing system backup;
- Configure systems firewalls.



5.3 Personnel controls

PACI personnel will follow all personnel rules and guides implemented in Kuwait sensitive governmental units.

5.3.1 Qualifications, experience, and clearance requirements

PACI personnel will have to have appropriate educational levels as stated in each job profile with qualifications to perform certification related processes accurately and reliably.

PACI personnel have to present proof of government clearances, criminal clearance certificate, and others as required by HR rules and procedures.

5.3.2 Background check procedures

PACI require original credential documents to be presented and reviewed including Civil ID Card and most relevant educational degree obtained.

Clear official criminal records certificate is required, at minimum, other government clearances or others may be requested by HR rules and procedures.

5.3.3 Training requirements

PACI personnel will receive training relevant for their responsibilities. Employees shall be trained and informed on business processes, procedures and rules & instructions relating to operation roles.

Employees will be informed about security principles and the existing information security management system, and overall security awareness.

5.3.4 Retraining frequency and requirements

Updated training will be provided as needed including updated rules & procedures.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of policies and procedures imposed by Kuwait Labor Law and PACI internal regulations.

5.3.7 Independent contractor requirements

Independent contractors will have to sign a non disclosure agreement and optionally a service contract with the security clauses and service principles relevant to the needed task.



5.3.8 Documentation supplied to personnel

PACI personnel will have access to documents relevant to their job and job responsibilities to ensure that they can meet their job responsibilities in full.

5.4 Audit logging procedures

5.4.1 Types of events recorded

PACI CA will log the following events manually or automatically:

- CA key life cycle events including: CAs key generation, backup, storage, archival, and destruction.
- Subscriber certificate life cycle events including: Certificate Applications, renewal - rekey, suspension and revocation.
- System generation and issuance of Certificates and CRLs.

Security-related events including:

- Successful and unsuccessful PKI system access attempts.
- PKI and security system actions performed by personnel.
- Security sensitive files or records read, written or deleted.
- System crashes, hardware failures and other events.
- Firewall and router activity.

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.

PACI will log Certificate Application information including:

- Subscriber identification type.
- Subscriber identification number & other data.
- Identity of entity accepting the application.

5.4.2 Frequency of processing log

Logs will be continuously checked and backed up and archived periodically.

5.4.3 Retention period for audit log

Audit logs are retained on-site for one year after processing and then archived.



5.4.4 Protection of audit log

Audit logs are protected by physical and electronic security measures that include mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit log backup procedures

Incremental backups of audit logs are created periodically and full backups are performed monthly.

5.4.6 Audit collection system (internal vs. external)

The audit log collection system done through the internal systems.

5.4.7 Notification to event-causing subject

No notice is required to be given to the event-causing subject.

5.4.8 Vulnerability assessments

Measure will be taken toward any security gaps identified by analyzing audit logs.

5.5 *Records archival*

5.5.1 Types of records archived

- Certificate Application information.
- Relevant paper forms to the Certificate Application.
- Certificate lifecycle information e.g. revocation, re-key and renewal application information.
- Relevant paper forms to the Certificate lifecycle.
- All audit data collected in terms of Section 5.4.

5.5.2 Retention period for archive

Archived records shall be retained for at least 10 years.

5.5.3 Protection of archive

Archives are protected by physical and electronic security measures, and kept open for access by authorized personnel only.

Electronic archives are protected against unauthorized viewing, modification or deletion.



Archives on paper are retained in special locked units to which only authorized personnel can access.

5.5.4 Archive backup procedures

Incremental backups of electronic archives are created periodically and full backups are performed monthly. No backup is made for archives on paper.

5.5.5 Requirements for time-stamping of records

Date & time will be part of Certificates, CRLs and other revocation database entries.

5.5.6 Archive collection system (internal or external)

All archive collection systems are internal.

5.5.7 Procedures to obtain and verify archive information

Upon authenticated request, only controlled access is provided for archives.

5.6 Key changeover

Re-keying process for PACI root CA and online CAs certificates shall be performed by PACI key management team in a secure controlled and witnessed events.

PACI root CAs will be re-keyed at the end of its life time.

PACI online CAs can be renewed as root CA life time permit.

New CAs key pairs, for root or online CAs, will be generated as necessary if technology update require.

At the time of re-keying of PACI root CA, PACI will support both root CAs hierarchy.

At the time of re-keying of PACI online CA, new online CA will be signed under the new root.

At the time a new online CA is ready all new Subscribers certificate will be issued under the new online CA.

PACI will ensure that the old online CA will be available to sign and publish the CRLs until the last valid subscriber certificate is expired.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

When incident or compromise occurs, PACI CA will execute its Disaster Recovery & Business Continuity plans which ever suite the situation.



5.7.2 Computing resources, software, and/or data are corrupted

Damaged computing resources (HW) is replaced with new, and then repair effort is made to restore the damaged units.

Corrupted software and/or data will be restored by executing the adequate restore procedure to ensure full integrity which could include using the latest backup stored in the off-site location to restore full certificate system components like: systems, logs, certificate information, and database records to retain services.

5.7.3 Entity private key compromise procedures

If PACI CA private key is compromised, the following procedures will be executed:

- Revoke all certificates issued using that key.
- Revoke the compromised CA.
- Re-key the revoked CA.
- New certificates shall be issued to replace the revoked certificates using the new CA.
- Publish appropriate notice to all parties.

5.7.4 Business continuity capabilities after a disaster

When incident or compromise occurs, PACI will execute its Disaster Recovery & Business Continuity plans which ever suite the situation.

PACI will restore essential operations in sequence within appropriate time limit:

- Restore and publish revoked certificates information (CRLs).
- Enable certificate revocation.
- Enable certificate issuance.
- Restore full center capabilities.

5.8 CA or RA termination

In case that PACI have to terminate its certificate services, the following procedures will be executed:

- Publicly announce the cease of service notice.
- Stop issuing new certificates.
- Keep needed services to support currently valid certificates.
- After the expiry of last valid certificate, PACI will stop all its certification services.
- Prepare all records to be surrendered to proper authorities, if required.



6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

PACI generate its CAs key pairs in a controlled and secure environment with the presence of PACI qualified personnel and named participants. The cryptographic modules used, meet the requirements of at least FIPS 140-1 level 3 or higher. Private keys are protected against unauthorized access by physical and technical security measures.

Civil ID Card Issuance System RA key pair is generated in the relevant automated system and sent to PACI CA for certification using controlled and secured methods. Manual RA certificates are created on Smart Cards equivalent to Civil ID cards specifications.

PACI will generate the private key on behalf of the Subscriber on the Civil ID Card or equivalent Smart Card (for non Civil ID Card holders) at PACI designated sites using Civil ID Card Issuance System. Private Key use will be controlled by Card PIN. A Card Pin is generated, printed, and securely enveloped at PACI designated sites from Civil ID Card Issuance System.

6.1.2 Private key delivery to subscriber

Civil ID card or equivalent Smart Card holding the Subscriber Private Key will be delivered in person to the Subscribers after identification checks and hand written signatures also the Card PIN.

6.1.3 Public key delivery to certificate issuer

Subscriber Public Key is delivered to the certificate issuer through the use of a PKCS#10 Certificate Signing Request (CSR) automatically and securely from Civil ID Card Issuance System.

6.1.4 CA public key delivery to relying parties

PACI Root CA and online CAs public keys will be publicly accessible through www.paci.gov.kw.

6.1.5 Key sizes

PACI Root CA key size will not be less than 2048 bit.

PACI on line CAs key size will not be less than 2048 bit.

RA certificate key size will not be less than 1024 bit.

Subscriber certificate key size will not be less than 1024 bit.



6.1.6 Public key parameters generation and quality checking

Not applicable.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Certification Authorities shall be used for signing certificates and CRLs. Card ID Subscriber certificates will be used for Civil ID card identification and authentication. Subscriber Authentication & Signing certificate will be used for Authentication & Signing.

6.2 *Private Key Protection and Cryptographic Module Engineering Controls*

6.2.1 Cryptographic module standards and controls

PACI CAs is created on hardware cryptographic modules that meet the requirements of FIPS 140-1 level 3 or higher.

6.2.2 Private key (m out of n) multi-person control

Use of sensitive CA cryptographic operations is under split password method with the possession of multi-person control, m of n. To activate and use of PACI CAs private key m authorized persons of n must present their activation data. The m number needed to activate a CA is 3 out of 10, n.

6.2.3 Private key escrow

CAs private keys are not escrowed.

Subscribers' private key escrow is not supported.

6.2.4 Private key backup

CAs Private Key must have backup for operations load and disaster recovery purposes only. Backup cryptographic hardware modules standard and m of n must be the same as the prime unit. All Backup modules will be stored at PACI center and controlled by the key management team except the disaster recovery units which must be stored at off-site location.

Backup of subscriber private key is not applicable, as smart card standard forbids private key leaving the card.



6.2.5 Private key archival

Expired CAs and its associated key pairs are stored on cryptographic hardware module that meets the standard stated in this document. Private key is stored for archival purpose only and will not be used.

6.2.6 Private key transfer into or from a cryptographic module

CAs private keys are transferred between cryptographic hardware modules only. The transfer will be in encrypted form.

6.2.7 Private key storage on cryptographic module

CAs private keys held on cryptographic hardware modules shall be stored in encrypted form.

6.2.8 Method of activating private key

To activate and use PACI CAs private key m authorized persons of n must present their activation data. The m number needed to activate a CA is 3 out of 10, n .

Card Pin will be used to activate the Subscriber private key.

6.2.9 Method of deactivating private key

CAs cryptographic hardware modules shall be removed from the reader to be deactivated or power is shut down off the reader.

6.2.10 Method of destroying private key

Two of the key management team is responsible for destroying PACI CAs private keys. To destroy the CAs private key, the CA is deleted according to the manufacturer's instructions.

6.2.11 Cryptographic Module Rating

PACI CAs is created on hardware cryptographic modules that meet the requirements of FIPS 140-1 level 3 or higher.

6.3 Other aspects of key pair management

6.3.1 Public key archival

PACI CAs public keys and Subscribers public keys are archived for 5 years after their expiration.



6.3.2 Certificate operational periods and key pair usage periods

PACI root CA "PACI Policy CA" certificate validity can be up to 15 years.

PACI online CA "PACI ID Issuance CA" certificate validity can be up to 10 years.

Subscriber certificate validity cannot exceed the Civil ID Card validity.

Subscriber certificate validity up to 5 years or Civil ID Card validity which comes first.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation Data will be created by PACI key managements team. Activation data will be stored on secured media approved by the hardware cryptographic modules manufacture.

6.4.2 Activation data protection

Activation data secured media will be stored at PACI location under the control of their holder in a locked place.

6.4.3 Other aspects of activation data

Activation data will be stored in a separate place other than the hardware cryptographic modules they protect. DR hardware cryptographic modules off-site store will be different from than the DR activation data store location.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Security controls are implemented to access and operate all information systems:

- Computer systems hardware will be of known trustworthy reliable brands.
- Computer systems software will be original products.
- Systems are protected against unauthorized access and security gaps.
- Controls for penetration and intrusion will be established and handled.
- Computer systems will be protected against network security hacking by firewalls and each firewall will have a failsafe second unit.
- Access rights to computer systems and authentication are ensured by passwords and / or authentication medias.
- Access rights to computers have been limited to the roles assigned to authorized persons.
- Since operational records are constantly logged, problems that may arise in the computer systems can be identified in short time and accurately and also handled.
- Production network will be logically or physically separated from other zones.



6.5.2 Computer security rating

Not applicable.

6.6 *Life cycle technical controls*

6.6.1 System development controls

Since PACI utilizes VeriSign solution, PACI will have VeriSign assurance, controls guaranty and also support governed by the contract.

6.6.2 Security management controls

The configuration, modification or upgrade of any system within PACI will be documented and controlled.

6.6.3 Life cycle security controls

Not applicable.

6.7 *Network security controls*

All network devices such as firewalls and routers will be installed correctly and securely in accordance with the network configuration best practices procedures. All systems within PACI are protected by appropriate network security methods as per manufacturer recommendations. Critical network devices will have a redundant mechanism to ensure services continuity.

6.8 *Time-stamping*

Date & Time will be part of Certificates, CRLs, and other revocation database entries.



7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

All PACI CA issued X.509 certificate will have the following basic information:

- Subscriber information (depend on certificate type)
- Certification Authority information.
- Certificate validity period start and end dates.
- Signature algorithm.
- Public key of subscriber.
- Certificate unique serial number.
- Signature of Certification Authority.

Subscriber information for Card ID certificate:

Civil ID

Card serial number

Document number

Application use

Subscriber information for Authentication & Signing certificate:

Full Latin name

Civil ID

Full name in Arabic

Email

Title

Application use

7.1.1 Version number(s)

PACI CA issued certificates will be X.509 Version 3 Certificates.

7.1.2 Certificate extensions

PACI CA will support all certificate extensions defined under X.509 v3 standard. Certificate extension will be appropriately set according to the certificate type: key usage, certificate policies extension, subject alternative names, basic constraints, extended key usage, CRL distribution points, authority key identifier, and subject key identifier.

7.1.3 Algorithm object identifiers

PACI CA supports the following algorithm, not limited to:

- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)



rsadsi(113549) pkcs(1) pkcs-1(1) 5}
- sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) 11}

PACI will use SHA1 algorithm.

Issued certificate will include the Object identifiers of algorithm used in the respective field.

7.1.4 Name forms

Certificates Issuer and Subject Distinguished Name are in accordance with Section 3.1.1 of this document.

7.1.5 Name constraints

Not applicable.

7.1.6 Certificate policy object identifier

Not applicable.

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

Not applicable.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL profile

PACI CRLs will include the basic fields:

- Version number.
- Issuer.
- Effective date.
- Next update.
- Revoked certificates list.



7.2.1 Version number(s)

PACI supports both X.509 Version 1 and Version 2 CRLs. Default version is version 1.

7.2.2 CRL and CRL entry extensions

Not applicable.

7.3 OCSP profile

PACI support OCSP (Online Certificate Status Protocol). OCSP is a way to obtain timely information about the revocation status of a particular certificate. OCSP services will be provided upon approving designated requests for real-time Certificate status check.

PACI OCSP responders will conform to RFC 2560.

7.3.1 Version number(s)

PACI will support the v1 protocol version under the RFC 2560 Internet X.509 Public Key Infrastructure.

7.3.2 OCSP extensions

PACI support extensions defined in RFC 2560 and could be used.



8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Not applicable.

8.1 Frequency or circumstances of assessment

Not applicable.

8.2 Identity/qualifications of assessor

Not applicable.

8.3 Assessor's relationship to assessed entity

Not applicable.

8.4 Topics covered by assessment

Not applicable.

8.5 Actions taken as a result of deficiency

Not applicable.

8.6 Communication of results

Not applicable.



9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Not applicable.

9.1.1 Certificate issuance or renewal fees

Not applicable.

9.1.2 Certificate access fees

Not applicable.

9.1.3 Revocation or status information access fees

Not applicable.

9.1.4 Fees for other services

Not applicable.

9.1.5 Refund policy

Not applicable.

9.2 *Financial responsibility*

Not applicable.

9.2.1 Insurance coverage

Not applicable.

9.2.2 Other assets

Not applicable.



9.2.3 Insurance or warranty coverage for end-entities

Not applicable.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All public information presented to PACI will be treated as public information. Information needs to be public for Subscriber identification and authentication by others will be public. Other information will be confidential unless need to be public.

PACI center information are included in the scope of confidential information, including but not limited to: documents relating certification services, private keys of certification authorities, software and hardware specific information, operational records, audit reports, access system to on-site areas and devices, facility layout and interior design, emergency action plans, business plans.

9.3.2 Information not within the scope of confidential information

Information which will be kept public like issued certificate, CRLs and other publicly accusable information are not within the scope of confidential information by nature.

9.3.3 Responsibility to protect confidential information

PACI have the responsibility of protecting confidential information from compromise and disclosure to unauthorized access by sufficient security means.

9.4 Privacy of personal information

9.4.1 Privacy plan

PACI will protect personal information presented by the Subscribers.

9.4.2 Information treated as private

Subscribers' personal information that is not publicly available as part of issued certificate and online CRLs is treated as private.

9.4.3 Information not deemed private

Any publicly accusable information is not deemed private.



9.4.4 Responsibility to protect private information

PACI have the responsibility of protecting private information by sufficient security means.

9.4.5 Notice and consent to use private information

Subscribers' private information is used by PACI for issuing certificates purposes only.

9.4.6 Disclosure pursuant to judicial or administrative process

Private information required in the judicial and administrative processes shall be given only to the requesting authority.

9.4.7 Other information disclosure circumstances

Not applicable.

9.5 *Intellectual property rights*

PACI retain all Intellectual Property Rights for and to the certificates and revocation information that its issue including but not limited to: all internal and external documents relating to certification services, databases, and websites.

9.6 *Representations and warranties*

9.6.1 CA representations and warranties

PACI represents and warrants that contents of all issued certificates are accurate, identity validation steps have been performed accurately and reliably, the right certificate has been issued to the right applicant and delivered to the right person, published certificate status information and revocation information is updated and accurate, and its performed all practice requirements and obligations included in CP and CPS.

9.6.2 RA representations and warranties

PACI represents and warrants that contents of all issued certificates are accurate, identity validation steps have been performed accurately and reliably, the right certificate has been issued to the right applicant and delivered to the right person, published certificate status information and revocation information is updated and accurate, and its performed all practice requirements and obligations included in CP and CPS.



9.6.3 Subscriber representations and warranties

Subscribers represent and warrant that they will submit updated and accurate information and documents to PACI during certificate application and renewal and revocation requests use their certificates under the conditions stated by PACI and Subscribers private key is protected and that no unauthorized person has ever had access to the Subscriber private key.

9.6.4 Relying party representations and warranties

Relying Parties acknowledge that they have sufficient information from PACI to make an informed decision as to the extent to which they choose to rely on the information in a Certificate and that they shall bear the consequences of their failure to perform the Relying Party obligations.

9.6.5 Representations and warranties of other participants

Not applicable.

9.7 *Disclaimers of warranties*

Not applicable.

9.8 *Limitations of liability*

Not applicable.

9.9 *Indemnities*

Not applicable.

9.10 *Term and termination*

9.10.1 Term

The CPS becomes effective upon publication in the repository.

9.10.2 Termination

This version of the CPS document is valid until a new version is available.



9.10.3 Effect of termination and survival

The effect of termination shall take place at the expiry or revocation all certificates issued under its effect.

9.11 Individual notices and communications with participants

All individual notices from PACI CA to subscribers shall be made by e-mail or other available messaging services. Notices from PACI CA to relying parties shall be published over the web at www.paci.gov.eg.

9.12 Amendments

Amendments are used while the CPS document undergo minor changes that would not affect the use and acceptability of certificates already issued.

9.12.1 Procedure for amendment

It's the responsibility of PACI CPS designated committee to set the approval procedure.

9.12.2 Notification mechanism and period

Amendments shall be published over the web. Amendments will stay active till the next version of the document is released.

9.12.3 Circumstances under which OID must be changed

Major changes that require new versions may require OID change.

9.13 Dispute resolution provisions

Kuwait court have jurisdiction for resolution of disputes.

9.14 Governing law

Kuwait Laws governs as applicable.

9.15 Compliance with applicable law

Not applicable.



9.16 *Miscellaneous provisions*

Not applicable.



Signatures & Approvals

PACI PKI Key Manager

Signature:

Date:

Mr. Nasser Al Otaibi

PACI PKI Key Manager

Signature:

Date:

Mr. Tareq Al Rashed

PACI Director of System
Development

Signature:

Date:

Mr. Mansour Al Methen

PACI Director General

Signature:

Date:

Mr. Musaed Al Asousi
