# IUCC Certification Authority

## Certificate Policy and Certification Practice Statement

DRAFT VERSION 1.4

Document OID: 1.3.6.1.4.1.17004.10.1.4

5 December 2003

# Contents

Contents .... 2
1. INTRODUCTION .... 7
1.1 Overview .... 7
1.1.1 General Definitions .... 7
1.2 Identification .... 8
1.3 Community and Applicability .... 8
1.3.1 Certification authorities .... 8
1.3.2 Registration authorities .... 8
1.3.3 End entities .... 9
1.3.4 Applicability .... 10
1.4 Contact Details .... 10
1.4.1 Specification administration organization .... 10
1.4.2 Contact person .... 10
1.4.3 Person determining CPS suitability for the policy .... 10
2. GENERAL PROVISIONS .... 10
2.1 Obligations .... 10
2.1.1 CA obligations .... 10
2.1.2 RA obligations .... 11
2.1.3 Subscriber obligations .... 11
2.1.4 Relying party obligations .... 12
2.1.5 Repository obligations .... 12
2.2 Liability .... 12
2.2.1 CA liability .... 12
2.2.2 RA liability .... 12
2.3 Financial Responsibility .... 12
2.3.1 Indemnification by relying parties .... 13
2.3.2 Fiduciary relationships .... 13
2.3.3 Administrative processes .... 13
2.4 Interpretation and Enforcement .... 13
2.4.1 Governing law .... 13
2.4.2 Severability, survival, merger, notice .... 13
2.4.3 Dispute resolution procedures .... 13
2.5 Fees .... 13
2.5.1 Certificate issuance or renewal fees .... 13
2.5.2 Certificate access fees .... 13
2.5.3 Revocation or status information access fees .... 14
2.5.4 Fees for other services such as policy information .... 14
2.5.5 Refund policy .... 14
2.6 Publication and Repository .... 14
2.6.1 Publication of CA information .... 14
2.6.2 Frequency of publication .... 14
2.6.3 Access controls .... 14
2.6.4 Repositories .... 14
2.7 Compliance Audit .... 14

2.7.1 Frequency of entity compliance audit ..... 15
2.7.2 Identity/qualifications of auditor ..... 15
2.7.3 Auditor's relationship to audited party ..... 15
2.7.4 Topics covered by audit ..... 15
2.7.5 Actions taken as a result of deficiency ..... 15
2.7.6 Communication of results ..... 15
2.8 Confidentiality ..... 15
2.8.1 Types of information to be kept confidential ..... 15
2.8.2 Types of information not considered confidential ..... 15
2.8.3 Disclosure of certificate revocation/suspension information ..... 15
2.8.4 Release to law enforcement officials ..... 15
2.8.5 Release as part of civil discovery ..... 16
2.8.6 Disclosure upon owner's request ..... 16
2.8.7 Other information release circumstances ..... 16
2.9 Intellectual Property Rights ..... 16
3. IDENTIFICATION AND AUTHENTICATION ..... 16
3.1 Initial Registration ..... 16
3.1.1 Types of names ..... 16
3.1.2 Need for names to be meaningful ..... 17
3.1.3 Rules for interpreting various name forms ..... 17
3.1.4 Uniqueness of names ..... 17
3.1.5 Name claim dispute resolution procedure ..... 17
3.1.6 Recognition, authentication and role of trademarks ..... 18
3.1.7 Method to prove possession of private key ..... 18
3.1.8 Authentication of organization identity ..... 18
3.1.9 Authentication of individual identity ..... 18
3.2 Routine Rekey ..... 18
3.3 Rekey After Revocation ..... 18
3.4 Revocation Request ..... 18
4. OPERATIONAL REQUIREMENTS ..... 19
4.1 Certificate Application ..... 19
4.2 Certificate Issuance ..... 19
4.3 Certificate Acceptance ..... 19
4.4 Certificate Suspension and Revocation ..... 20
4.4.1 Circumstances for revocation ..... 20
4.4.2 Who can request revocation ..... 20
4.4.3 Procedure for revocation request ..... 20
4.4.4 Revocation request grace period ..... 20
4.4.5 Circumstances for suspension ..... 20
4.4.6 Who can request suspension ..... 20
4.4.7 Procedure for suspension request ..... 21
4.4.8 Limits on suspension period ..... 21
4.4.9 CRL issuance frequency (if applicable) ..... 21
4.4.10 CRL checking requirements ..... 21
4.4.11 On-line revocation/status checking availability ..... 21
4.4.12 On-line revocation checking requirements ..... 21

4.4.13 Other forms of revocation advertisements available 21
4.4.14 Checking requirements for other forms of revocation advertisements 21
4.4.15 Special requirements re key compromise 21
4.5 Security Audit Procedures 21
4.5.1 Types of event audited 21
4.5.2 Frequency of processing log 22
4.5.3 Retention period for audit log 22
4.5.4 Protection of audit log 22
4.5.5 Audit log backup procedures 22
4.5.6 Audit collection system (internal vs external) 22
4.5.7 Notification to event-causing subject 22
4.5.8 Vulnerability assessments 22
4.6 Records Archival 22
4.6.1 Types of event recorded 22
4.6.2 Retention period for archive 22
4.6.3 Protection of archive 23
4.6.4 Archive backup procedures 23
4.6.5 Requirements for time-stamping of records 23
4.6.6 Archive collection system (internal or external) 23
4.6.7 Procedures to obtain and verify archive information 23
4.7 Key Changeover 23
4.8 Compromise and Disaster Recovery 23
4.8.1 Computing resources, software, and/or data are corrupted 23
4.8.2 Entity public key is revoked 23
4.8.3 Entity key is compromised 23
4.8.4 Secure facility after a natural or other type of disaster 24
4.9 CA Termination 24
5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS 24
5.1 Physical Controls 24
5.1.1 Site location and construction 24
5.1.2 Physical access 25
5.1.3 Power and air conditioning 25
5.1.4 Water exposures 25
5.1.5 Fire prevention and protection 25
5.1.6 Media storage 25
5.1.7 Waste disposal 25
5.1.8 Off-site backup 25
5.2 Procedural Controls 25
5.2.1 Trusted roles 25
5.2.2 Number of persons required per task 25
5.2.3 Identification and authentication for each role 25
5.3 Personnel Controls 26
5.3.1 Background, 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 Contracting personnel requirements.......... 26
5.3.8 Documentation supplied to personnel .......... 26
6. TECHNICAL SECURITY CONTROLS.......... 26
6.1 Key Pair Generation and Installation .......... 26
6.1.1 Key pair generation .......... 26
6.1.2 Private key delivery to entity .......... 27
6.1.3 Public key delivery to certificate issuer .......... 27
6.1.4 CA public key delivery to users .......... 27
6.1.5 Key sizes .......... 27
6.1.6 Public key parameters generation .......... 27
6.1.7 Parameter quality checking .......... 27
6.1.8 Hardware/software key generation.......... 27
6.1.9 Key usage purposes (as per X.509 v3 key usage field).......... 27
6.2 Private Key Protection .......... 27
6.2.1 Standards for cryptographic module .......... 27
6.2.2 Private key (n out of m) multi-person control.......... 28
6.2.3 Private key escrow .......... 28
6.2.4 Private key backup .......... 28
6.2.5 Private key archival.......... 28
6.2.6 Private key entry into cryptographic module .......... 28
6.2.7 Method of activating private key .......... 28
6.2.8 Method of deactivating private key.......... 28
6.2.9 Method of destroying private key .......... 28
6.3 Other Aspects of Key Pair Management.......... 28
6.3.1 Public key archival.......... 28
6.3.2 Usage periods for the public and private keys .......... 29
6.4 Activation Data .......... 29
6.4.1 Activation data generation and installation.......... 29
6.4.2 Activation data protection .......... 29
6.4.3 Other aspects of activation data .......... 29
6.5 Computer Security Controls.......... 29
6.5.1 Specific computer security technical requirements.......... 29
6.5.2 Computer security rating.......... 29
6.6 Life Cycle Technical Controls .......... 29
6.6.1 System development controls.......... 29
6.6.2 Security management controls .......... 30
6.6.3 Life cycle security ratings .......... 30
6.7 Network Security Controls.......... 30
6.8 Cryptographic Module Engineering Controls .......... 30
7. CERTIFICATE AND CRL PROFILES .......... 30
7.1 Certificate Profile .......... 30
7.1.1 Version number(s).......... 30
7.1.2 Certificate extensions .......... 30
7.1.3 Algorithm object identifiers .......... 30

7.1.4 Name forms .......... 30
7.1.5 Name constraints .......... 30
7.1.6 Certificate policy Object Identifier .......... 31
7.1.7 Usage of Policy Constraints extension .......... 31
7.1.8 Policy qualifiers syntax and semantics .......... 31
7.1.9 Processing semantics for the critical certificate policy extension .......... 31
7.2 CRL Profile .......... 31
7.2.1 Version number(s) .......... 31
7.2.2 CRL and CRL entry extensions .......... 31
8. SPECIFICATION ADMINISTRATION .......... 31
8.1 Specification change procedures .......... 31
8.2 Publication and notification policies .......... 31
8.3 CPS approval procedures .......... 31
9. VERSIONS .......... 32
9.1 Change log .......... 32
Registration Authority Agreement .......... 33
Bibliography .......... 34

# 1. INTRODUCTION

This certification Policy and Practice Statement (CP/CPS) is written according to the framework layed out by RFC2527 [2].

## 1.1 Overview

The Israel InterUniversity Computation Center (IUCC) is a non-profit organization located in Tel Aviv, Israel [1] incorporating all Israeli universities. This document is the combined Certificate Policy and Certification Practice Statement of the IUCC Certification Authority. It describes the set of procedures followed by the IUCC CA.

### 1.1.1 General Definitions

The following definitions and associated abbreviations are used in this document.

IUCC
The Israel InterUniversity Computation Center, a non-profit organization located in Tel-Aviv, Israel [1].

Certificate
Synonymous with Public Key Certificate.

Certification Authority (CA)
An entity trusted by one or more users to create and assign public key certificates and be responsible for them during their whole lifetime.

Certificate Policy (CP)
A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certification Practice Statement (CPS)
A statement of the practices which a certification authority employs in issuing certificates.

Certification Authority Request Gateway (CA-GATE)
A computer configured with appropriate software to support the procedures described in a CPS.

Certificate Revocation List (CRL)
A time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

Public Key Certificate
A data structure containing the public key of an end entity and some other information, which is digitally signed with

| | |
|---|---|
| | the private key of the CA which issued it. |
| Registration Authority (RA) | An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e. an RA is delegated certain tasks on behalf of a CA). In this document the term “team leader” is synonymous with RA. |
| Relying party | A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. |
| Repository | A storage area, usually online, which contains lists of issused certificates, CRLs, policy documents, etc. |
| Subscriber | A person or server to whom a Public Key Certificate is issued.  Referred to in this document also as “user” or “end-entity”. |

Within this document the words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, “OPTIONAL” are to be interpreted as in RFC 2119 [9].

## 1.2 Identification

This document is named *IUCC Certification Authority Certificate Policy and Certification Practice Statement.* The version is *1.4*, dated *December 5, 2003*. The following ASN.1 Object Identifier (OID) has been assigned to this document: ***1.3.6.1.4.1.17004.10.1.4.*** This OID is constructed as shown in the table below

| | |
|---|---|
| IANA | 1.3.6.1.4.1 |
| IUCC | .17004 |
| IUCC CA | .10 |
| CP/CPS | .1 |
| Major Version | .4 |
| Minor Version | .0 |

## 1.3 Community and Applicability

### 1.3.1 Certification authorities

IUCC CA does not issue certificates to subordinate Certification Authorities.

### 1.3.2 Registration authorities

IUCC CA delegates the authentication of individual identity to the following Registration Authorities (RAs). These Registration Authorities constitute the eight member organizations that comprise the IUCC. Such trusted intermediaries are formally assigned by IUCC CA and their identities and contact details are published in an on-line accessible repository.

- TAU RA: responsible for identifying people, servers and services at Tel Aviv University, Ramat Aviv.
- HAIFA RA: responsible for identifying people, servers and services at Haifa University, Haifa.
- BGU RA: responsible for identifying people, servers and services at Ben Gurion University, Beersheva.
- HUJI RA: responsible for identifying people, servers and services at Hebrew University, Jerusalem.
- BIU RA: responsible for identifying people, servers and services at Bar-Ilan University, Ramat Gan.
- TECHNION RA: responsible for identifying people, servers and services at the Technion, Haifa.
- OPENU RA: responsible for identifying people, servers and services at Open University, Ramat Aviv.
- WEIZMANN RA: responsible for identifying people, servers and services at the Weizmann Institute of Science, Rehovot.
- DEFAULT IUCC RA: if a person, server or service is not attached to one of the previously mentioned universities, they must use the DEFAULT IUCC RA as a registration authority. Moreover, only this RA is recognized as being able to approve host certificate requests.

RAs must sign an agreement with IUCC CA, stating their adherence to the procedures described in this document. RAs are not allowed to issue certificates under this CP/CPS.

### 1.3.3 End entities

Certificates can be issued to a natural person (user certificate), a computer (host certificate) or a service (service certificate). The entities that are eligible for certification by IUCC CA are:

- IUCC Users: All individuals related to organizations who are members of IUCC (as detailed in section 1.3.2) and who are involved in the research , deployment or end-use of multi-domain distributed computing and who’s focus is research and/or education.
- IUCC Computers: Computers connected in the IUCC network or located at one of its member universities (as detailed in section 1.3.2).
- IUCC Services: Computer services managed by IUCC Users and running on IUCC Computers or located at one of IUCC’s member universities (as detailed in section 1.3.2).

### 1.3.4 Applicability

The authorised uses of certificates issued by IUCC CA are:

- e-mail signing and encryption (S/MIME)
- authentication and encryption of communications (SSL/TLS)
- network layer encryption (IPsec)
- object-signing

The certificates issued by IUCC CA must not be used for financial transactions of any kind, including gifts.

## 1.4 Contact Details

### 1.4.1 Specification administration organization

The Security Officer of the IUCC Grid Deployment Group, known as the Israel Academic Grid (IAG) is responsible for the management of the IUCC CA [3].

| | |
|---|---|
| General web address: | http://certificate.iucc.ac.il |
| Policy documents: | http://certificate.iucc.ac.il/ca/policy |
| Certification repository: | http://certificate.iucc.ac.il/ca |

### 1.4.2 Contact person

Hank Nussbacher
IUCC
Computer Center
Tel Aviv University
Ramat Aviv Israel
Phone: +972 (0)3 6408309

### 1.4.3 Person determining CPS suitability for the policy

The person named in section 1.4.2 determines CPS suitability for the policy.

# 2. GENERAL PROVISIONS

## 2.1 Obligations

### 2.1.1 CA obligations

IUCC CA is solely responsible for the issuance and management of certificates referencing this document. IUCC CA shall:

- ensure that all services, operations and infrastructure conform to this CP/CPS
- handle certificate requests and issue new certificates :
    - accept and confirm certification requests from entities requesting a certificate according to the procedures described in this document
    - authenticate entities requesting a certificate, where applicable with the assistance of the designated RAs listed in section 1.3.2
    - issue certificates based on requests from authenticated entities
    - send notification of issued certificates to requesting entities
    - make issued certificates publicly available
- handle certificate revocation requests and certificate revocation :
    - accept and confirm revocation requests from entities requesting that a certificate be revoked according to the procedures described in this document
    - authenticate entities requesting that a certificate be revoked
    - make certificate revocation information publicly available

### 2.1.2 RA obligations

RAs must sign an agreement to adhere to the procedures described in this document. Each RA shall:

- authenticate the identity of the person requesting a certificate
- validate the connection between a public key and the requester identity including a suitable proof of possession method
- confirm such validation to the CA
- request revocation of a certificate in the event that it becomes aware of circumstances justifying such revocation
- log all transactions and requests

### 2.1.3 Subscriber obligations

In requesting a certificate, subscribers agree to:

- accept conditions and adhere to the procedures described in this document
- only to provide true and accurate information to IUCC CA and/or its delegated Registration Authorities and only such information as he/she is entitled to submit for the purposes of this document.
- use the certificate exclusively for authorized and legal purposes, consistent with this document
- by using the authentication procedures described in this document subscribers accept the restrictions to liability described in section 2.2.
- by using the authentication procedures described in this document subscribers accept the statements relating to confidentiality of information in section 2.8.

- generate a key pair using a trustworthy method
- take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate
- notify IUCC CA and/or its delegated Registration Authorities immediately in case a private key is lost or compromised

### 2.1.4 Relying party obligations

In using a certificate issued by the IUCC CA relying parties agree to:

- accept conditions and adhere to the procedures described in this document
- use the certificate exclusively for authorized and legal purposes, consistent with this document
- verify the certificate revocation information before validating a certificate

### 2.1.5 Repository obligations

IUCC CA maintains an online accessible repository of certificate revocation information as well as certificates and CRLs. The repository is operated at a best-effort basis, where the intended availability is continuous.

## 2.2 Liability

### 2.2.1 CA liability

IUCC CA shall control the identity of the subjects requesting a certificate in accordance with the procedures described in this document. Although it aims to achieve a reasonable level of security, IUCC CA provides its certification services on a best effort basis only and provides no warranties, express or implied, including in respect of security and confidentiality, and of fitness for a particular purpose. IUCC accepts no liability for or in connection with the certification services and the parties using or relying on them shall hold IUCC free and harmless from liability resulting from such use or reliance.

### 2.2.2 RA liability

Section 2.2.1 applies mutatis mutandis to the liability of the RA. It is the RA’s responsibility to authenticate the identity of subscribers requesting certificates, according to the practices described in this document. It is the RA’s responsibility to request revocation of a certificate if the RA is aware that circumstances for revocation are satisified.

## 2.3 Financial Responsibility

See section 2.2

### 2.3.1 Indemnification by relying parties

No stipulation.

### 2.3.2 Fiduciary relationships

No stipulation.

### 2.3.3 Administrative processes

No stipulation.

## 2.4 Interpretation and Enforcement

### 2.4.1 Governing law

This document is subject to all applicable Israeli laws.

### 2.4.2 Severability, survival, merger, notice

IUCC shall be entitled to terminate the certification services at any time. IUCC CA will make all reasonable efforts to notify all its subscribers, all cross-certifying CAs, and any relying parties known to IUCC CA to be currently and actively relying on certificates issued by IUCC CA on such termination. All certificates issued by IUCC CA that reference this document will be revoked no later than the time of termination.

### 2.4.3 Dispute resolution procedures

In case of a dispute based on the contents of this document, the Director General of IUCC shall be responsible to resolve all disputes related to the interpretation and enforcement of conditions and rules described in this document.

## 2.5 Fees

No fees are charged for any service provided by IUCC CA.

### 2.5.1 Certificate issuance or renewal fees

See section 2.5.

### 2.5.2 Certificate access fees

See section 2.5.

### 2.5.3 Revocation or status information access fees

See section 2.5.

### 2.5.4 Fees for other services such as policy information

See section 2.5.

### 2.5.5 Refund policy

See section 2.5.

## 2.6 Publication and Repository

### 2.6.1 Publication of CA information

IUCC CA operates a secure online repository that contains:

- IUCC CA's certificate for its signing key
- a Certificate Revocation List (CRL) signed by IUCC CA
- all past and current versions of this document
- a user guide explaining how end entities should request a certificate

### 2.6.2 Frequency of publication

Certificates are published as soon as issued. The frequency of CRL publication is specified in subsection 4.4.9. New versions of CP/CPSs are published as soon as they have been approved.

### 2.6.3 Access controls

IUCC CA does not impose any access control on its CP/CPSs, CRLs and guides.

### 2.6.4 Repositories

A website is maintained by IUCC CA. It contains all the information published by IUCC CA specified in section 2.6.1. The website can be reached at the following address: http://certificate.iucc.ac.il/ca.

## 2.7 Compliance Audit

No external audit will be required, only a yearly self-assessment by IUCC CA that its operation is according to this document.

### 2.7.1 Frequency of entity compliance audit

No stipulation.

### 2.7.2 Identity/qualifications of auditor

No stipulation.

### 2.7.3 Auditor's relationship to audited party

No stipulation.

### 2.7.4 Topics covered by audit

No stipulation.

### 2.7.5 Actions taken as a result of deficiency

No stipulation.

### 2.7.6 Communication of results

No stipulation.

## 2.8 Confidentiality

IUCC CA collects each subscriber’s full name and e-mail address. The full name is included in the issued certificate. No other information is collected from subscribers.

### 2.8.1 Types of information to be kept confidential

Under no circumstances does IUCC CA have access to the private keys of any subscriber to whom it issues a certificate.

### 2.8.2 Types of information not considered confidential

Data contained in CRLs and the subscriber’s certificate shall not be considered confidential and will be published in a publicly accessible location.

### 2.8.3 Disclosure of certificate revocation/suspension information

No information about the reason for a revocation is published.

### 2.8.4 Release to law enforcement officials

IUCC CA will not disclose certificate or any certificate related information to any third party, aside from information publically available, except when so required by a legal authority of competent jurisdiction.

### 2.8.5 Release as part of civil discovery

See section 2.8.4

### 2.8.6 Disclosure upon owner's request

See section 2.8.1

### 2.8.7 Other information release circumstances

See section 2.8.2.

## 2.9 Intellectual Property Rights

The structure of this CP is according to RFC2527 [2] with content based on the Global Grid Forum Certificate Policy Model [4], version 7 (October 2002). Parts of this document are inspired by CERN CA Certificate Policy and Certification Practice Statement [5], v1.1 (April 2003), the DutchGrid and NIKHEF Medium-security X.509 Certification Authority Certification Policy and Practice Statement [6], v2.1 (November 2001), and the American Bar Association PKI Assessment Guidelines [7] (June 2001) v0.30.

IUCC asserts no copyrights on information published by IUCC CA. Others may use this text without prior approval; acknowledgements are welcomed but not required. Unmodified copies may be published without permission.

# 3. IDENTIFICATION AND AUTHENTICATION

## 3.1 Initial Registration

### 3.1.1 Types of names

Each entity has a clear and unique Distinguished Name in the certificate subject field, structured according to X.501.

Any name under this CP/CPS will start with "*O=IUCC*". Thereafter, the subscribers class, defined as either "users", "hosts" or "servers", shall be attached in the form "*O=class*". The "users" class shall contain only certificates for subscribers that are natural persons.

The "hosts" class shall contain only certificates for subscribing entities that are automated systems, applications or services. The private key for "hosts" certificates may be stored in an unencrypted form. The "servers" class shall contain only certificates for subscribers that are automated systems, applications or services. The private key for such entities must be stored in proper encrypted form only.

The subject name must contain the affiliation of the subscriber to his organisation. This organisation must be one of the organisational end-entities detailed in section 1.3.2. If an organisation consists of multiple administrative divisions, the division name must be included in the subject name as an organizationalUnit. Changes in division name that do not change the organisational layout of an organisation, do not constitute reason to invalidate the current unit name.

The subject name must contain the full name of the subscriber.  In case more than one first name is associated with the subscriber, no more than one of these need be specified in the subject name; which first name is included is left to the subscriber. Additional attributes may be post pended to the full name of the subscriber. Such attributes will be clearly separated from this full name.

In case the subscriber is an internetwork entity, the fully-qualified domain name (FQDN) must be used in the subject. In case no such FQDN is assigned, the entity is not eligible for certification under this policy. An identifier representing a network service may precede the FQDN. The domain name part of the FQDN will be used as an organizationalUnitName. Hosts contained within the same logical network entity may be aggregated into the same organisational unit, even when the domain name part is different.

### 3.1.2 Need for names to be meaningful

For a user certificate, the CN must be the full name of the subscriber. For a host certificate, the CN must be the fully qualified domain name registered in the IUCC network. In this case it can be an alias. For a service certificate, the CN must be related to the type of service the certificate is identifying.

### 3.1.3 Rules for interpreting various name forms

See section 3.1.1.

### 3.1.4 Uniqueness of names

The name must be unique for each certificate issued by IUCC CA. If the name presented by the subscriber is not unique, additional numbers or letters are appended to the name to ensure uniqueness. *Certificates must apply to unique individuals or resources. Users must not share certificates.*

### 3.1.5 Name claim dispute resolution procedure

The person named in section 1.4.2

### 3.1.6 Recognition, authentication and role of trademarks

No stipulation.

### 3.1.7 Method to prove possession of private key

No stipulation.

### 3.1.8 Authentication of organization identity

If the name of an organization is requested to be part of a subject name, IUCC CA may take steps to ascertain that the organization consents to such use.

### 3.1.9 Authentication of individual identity

A requesting party requesting a certificate must meet in person with the RA and show their Israeli identity card or any valid national passport. If the Israeli identity card or national passport is valid and the photo image corresponds to the bearer, the RA shall consider that the user is correctly identified. It may also consider that the requesting party is correctly identified if the requesting party is well known to the RA personally. If authentication is not completed within nine days of receipt of the certificate request by the RA the request will be deemed to have expired and any authentication of identity must then be preceded by a new certificate request.

## 3.2 Routine Rekey

Rekeying of certificates will follow the same procedure as an initial registration. A request for rekeying of a certificate must be submitted prior to certificate expiration. Otherwise, a new key will be issued.

## 3.3 Rekey After Revocation

A public key whose certificate has been revoked shall not be re-certified.

## 3.4 Revocation Request

Unless IUCC CA can independently verify that a key compromise has occurred, a revocation request must be authenticated before being accepted. Authentication can be by the procedure described in section 3.1.9, or via a digitally signed message with a non-expired and non-revoked certificate issued under this CP/CPS, regardless of the document version.

# 4. OPERATIONAL REQUIREMENTS

## 4.1 Certificate Application

The IUCC CA will reject certificate applications that are deemed to be not legitimate.

Applicants must generate their own key pair via the methods as available at the time by the IUCC. The IUCC CA will never generate a key pair for an applicant. The minimum key length for all application is at least 1024 bits. The maximum validity period for a certificate is related to the key length, such that keys with a length of 1024 bits are signed for a period of one year, and keys with a length of 2048 bits are signed for a period of three years.

Certificate application is by submitting a PEM-formatted certificate request by electronic mail to ca@mail.iucc.ac.il. In case the requester is a person requesting his or her own certificate, then the procedures detailed in section 3.1 apply. In case the entity is a machine or service, the certificate request must be signed by a valid certificate pertinent to the authorized administrator for the machine or service or via the procedures deatiled in section 3.1.

## 4.2 Certificate Issuance

The first step in the issuance process is the approval of the request by an RA. The following requirements must be fulfilled:

- RA must authenticate the applicant according to the procedures described in section 3.1.9
- RA must check if the request sender can apply for a certificate according to section 1.3.3
- RA is recognized by IUCC CA as a RA for the applicant, as specified in section 1.3.2.

If all the above requirements are fulfilled, then RA *approves* the request and passes on the request to the CA for issusace of a certificate. The applicant for the certificate will be notified at the email address on record in regards to the issuance of the certificate. If the email fails and is not delivered after a period of 5 days, the certificate is revoked without further notice.

A request for certification is normally handled within one week, however during national holidays the response time may be three weeks.

## 4.3 Certificate Acceptance

No stipulation.

# 4.4 Certificate Suspension and Revocation

## 4.4.1 Circumstances for revocation

A certificate is revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

- the subscriber's private key is lost or suspected to be compromised
- the information in the subscriber's certificate is suspected to be inaccurate
- the subscriber no longer needs the certificate to access Relying Parties' resources
- the subscriber has violated his/her obligations’

In addition, the CA will revoke all certificates in the event that its key has been compromised or in the event that the CA has been terminated.

## 4.4.2 Who can request revocation

A certificate revocation can be requested by the holder of the certificate concerned or by any other entity presenting evidence of circumstances as described in section 4.4.1.

## 4.4.3 Procedure for revocation request

The entity requesting revocation of a certificate must authenticate themselves in one of the following ways:

- by sending a message, signed by a valid IUCC CA certificate, to IUCC CA or RAs.
- by contacting IUCC CA or RAs, who will check the identity of the requesting entity using the procedure for the authentication of identity as described in section 3.1.9.

In both cases above, the requesting entity must specify the reason for the revocation request and provide evidence of circumstances as described in section 4.4.1.

## 4.4.4 Revocation request grace period

There will be no grace period associated with certificate revocation. IUCC CA handles revocation requests with priority and a certificate will be revoked as soon as possible after circumstances for revocation, as described in section 4.4.1, are established.

## 4.4.5 Circumstances for suspension

There is no provision for certificate suspension.

## 4.4.6 Who can request suspension

No stipulation.

### 4.4.7 Procedure for suspension request

No stipulation.

### 4.4.8 Limits on suspension period

No stipulation.

### 4.4.9 CRL issuance frequency (if applicable)

CRLs are issued after every certificate revocation and at least every 30 days.

### 4.4.10 CRL checking requirements

Before use of a certificate, a relying party must validate it against the most recently issued CRL.

### 4.4.11 On-line revocation/status checking availability

IUCC CA does not offer on-line status checking.

### 4.4.12 On-line revocation checking requirements

No stipulation.

### 4.4.13 Other forms of revocation advertisements available

No stipulation.

### 4.4.14 Checking requirements for other forms of revocation advertisements

No stipulation.

### 4.4.15 Special requirements re key compromise

No stipulation.

## 4.5 Security Audit Procedures

### 4.5.1 Types of event audited

No events are audited.

### 4.5.2 Frequency of processing log

See section 4.5.1.

### 4.5.3 Retention period for audit log

See section 4.5.1..

### 4.5.4 Protection of audit log

See section 4.5.1.

### 4.5.5 Audit log backup procedures

See section 4.5.1.

### 4.5.6 Audit collection system (internal vs external)

See section 4.5.1.

### 4.5.7 Notification to event-causing subject

See section 4.5.1.

### 4.5.8 Vulnerability assessments

No stipulation.

## 4.6 Records Archival

### 4.6.1 Types of event recorded

The following events are recorded and archived:

- certificate requests
- approved certificate requests
- issued certificates
- all electronic mail sent to and sent by the IUCC CA

### 4.6.2 Retention period for archive

The minimum retention period is three years.

### 4.6.3 Protection of archive

Archives are stored in a room with restricted access.

### 4.6.4 Archive backup procedures

Archives are not backed up.

### 4.6.5 Requirements for time-stamping of records

No stipulation.

### 4.6.6 Archive collection system (internal or external)

The record archival is performed on the offline CA. There is an archive directory which contains all events recorded.

### 4.6.7 Procedures to obtain and verify archive information

No stipulation.

## 4.7 Key Changeover

CA's private signing key is changed periodically. To avoid interruption of validity of all subordinate keys the new CA key is generated one year before the old one looses validity and, from that point onwards, new certificates are signed with the new key. The new public key is posted in the repository.

## 4.8 Compromise and Disaster Recovery

### 4.8.1 Computing resources, software, and/or data are corrupted

The private keys of the IUCC CA are only available in encrypted format on media in a secure location.  The machine used to activate the private key is not accessible via any network.  If the CA equipment is damaged or rendered inoperative, but the CA private key is not destroyed or compromised, CA operation will be reestablished as quickly as possible. If the private key is destroyed the case will be treated as in section 4.8.3.

### 4.8.2 Entity public key is revoked

See section 4.8.3.

### 4.8.3 Entity key is compromised

If the private key of IUCC CA is, or is suspected to be, compromised, IUCC CA shall:

- make all reasonable effort to inform subscribers and cross-certifying CAs
- terminate distribution services for certificates and CRLs issued using the compromised key.
- generate a new CA key pair and certificate and make the latter available in the public repository.
- request revokation of the compromised certificate.
- immediately revoke all certificates issued using the compromised key, and notify subscribers of such revocation.

In the case of such a CA key compromise, new certificates will be issued only in accordance with the initial entity identification procedures defined in section 3.1.

If an RA's private key is compromised, or is suspected of being compromised, the RA informs IUCC CA and requests a revocation of the RA's certificate.

If an entity private key is compromised or suspected to be compromised, the entity or its administrator must request a revocation of the certificate and make all reasonable efforts to inform any known relying parties.

### 4.8.4 Secure facility after a natural or other type of disaster

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the IUCC CA will take whatever action it deems appropriate.

## 4.9 CA Termination

Before IUCC CA terminates its services, IUCC CA shall:

- make all reasonable efforts to inform subscribers and cross-certifying CAs
- make knowledge of its termination widely available
- cease issuing certificates and CRLs
- revoke all certificates issued by the IUCC CA
- destroy all copies of private keys of the IUCC CA

# 5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

## 5.1 Physical Controls

### 5.1.1 Site location and construction

IUCC CA operates in the Tel Aviv University Computer Center, Ramat Aviv. The access to the computer room is controlled. The machine is only accessible in person by properly authorized personnel. It is also located in a separate locked cabinet.

### 5.1.2 Physical access

Physical access to the hardware is restricted to personnel authorized to enter the computer room.

### 5.1.3 Power and air conditioning

No stipulation.

### 5.1.4 Water exposures

No stipulation.

### 5.1.5 Fire prevention and protection

No stipulation.

### 5.1.6 Media storage

No stipulation.

### 5.1.7 Waste disposal

No stipulation.

### 5.1.8 Off-site backup

No stipulation.

## 5.2 Procedural Controls

### 5.2.1 Trusted roles

No stipulation.

### 5.2.2 Number of persons required per task

No stipulation.

### 5.2.3 Identification and authentication for each role

No stipulation.

## 5.3 Personnel Controls

### 5.3.1 Background, qualifications, experience, and clearance requirements

No stipulation.

### 5.3.2 Background check procedures

No stipulation.

### 5.3.3 Training requirements

No stipulation.

### 5.3.4 Retraining frequency and requirements

No stipulation.

### 5.3.5 Job rotation frequency and sequence

No stipulation.

### 5.3.6 Sanctions for unauthorized actions

No stipulation.

### 5.3.7 Contracting personnel requirements

No stipulation.

### 5.3.8 Documentation supplied to personnel

No stipulation.

# 6. TECHNICAL SECURITY CONTROLS

## 6.1 Key Pair Generation and Installation

### 6.1.1 Key pair generation

Key pairs for the IUCC CA are generated exclusively by IUCC CA staff members on a dedicated, disconnected system, using a recent, trustworthy version of the OpenSSL software package.

### 6.1.2 Private key delivery to entity

Each applicant must generate their own key pair.

### 6.1.3 Public key delivery to certificate issuer

Applicant’s public keys are delivered to the RA in an email containing the certificate request. The public key arrives at IUCC CA in an email signed by the RA.

### 6.1.4 CA public key delivery to users

The certificate will be delivered in PEM format according to the procedures detailed in section 4.2.

### 6.1.5 Key sizes

For a user certificate the key size is 1024 bits. For host certificate the key size is 2048 bits. IUCC CA key length is 2048 bits.

### 6.1.6 Public key parameters generation

No stipulation.

### 6.1.7 Parameter quality checking

No stipulation.

### 6.1.8 Hardware/software key generation

No stipulation.

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

For certificates issued by IUCC CA under this policy, the *keyUsage* extension is defined in subsection 7.1.2.

## 6.2 Private Key Protection

### 6.2.1 Standards for cryptographic module

IUCC CA does not use any cryptographic module.

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

No stipulation.

### 6.2.3 Private key escrow

IUCC CA keys are not given in escrow. IUCC CA is not available for accepting escrow copies of keys of other parties.

### 6.2.4 Private key backup

An encrypted backup of the IUCC CA private key is kept on a removable magnetic media, in a secured controlled environment.

### 6.2.5 Private key archival

No stipulation.

### 6.2.6 Private key entry into cryptographic module

See section 6.2.1.

### 6.2.7 Method of activating private key

The activation of the CA private key is performed by providing the passphrase.

### 6.2.8 Method of deactivating private key

No stipulation.

### 6.2.9 Method of destroying private key

After termination of the CA and after the archival period for archives has expired, all media that contain the private key of the CA (including those specified in 6.2.4) will be securely and permanently destroyed, according to then best current practice.

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Public key archival

The public key is archived as part of the certificate archival.

### 6.3.2 Usage periods for the public and private keys

IUCC CA root certificates have a validity of  five years. For other entity certificates, the maximum validity period for a certificate is three years.

## 6.4 Activation Data

### 6.4.1 Activation data generation and installation

All passphrases used by the IUCC CA have a length of  at least 15 characters, consist of both letters, numbers and signs and does not contain consecutive or repetitive keystrokes. The length of the passphrase is checked by *openssl* during the private key generation process.

### 6.4.2 Activation data protection

All current staff members of the IUCC CA know all pass phrases.  Change of staff will imply a change in the passphrases.

### 6.4.3 Other aspects of activation data

No stipulation.

## 6.5 Computer Security Controls

### 6.5.1 Specific computer security technical requirements

The CA machine used for signing is maintained at an appropriate level of security by applying relevant security patches.  The machine is not connected to any network and unauthorized physical access is prohibited.

The machine used by the CA to hold online repositories is maintained at a high level of security by applying all recommended and applicable security patches.  The machine(s) are protected by a suitable firewall.

### 6.5.2 Computer security rating

No stipulation.

## 6.6 Life Cycle Technical Controls

### 6.6.1 System development controls

No stipulation.

### 6.6.2 Security management controls

All IUCC systems are scanned once a quarter via commercial products to determine if any security holes exist.

### 6.6.3 Life cycle security ratings

No stipulation.

## 6.7 Network Security Controls

Certificates are issued on a machine not connected to any kind of network.

## 6.8 Cryptographic Module Engineering Controls

No stipulation.

# 7. CERTIFICATE AND CRL PROFILES

## 7.1 Certificate Profile

### 7.1.1 Version number(s)

X.509 v3 (0x2)

### 7.1.2 Certificate extensions

The following extensions are set in entity certificates:

- **subjectAltName** email address, when requested by subscriber
- **nsComment** a descriptive string with reference to this CP/CPS
- **nsCAPolicyURL** a link to this CP/CPS
- **nsCertType** server, client, email

### 7.1.3 Algorithm object identifiers

No stipulation.

### 7.1.4 Name forms

See section 3.1.1.

### 7.1.5 Name constraints

See section 3.1.2.

### 7.1.6 Certificate policy Object Identifier

See section  1.2.

### 7.1.7 Usage of Policy Constraints extension

No stipulation.

### 7.1.8 Policy qualifiers syntax and semantics

No stipulation.

### 7.1.9 Processing semantics for the critical certificate policy extension

No stipulation.

## 7.2 CRL Profile

### 7.2.1 Version number(s)

X.509 v1 (0x0)

### 7.2.2 CRL and CRL entry extensions

No stipulation.

# 8. SPECIFICATION ADMINISTRATION

## 8.1 Specification change procedures

Users will not be advised in advance of changes to IUCC CA's CP and CPSs. Changes are made available as defined in section 2.6.

## 8.2 Publication and notification policies

This document and any older versions are available from the on-line repository given in section 2.1.5.

## 8.3 CPS approval procedures

No stipulation.

# 9. VERSIONS

## 9.1 Change log

version 1.1 drafted August 2003

version 1.2 drafted September 2003:

a) changed all references from iag.proj.ac.il to certificate.iucc.ac.il
b) changed 1.3.3 to reference institutes listed in 1.3.2
c) completely revised section 3.1.1
d) changed 3.1.9 to clarify that any national passport is valid for authentication purposes
e) changed 4.2 to reflect the fact that only the CA issues certificates and not the RA
f) completely revised section 6.2.9
g) changed 6.3.2 to eliminate contradiction with 4.1 – now maximum validity of a certificate is 3 years
h) corrected spelling mistake in 6.5.1

version 1.3 drafted November 30, 2003

a) fixed 1.2 to be version 1.3

version 1.4 drafted December 5, 2003

a) changed 4.4.9 from 35 days to 30 days
b) changed 6.4.1 from 8 characters to 15 characters
c) changed 1.3.2 from people to people, servers or services
d) added in 2.1.2 that the RA log all transactions
e) changed 6.3.2 from 2 years to 5 years

# Appendix A.

## Registration Authority Agreement

This forms part of the operating procedures of the IUCC Certification Authority (CA).

1. In acting as a Registration Authority (RA) for IUCC CA I have read and understood and accept the responsibilities and tasks assigned to an RA laid out in IUCC CA Certification Policy and Practice Statement (CP/CPS) document available on the IUCC CA web site - http://certificate.iucc.ac.il/ca

2. I understand that IUCC CA will notify me by email of changes to CP/CPS and I will immediately notify IUCC CA if I am no longer willing to act as an RA under any new CP/CPS.

3. I understand that failure to fulfil my responsibilities and tasks under this agreement may result in the termination of my appointment as an RA.

4. In the event of resignation, I will inform the IUCC CA at least 90 days prior to my resignation.

Signed by ____________________ on ________________ email:______________

Signature:__________________________________________________

# Bibliography

1. The Israel InterUniversity Computation Center – http://www.iucc.ac.il
2. S. Chokani and W. Ford, “Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework”, RFC 2527, March 1999 - http://www.ietf.org/rfc/rfc2527.txt
3. IUCC CA Security Group - http://certificate.iucc.ac.il/ca - Email: *iucc-globus-ca@mail.iucc.ac.il*
4. Global Grid Forum Certificate Policy Model - http://caops.es.net
5. CERN Certification Authority Certificate Policy and Certification Practice Statement - http://globus.home.cern.ch/globus/ca/
6. DutchGrid and NIKHEF Medium-security X.509 Certification Authority Certification Policy and Practice Statement - http://certificate.nikhef.nl/medium/policy
7. American Bar Association PKI Assessment Guidelines - http://www.abanet.org/scitech/ec/isc/pag/pag.html
8. S. Bradner, “Key words for use in RFCs to Indicate Requirement Levels”, RFC 2119, March 1997 - http://www.ietf.org/rfc/rfc2119.txt