Malaysian Identity Federation and Access Management Certification Authority Certificate Policy and Certification Practice Statement

Version 2.2

Document OID: 1.3.6.1.4.1.36355.2.1.2.2

February 2012

Contents

Chapter 1

Introduction

1.1 Overview

This document is based on the structure suggested by the "RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" [7]. Sections that are not included have a default value of "No stipulation". This document describes the set of rules and procedures established by the Malaysian Identity Federation and Access Management (MYIFAM).

1.2 Document name and identification

This document is named Malaysian Identity Federation and Access Management Certificate Policy And Certificate Practice Statement. The following ASN.1 Object Identifier (OID) has been assigned to this document: 1.3.6.1.4.1.36355.2.1.2.2. This OID is constructed as shown in the table below:

IANA	1.3.5.4.1
BIRUNI Grid Computing Centre	.36355
MYIFAM	.2
CP/CPS	.1
Major Version	.2
Minor Version	.2

1.3 PKI participants

1.3.1 Certification authorities

MYIFAM CA is managed by the Infocomm Development Centre - Universiti Putra Malaysia

1.3.2 Registration authorities

The MYIFAM CA delegates the authentication of individual identity to Registration Authorities. RAs must sign an agreement with the MYIFAM CA, stating their adherence to the procedures described in this document. RAs are not allowed to issue certificates under this CP/CPS. The list of RAs is available from the MYIFAM CA website. Every organization has only one Registration Authority who is in charge of an organization. Only permanent staff members are eligible to become a RA for their organization.

The following is the MYIFAM CA RA registration procedure:

- RA candidate must accept the CP/CPS and agree to all RA responsibilities.
- RA candidate must be an employee of the institution or organization and provide work ID or proof of work.
- Complete the RA application form and fax it to MYIFAM CA.
- Send a verification e-mail to MYIFAM CA.
- MYIFAM CA will then arrange a face to face meeting with RA candidate.
- After completing the request, MYIFAM CA will publish the RA contact information on MYIFAM CA website and reserve the right to issue the name space for the institution.

1.3.3 Subscribers

MYIFAM CA issues certificates for users and hosts/services under the National Distributed Computing Initiative (NDCI) which include all institutions and organizations that are recognized by respective ministries to be involved/associated in/with Distributed-, Grid-, Cloud- and Emerging Computing Applications/Projects.

1.3.4 Relying parties

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued by MYIFAM CA may be used by subscribers for purposes of :

- e-mail signing and encryption (S/MIME).
- authentication and encryption of communication (SSL/TLS).
- object-signing

1.4.2 Prohibited certificate uses

The certificates issued by MYIFAM CA must not be used for financial transaction.

1.5 Policy administration

1.5.1 Organization administering the document

Infocomm Development Centre
Putra Infoport, Jalan Kajang/Puchong
Universiti Putra Malaysia, Serdang 43400
Selangor D.E, Malaysia

Tel: +60-3-89471219
Fax: +60-3-89483514
http://myifam.upm.my
myifam@biruni.upm.my

1.5.2 Contact persons

Suhaimi Napis, PhD
Putra Infoport, Jalan Kajang/Puchong
Universiti Putra Malaysia, Serdang 43400
Selangor D.E, Malaysia
Phone: +60-3-89471010
Mobile: +60-193539955
Fax: +60-3-89483514
suhaimi@putra.upm.edu.my

A ticket system containing MYIFAM CA Managers has been setup to ensure quick response:
myifam@biruni.upm.my

1.5.3 Person determining CPS suitability for the policy

MYIFAM CA Managers (see 1.5.2) determine CPS suitability for the policy.

1.5.4 CPS approval procedures

The document shall be submitted to APGridPMA for acceptance and accreditation.

1.5.5 Definitions and acronyms

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

- **UPM** - The Universiti Putra Malaysia, a University established under the Universitities and University Colleges Act 1971.
- **MYIFAM** - The Malaysian Identity Federation and Access Management.

- **iDEC** - The Infocomm Development Centre.
- **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. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.
- **Certification Practice Statement (CPS)** - A statement of the practices, which a certification authority employs in issuing certificates.
- **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 Revocation List (CRL)** - A time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.
- **MYIFAM CA** - Refers to the CA service provided by MYIFAM.
- **FQDN** - Fully Qualified Domain Name.
- **Policy qualifier** - Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.
- **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).
- **Relying party** - A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Chapter 2

General Provisions

2.1 Obligations

2.1.1 MYIFAM CA Obligations

The MYIFAM CA is responsible for the following aspects of issuance and management of certificates:

- Issue and publish certificates based on validated requests.
- Accept certification requests validated by the RA.
- Deliver the certificate to end entity.
- Accept revocation requests from RA's or end entities.
- Ensuring that all aspects of the CA services, CA operations and CA infrastructure, related to certificates issued under this policy, are performed in accordance with the requirements, representations and warranties of this document.

2.1.2 MYIFAM CA RA Obligations

The MYIFAM CA RA is responsible for the following aspects:

- Authenticate entities requesting a certificate according to the procedures described in this document.
- Determine if the person requesting the certificate has the right to have a MYIFAM CA certificate.
- Send validated certificate requests to MYIFAM CA.
- Create and send validated revocation requests to the MYIFAM CA.
- Follow the policies and procedures described in this document.
- The RA communicates with the MYIFAM CA via telephonic conversation which is followed by the signed e-mail.

2.1.3 Subscriber Obligations

In all cases, the MYIFAM CA shall require the subscriber to:

- Read and accept the policies and procedures published in this document.
- Generate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key.
- Use a strong passphrase with a minimum length of 12 characters to protect the private key of personal certificates.
- Use the certificate exclusively for authorized and legal purposes, consistent with this policy.
- Notify the MYIFAM CA when the certificate is no longer required.
- Notify the MYIFAM CA when the information in the certificate becomes wrong or inaccurate.
- Instruct the MYIFAM CA to revoke the certificate promptly upon an actual or suspected loss, disclosure, or other compromise of the subscriber's private key.
- Accepts the statements relating to confidentiality of information in section 10.3.1.

Chapter 3

Publication and repository responsibilities

3.1 Repositories

A MYIFAM CA website is published at the following address: http://myifam.upm.my, it contains all information and tools to use the MYIFAM CA services.

3.1.1 Publication of certification information

MYIFAM CA website publishes:

- MYIFAM CA certificate in PEM formatted.
- All Certificates issued by MYIFAM CA in PEM formatted.
- A Certificate Revocation List (CRL) signed by MYIFAM CA certificate in PEM formatted and compliant with RFC5280 [6].
- All versions of the CP/CPS under which valid Certificates are issued.
- List of appointed RAs.
- Other information relevant to the MYIFAM CA.

3.1.2 Time or frequency of publication

- Certificates will be published as soon as issued.
- CRLs are issued after every certificate revocation or at least every twenty-three (23) days (maximum lifetime thirty (30) days).
- New version of CP/CPS is published as soon as they have been approved.

3.1.3 Access controls on repositories

The online repository is available 24 hours a day, 7 days a week, subject to reasonable scheduled maintenance. MYIFAM CA doesn't impose any access control on its CP/CPS, its Certificate and issued certificates and CRLs. The CRL list is signed by MYIFAM CA private key.

Chapter 4

Identification and authentication

4.1 Naming

4.1.1 Types of names

Name components vary depending on the type of certificate. Names will be consistent with the name requirements specified in "RFC 5280 -Internet X.509 Public Key Infrastructure Certificate and CRL profile" [6].

- In case of personal certificate the subject name must include the person's full name.

  DC=Domain Component, DC=Domain Component, DC=Domain Component, C=Country, O=Organization, OU=Unit, CN=First Name Last Name Unique ID

- In case of host certificate the subject name must include the FQDN of the host.

  DC=Domain Component, DC=Domain Component, DC=Domain Component, C=Country, O=Organization, OU=Unit, CN=DNS server name(FQDN)

4.1.2 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 functional fully qualified domain name.

4.1.3 Anonymity or pseudonymity of subscribers

Subscribers must not be anonymous or pseudonymous. The MYIFAM CA RA validates identity of subscribers.

4.1.4 Rules for interpreting various name forms

Many languages have special characters that are not supported by the ASCII character set used to define the subject in the certificate. To work around this problem local substitution rules can be used:

- In general national characters are represent by their ASCII equivalent E.g. è, é, à, ç are represented by e, e, a, c.
- The German "umlaut" characters may received special treatment ä, ö, ü represented by either ae, oe, ue or a, o , u.

4.1.5 Uniqueness of names

The Distinguished Name must be unique for each subject name certified by MYIFAM CA. To ensure the uniqueness of names, a special ID (i.e. MYIFAM CA ID) will be added after the person's first and last name. This ID is an integer number.

4.1.6 Recognition, authentication, and role of trademarks

No stipulation.

4.2 Initial identity validation

4.2.1 Method to prove possession of private key

The public and private keys are generated on the user station when he/her fills the certificate request form with Netscape, Mozilla or Internet Explorer browser.

4.2.2 Authentication of organization identity

If the name of an organization is requested to be part of subject name, MYIFAM CA may take steps to ascertain that the organization consent to such use. The information of authenticated organization is published on http://myifam.upm.my/contact.html.

4.2.3 Authentication of individual identity

Procedures differ if the subject is a user or host :

- **User certificate:** A user requesting a user certificate must meet in person with the RA and show their work ID. If the ID card is valid and the photo image corresponds to the bearer, the RA shall consider that the user is correctly identified. The RA will sign the user's application form. Then the user will fax the application form to the CA. Once the user's identification is verified, MYIFAM will authenticate the subscriber and issue a certificate without namespace clash with other CAs in APGridPMA [1], EUGridPMA [5] and American Grid PMA (TAGPMA) [8].
- **Host certificate:** A user requesting host certificate must:
  - Have valid MYIFAM CA user certificate.
  - Register the FQDN with MYIFAM CA and must prove that he/she is the owner of the associated FQDN or the responsible administrator of the machine to use the FQDN identifiers asserted in the certificate.

4.2.4 Non-verified subscriber information

None.

4.2.5 Validation of authority

No stipulation.

4.2.6 Criteria for interoperation

No stipulation.

4.3 Identification and authentication for re-key requests

Rekeying of certificates can be requested by an online procedure, which checks the validity of certificates.Re-key after expiration is not possible, user has to request a new certificate.

4.3.1 Identification and authentication for re-key after revocation

Rekey after revocation follows the same rules as an initial registration.

4.3.2 Identification and authentication for revocation request

Certificate revocation request must be sent in the following ways:

- Send e-mail to myifam@biruni.upm.my signed with a valid and trusted certificate.
- Contact personally the CA/RA staff in order to verify his/her identity and the validity of the request.

Communication All communications between the MYIFAM CA and the RA regarding certificate issuance or changes in the status of a certificate must be by secure and auditable methods. In such, both the MYIFAM CA and the RA must record those information at least in a spreadsheet format shall be used for auditing purposes. The MYIFAM CA RA may pass this information to the MYIFAM CA staff personally in encrypted e-mail.

Chapter 5

Certificate life-cycle operational requirements

5.1 Certificate Application

5.1.1 Who can submit a certificate application

User can apply for a certificate if he is eligible for a certificate as defined in section 1.3.3.

5.1.2 Enrollment process and responsibilities

Procedures are different if the subject is a person or a server. For every certificate applications, the subject has to generate his/her own key pair. Minimum key length is 1024 bits.

- **User** - Certificate requests are submitted by an online procedure, using a Netscape, Mozilla or Internet Explorer browser.
- **Host** - Certificate requests are submitted by an online procedure, using a Netscape, Mozilla or Internet Explorer browser with a valid personal MYIFAM user certificate.

5.2 Certificate application processing

5.2.1 Performing identification and authentication functions

No stipulation.

5.2.2 Approval or rejection of certificate applications

MYIFAM issues the certificate if, and only if, the authentication of the subject is successful. If the subject is a person, a message is sent to his/her e-mail address with the instructions on how to download it from the MYIFAM web server. If the subject is a host or a service entity, the certificate itself is sent to the address specified in the request email. If the authentication is unsuccessful, the certificate is not issued and e-mail with the reason is sent to the subject.

5.2.3 Time to process certificate applications

Certificate issuing and processing is done within 3 working days: identity verification has been made previously by the MYIFAM CA RA, and is mandatory to proceed with the request for a certificate.

5.3 Certificate issuance

5.3.1 CA actions during certificate issuance

No stipulation.

5.3.2 Notification to subscriber by the CA of issuance of certificate

Certificate request is done using MYIFAM CA secure website, in a wizard form and will notify the user when the certicate is ready via email. The email contains a link to download the issued certificate.

5.4 Certificate acceptance

5.4.1 Conduct constituting certificate acceptance

No stipulation.

5.4.2 Publication of the certificate by the CA

User and Host Certificates are published to MYIFAM CA website (http://myifam.upm.my).

5.4.3 Notification of certificate issuance by the CA to other entities

During the period of issuance, MYIFAM CA manager send the notification to the entity. Also forward this message to RA.

5.5 Key pair and certificate usage

5.5.1 Subscriber private key and certificate usage

By accepting the certificate the subscriber assures all participants of the MYIFAM CA and all parties relying on the trustworthiness of the information contained in the certificate that:

- A basic understanding exists of the use and purpose of certificates,
- All data and statements given by the subscriber with relation to the information contained in the certificate are truthful and accurate,
- The private key will be maintained in a safe and secure manner,
- No unauthorized person has or will ever have access to the private key,

- The certificate will solely and exclusively be put to such uses as are in accordance with this Certificate Policy,
- Immediate action will be undertaken on the subscriber's part to revoke the certificate if information in the certificate no longer proves to be correct or if the private key is missing, stolen, or is in any other way compromised.

5.5.2 Relying party public key and certificate usage

Every person using a certificate issued within the framework of this CP for verification signature or for purposes of authentication or encryption

- Must verify the validity of the certificate before using it,
- Must use the certificate solely and exclusively for authorized and legal purposes accordance with this CP, and
- Should have a basic understanding of the use and purpose of certificates.

5.6 Certificate renewal

5.6.1 Circumstance for certificate renewal

MYIFAM does not renew subscribers' certificates. Subscribers must follow the re-key procedure as described in section 5.7.

5.6.2 Who may request renewal

Refer to section 5.6.1.

5.6.3 Processing certificate renewal requests

Refer to section 5.6.1.

5.6.4 Notification of new certificate issuance to subscriber

Refer to section 5.6.1.

5.6.5 Conduct constituting acceptance of a renewal certificate

Refer to section 5.6.1.

5.6.6 Publication of the renewal certificate by the CA

Refer to section 5.6.1.

5.6.7 Notification of certificate issuance by the CA to other entities

Refer to section 5.6.1.

5.7 Certificate re-key

5.7.1 Circumstance for certificate re-key

The lifetime of MYIFAM CA certificates must be no longer than 400 days. If users would get the brand-new certificate and private key, they must follow the online procedure to get these from MYIFAM CA manager. Subscribers must regenerate the key pairs in the following circumstance:

- Expiration of the certificates signed by MYIFAM CA.
- Recovation of the certificates by MYIFAM CA.
- If the current private key is suspected to be compromised.

5.7.2 Who may request certification of a new public key

Refer to section 1.3.3.

5.7.3 Processing certificate re-keying requests

- User certificate: Re-key request before expiration of the user certificate can be accomplished by sending an online request with the current user certificate. Subscriber follows the authentication procedure to get a new certificate. Please note that the user certificate must be imported to the browser to access the secure re-key page.
- Host certificate: Requests must be signed with a valid personal MYIFAM CA user certificate.

5.7.4 Notification of new certificate issuance to subscriber

Refer to section 5.3.2

5.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

5.7.6 Publication of the re-keyed certificate by the CA

Refer to section 5.4.2.

5.7.7 Notification of certificate issuance by the CA to other entities

Refer to section 5.4.3.

5.8 Certificate modification

Certificates must not be modified. In case of changes, the old certificate must be revoked, and a new certificate must be requested.

5.8.1 Circumstance for certificate modification

No stipulation.

5.8.2 Who may request certificate modification

No stipulation.

5.8.3 Processing certificate modification requests

No stipulation.

5.8.4 Notification of new certificate issuance to subscriber

No stipulation.

5.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

5.8.6 Publication of the modified certificate by the CA

No stipulation.

5.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

5.9 Certificate revocation and suspension

This section explains the circumstances under which a certificate should be revoked. No provision is made for the suspension (temporary invalidity) of certificates. Once a certificate has been revoked, it may not be renewed or extended.

5.9.1 Circumstances for revocation

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

- The entity's private key is lost or suspected to be compromised
- The information in the entity's certificate is suspected to be inaccurate
- The entity requests for revocation
- The entity violates its obligations
- The entity leaves the organization

- RA can also request revocation with any reasons describe above.
- Name space conflict - If new CA service started up in their their organization, MYIFAM CA would actively revoke their certificate to avoid name space conflict. Also, MYIFAM CA would inform the users/hosts admin to apply certificates from applicable CA organization.

5.9.2 Who can request revocation

The revocation of the certificate can be requested by:

- The certificate subscriber.
- Any other entity presenting proof of knowledge of the private key compromise or of the modification of the subscriber's data.
- The MYIFAM CA RAs.
- The MYIFAM CA.

5.9.3 Procedure for revocation request

If the conditions to acceptance of the request (see section 5.9.2) are met, the certificate will be revoked in one of the following ways:

- Sending an email, signed by a valid and trusted certificate, to myifam@biruni.upm.my, RA will contact subscriber for confirmation.
- In the other cases, authentication is performed with the same procedure used to authenticate the identity of person.

5.9.4 Revocation request grace period

Should circumstances for revocation of a certificate exist (see section 5.9.1), the subscriber is obliged to notify the MYIFAM CA immediately of the same, and to initiate revocation of the certificate.

5.9.5 Time within which CA must process the revocation request

The MYIFAM CA will process a request for revocation of a certificate instantly if the conditions to acceptance of the request (see section 5.9.2) are met.

5.9.6 Revocation checking requirement for relying parties

The provisions of section 5.5.2 apply.

5.9.7 CRL issuance frequency (if applicable)

The provisions of section 3.1.2 apply.

5.9.8 Maximum latency for CRLs (if applicable)

The provisions of section 3.1.2 apply.

5.9.9 On-line revocation/status checking availability

MYIFAM CA provides an on-line procedure where the validity of users and host certificate can be verified, by simply login in the MYIFAM CA WebSite located at http://myifam.upm.my. CRLs are available from the URL given in the associated CPS section 3.1.

5.9.10 On-line revocation checking requirements

No stipulation.

5.9.11 Other forms of revocation advertisements available

Currently no other forms of revocation advertisements are available.

5.9.12 Special requirements re-key compromise

Should a private key become compromised, the certificate so affected shall immediately be revoked. Should the private key of the MYIFAM CA become compromised, all certificates issued by the MYIFAM CA shall be revoked.

5.9.13 Circumstances for suspension

Suspension of certificates is not supported.

5.9.14 Who can request suspension

Not applicable.

5.9.15 Procedure for suspension request

Not applicable.

5.9.16 Limits on suspension period

Not applicable.

5.9.17 Certificate status services

Certificate status services are not supported by the MYIFAM CA.

5.9.18 Operational characteristics

Not applicable.

5.9.19 Service availability

Not applicable.

5.9.20 Optional features

Not applicable.

5.9.21 End of subscription

The term of the contractual relationship is given by the period of validity as indicated in the certificate. The minimum period for the archiving of documents and certificates corresponds to the period of validity of the certificate of the MYIFAM CA with the addition of a further period of 400 days.

5.9.22 Key escrow and recovery

The MYIFAM CA does not support key escrow and recovery.

5.9.23 Key escrow and recovery policy and practices

Not applicable.

5.9.24 Session key encapsulation and recovery policy and practices

Not applicable.

Chapter 6

Physical, Procedural and Personnel Security Controls

6.1 Physical Controls

6.1.1 Site Location and Construction

The MYIFAM CA is located safely at Infocomm Development Centre Alpha building in Serdang, Malaysia.

6.1.2 Physical Access

Physical access to the MYIFAM CA is restricted to authorized personnel. The access key is controlled by one of the MYIFAM CA staff who is assigned to secure the facilities safety. All access to the facilities needs to be recorded and endorsed by the CA Manager.

6.1.3 Power and Air Conditioning

The CA signing machine and the CA web server are both protected by uninterruptible power supplies. Environment temperature in rooms containing CA related equipment is maintained at appropriate levels by suitable air conditioning systems.

6.1.4 Water Exposures

Due to the location of the MYIFAM CA facilities floods are not expected.

6.1.5 Fire Prevention and Protection

The Infocomm Development Centre Alpha building is equipped with various smoke and fire detectors.

6.1.6 Media Storage

The MYIFAM CA key is kept in several removable storages. Backup copies of CA related information are kept in removable media.

6.1.7 Waste Disposal

All MYIFAM CA paper waste MUST be shredded. Electronic media MUST be physically/mechanically destroyed before disposal.

6.1.8 Off-Site Backup

No off-site backups are currently performed.

6.2 Procedural Controls

6.2.1 Trusted Roles

No Stipulations.

6.2.2 Number of Persons Required per Task

No Stipulations.

6.2.3 Identification and Authentication for Each Role

No Stipulations.

6.2.4 Roles Requiring Separation of Duties

No Stipulations.

6.3 Personnel Controls

6.3.1 Qualifications, Experience, and Clearance Requirements

The role of the CA requires a suitably trained person that is familiar with the importance of a PKI, and who is technically and professionally competent.

6.3.2 Background Check Procedures

No other personnel are authorized to access MYIFAM CA facilities without the physical presence of CA personnel.

6.3.3 Training Requirements

Internal training is given to CA operators.

6.3.4 Retraining Frequency and Requirement

No Stipulation

6.3.5 Job Rotation Frequency and Sequence

Job rotation is not performed.

6.3.6 Sanctions for Unauthorized Actions

No Stipulation.

6.3.7 Independent Contractor Requirements

No Stipulation

6.3.8 Documentation Supplied to Personnel

- Copies of this document;
- MYIFAM CA Operations Manual.

6.4 Audit Logging Procedures

6.4.1 Types of Events Recorded

- Certification requests;
- Revocation requests;
- Issued certificates;
- Issued CRLs.

6.4.2 Frequency of Processing Logs

No Stipulation.

6.4.3 Retention Period for Audit Logs

Logs will be kept for a minimum of 3 years.

6.4.4 Protection of Audit Log

All audit logs are accessible to the MYIFAM CA managers and to authorized audit personnel only.

6.4.5 Audit Log Backup Procedures

Audit logs are copied to an offline medium every one month.

6.4.6 Audit Collection System (internal vs. external)

Audit collection is internal to MYIFAM CA service.

6.4.7 Notification to Event-Causing Subject

No stipulation

6.4.8 Vulnerability Assessments

No stipulation

6.5 Records Archival

6.5.1 Types of Records Archived

The following events are stored and backed-up in safekeeping:

- certification requests
- issued certificates
- revocation request
- issued CRLs
- all e-mail messages sent to MYIFAM CA
- all e-mail messages sent by MYIFAM CA
- CA system logs will be recorded and archived, including
  - boot / shutdown system log
  - system message log
  - secure message log
  - /root directory

6.5.2 Retention Period for Archive

The minimum retention period is three years. Identity validation records are kept at least as long as there are valid certificates based on such a validation.

6.5.3 Protection of Archive

The archive is accessible to MYIFAM CA personnel and authorized audit personnel only.

6.5.4 Archive Backup Procedures

Archives are copied to an offline medium and stored in a restricted access area every one month.

6.5.5 Requirements for Time-Stamping of Records

No stipulation

6.5.6 Archive Collection System (Internal or External)

Archive collection is internal to MYIFAM CA service.

6.5.7 Procedures to Obtain and Verify Archive Information

No stipulation

6.6 Key Changeover

MYIFAM CA's private signing key is changed periodically. To avoid interruption of validity of all subordinate keys the new MYIFAM CA private key should be generated 400 days before the expiration of the old key. From that point on new certificates are signed by the newly generated signing key. The new MYIFAM CA public key is posted in the on-line repository.

6.7 Compromise and Disaster Recovery

6.7.1 Incident and Compromise Handling Procedure

If the CA's private key is (or suspected to be) compromised, the CA will:

- Inform subscribers and subordinate RAs;
- Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

If the CA server is damaged, the CA will

- Replace a new server machine
- Recover all functions and the database with archived files and directories

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

Refer to section 6.7.1.

6.7.3 Entity Private Key Compromise Procedure

Refer to section 6.7.1.

6.7.4 Business Continuity Capabilities After a Disaster

The plans for business continuity and disaster recovery for research activities and education are applicable.

6.7.5 CA or RA Termination

Before MYIFAM CA terminates its services, it will:

- Inform subscribers, subordinate CAs and cross-certifying CAs;
- Make widely available information of its termination;
- Stop issuing certificates and CRLs.
- Destroy its private key's and all copies.

Chapter 7

Technical Security Controls

7.1 Key Pair Generation and Installation

7.1.1 Key Pair Generation

Each subscriber must generate his/her own key pair. MYIFAM CA does not generate private keys for subjects. The private key should not be known by other than the authorized user of the key pair.

7.1.2 Private Key Delivery to Subscriber

The MYIFAM CA does not generate private keys hence does not deliver private keys. Entities' private key will be generated by browser application in personal computer.

7.1.3 Public Key Delivery to Certificate Issuer

Entities' public keys are delivered to issuing CA in a secure and trustworthy manner.

7.1.4 CA Public Key Delivery to Relying Parties

CA certificate can be downloaded from the MYIFAM CA secure web site.

7.1.5 Key Sizes

- The minimum key length for user or host certificate is 1024 bits
- The CA key length is 2048 bits.

7.1.6 Public Key Parameters Generation and Quality Checking

No Stipulation.

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

MYIFAM CA private key is the only key used for signing CRLs and Certificates for person, server and service. The Certificate key Usage field must be used in accordance with the "RFC 3647 - Internet X.509 Public Key Infrastructure Certificate and CRL profile" [7].

7.2 Private Key Protection and Cryptographic Module Engineering Controls

7.2.1 Cryptographic Module Standards and Controls

No Stipulation

7.2.2 Private Key (n out of m) Multi-person Control

The CA's private key is not under (n out of m) multi-person control. But the MYIFAM CA implements multi-person control for the access to the CA server as described in section 6.1. Backup Copy of the CA's private key is under (2 out of 5) multi-person control.

7.2.3 Private Key Escrow

Private keys must not be escrowed.

7.2.4 Private Key Backup

The MYIFAM CA's private key is kept encrypted in multiple copies in floppy disks and CDROMs in safe places. For emergencies, the passphrase is in a sealed envelope kept in a safe.

7.2.5 Private Key Archival

Refer to section 7.2.4.

7.2.6 Private Key Transfer Into or From a Cryptographic Module

Not applicable.

7.2.7 Private Key Storage on Cryptographic Module

Not applicable

7.2.8 Method of Activating Private Key

No stipulation.

7.2.9 Method of Deactivating Private Key

No stipulation.

7.2.10 Method of Destroying Private Key

No stipulation.

7.2.11 Cryptographic Module Rating

Not applicable

7.3 Other Aspects of Key Pair Management

- The lifetime of MYIFAM CA certificate is twenty years.
- The lifetime of user certificate is 400 days.
- The lifetime of host certificate is 400 days.

7.3.1 Public Key Archival

Public key archival is not supported.

7.3.2 Certificate Operational Periods and Key Pair Usage Periods

Refer to section 7.3.

7.3.3 Activation Data

The MYIFAM CA's private key is protected by a 15 characters passphrase.

7.3.4 Activation Data Generation and Installation

No stipulation.

7.3.5 Activation Data Protection

No stipulation.

7.3.6 Other Aspects of Activation Data

No stipulation.

7.4 Computer Security Controls

7.4.1 Specific Computer Security Technical Requirements

- The CA system is a dedicated machine
- The operating systems of CA/RA computers are maintained at a high level of security by applying all the relevant patches;

- Monitoring is performed to detect unauthorized software changes;
- CA systems configuration is reduced to the base minimum.

7.4.2 Computer Security Rating

No Stipulation.

7.5 Life Cycle Technical Controls

7.5.1 System Development Controls

No Stipulation.

7.5.2 Security Management Controls

No Stipulation.

7.5.3 Life Cycle Security Controls

No Stipulation.

7.6 Network Security Controls

- The CA signing machine is kept off-line;
- CA website machines other than the signing machine are protected by a firewall.

7.7 Time-Stamping

All time stamping of entries created on the online servers at the MYIFAM CA is based on the network time provided by the time servers of Academia Sinica (stdtime.sinica.edu.tw). The standard time used is Coordinated Universal Time (UTC).

Chapter 8

Certificate, CRL, and OCSP Profiles

8.1 Certificate Profile

All certificates issued by MYIFAM CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 5280 [6].

8.1.1 Version Number(s)

X.509 v3.

8.1.2 Certificate Extensions

Basic constraints (critical):	Not a CA
Key usage (critical):	Digital signature, non-repudiation, key encipherment, data encipherment.
Subject key identifier	hash
Authority key identifier	key id
Subject alternative name	email address
Issuer alternative name	email address, http URI
CRL distribution points	http URI
Certificate policies	OID, 1.2.840.113612.5.2.2.1

8.1.3 Algorithm Object Identifiers

No Stipulation.

8.1.4 Name Forms

Issuer:

DC=MY, DC=UPM, DC=MYIFAM, C=MY, O=MYIFAM, CN=Malaysia Identity Federation and Access Management

Person DN:

DC=MY, DC=UPM, DC=MYIFAM, C=MY, O=Organization, OU=Users, CN=First Name Last Name Unique ID

Server name DN:

DC=MY, DC=UPM, DC=MYIFAM, C=MY, O=Organization, OU=Hosts, CN=DNS server name(FQDN)

8.1.5 Name Constraints

Subject attribute constrains:

- Domain Components: must be "MY", "UPM" and "MYIFAM".
- Country Name: must be MY".

8.1.6 Certificate Policy Object Identifier

Refer to section 1.2

8.1.7 Usage of Policy Constraints Extensions

No Stipulation.

8.1.8 Policy Qualifier Syntax and Semantics

No Stipulation.

8.1.9 Processing Semantics for the Critical Certificate Policies Extension

No Stipulation.

8.2 CRL Profile

8.2.1 Version Number(s)

x.509 v1.

8.2.2 CRL and CRL Entry Extensions

No Stipulation.

8.3 OCSP Profile

8.3.1 Version Number(s)

No Stipulation.

8.3.2 OCSP Extensions

No Stipulation.

Chapter 9

Compliance audit and other assessments

9.1 Frequency or circumstances of assessment

- The MYIFAM CA shall make at least once a year a self-assessment to check the compliance of the operation with the CP/CPS document in effect.
- The MYIFAM CA shall make at least once a year assess the compliance of the procedures of each RA with the CP/CPS document in effect.

9.2 Identity/qualifications of assessor

No stipulation.

9.3 Assessor's relationship to assessed entity

The assessments are made by personnel of MYIFAM CA. An external audit can be performed by any academic institution or relying party. If other trusted CAs or relying parties request an external assessment, the costs of the assessment must be paid by the requesting party, except for the costs of MYIFAM CA personnel and infrastructure.

9.4 Topics covered by assessment

The audit will verify that the services provided by the CA comply with the latest approved version of the CP/CPS.

9.5 Actions taken as a result of deficiency

In case of a deficiency, the MYIFAM CA responsible will announce the steps that will be taken to remedy the deficiency, including a timetable. If a discovered deficiency has direct consequences on the reliability of the certification process, the certificates (suspected to be) issued under the influence of this problem shall be revoked immediately.

9.6 Communication of results

The MYIFAM CA staff will make the result publicly available on the MYIFAM CA web site with all relevant details.

Chapter 10

Other business and legal matters

10.1 Fees

No fees are charged for the MYIFAM CA certification service and therefore there are no financial encumbrances.

10.1.1 Certificate issuance or renewal fees

Refer to section 10.1.

10.1.2 Certificate access fees

Refer to section 10.1.

10.1.3 Revocation or status information access fees

Refer to section 10.1.

10.1.4 Fees for other services

Refer to section 10.1.

10.1.5 Refund policy

Refer to section 10.1.

10.1.6 Financial responsibility

No Financial responsibility is accepted for certificates issued under this policy.

10.1.7 Insurance coverage

No stipulation.

10.1.8 Other assets

No stipulation.

10.1.9 Insurance or warranty coverage for end-entities

No stipulation.

10.2 Confidentiality of business information

10.2.1 Scope of confidential information

No stipulation.

10.2.2 Information not within the scope of confidential information

No stipulation.

10.2.3 Responsibility to protect confidential information

No stipulation.

10.3 Privacy of personal information

10.3.1 Privacy plan

MYIFAM CA does not retain any specific private information, however subscribers personal informations are kept securely and not to be distributed to the third party unless for incident investigation purpose.

10.3.2 Information treated as private

Refer to section 10.3.1.

10.3.3 Information not deemed private

Refer to section 10.3.1.

10.3.4 Responsibility to protect private information

Refer to section 10.3.1.

10.3.5 Notice and consent to use private information

Refer to section 10.3.1.

10.3.6 Disclosure pursuant to judicial or administrative process

Refer to section 10.3.1.

10.3.7 Other information disclosure circumstances

Refer to section 10.3.1.

10.3.8 Intellectual property rights

MYIFAM CA does not claim any intellectual property rights on certificates which are issued. Parts if this document are inspired or even copied (in no particular order) from the ASGCCA [2] , CERN CA [3] and PK-GRID-CA [4] and may indirectly derive from documents they draw from. Anybody may freely copy from any version of the MYIFAM Certification Practices Statement provided they include an acknowledgment of the source.

10.4 Representations and warranties

10.4.1 CA representations and warranties

No stipulation.

10.4.2 RA representations and warranties

No stipulation.

10.4.3 Subscriber representations and warranties

No stipulation.

10.4.4 Relying party representations and warranties

No stipulation.

10.4.5 Representations and warranties of other participants

No stipulation.

10.5 Disclaimers of warranties

MYIFAM CA uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CP/CPS document. However it declines any warranty as to their full correctness. Also MYIFAM CA cannot be held responsible for any misuse of its certificate by a subscriber or any other party who got in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a relying party. Any relying party that accepts a certificate for any usage for which it was not issued does so on its own risk and responsibility.

10.6 Limitations of liability

MYIFAM CA declines any liability for damages incurred by a relying party accepting one of its certificates, or by a subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party. It also declines any liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with this CP/CPS.

10.7 Indemnities

MYIFAM CA declines any payment of indemnities for damages arising from the use or rejection of certificates it issues. End entities shall indemnify and hold harmless MYIFAM CA and all appropriate RAs operating under this CP/CPS against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate which violates the provisions of this CP/CPS document.

10.8 Term and termination

10.8.1 Term

This document becomes effective after its publication on the Web site of the MYIFAM CA starting at the date announced there. No term is set for its expiration.

10.8.2 Termination

This CP/CPS remains effective until it is superseded by a newer version.

10.8.3 Effect of termination and survival

Its text shall remain available for at least 5 years after the last certificate issued under this CP/CPS expires or is revoked.

10.9 Individual notices and communications with participants

All e-mail communications between the CA and its accredited RAs must be signed with a certified key. All e-mail communications between the CA or an RA and a subscriber must be signed with a certified key in order to have the value of a proof. All requests for any action must be signed.

10.10 Amendments

10.10.1 Procedure for amendment

Amendments to this CP/CPS must undergo the same procedures as for the initial approval (see 1.5.4). Rephrasing provisions to improve their understandability as well as pure spelling corrections

are not considered amendments.

10.10.2 Notification mechanism and period

The amended CP/CPS document shall be published on MYIFAM CA Web pages at least 2 weeks before it becomes effective. MYIFAM CA will inform its subscribers and all relying parties it knows of by means of an e-mail.

10.10.3 Circumstances under which OID must be changed

Any amendment shall cause the OID to be changed. The decision is made by the MYIFAM CA manager and submitted to the APGridPMA [1] for approval.

10.10.4 Dispute resolution provisions

Disputes arising out of the CP/CPS shall be resolved by the MYIFAM CA manager.

10.11 Governing law

MYIFAM CA and its operation are subject to the Malaysia law. All legal disputes arising from the content of this CP/CPS document, the operation of MYIFAM CA and its accredited RAs, the use of their services, the acceptance and use of any certificate issued by MYIFAM CA shall be treated according to Malaysia law.

10.12 Compliance with applicable law

All activities relating to the request, issuance, use or acceptance of a MYIFAM CA certificate must comply with the Malaysia law. Activities initiated from or destined for another country than Malaysia must also comply with that country's law.

10.13 Miscellaneous provisions

10.13.1 Entire agreement

This CP/CPS document supersedes any prior agreements, written or oral, between the parties covered by this present document.

10.13.2 Assignment

No provisions.

10.13.3 Severability

Should a clause of the present CP/CPS document become void because it is conflicting with the governing law (see 10.11) or because it has been declared invalid or unenforceable by a court or other law-enforcing entity, this clause shall become void (and should be replaced as soon as possible by a conforming clause), but the remainder of this document shall remain in force.

10.13.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

10.13.5 Force Majeure

Events that are outside the control of MYIFAM CA will be dealt with immediately by the AP-GridPMA [1].

10.14 Other provisions

No stipulation.

References

[1] Asia Pacific Grid Policy Management Authority. http://www.apgridpma.org

[2] ASGC CA Certificate Policy and Certification Practice Statement. Available via Website. http://ca.grid.sinica.edu.tw/CPS/ASGCCA-CPCPS-v2.1.doc. Cited 7 Aug 2010

[3] CERN CA Certificate Policy and Certification Practice Statement. Available via Website. https://ca.cern.ch/ca/CRL/Policy/cp-cps.pdf. Cited 15 Aug 2010

[4] PK-GRID-CA Certificate Policy and Certification Practice Statement. Available via Website. http://www.ncp.edu.pk/pk-grid-ca/docs/cps-1.1.1.4.pdf. Cited 8 Apr 2011

[5] EU Grid Policy Management Authority. http://www.eugridpma.org/

[6] RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Available via Website. http://www.ietf.org/rfc/rfc5280.txt. Cited 8 Apr 2011

[7] RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". Available via Website. http://www.ietf.org/rfc/rfc3647.txt. Cited 15 Aug 2010

[8] The America Grid Policy Management Authority. http://www.tagpma.org/