Polish Grid Certification Authority
Certificate Policy
and
Certification Practice Statement

version 0.8

January 9, 2015

1 Introduction

1.1 Overview

This document is written according to the structure suggested by the RFC 2527. This document describes the set of rules and operational practices used by the Polish Grid CA. The Polish Grid CA is the top level Certification Authority for Polish Grid (www.man.poznan.pl/plgrid-ca)

1.2 Document name and identification

Title: Polish Grid CA Certificate Policy and Certification Practice Statement.
Version: Version 0.8 (30 December 2014)
Expiration: This document is valid until further notice.
OID: 1.3.6.1.4.1.2698.1.5.1.0.8

The structure of the OID is following:

1.3.6.1.4.1	IANA private enterprises
2698	Poznań Supercomputing and Networking Center
1	Documents
5	Polish Grid CA
1	CP/CPS
0.8	Version

1.3 Community and Applicability

1.3.1 Certification Authorities

Polish Grid CA signs certificates for Polish Grid community. It does not issue certificates to subordinate CA.

1.3.2 Registration Authorities

The Polish Grid CA also performs the role of a RA. Additional registration authorities may be created by the Polish Grid CA as required. The current list of registration authorities may be obtained from the following URL: http://www.man.poznan.pl/plgrid-ca/ra-list.html.
The list will be verified at least once a year.

1.3.3 End Entities

Certificates can be issues to natural persons and to computer entities. The entities that are eligible for certification by the Polish Grid Certification Authority are all those entities related to organizations, formally based in and/or having offices inside Poland, that are involved in the research or deployment of multi-domain distributed computing infrastructure, intended for cross organizational

sharing of resources. The focus of these organizations should also be in research and/or education.

1.3.4 Applicability

The issue certificate types and suitability is as follows:

a) Personnel certificates: authentication, non-repudiation and communication encryption.

b) Server certificates: authentication, non-repudiation and communication encryption.

c) Services certificates: authentication, non-repudiation and communication encryption.

d) Robot certificates: authentication, non-repudiation and communication encryption.

The certificates issued by the Polish Grid Certification Authority may not be used for financial transactions and for any commercial usage.

1.4 Contact Details

The Polish Grid CA is managed by Poznan Supercomputing and Networking Center in Poznan. The contact person for this document and Polish Grid CA in general is:

Pawel Wolniewicz
Polish Grid CA
Poznan Supercomputing and Networking Center
ul. Noskowskiego 10
61-704 Poznan Poland

phone: +48 61 8582052
fax: +48 61 8525954
e-mail: plgrid-ca@man.poznan.pl

2 General Provision

2.1 Obligations

2.1.1 CA Obligations

a) Accept certification requests from entitled entities;

b) Issue certificates based on requests after successful authentication;

c) Notify the subscriber of the issuing of the certificate;

d) Accept revocation requests from acceptable persons;

e) Authenticate revocation requests before performing revocations;

f) Issue Certificate Revocation List (CRL) according with the rules described in this document;

g) Publish the issued CRL;

h) Follow the policies and procedures described in this document.

2.1.2 RA Obligations

a) Authenticate entities according with the procedures described in this document;

b) Validated certificate requests and revocation requests;

c) Create and send validated revocation requests to the Polish Grid CA;

d) Follow the policies and procedures described in this document.

2.1.3 Subscriber Obligations

a) Read and accept the policies and procedures published in this document;

b) Generate a key pair using a trustworthy method;

c) Keep the private key safe and adequately protected by system methods;

d) Protect the private key of personal certificates with passphrase which has a minimum of 12 characters and follow current best practice in choosing high-quality passwords.

e) Notify the CA in case of possible private key destruction, loss or compromise;

f) Notify the CA when the certificate is no longer required;

g) Notify the CA when the information in the certificate becomes wrong or inaccurate.

h) Subscribers must not share certificates.

For the conditions e), f), g) subscriber must inform CA as soon as possible, but within one working day.

2.1.4 Relaying Party Obligations

a) Read and accept the policies and procedures published in this document;

b) Verify the CRL before validating a certificate;

c) Use the certificates for permitted uses only.

2.1.5 Repository Obligations

a) Polish Grid CA will keep a web server repository;

b) Polish Grid CA will publish its public key on its web server;

c) Polish Grid CA will publish its CRLs on its web server as soon as issued.

2.2 Liability

a) Polish Grid CA guarantees to control the identity of the certification requests according to the procedures described in this document;

b) Polish Grid CA guarantees to control the identity of the revocation requests according to the procedures described in this document;

c) Polish Grid CA is run on a best effort basis and does not give any guarantees about the service security or suitability;

d) Polish Grid CA will take no responsibility for any problems arising from its operation or use made of certificates it issues;

d) Polish Grid CA denies any kind of responsibilities for damages or impairments resulting from its operation.

2.3 Financial responsibility

No financial responsibility is accepted.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

The interpretation of this policy is according to the Polish law.

2.4.2 Dispute Resolution Procedures

Legal disputes arising from the operation of the Polish Grid CA will be resolved according with the Polish law.

2.5 Fees

No fees are charged.

2.6 Publication and Repositories

2.6.1 Publication of CA Information

Polish Grid CA publishes the following information through its online repository:

a) The CA certificate;

b) The latest CRL;

c) A copy of this document containing the CP and CPS;

d) Other relevant information.

2.6.2 Frequency of Publication

New information will be published as soon as available.

CRLs will be published as soon as issued and at least every 30 days.

2.6.3 Access Controls

Polish Grid CA does not impose any access control on its Policy, its Certificate and CRLs.

Polish Grid CA may impose a more restricted access control policy to the repository at its discretion.

The Polish Grid CA web site is maintained in a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site should be available most of the time.

2.6.4 Repositories

The Polish Grid CA online repository is available at http://www.man.poznan.pl/plgrid-ca.

Therepositoryisoperatedatabest-effortbasis, wherethe intendedavailabilityis continuous.

2.7 Compliance Audit

Polish Grid CA management will conduct internal operational audits of the CA/RA staff compliance to this CP/CPS at least once a year.

The Polish Grid CA accepts external Compliance Audits when requested by a policy management authority in which Polish Grid CA is a member. Any costs associated to such compliance audit must be carried by the requesting party.

2.8 Confidentiality

Polish Grid CA collects personal information about the subscribers (e.g. full name, organization, e-mail-address). These data will be protected according to the Polish Law.

2.8.1 Confidential Information kept by the CA/RA

All information about subscriber that is not present in the certificate and CRL is considered confidential and will not be released outside.

2.8.2 Types of Information not Considered Confidential

Information included in issued certificates and CRLs is not considered confidential.

2.8.3 Disclosure of certificate Revocation/Suspension information

The CA will notify and inform the following entities:

a) The subject of the personal certificate;
b) The requester of the service, server or robot certificate;
c) The Poznan Supercomputing and Networking Center security officer in case of security compromise.

2.8.4 Release of Information to Law Enforcement Officials

Any confidential information collected by the CA will be subject to Polish law.

2.8.5 Information that can be revealed as Part of Civil Discovery

Any confidential information collected by the CA will be subject to Polish law.

2.8.6 Conditions for Disclosure Upon Owner's Request

Any confidential information collected by the CA will be subject to Polish law.

2.8.7 Other Circumstances for Disclosure of Confidential Information

Any confidential information collected by the CA will be subject to Polish law.

2.9 Intellectual Property Rights

This document is based on the following sources:

a) RFC 2527;
b) EuroPKI Certificate Policy;
c) NIKHEF Certificate Policy and Certificate Practice Statement;
d) LIP Certificate Policy and Certificate Practice Statement;
e) Grid-Ireland CA Certificate Policy and Certificate Practice Statement;

This text may be used by others without prior approval; acknowledgements are welcomed but not required.

Unmodified copies may be published without permission.

No intellectual property rights are claimed on issued certificates or certificate revocation lists.

3   Identification and Authentication

3.1   Initial Registration

3.1.1   Types of Names

The subject names obey to the X.500 standard:

a) For persons the name includes the person name;

b) For servers the subject includes the server DNS FQDN name.It may be prefixed with "host/".

c) For services the subject includes the server DNS FQDN name, prefixed with the service name.

d) For robots the subject includes the robot purpose and the owner name , prefixed with "Robot - ".

3.1.2   Name Meanings

The format of a Polish Grid distinguish name is: "C=PL, O=GRID, O=organisation, CN=subject-name"

The common name CN in the certificate subject must be obtainable from the real subject name. For personal and robot certificates it must be obtainable from a name of a person.

The distinguished name O must be one of the organization involved in Polish Grid activities.

Current list of values available for distinguished name O can be obtained from the following URL http://www.man.poznan.pl/plgrid-ca/ra-list.html.

3.1.3   Rules for interpreting various name forms

See Section 3.1.1 and 3.1.2

3.1.4   Uniqueness of Names

The distinguished name for each certificate must be unique. In case of real subject name duplication, additional string will be appended to the distinguished name to guarantee uniqueness. Letter case, punctuation and whitespace must not be used for distinguishing names. If the name presented by Subscriber is not unique then the CA or RA will ask Subscriber to create another requested with some variation added to the common name.

Polish Grid CA ensures that a DN is not reused. The same DN can be used if the request is a rekey. In other cases an RA will consult original identification records to ensure that the Subscriber is the same person for which the original certificate was issued. If this identity cannot be fully guarantied, the DN will never be reused.

3.1.5   Method to Prove Possession of Private Key

Requests must be submitted in PKCS10 format. Signature is verified by CA.

3.1.6 Authentication of Organization Identity

No stipulation.

3.1.7 Authentication of Individual Identity

Procedures differ if the subject is a person, a robot, a service or a server:

Person or robot certificate: The identity must be confirmed during face-to-face contact with relevant RA. The applicant must hand to RA the signed paper verifications form; the digest of certificate request printed on the verification form must match the certification request sent to CA. The subject authentication is performed through the presentation of a valid official identification document (Passport or Identity card).

Server or service certificate: Requests should be submitted via Polish Grid Registration Portal https://plgrid-ca.pl. If the submission was not authenticated by using the valid personal Polish Grid CA certificate of the corresponding system administrator, than the identity of the requester must be confirmed during face-to-face contact with relevant RA. RA must verify to the reasonable extent that the applicant is entitled to the use of the FQDN presented in the subject names. RA reserves the right to ask for additional documents confirming the right to use the given FQDN.

3.2 Routine Re-key

Certificates can by only re-keyed, not renewed. Rekey before expiration can be accomplished by sending a re-key request signed with the current user certificate. The DN of the new X.509 request must match the DN of the certificate used to submit the request. If thelast identificationaccordingto theproceduresinsection3.1.7was conducted more than5 years ago, then the procedure detailed in section 3.1.7 must be used.

Rekey after expiration follows the same authentication procedure as new certificate.

3.3 Rekey After Revocation

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

3.4 Revocation

Certificate revocation requests can be sent by e-mail to plgrid-ca@man.poznan.pl, or by using Polish Grid CA Registration Portal https://plgrid-ca.pl. Revocation requests are treated as authenticated if they are signed by a valid personal Polish Grid CA or TERENA eScience Personal CA certificate, where the e-mail address in the request must belong to the person that owns the certificate. Otherwise the Polish Grid CA staff will adopt the same procedure used for the authentication of identity of a person.

4 Operational Requirements

4.1 Certification Application

Applicants must generate their own key pair. The minimum key length for all applications is at least 2048 bits. The maximum validity period for a certificate is 400 days. The requests must obey to the Polish Grid CA distinguished name scheme.

Applicants should apply for a certificates by using Polish Grid Registration Portal https://plgrid-ca.pl. On special cases other at least equally secure procedures can be applied for transferring certificate requests to CA. Procedures outlined in 3.1.7 are applied.

4.2 Certificate Issuance

Polish Grid CA issues the certificate if, and only if, the authentication of the subject is successful. The applicant will be notified about the issuance of the certificate by e-mail. If the authentication is not successful, the certificate is not issued and the applicant will also be notified.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

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

a) The private key has been lost or compromised;

b) The information in the subscribers certificate is suspected to be inaccurate;

c) The subscriber no longer needs the certificate

d) The subject has failed to comply with the rules in this policy;

e) The system to which the certificate has been issued has been retired.

4.4.2 Who can request revocation

A certificate revocation can be requested by the holder of the certificate to be revoked, by Registration Atuhority, by CA or by any other entity presenting proof of knowledge of the private key compromise or of the variation of the subscribers data.

4.4.3 Procedure for Revocation Request

The entity requesting revocation should use revocation form at Polish Grid Registration Portal https://plgrid-ca.pl or send the revocation request by e-mail signed with a valid Polish Grid CA or TERENA eScience Personal CA certificate. If this is not possible the RA must be contacted directly. Authentication can be performed as described in 3.1.7.

Polish Grid CA will process all revocation requests within 1 working day.

4.4.4 Circumstances for Suspension

No stipulation.

4.4.5 Who can request suspension

No stipulation.

4.4.6 Procedure for suspension request

No stipulation.

4.4.7 Limits on Suspension Period

No stipulation.

4.4.8 CRL Issuance Frequency

CRLs are issued no later than one hour after certificate revocation and at least 7 days before expiration. Maximum CRL lifetime is 30 days.

4.4.9 CRL Checking Requirements for Relaying Parties

A relying party must download the CRL at least once a day and implement its restrictions while validating certificates.

4.4.10 Online Revocation/status Checking Availability

No stipulation.

4.4.11 Online Revocation Checking Requirements

No stipulation.

4.4.12 Other Forms of Revocation Advertisement

No stipulation.

4.4.13 Requirements for Relying Parties on Other Forms of Revocation Advertisement

No stipulation.

4.4.14 Variations of the Above in Case of Private Key Compromise

No stipulation.

4.5 Security Audit Procedures

4.5.1 Types of Events Audited

a) Certification requests;

b) Revocation requests;

c) Validation records;

d) Issued certificates;

e) Issued CRLs;

f) Boots of the equipment;

g) Interactive logins on this system.

4.5.2 Processing Frequency of Audit Logs

No stipulation

4.5.3 Retention Period for Audit Logs

Logs will be kept for a minimum of 3 years.

4.5.4 Protection of Audit Logs

Only authorized CA personnel and authorized external auditors are allowed to view and process audit logs. Audit logs are copied to an off-line medium.

4.5.5 Backup Procedures

Audit logs are copied to an off-line medium, which are stored in a room with restricted access.

4.5.6 Accumulation System

The audit log accumulation system is internal to the Polish Grid CA.

4.5.7 Accumulation System

No stipulation.

4.5.8 Vulnerability Assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of Events Recorded

a) Certification requests;

b) Revocation requests;

c) Issued certificates;

d) Issued CRLs.

e) All e-mail messages sent to the Polish Grid CA;

f) All e-mail messages received by the Polish Grid CA;

No personal information are stored by CA. By signing certificate request to CA, RA confirms that the request was validated and properly authenticated. As the only authentication method allowed is to check an applicants ID, the signed mail from RA to CA is a validation record as well.

Individual RAs may record additional information about personal identification data for given DN. Such information can be use exclusively to ensure uniqueness of DNs and proper authentication of next requests.

4.6.2 Retention Period for Records

Logs will be kept for a minimum of 3 years.

4.6.3 Protection of Records

Records are copied to an off-line medium, which are stored in a room with restricted access.

4.6.4 Backup Procedures

No stipulation.

4.6.5 Time-stamping Requirements

No stipulation.

4.6.6 Archive Collection System

The archive system is internal to the Polish Grid CA.

4.6.7 Procedures to Obtain and Verify Archive Information

No stipulation.

4.7 Key Changeover

If the CA key need to be changed then the CA will generate a new key pair at least 400 days (maximum certificate lifetime) before the expiry of the CA certificate. Only new key will be used for certificate signing purposes. For this overlapping period old certificates will be still available for validation purposes.

4.8 Compromise and Disaster Recover

If the CA private key is or is suspected to be compromised the CA will:

a) Notify subscribers, RAs, identified relying parties, known cross-certifying CAs and any coordinating organisations in which CA participates;

b) Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

c) Notify relevant security contacts.

d) Generate new key pair.

If the CA machine is corrupted then it will be replaced with new machine in at most two working day. If the hard disk of the CA machine is corrupted then it will be replaced with new one, and CA data will be restored from last backup. The corrupted disk will be physically destroyed in a way that reading data from the disk will not be possible.

If any backup media containing CA private key will be lost then it will be treated as a key compromise and adequate procedure will be followed.

4.9 CA Termination

Upon termination the Polish Grid CA will:

a) Notify subscribers, RAs and cross-certifying CAs;

b) Stop issuing and distributing certificates and CRLs.

c) Notify widely as possible the end of the service.

5 Physical, Procedural, and Personnel Security Controls

5.1 Physical Security Controls

5.1.1 Site Location

The Polish Grid CA is located at Poznan Supercomputing and Networking Center, Poznan, Poland.

5.1.2 Physical Access

The Polish Grid CA operates in a secure machine room, where physical access is restricted to authorized people.

5.1.3 Power and Air Conditioning

The Polish Grid CA operates in an environmentally controlled machine room with air conditioning system and UPS.

5.1.4 Water Exposures

No stipulation.

5.1.5 Fire Prevention and Protection

Polish Grid CA facilities obey to the Polish law regarding fire prevention and protection in buildings.

5.1.6 Media Storage

The Polish Grid CA key and backup copies of CA related information are kept in encrypted form in several removable storage media. Backup copies of CA related information are kept in removable media in secure machine room.

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

No off-site backups are currently performed.

5.2 Procedural Controls

Not defined.

5.3 Personnel Security Controls

5.3.1 Background Checks and Clearance Procedures for CA Personnel

CA personnel is recruited from the Poznan Supercomputing and Networking Center team.

5.3.2 Background Checks and Security Procedures for Other Personnel

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

5.3.3 Training Requirements and Procedures

Internal training is given to CA operators.

5.3.4 Training Period and Retraining Procedures

No stipulation.

5.3.5 Frequency and Sequence of Job Rotation

Job rotation is not performed.

5.3.6 Sanctions Against Personnel

No stipulation.

5.3.7 Controls on Contracting Personnel

No stipulation.

5.3.8 Documentation Supplied to Personnel

a) Copies of this document;
b) Polish Grid CA Operations Manual;

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Each entity must generate its own key pair. The Polish Grid CA does not generate private keys for subjects.

6.1.2 Private Key Delivery to Entity

No stipulation.

6.1.3 Public Key Delivery to Users

Public keys are delivered by the SSL protected HTTP protocol via the Polish Grid CA Registration Portal web interface. Optionally public keys can be delivered by signed E-mail, removable media or can be copied to the user directory by CA personnel.

6.1.4 CA Public Key Delivery to Users

The Polish Grid CA certificate can be downloaded from the Polish Grid CA web site.

6.1.5 Key Sizes

a) The minimum key length for a personnel or server certificate is 2048 bits;

b) The 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

Keys may be used for authentication, non-repudiation, data encipherment, message integrity and session establishment. Certificates and CRLs are signed by the CA private key.

6.2 Private Key Protection

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

No stipulation.

6.2.2 Private Key Escrow

No stipulation.

6.2.3   Private Key Archival and Backup

Backups of Polish Grid CA private key are kept encrypted on removable media in a safe and locked up place with restricted access. The passphrase is in a sealed envelope kept in a secure place with access restricted to PSNC management.

6.3   Other Aspects of Key Pair Management

The Polish Grid CA private key has currently a validity of eighteen years and is valid to Aug 28 10:03:11 2020 GMT.

6.4   Activation Data

The Polish Grid CA private key is protected by a passphrase with a minimum of 15 characters.

6.5   Computer Security Controls

6.5.1   Specific Security Technical Requirements

a) The operating systems of CA/RA computers are maintained at a high level of security by applying all the relevant patches;

b) Monitoring is performed to detect unauthorized software changes;

c) The off-line CA signing system is a dedicated machine, running no other services than those needed for the CA signing operations.

d) The signing machine is kept powered off between uses.

6.5.2   Computer Security Rating

No stipulation.

6.6   Life Cycle Security Controls

No stipulation.

6.7   Network Security Controls

The CA signing machine is not connected to any kind of network;

6.8   Cryptographic Module Engineering Controls

No stipulation.

7 Certificate and CRL Profile

7.1 Certificate Profile

7.1.1 Version Number

X.509 v3.

7.1.2 Certificate Extensions

CA certificate extensions:

- Basic constraints (Critical):
  CA:TRUE
- Key usage (Critical):
  Certificate Sign, CRL sign,
- Subject key identifier
- Authority key identifier
- Subject alternative name:
  email:plgrid-ca@man.poznan.pl, URI:http://www.man.poznan.pl/plgrid-ca/
- X509v3 CRL Distribution Points:
  URI:http://www.man.poznan.pl/plgrid-ca/crl.der
- Signature Algorithm: sha1WithRSAEncryption

Subscriber certificate extensions:

Personal certificate profile:

- Subject key identifier
- Authority key identifier
- Basic constraints (Critical):
  CA:FALSE
- Key usage (Critical):
  Digital Signature, Key Encipherment, Data Encipherment.
- Extended Key Usage:
  quad TLS Web Client Authentication, E-mail Protection
- X509v3 Certificate Policies:
  Policy:1.3.6.1.4.1.2698.1.5.1.0.8
  Policy:1.2.840.113612.5.2.2.1
  CPS: http://www.man.poznan.pl/plgrid-ca/ca-policy.html
- X509v3 CRL Distribution Points:
  URI:http://www.man.poznan.pl/plgrid-ca/crl.der

- Signature Algorithm: sha256WithRSAEncryption

  Optional extension (on request):
- X509v3 Subject Alternative Name: email

Host or service certificate profile:

- Subject key identifier
- Authority key identifier
- Basic constraints (Critical):
  CA:FALSE
- Key usage (Critical):
  Digital Signature, Key Encipherment, Data Encipherment.
- Extended Key Usage
  TLS Web Client Authentication, TLS Web Server Authentication
- X509v3 CRL Distribution Points:
  URI:http://www.man.poznan.pl/plgrid-ca/crl.pem
- X509v3 Certificate Policies:
  Policy: Policy:1.3.6.1.4.1.2698.1.5.1.0.8
  Policy:1.2.840.113612.5.2.2.1
- X509v3 Subject Alternative Name:
  DNS: FQDN
- Signature Algorithm: sha256WithRSAEncryption

Robot certificate profile:

- Subject key identifier
- Authority key identifier
- Basic constraints (Critical):
  CA:FALSE
- Key usage (Critical):
  Digital Signature, Key Encipherment, Data Encipherment.
- Extended Key Usage:
  quad TLS Web Client Authentication, TLS Web Server Authentication
- X509v3 Certificate Policies:
  Policy:1.3.6.1.4.1.2698.1.5.1.0.8
  Policy:1.2.840.113612.5.2.2.1
  CPS: http://www.man.poznan.pl/plgrid-ca/ca-policy.html
- X509v3 Subject Alternative Name: email
- X509v3 CRL Distribution Points:
  URI:http://www.man.poznan.pl/plgrid-ca/crl.der
- Signature Algorithm: sha256WithRSAEncryption

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name Forms

Issuer: C=PL, O=GRID, CN=Polish Grid CA
Subject: C=PL, O=GRID, O=organisation, CN=Subject-Name

7.1.5 Name Constraints

Subject attribute constraints:

countryName: Must be "PL".

organizationName: Must be "GRID".

organizationName(2): Must be the Polish scientific organization involved in Polish Grid activities. Current list of values available for organizationalUnitName can be obtained from the following URL http://www.man.poznan.pl/plgrid-ca/ra-list.html.

commonName: Depends on the certificate profile:

- For personal certificates CN must include name and surname
- For service and hosts certificates CN must include DNS FQDN of the subject
- For robot certificates CN must include string "Robot - " followed by robot purpose and name and surname of the responsible person.

7.1.6 Certificate Policy Object Identifier

Polish Grid CA identifies this policy with the object identifier:
OID: as specified in 1.2.

7.1.7 Usage of Policy Constraints Extensions

No stipulation.

7.1.8 Policy Qualifier Syntax and Semantics

No stipulation.

7.2 CRL Profile

7.2.1 Version

X.509 v2.

7.2.2   CRL and CRL Entry Extensions

No stipulation.

8   Specification Administration

8.1   Specification Change Procedures

Users will not be warned in advance of significant changes to Polish Grid CA 's policy and CPS. New version of policy will be published on CA web page at least 2 weeks in advance. All significant changes will be submitted to EUGridPMA for acceptance.

8.2   Publication and Notification Procedures

The Polish Grid CA policy is available at http://www.man.poznan.pl/plgrid-ca/ca-policy.html

8.3   CPS Approval Procedures

No stipulation.