EuroPKI Certificate Policy

VERSION 1.1

January 2004

OID: 1.3.6.1.4.1.5255.1.1.1

Document History

Date	Editorial Notes
15 Ottobre 2000	Initial Version.
29 Gennaio 2004	Correction of typos and rephrasing of some sentences.

Index

1 Introduction

EuroPKI is a non-profit organization established to create and develop a pan-european public-key infrastructure (PKI). It has its roots in the PKI established by the ICE-TEL project and further developed by the ICE-CAR one. Both these projects were funded by the European Commission under the Telematics for Research programme.

More information is available at http://www.europki.org/ca/root/.

The structure of this document is according to RFC 2527 [1]. Therefore there are some sections that are maintained for compatibility, although they do not apply exactly to the services offered by EuroPKI. Appendix 1 provides a glossary of terms used in this document. It is mainly based on [1].

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 [2]. (see Appendix 2)

In this document the expression “conforming CA” is used to indicate a CA whose behaviour is conforming to the set of provisions specified in this document.

1.1 Overview

This document describes a set of rules that indicates the applicability of a certificate issued by conforming CA to its community of users and/or class of application with common security requirements.

A certificate policy MAY be used by a certificate user to help in deciding whether a certificate, and the binding therein, is sufficiently trustworthy for a particular application. An X.509 Version 3 certificate issued by a conforming CA SHOULD contain a reference to this certificate policy.

More detailed information about the practices which a conforming CA employs in its operations in issuing certificates can be found in the Certification Practice Statements (CPS).

Every conforming CA MUST issue its own CPS in order to provide information to potential clients of the CA about the underlying technical, procedural and legal foundations which are not specified in this policy.

1.2 Identification

This certificate policy is identified by the following unique registered Object Identifier (OID):

1.3.6.1.4.1.5255.1.1.1

The OID is composed by the following parts:

ISO assigned 1	1
Organization acknowledged by ISO 3	3
US Department of Defense 6	6
Internet 1	1
Private 4	4
IANA registered private enterprises 1	1
EuroPKI 5255	5225
Root CA 1	1
Major version 1	1
Minor version 1	1

1.3 Community and applicability

A conforming CA can choose freely which are the community and applicability of their issued certificates but it MUST clearly specify them in its own CPS. In every case a conforming CA MUST NOT issue certificates to entities that don't belong to its community or for applications that haven't been carefully evaluated (for instance high value B2B transactions). Moreover a conforming CA SHALL respect all the limitations imposed by the following sections of this policy.

1.3.1 Certification Authority

An issuing conforming CA has to take particular care when it has to decide if a certain organization or individual can manage a subordinate CA performing all the controls and checks detailed in this policy.

A conforming CA MAY use as many RAs (registration authorities) as it wishes. A conforming CA MAY also have the role of RA if the entity authentication can be done by the CA itself. Subordinate CAs MUST sign an agreement with the certifying CA, stating the obligation to adhere to the agreed procedures.

1.3.2 Registration authorities

Registration Authorities (RA) are needed for physical identification/authentication of entities. These authorities MUST not be permitted to issue certificates.

A registration authority (RA) is

- . an individual or
- . a group of people appointed by an organization or an organizational unit

trusted by a CA, serving as a contact point for registration of new end entities, i.e. end entities that want to have a certificate issued. RAs have to check the certificates requester's identity in an appropriate way.

The RA MUST sign an agreement with the certifying CA, stating the obligation to adhere to the agreed procedures.

1.3.3 End entities

The end entities to be certified under this policy can be a natural person (individual or representing an organization) or a computer entity (e.g. a computer, a router or an application), capable of performing cryptographic operations.

Each conforming CA MUST detail in the CPS who are the end entities that it is willing to certify.

1.3.4 Applicability

One of the purposes of this policy is to promote a wide use of public-key certificates in many different applications. In order to promote interoperability this policy strongly encourages CA to support S/MIME for securing e-mail exchanges. It is also suggested that IPsec (to offer network layer security) and SSL/TLS (to offer transport layer security for protecting application protocols like HTTP, Telnet, FTP) SHOULD be supported. It's important to notice that this policy in principle doesn't want to put a priori limitation to the use of the certificates except for the case in which certificatesare used in a way that is prohibited by the law of the countries where the issuing CA are established. However in order to evaluate if certificates issued under this policy are suitable for a certain application the chapter 2 about "General provisions" has to be read carefully and fully understood.

1.4 Contact Details

1.4.1 Specification administration organization

On behalf of EuroPKI this policy is fully managed by the Computer and Network Security Group (CNSG) of Politecnico di Torino, Italy (http://security.polito.it/).

1.4.2 Contact person

Contact point for questions related to this policy is:

address	Prof. Antonio Lioy EuroPKI Root Certification Authority c/o Politecnico di Torino Dip. Automatica e Informatica corso Duca degli Abruzzi, 24 10129 Torino (Italy)
Phone	+39 0115647021 / +39 0115647054
Fax	+39 0115647099
URI	http://www.europki.org/ca/root/
e-mail	ca@europki.org

1.4.3 Person determining CPS suitability for the policy

In order to obtain an evaluation of CPS suitability for the policy, conforming CAs have to contact the person mentioned in 1.4.2. See section 8.3 for details about CPS approval procedures.

2 General provisions

This chapter describes obligations for relevant parties and makes statements on liability, financial/economical issues. Moreover there's a section about confidentiality that classifies information into confidential information and publicly available and distributable information. Auditing statements are also located here.

2.1 Obligations

2.1.1 CA obligations

A conforming CA SHALL operate a certification authority service.

The main obligations of a CA are:

- . handle certificate requests and issue new certificates:
    - accept and confirm certification requests from entities requesting a certificate according to the agreed procedures contained in this policy and in the CPS
    - authenticate entities requesting a certificate, possibly by the help of separately designated RAs
    - issue certificates based on authenticated entities' requests
    - send notification of issued certificate to requesters
    - make issued certificates publicly available
- handle certificate revocation requests and certificate revocation
    - accept and confirm revocation requests from entities requesting a certificate to be revoked according to the agreed procedures contained in CPS/policy
    - authenticate entities requesting a certificate to be revoked
    - make CRLs publicly available

2.1.2 RA obligations

An RA SHALL operate an RA service. This includes:

- . to authenticate the identity of the subject
- . to validate the connection between a public key and the requester identity including a suitable proof of possession method

- . to confirm such validation versus the CA
- . to adhere to the agreement made with the CA

2.1.3 Subscriber obligations

A subscriber SHALL behave according to the issuing CA CPS. This includes:

- . to read and adhere to the agreed procedures
- . to properly protect its private key, being the only possessor if the subscription refers to an individual person. In the case of a private key of a hardware or software component the protection and the control of the key MAY be under the responsibilities of more than one authorized person
- . to accept that in the usage of public key certificates CA's liability is limited according to what is specified by section 2.2
- . to authorize the treatment and conservation of personal data
- . to notify immediately the CA upon private key compromise

2.1.4 Relying party obligations

A relying party MUST be familiar with the CPS and this policy before drawing any conclusion on how much trust he can put in the use of a certificate issued from a conforming CA. A relying party MUST check CRLs when validating the use of a certificate. Moreover a relying party MUST ONLY use the certificate for the proscribed applications and MUST NOT use the certificates for forbidden applications.

2.1.5 Repository obligations

Each conforming CA SHALL use a publicly accessible repository to store certificates and Certificate Revocation Lists (CRLs).

The repository SHALL be available as much as practically possible, subject to the general characteristic of the organization that technically manage the CA.

2.2 Liability

2.2.1 CA liability

Conforming CA MAY accept liability. Considering that this policy is primarily established to promote the adoption of certificates as a mean to increase computer and network security in a broad variety of applications, the subsection 1.3.4 states that there are no a priori limitation to applicability of certificates issued under this policy. If no limitation is put on certificate applicability, this policy suggests that CA liability will be restricted to the guarantee of making the necessary controls to verify

the identity of every requester as described in the CPS and to the adoption of the minimal security measures needed to protect CA's private key. In every case the complete list of accepted liabilities MUST be specified in the CPS.

2.2.2 RA liability

Cf. subsection 2.2.1

2.3 Financial responsibility

With regards to what is stated in subsection 1.3.4, 2.2.1 and section 2.5, no financial responsibility is accepted for certificates issued under this certificate policy.

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

Interpretation of this policy is according to the law of the country where the conforming CA is established. This MUST be detailed in the CPS.

2.4.2 Severability, survival , merger, notice

No stipulation

2.4.3 Dispute resolution procedures

No stipulation

2.5 Fees

2.5.1 Certificate issuance or renewal fees

This policy suggests that no fees are charged for issuing certificates. However the CA MAY charge fees, but this MUST explicitly be stated in the CPS.

2.5.2 Certificate access fees

This policy suggests that no fees are charged for allowing certificate access. However the CA MAY charge fees, but this MUST explicitly be stated in the CPS.

2.5.3 Revocation or status information access fees

This policy suggests that no fees are charged for allowing certificates revocation or status information access.

2.5.4 Fees for other services such as policy information

This policy suggests that no fees are charged for allowing policy and CPS information access.

2.5.5 Refund policy

No stipulation

2.6 Publication and Repository

2.6.1 Publication of CA information

A conforming CA SHALL make available:

- . the policy and CPS it operates according to
- . all issued certificates except those certificates of subscribers that explicitly requested that their certificate SHALL not be made publicly available
- . signed certificate revocation lists

2.6.2 Frequency of publication

Certificates SHALL be published as soon as they are issued. The frequency of CRL publication is specified in 4.4.9. Also policy and CPS SHALL be published as soon as they are updated.

2.6.3 Access control

There SHOULD be no access control to policy, CPS and CRL. There MAY be access control to certificates (for instance to prevent bulk acquisition of data like e-mail addresses or when CA decides to charge fees for certification services).

2.6.4 Repositories

There SHALL exist at least a repository for publishing the information mentioned above.

2.7 Compliance audit

No external audit is REQUIRED, only a self-assessment by the organization operating the conforming CA, that the operation is according to this policy. But any external compliance control is allowed.

Every conforming CA MAY specify in the CPS more detailed information about compliance audit

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

The CA collects personal information about the subscribers (e.g. full name, organization, and e-mail address). These data MUST be processed in a way that ensures privacy protection according to the laws of the country where the CA is established.

2.8.1 Types of information to be kept confidential

All subscribers' information that is not present in the certificate or CRL issued by a conforming CA is considered confidential and SHALL not be released to third parties without explicit subscriber's authorization.

2.8.2 Types of information not considered confidential

Information included in public certificates and CRLs issued by a conforming CA are not considered confidential.

2.8.3 Disclosure of certificate revocation/suspension information

When a certificate is revoked/suspended, a reason code MAY be included in the CRL entry for the action. This reason code is not considered confidential and may be shared with all other users and relying parties. However, no other details concerning the revocation are normally disclosed.

2.8.4 Release to law enforcement officials

A conforming CA will not disclose certificate-related or subscriber personal information to any third party, except when required by law enforcement officials that exhibit a regular warrant.

2.8.5 Release as part of civil discovery

No stipulation.

2.8.6 Disclosure upon owner's request

A conforming CA will not disclose certificate or certificate-related information to any third party, except when required by the owner, with a signed request.

2.8.7 Other information release circumstances

No stipulation.

2.9 Intellectual Property Rights

A conforming CA MUST not claim any IPR on issued certificates. Moreover anybody is allowed to copy from the EuroPKI CPS or policy, provided that a proper reference to the source is given.

3 Identification and authentication

This component describes the procedures used to identify and authenticate a certificate requester to a CA or RA before certificate issuance. It also describes how parties requesting rekey or revocation are

authenticated. This component also addresses naming practices, including name ownership recognition and name dispute resolution.

3.1 Initial Registration

3.1.1 Types of names

The naming attributes of the subscriber to be requested to identify and authenticate the requester depend on the type of certificate that the subscriber requires.

In the choice of the types and format of names used in the fields of the certificate EuroPKI policy is conforming to RFC 2459 [3].

Conforming CA MUST detail in the CPS the types and format of names used.

3.1.2 Need for names to be meaningful

The Subject and Issuer name contained in a certificate MUST be meaningful in the sense that the issuing CA has proper evidence of the existent association between these names and the entities to which they belong .

If an e-mail address is included in the certificate this has not necessarily to follow a semantic rule that could be used to identify person and/or organization.

3.1.3 Rules for interpreting various name forms

Conforming CA MUST detail in the CPS the rules for interpreting various name forms used in the certificates.

3.1.4 Uniqueness of names

The DN MUST be unique for each subject entity certified by the one CA as defined by the issuer name field.

3.1.5 Name claim dispute resolution procedure

Disputes are managed according to the law of the country where the CA is established.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method to prove possession of private key

The adoption of proper method to prove possession of the private key corresponding to the public key being certified is strongly RECOMMENDED.

The method adopted MUST be detailed in the CPS. If a method to prove possession is chosen, conforming CA MUST NOT issue certificate for which the proof of possession fails. This policy discourages generation of private key done by issuing CA as a proof of possession.

3.1.8 Authentication of organization identity

Every time a subscriber requires the inclusion of the name of a certain organization in a certificate, issuing CA MUST have evidence that the organization has completely knowledge about this fact. In order to obtain this result issuing CA MUST require some documents. In all cases suitable legal documents that prove the data to be certified MUST be presented by means of out-of-band methods. The CA or RA MAY perform the authentication. The details MUST be specified in the CPS.

3.1.9 Authentication of individual identity

In many cases public-key certificates constitute a mean to guarantee strong cryptographic authentication of communicating entities. Bearing in mind this premise EuroPKI policy states that authentication of individual identity is REQUIRED. The RECOMMENDED method of authentication requires that individual presents personally to the authenticating CA or RA showing suitable identification documents (e.g. passport, driver's license, government badge etc.). Other methods like videoconference MAY be adopted. If the subject to be certified is a software component the person who submits the request MUST prove that he has the necessary authorization (As an example you can consider the request for the web server www.europki.org: only people directly authorized from who registered the domain europki.org can make such a request). The exact procedure MUST be detailed in the CPS.

3.2 Routine rekey

This policy doesn't mandate any compulsory rekey. After certificate expiration, the CA MAY issue a new certificate both for the same key or for a new key. The rekey authentication MAY be accomplished with the same procedure indicate in section 3.1 for initial registration or using digitally signed requests. These requests MUST be sent to the CA before certificate expiration.

A CA MAY issue more than one certificate for the same key.

3.3 Rekey after revocation

A public key whose certificate has been revoked for private key compromise MUST NOT be re-certified. The public key MAY be re-certified if the revocation is only due to certificate suspension. In the latter case the rekey authentication MAY be accomplished with the same procedure indicated in section 3.1 for initial registration or using digitally signed requests. These requests MUST be sent to the CA before certificate expiration.

3.4 Revocation request

A proper authentication method is required in order to accept revocation request. Conforming CA MUST accept as a revocation request a message digitally signed with a not expired and not previously revoked certificate issued under this policy. The same procedures adopted for the authentication during initial registration are also considered suitable. Alternative procedures MAY be supported such as secure communication of a revocation PIN (Personal Identification Number).

The exact procedures supported MUST be detailed in the CPS.

4 Operational requirements

This component is used to specify requirements imposed upon entities involved in the certification and certificate revocation process.

4.1 Certificate Application

This policy permits two alternatives procedures for certificate application:

- certification of entities done entirely by the CA. The details about this procedure MUST be specified in the CPS
- an entity generates its own key pair and submit public key and other required data to the CA. After that the request MUST carefully follow the procedures detailed in this policy and in the CPS for identification and authentication

4.2 Certificate Issuance

Conforming CA and RA MUST carefully check the compliance and validity of documents presented by the subscribers. After the authentication accomplished by methods specified in section 3.1, CA SHOULD issue the certificate. In the case of issuance CA MUST notify the requester. If for any reasons CA decides not to issue the certificate (even if the checks and the authentication were correct) it SHOULD notify the reason for this choice to the requester.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

Conforming CA is responsible for issuing CRLs and for publishing signed versions. Although [3] doesn't require CAs to issue CRLs, conforming CA MUST issue timely CRLs.

The CA SHALL update its CRL with revoked subject CA certificates.

4.4.1 Circumstances for revocation

A certificate SHALL be revoked when information in the certificate is known to be suspected or compromised. This include situations where:

- . the subscriber's data changed
- . the subscriber's private key is compromised or is suspected to have been compromised
- . the subscriber's information in the certificate is suspected to be inaccurate
- . the subscriber is known to have violated his obligations

4.4.2 Who can request revocation

Conforming CA MUST accept a revocation request made by the holder of the certificate to be revoked. Moreover the revocation request MAY come from the CA that issued the certificate or from associated RA.

Other entities MAY require revocation, presenting evident proof of knowledge of the private key compromise or the change of subscriber's data.

4.4.3 Procedure for revocation request

The entity requesting the revocation SHALL be properly authenticated. The authentication method SHOULD be as strong as the one used in the issuing procedure. Conforming CA MUST accept as a revocation request a message digitally signed with a not expired and not previously revoked certificate issued under this policy. An alternative procedure MAY require the entity to visit RA or CA and to present a viable identity document.

If the entity is a CA, the CA SHALL in addition:

- . Inform subscribers and cross-certifying CAs
- . Terminate the certificate and CRLs distribution service for certificates/CRLs issued using the compromised private key.

4.4.4 Revocation request grace period

The conforming CA decides what is the amount of time necessary to accept the request.

4.4.5 Circumstances for suspension

A CA MAY temporarily suspend a subscriber's certificate if the subscriber requests that service. Unlike revocation, suspension of a user allows for re-enabling at a later time. In every case conforming CA are not required to offer the suspension service.

Information on public keys of disabled users MAY be available from CA repository.

4.4.6 Who can request suspension

In the case that a CA offers the suspension service, CA MUST accept a suspension request made by the holder of the certificate to be suspended.

4.4.7 Procedure for suspension request

The entity requesting the suspension SHALL be properly authenticated. Conforming CA MUST accept as a suspension request a message digitally signed with a not expired and not previously revoked certificate issued under this policy . An alternative procedure MAY require the entity to visit RA or CA and to present a viable identity document.

4.4.8 Limits on suspension period

No stipulation.

4.4.9 CRL issuance frequency (if applicable)

CRLs SHOULD be issued at least every 40 days by conforming CA.

4.4.10 CRL checking requirements

Relying party MUST verify a certificate against the most recent CRL issued from conforming CA in order to validate the use of the certificate.

4.4.11 On-line revocation/status checking availability

Conforming CA MAY support on-line revocation/status checking. Bearing in mind that this policy requires conforming CA to issue CRL, it isn't mandatory to implement on-line revocation/status checking procedures. However this policy suggests taking into consideration OCSP [4] as such a mechanism.

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.

4.5 Security Audit Procedures

This policy recognizes the importance of security audit procedures suggesting that conforming CA specifies all this kind of provisions in the CPS.

4.5.1 Types of event recorded

No stipulation

4.5.2 Frequency of processing log

No stipulation

4.5.3 Retention period for audit log

No stipulation

4.5.4 Protection of audit log

No stipulation

4.5.5 Audit log backup procedures

No stipulation

4.5.6 Audit collection system (internal vs external)

No stipulation

4.5.7 Notification to event-causing subject

No stipulation

4.5.8 Vulnerability assessments

No stipulation

4.6 Records Archival

This section specifies the type of events that are recorded for archival purposes from CA and RA and how this collected data are maintained. For further details not explicitly stipulated here the reference is the CPS.

4.6.1 Types of event recorded

Conforming CA SHOULD archive:

- . certification requests corresponding to actually issued certificates
- . issued certificates
- . issued CRLs
- . all signed agreements with other parties (e.g. RA)
- . document collected from the subscriber during the enrolment procedure
- all relevant messages exchanged with RA

The RAs SHOULD archive:

- . all validation information collected from the subscriber
- all relevant messages exchanged with CA

4.6.2 Retention period for archive

The minimum retention period is 2 years.

4.6.3 Protection of archive

No stipulation

4.6.4 Archive backup procedures

No stipulation

4.6.5 Requirements for time-stamping of records

No stipulation

4.6.6 Archive collection system (internal or external)

No stipulation

4.6.7 Procedures to obtain and verify archive information

No stipulation

4.7 Key changeover

No stipulation.

4.8 Compromise and Disaster Recovery

If a CA's private key is compromised or suspected to be compromised, the CA SHALL at least:

- inform subscribers, cross-certifying CAs and relying parties
- terminate the certificates and CRLs distribution service for certificates/CRLs issued using the compromised private key
- request the revocation of the CA's certificate

If a RA's private key is compromised or suspected to be compromised, the RA SHALL at least inform the CA and request the revocation of the RA's certificate If an entity's private key is compromised or suspected to be compromised, the entity SHALL at least inform the relying parties and request the revocation of the entity's certificate.

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

No stipulation

4.8.2 Entity public key is revoked

No stipulation

4.8.3 Entity key is compromised

No stipulation

4.8.4 Secure facility after a natural or other type of disaster

No stipulation

4.9 CA Termination

Termination of a CA is regarded as the situation where all services associated with a logical CA are terminated permanently.

Before the CA terminates its services the following procedures MUST be completed as a minimum:

- inform all subscribers, cross certifying CA's, higher level CAs, and relying parties with which the CA has agreements or other form of established relations

- make publicly available information of its termination
- stop distributing certificates and CRLs.

A subordinate CA MAY terminate or continue operation as a self-standing CA.

5 Physical, procedural, and personnel security controls

5.1 Physical Controls

Security requirements imposed on the conforming CA are indicated in the CPS. In every case this policy states that CA MUST be run on a dedicated workstation. The workstation MUST be physically secured.

5.1.1 Site locations and construction

No stipulation

5.1.2 Physical access

The physical access to the site in which the CA operates MUST be restricted only to explicitly authorized people.

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

All the issues related to procedural control like the definition of trusted roles MUST be specified in the CPS.

5.2.1 Trusted roles

No stipulation

5.2.2 Number of person 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

The personnel operating the CA MUST be technically and professionally competent. Every conforming CA SHOULD specify in the CPS further details concerning this particular topic and the related issues.

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

This component is used to define the provisions for key management and the corresponding technical security controls.

6.1.1 Key pair generation

Conforming CA's cryptographic keys are generated by the package chosen for certificate handling.

End entities' cryptographic keys are locally generated by their application during the requesting process or by the CA during the enrollment procedure. This policy suggests the adoption of the former procedure for signing key pair to be used for nonrepudiation purposes. The latter procedure MAY be adopted for encryption key pair or bulk authentication key pair.

6.1.2 Private key delivery to entity

The entity MAY generate his own key pair. It is important to notice that in the case of key pair generation done by CA, the key pair MUST be given to the end entity in a secure way. Further details MUST be specified in the CPS.

6.1.3 Public key delivery to certificate issuer

For individual certification, the entity SHALL submit a certification request containing the public key, locally generated, to the CA/RA. Every conforming CA MUST specify in its CPS the procedures for delivering public key.

Conforming CAs MUST support at least PKCS#10 and SPKAC formats, and optionally MAY support other ones. If the public key is not generated by the entity in the presence of the CA/RA staff then the CA SHOULD NOT accept formats that do not provide proof of possession.

6.1.4 CA public key delivery to users

Conforming CA MUST provide mechanisms to deliver CA public key to the users in a trustworthy manner. Further details MUST be specified in the CPS.

In every case CA's public keys MUST be publicly available in a repository accessible via standard protocol such as HTTP or LDAP.

6.1.5 Key sizes

The minimum length of the private key of an end entity to be certified MUST be decided by the CA issuer and MUST NOT be less than the value of 512 bits. It is RECOMMENDED that the key would have a minimum length of 1024 bits.

A CA key pair MUST have a minimum length of 1024 bits. It is RECOMMENDED a length of 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

The keys can be generated in software or in hardware (e.g. on a cryptodevice) depending on the various tools available to the entities.

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

The purposes for which a key can be used MAY be restricted by a CA through the KeyUsage extension in the certificate. This is a field that indicates the purpose for which the certified public key is used.

Certificates issued under this policy MUST have the KeyUsage extension flagged as critical. This means that the certificate SHALL be used only for a purpose for which the corresponding key usage bit is set to one.

CA Certificates

In CA's certificates KeyUsage extension MUST contain the following bits set to one:

digitalSignature - nonRepudiation - keyCertSign - cRLSign

It MAY contain also other bits set to one.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

This policy doesn't mandate the adoption of cryptographic module compliant with pre-determined standards. Every conforming CA MAY give in the CPS more details about the adoption of standard compliant module.

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

The private key of individual MUST NOT be under (n out of m) multi-person control. Only private keys belonging to a CA, a hardware component or a software component MAY be under such a control: in this case the type of control MUST be specified in the CPS.

6.2.3 Private key escrow

This policy discourages the implementation of private key escrow policy both for end entities and CA. Implementation of such policies MAY be permitted if and only if the governing law of the country in which the CA is established explicitly requires them.

6.2.4 Private key backup

This policy suggests that all the parties SHOULD maintain a backup copy of the private key in order to reconstitute it in case of destruction of the key. This backup MUST be carefully protected especially in the case of backup of private key CA.

6.2.5 Private key archival

This policy suggests the implementation of a procedure for private key archival only for private key used for encryption/decryption. Indeed it MAY be necessary to maintain a copy of a private key in order to correctly decrypt messages even if the corresponding public-key certificate is expired.

6.2.6 Private key entry into cryptographic module

The private key of all entities SHOULD be stored in an encrypted form. This provision is particularly important if the entity is a CA.

6.2.7 Method of activating private key

Specific details about how to activate private key SHOULD be found in the CPS. As a general suggestion this policy recommends that for the activation of a private key some specific activation data MUST be entered in the cryptographic module. At least the activation data MUST consist in a PIN or passphrase, but for the most valuable private key (e.g. the ones belonging to CA) the use of hardware tokens or biometrics data is suggested.

6.2.8 Method of deactivating private key

No stipulation

6.2.9 Method of destroying private key

No stipulation

6.3 Other aspects of key pair management

6.3.1 Public key archival

Conforming CA MUST archive all issued certificates. Mechanisms to provide integrity controls other than digital signatures MAY be implemented.

6.3.2 Usage periods for the public and private keys

No stipulation

6.4 Activation data

6.4.1 Activation data generation and installation

Pass phrases or PINs SHALL be selected according to “best practice”. This means that it is necessary to suggest a suitable minimal length for the pass phrases and to enforce mechanisms to check that pass phrases show enough entropy.

6.4.2 Activation data protection

Pass phrases protecting private keys SHALL be accessible only to the legitimate users (e.g. certificate holder for personal certificates, CA operators for CA signing keys, etc). An exception for this indication is the implementation of a secure archival/backup mechanism for activation data. Such a mechanism MUST be clearly defined in the CPS.

6.4.3 Other aspects of activation data

No stipulation

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

No stipulation

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

No stipulation

6.6.3 Life cycle security rating

No stipulation

6.7 Network security controls

This policy strongly suggests that the machine on which the cryptographic module used for CA operations SHOULD be kept off-line to prevent network attacks. In every case network access to the CA workstation MUST be limited in order to protect the CA's private key in an appropriate way from disclosure

6.8 Cryptographic module engineering controls

No stipulation

7 Certificate and CRL profiles

7.1 Certificate Profile

In order to promote interoperability this policy strongly encourages conforming CA to issue certificates profiling them accordingly to [3]. In every case CPS MUST detail the specific profile adopted.

7.1.1 Version number(s)

The version field in the certificate SHALL be at least 2, that is a conforming CA MUST issue X.509 certificates version 3 or higher.

7.1.2 Certificate extensions

In compliance with [3], the inclusion of the following certificate extensions is RECOMMENDED:

Extension name	Extension Value
SubjectKeyIdentifier	NOT CRITICAL
AuthorityKeyIdentifier	NOT CRITICAL
BasicConstraints	CRITICAL
KeyUsage	CRITICAL
CertificatePolicies	NOT CRITICAL

It is also RECOMMENDED the use of other two extensions: CRLDistributionPoint for providing information useful to retrieve the CRL, and SubjectAltNames when there is the need to include an RFC822 e-mail address to a certificate. Both these two extensions SHOULD be marked as NOT CRITICAL.

7.1.3 Algorithm object identifiers

No stipulation

7.1.4 Name forms

All related issues MUST be specified in the CPS

7.1.5 Name constraints

All related issues MUST be specified in the CPS

7.1.6 Certificate policy Object Identifier

Other certificate policy object identifiers are applicable if and only if the other policies identified are compliant with this policy. Conforming CA MUST contact the maintainers of the various policies to verify the level of mutual compliance. However in order to promote interoperability, following RFC 2459, this policy suggests to include only one certificate policy object identifier in a certificate.

7.1.7 Usage of policy constrains extension

All related issues MUST be specified in the CPS

7.1.8 Policy qualifiers syntax and semantics

The Certificate Policies extension field has a provision for conveying, along with each certificate policy identifier, additional policy-dependent information in a qualifier field.

This policy suggests that the qualifier field SHOULD be a CPS Pointer qualifier that contains a pointer to a Certification Practice Statement (CPS) published by the CA.

The pointer is in the form of a uniform resource identifier (URI).

7.2 CRL Profile

7.2.1 Version number(s)

The version field in the CRLs SHALL be at least 1, that is a conforming CA MUST issue X.509 CRLs version 2 or higher.

7.2.2 CRL and CRL entry extensions

No stipulation.

8 Specification administration

8.1 Specification change procedures

Editorial changes can be made to the policy and CPS. In case of substantial changes of the policy all CAs and users SHALL be notified in advance. Moreover all CAs SHALL update the policy in accordance with the policy changes at upper levels if needed.

Policy changes that imply minor technical adjustments SHALL be notified in advance.

8.2 Publication and notification policies

This policy is available via Web at the URI http://www.europki.org/ca/root/cps/

8.3 CPS approval procedures

Conforming CA MUST be evaluated for compliance with this policy. In order to obtain CPS approval conforming CAs MAY submit their CPS to the contact people specified in section 1.4.3. After that, a conforming CA MUST wait for the answer. The time limit for completing the evaluation is established in 60 days. It might be acceptable that a conforming CA self-certify its own compliance with the policy; in this case, if later non-compliance with the policy is reported to EuroPKI, then the CA certificate SHALL be revoked.

APPENDIX 1: Glossary

Certification Authority (CA) - An authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user's keys. It is important to note that the CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.

CA-certificate - A certificate for one CA's public key issued by another CA.

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 path - An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

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

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

Issuing certification authority (issuing CA) - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Public Key Certificate (PKC) - 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.

Public Key Infrastructure (PKI) - The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke PKCs based on public-key cryptography.

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). [Note: The term Local Registration Authority (LRA) is used elsewhere for the same concept.]

Relying party (RP) - A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Subject certification authority (subject CA) - In the context of a particular CAcertificate, the subject CA is the CA whose public key is certified in the certificate

IPR – Intellectual Property Rights

Appendix 2: Key words for use in RFCs to Indicate Requirement Levels

According to RFC 2119 [2] “Key words for use in RFCs to Indicate Requirement Levels”, we specify how the main keywords used in RFCs should be interpreted.

Authors who follow these guidelines should incorporate this phrase near the beginning of their document:

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHAL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1. **MUST** This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. **MUST NOT** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. **SHOULD** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. **SHOULD NOT** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

5. **MAY** This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

References

[1] RFC 2527 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” March 1999 [ftp://ftp.isi.edu/in-notes/rfc2527.txt]

[2] RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels” March 1997 [ftp://ftp.isi.edu/in-notes/rfc2119.txt]

[3] RFC 2459 “Internet X.509 Public Key Infrastructure: Certificate and CRL Profile” January 1999 [ftp://ftp.isi.edu/in-notes/rfc2459.txt]

[4] RFC 2560 “Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol – OCSP” June 1999 [ftp://ftp.isi.edu/in-notes/rfc2560.txt]