European Patent Office Certification Practice Statement

Version 1.10

Effective date: 1 January 2011

European Patent Office
Bayerstrasse 35
80335 München
Germany
Tel.: +31 (0)70 340 4500
http://www.epo.org

European Patent Office Certification Practice Statement

Revision date: 16 May 2011

Published by
European Patent Office (EPO)

The EPO is the executive body of the European Patent Organisation, which has its headquarters at Erhardtstrasse 27, 80469 Munich, Germany and is represented by the President of the EPO.

Contact
Enquiries about this Certification Practice Statement (CPS) should be addressed to eBusiness User Support, European Patent Office, Bayerstrasse 35, 80335 München, Germany, e-mail: support@epo.org.

Copyright
Unless otherwise stated (e.g. that use is restricted or subject to prior permission), the reproduction of any part of the information in this document is authorised, provided that no changes are made to the data and that the source is acknowledged.

Logo
The EPO's official logo is protected worldwide as an emblem of an international organisation under the Paris Convention for the Protection of Industrial Property.

Disclaimer
This document details certain services which are limited in scope and available for a specific user group. Certain limitations of liability apply as detailed herein.

The EPO cannot guarantee that the wording of the legal provisions in this document is identical to the wording of the officially adopted text. The authentic text of the European Patent Convention (EPC) and its constituent parts is that of the printed version of the EPC published by the EPO, and, where appropriate, the text of amendments thereto as published in the printed version of the EPO's Official Journal.

This disclaimer is not intended to limit the EPO's liability in contravention of the relevant provisions of the EPC or of national law to which the EPC and this document refer.

Miscellaneous
Nothing in the foregoing is to be understood as waiving the European Patent Organisation’s privileges and immunities as an international organisation, in particular those conferred by the Protocol on Privileges and Immunities of the European Patent Organisation dated 5 October 1973.

Subject to the legal provisions in force, the EPO reserves the right to modify, in full or in part and without prior notice, the services and information described in this document.

Document control

Amendment history

Version	Date	Description
1.00	01 March 2008	Document released
1.10	16 May 2011	Document updated following revision of legal instruments and organisational changes

TABLE OF CONTENTS

GLOSSARY

Certificate	[Annex F] A certificate binds an entity's name (and other additional attributes) with the corresponding public key. A certificate must comply with ITU Recommendation X.509 version 3 and at a minimum must: ■ contain a public key that corresponds to a private key under the sole control of the subject ■ name or otherwise identify its subject ■ identify the CA issuing the certificate ■ identify the validity period ■ contain a certificate serial number ■ include end-entities' e-mail addresses ■ be digitally signed by the CA issuing the certificate
Certificate Policy	[RFC 2527] 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.
Certificate requester	A person who applies for a smart card containing Subscriber certificates in order to access the EPO's secure services. Once approved by the EPO this person is referred to as a Subscriber.
Certificate Authority (CA)	[Annex F] A CA is a trusted party that issues and revokes public key certificates for a user community. The CA is responsible for verifying the information appearing on the public key certificates. A CA is supported by CA servers, or computer systems, and the policies and procedures surrounding the operation of these servers. The term "server" refers specifically to the hardware and software that actually generates certificates and CRLs.
Certificate revocation list (CRL)	[Annex F] A time-stamped list of revoked certificates that has been digitally signed by a CA.
Certification Practice Statement (CPS)	[RFC 2527] A statement of the practices which a CA employs when issuing certificates.
Compromise	[Annex F] The unauthorised disclosure, modification, substitution or use of sensitive plain text cryptographic keys and other critical security parameters.

Cryptographic module	[Annex F] The set of hardware, software and firmware, or some combination thereof, that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Distinguished name	[Annex F] The unique name of each certificate holder or Subscriber. Each entity in the PKI domain must have a clearly distinguishable and unique distinguished name, or DN, in the certificate subject name field.
EPO	European Patent Office
Low-level certificate	[Annex F] A digital certificate which has been issued to the applicant, for example as part of the registration of the online filing client, or obtained from a certification authority, and which identifies the applicant without prior verification of the applicant's identity.
Object identifier	[Annex F] A specially formatted number that is registered with an internationally recognised standards organisation. It can, and should, be used to identify an organisation's suite of PKI policy and practice documents.
Private key	[Annex F] In public key cryptography, the private key is the portion of a public–private key pair owned by a user that is known only to that user. A user's private key is used to digitally sign data and to decrypt data that was encrypted with the user's public key.
Public key	[Annex F] In public key cryptography, the public key is the portion of a public–private key pair owned by a user that is made known to others in the user community via a public key certificate. A user's public key is used by others to encrypt data for that user and is used by others to verify the user's digital signature.
Public key infrastructure domain	[Annex F] An independent entity consisting of one or more Certificate Authorities where Subscribers hold the same anchor or root certificate.

Registration Authority	[Annex F] An entity responsible for identification and authentication of certificate subjects, but not for signing or issuing certificates (i.e. a Registration Authority, or RA, is delegated certain tasks related to identity-proofing on behalf of a CA). The RA may delegate functions and corresponding authority to local registration authorities.
Relying Party	[RFC 2527] A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.
Repository	[Annex F] A system for storing and retrieving certificates and other information relating to the certificates.
Revocation of a certificate	[Annex F] Prematurely ending the operational period of a certificate from a specified time onwards.
Smart card	A storage medium for subscriber private keys and subscriber certificates.
Subscriber	[Annex F] The entity who is the natural person named or otherwise identified in a certificate issued to that person and who holds a private key that corresponds to a public key listed in the certificate.

Abbreviations

Annex F	Annex F, Appendix II to PCT - PKI Architecture for the e-PCT Standard, as in force from 1 October 2005
CA	Certificate Authority
CA for the EPO	Certificate Authority for the European Patent Office
CDS	Client data system
CMS	Card management system
CN	Certificate common name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate revocation list
DN	Certificate distinguished name
EPC	European Patent Convention
EPO	European Patent Office
EPO PKI	European Patent Office public key infrastructure
FREP	Filing representative
PCT	Patent Cooperation Treaty
PKI	Public key infrastructure
RA	Registration Authority
RA for the EPO	Registration Authority for the European Patent Office

References

In this EPO Certificate Practice Statement, reference is made to the following documents:

[Annex F] WIPO, Patent Cooperation Treaty, Administrative Instructions under the Patent Cooperation Treaty: Modifications relating to the Electronic Filing and Processing of International Applications, Annex F, Appendix II - PKI Architecture for the e-PCT Standard, as in force from 1 October 2005

[RFC2527] Network Working Group, Internet X.509 Public Key Infrastructure, Request for Comments: 2527, Certificate Policy and Certification Practices Framework, March 1999

[EPC] Convention on the Grant of European Patents (European Patent Convention) of 5 October 1973 as amended by the act revising Article 63 of the European Patent Convention of 17 December 1991 and the Act revising the European Patent Convention of 29 November 2000.

[CP] European Patent Office Certificate Policy

[RPA] Relying Party Agreement

[SA] Subscriber Agreement

1. INTRODUCTION TO THE EUROPEAN PATENT OFFICE CERTIFICATION PRACTICE STATEMENT

1.1 Overview

This Certification Practice Statement (CPS) complements the European Patent Office Certificate Policy (CP). Both documents support the European Patent Office public key infrastructure (EPO PKI) and follow the format proposed in RFC 2527.

Whereas the CP describes the requirements of the EPO PKI, the CPS expands upon the CP and describes the practices which the EPO employs for the issuance, use and revocation of Subscriber certificates within the EPO PKI to meet the requirements set out in the CP.

The content of some sections of the CP has been repeated in the CPS. This occurs where the CP content does not require further expansion or clarification in the CPS. To help with identification, this repeated content has been italicised in the CPS.

1.1.1 The European Patent Office and its online services

The European Patent Office (EPO) is the executive organ of the European Patent Organisation. It was established by the European Patent Convention (EPC) and has administrative and financial autonomy. It grants European patents using a unitary and centralised procedure (Article 4 EPC). The EPO also performs tasks under the Patent Cooperation Treaty (PCT) on the basis of Part X of the EPC.

The EPO has designed a range of online products and services to allow patent applicants, attorneys and other users to conduct their business with the EPO electronically.

1.1.2 Secure communications with the EPO

While a number of these products and services are available to the general public without registration, a secure environment is also provided in which permitted users can conduct secure electronic communication with the EPO.

Typically, these permitted users may be applicants or representatives (professional representatives, employees of representative firms, legal practitioners) (see Articles 133 and 134 EPC).

To facilitate the secure services it offers, the EPO provides the European Patent Office Public Key Infrastructure (EPO PKI) to permitted users. As part of this infrastructure, the Certificate Authority for the European Patent Office (CA for the EPO) issues Subscriber certificates to the permitted users.

This practice statement, known as the EPO Certification Practice Statement (CPS), describes the practices which the EPO employs for the issuance, use and revocation of Subscriber certificates within the EPO PKI.

1.1.3 Secure communications between permitted users and other industrial property institutions

In addition to the above, the EPO makes available under specific legal and other arrangements the use of its online services for the same purpose between other national and international organisations and institutions entrusted with the task of processing patent applications and permitted users.

Provided applicable conditions and requirements are fulfilled, the EPO PKI may therefore also be made available to applicants, their representatives and other permitted users for secure communications with other national and international organisations and institutions entrusted with the task of processing patent applications.

1.1.4 General description of the EPO PKI

The EPO PKI consists of the following components:

- *a certificate authority (the CA for the EPO), including a certificate revocation repository*
- *a registration authority (the RA for the EPO)*
- *subscribers*

Subscribers are permitted users as described in sections 1.1.2 and 1.1.3. Subscriber certificates are certificates that are issued on a smart card to applicants, their representatives (Articles 134(1),(8); 133(3) EPC) and any other user who needs to communicate with the EPO in electronic form as described in 1.1.1 above.

Subscriber certificates are issued at the discretion of the EPO to natural persons only and, in accordance with Annex F, are defined as 'low-level certificates'. See also section 3, Identification and authentication, and section 7, Certificate and certificate revocation list (CRL) profiles.

Subscriber certificates may be relied on by those Relying Parties as further detailed in the CP.

Although the EPO retains the responsibility, as defined in the CP, for all matters relating to the EPO PKI, for certain elements of the operation of the EPO PKI, the EPO has contracted out services, including the management and administration of the CA for the EPO services and the handling of the issuing of smart cards, to third parties.

1.1.5 Legal basis for the EPO PKI

The legal basis for the electronic filing of European patent applications, international (PCT) applications and other documents with the EPO and with the competent national authorities where so permitted is provided in Rule 2 EPC and Rule 89bis. 1 and 2 PCT.

Based on the above legal basis, the Decision of the President of the European Patent Office dated 12 July 2007 concerning the electronic signatures, data carriers and software to be used for the electronic filing of patent applications and other documents (Special Edition No. 3, OJ EPO 2007, A5), the Decision of the President of the European Patent Office dated 26 February 2009 concerning the electronic filing of documents (OJ EPO 2009, 182) and the Decision of the President of the European Patent Office dated 8 February 2010 concerning the EPO Online Filing software to be used for the electronic

filing of documents (OJ EPO 2010, 226), provide stipulations regarding such electronic filings, including the use of electronic signatures.

The EPO PKI meets the requirements set forth in Part 7 and Annex F of the Administrative Instructions under the PCT regarding electronic filing and processing of international applications. The documents associated with the EPO PKI derive, where applicable, their content and definitions from these sources.

The legal basis for electronic communications by the Subscriber with other designated parties depends on the applicable rules and regulations for communications with such parties and must be obtained from them.

1.2 Identification

The title of this document is the European Patent Office Certification Practice Statement.

A unique document identifier (object identifier) has not been assigned to this document.

1.3 Community and applicability

The EPO provides services as a CA to Subscribers. In order to provide these services, the EPO maintains the EPO PKI, which consists of several technical components.

This section contains a description of the components of the EPO PKI and describes the applicability of the certificates issued within the EPO PKI.

1.3.1 Certificate Authorities (CA)

The CA active within the EPO PKI is the CA for the European Patent Office (CA for the EPO). This CA for the EPO issues all Subscriber certificates.

The certificate of the CA for the EPO has been certified by the CA for the European Patent Organisation. This latter root CA may issue certificates for subordinate EPO CAs if required.

1.3.2 Registration Authority (RA) for the EPO

The RA for the EPO is responsible for the identification and authentication of certificate requesters within the EPO PKI.

1.3.3 Subscribers

Subscribers are natural persons who use the certificates and private keys generated within the EPO PKI and stored on a smart card.

The CA for the EPO distinguishes between two different groups of Subscriber:

- Subscribers who, at the time of application for a smart card, are known to the EPO as registered parties with an assigned FREP number, e.g. professional representatives, employees of professional representatives, legal practitioners. These Subscribers may access all the EPO's online services.

- Subscribers who, at the time of application for a smart card, are unknown to the EPO, e.g. first-time applicants or representatives. These Subscribers are able to access the Online Filing application only.

1.3.4 Relying Parties

1.3.4.1 EPO

The EPO shall be a Relying Party in respect of the CP.

1.3.4.2 Receiving Office

Other entities may be Relying Parties, provided that they qualify under the PCT as a receiving Office (see Article 10 PCT), and that as a receiving Office they have notified the International Bureau (see Section 703 Administrative Instructions) that they are prepared to receive international applications in electronic form and indicate, amongst others, that they accept the CA for the EPO for the issuance of certificates for the purpose of the electronic signature required to be used with the international filing (see Section 710(a) under (vi) Administrative Instructions).

The International Bureau is required to publish the notification referred to above (see Section 710(c) Administrative Instructions).

The scope of the Relying Party's entitlement under the above parameters to rely on certificates issued by the CA for the EPO is restricted to the PCT-related actions for which an electronic signature is required. Enlargement of the Relying Party's scope of entitlement to rely on certificates requires a legal basis in addition to the present paragraph.

1.3.4.3 Central industrial property office

Other entities may be Relying Parties, provided that they operate as the central industrial property office of either an EPC contracting state or a state which is not a party to the EPC but which has been designated by the EPO as a Relying Party. For this purpose, the EPO may where applicable set requirements and conditions to be fulfilled by the central industrial property office concerned.

1.3.4.4 Intergovernmental organisations

Certain entities which operate as intergovernmental organisations entrusted with the task of granting patents may be Relying Parties, provided that the EPO has designated them as such. For this purpose, the EPO may where applicable set requirements and conditions to be fulfilled by the intergovernmental organisation concerned.

1.3.5 Applicability

The EPO smart card contains two types of Subscriber certificate: authentication certificates, with which Subscribers can authenticate themselves to a network environment, and non-repudiation certificates, with which Subscribers can apply an electronic signature to a document.

Subscriber certificates may only be used in connection with services provided by the EPO or a Relying Party.

1.4 Contact details

1.4.1 Certification Practice Statement administration

The EPO's Security and Audit directorate is responsible for maintenance of the CPS document.

1.4.2 Contact for enquiries

Copies of this document can be downloaded from http://www.epo.org/applying/online-services/security/smart-cards.html for EPO-Smartcards.
In addition, enquires may be addressed to,eBusiness User Support, European Patent Office, Bayerstrasse 35, 80335 München, Germany, Tel.: +31 (0)70 340 4500, e-mail: support@epo.org

1.4.3 Body determining CPS suitability for the policy

The body which determines whether the CPS complies with the CP is named in section 1.4.1, Certification Practice Statement administration.

1.5 Entry into force/transitional law

The CPS entered into force on the date indicated on the cover page as the effective date.

The release date as mentioned in the CPS is the date on which the current version of the CPS was released and made available for publication in accordance with section 2.6.

In the event that the effective date is earlier than the release date, this section 1.5 confirms that the stipulations of the CPS apply to the EPO PKI as from that effective date.

Unless stipulated otherwise in the CPS, the latest version of the CPS will be the applicable practice statement and will therefore also apply to all certificates issued before its effective date.

Any further revisions of the CPS will take effect for the operation of the EPO PKI as from the effective date indicated on the revised document.

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA for the EPO obligations

The CA for the EPO shall perform the specific obligations as required by the CP and/or by related documentation based on the CP, including the CPS. Amongst other obligations the CA for the EPO shall:

- *act in accordance with the terms of the CP and the applicable CPS.*
- *take reasonable measures to ensure that its own private key remains confidential and provide a secure environment to control its use and access.*
- *provide access to the CP for permitted users of the EPO PKI.*
- *issue Subscriber certificates to Subscribers upon receipt of a valid request from the RA for the EPO, in accordance with the terms of the CPS.*
- *revoke Subscriber certificates when in receipt of a valid revocation request, and inform the Subscriber of the revocation, in accordance with the terms of the CP.*
- *post issued Subscriber certificates to the appropriate repository (note: access to this repository is restricted to authorised parties).*
- *generate key pairs for Subscribers on the smart card, forward Subscriber certificate requests for certification, return the Subscriber certificate to the smart card and mail the Subscriber the smart card and PIN of the smart card.*
- *generate a CRL and publish the CRL in the appropriate repository.*

2.1.2 RA for the EPO obligations

The RA for the EPO shall perform the specific obligations as required by the CP and/or by related documentation based on the CP, including this CPS. Amongst other obligations the RA for the EPO shall:

- *act in accordance with the terms of the CP and the applicable CPS.*
- *ensure that certificate requests are valid.*
- *receive and process applications for Subscriber certificates.*
- *receive revocation requests from authorised parties (section 4.4.2), make reasonable enquiries to establish the validity of these requests, and forward validated requests to the CA for the EPO.*
- *inform the Subscriber and the CA for the EPO of the revocation of the Subscriber certificate.*

2.1.3 Subscriber obligations

The Subscriber shall perform the specific obligations as required by the CP and/or by related documentation based on the CP, including the CPS and, where applicable, the Subscriber Agreement. Amongst other obligations the Subscriber shall:

- *ensure that the public and private keys and Subscriber certificates are only used in accordance with the terms of the CP.*
- *provide accurate and complete information when requesting a certificate.*
- *ensure that the private key and PIN protecting the smart card which stores the private key are protected at all times against loss, disclosure to any unauthorised party, modification and unauthorised use in accordance with the CP.*
- *ensure that knowledge of the Subscriber PIN is restricted to the Subscriber.*

- *submit a revocation request to the RA for the EPO immediately in the event of an actual or suspected compromise of the private keys, PIN or smart card, or any change to the information provided as part of the certificate application*.

2.1.4 Relying Party obligations

The Relying Party shall perform the specific obligations as required by the CP and/or by related documentation based on the CP, including the CPS and, where applicable, a Relying Party Agreement. Amongst other obligations the Relying Party shall:

- *independently assess the appropriateness of the use of a certificate for any given purpose and determine that the certificate will, in fact, be used for an appropriate purpose.*
- *check for certificate revocation or suspension prior to accepting verification of a certificate.*

2.1.5 Repository obligations

The EPO shall be responsible for the repository functions of the CA for the EPO. Upon revocation of a Subscriber certificate the CA for the EPO shall publish a notice of revocation in the revocation repository.

2.2 Liability

2.2.1 Scope of the EPO's liability

2.2.1.1

By operating the EPO PKI, especially by signing a certificate which indicates the use of the CP, the EPO shall ensure, to all who reasonably rely (see 1.3.4) on the information contained in the certificate, only that its certification and repository services, issuance and revocation of certificates, and issuance of CRLs are in accordance with the CP. The EPO shall be restricted to making reasonable efforts to ensure that the Subscribers and Relying Parties follow the requirements of the CP when dealing with any certificates containing a reference to the CP or the associated keys (see 2.2.4).

2.2.1.2

The EPO shall not be liable for any consequences arising from any use of certificates issued under the CP other than for communications between the EPO and permitted users (see 1.1.2 and 1.3.4.1). The EPO shall not be liable for the use of certificates issued under the CP for communications between permitted users and other industrial property institutions or any other third parties (see 1.1.3 and 1.3.4.2 / 1.3.4.3 / 1.3.4.4). This shall not prejudice the liability, if any, of Relying Parties towards the Subscribers concerned.

2.2.2 Limitation of liability

2.2.2.1

The availability of the EPO PKI may be affected by system maintenance or repair, or factors outside the control of the EPO. The EPO therefore disclaims any liability for non-availability of the EPO PKI.

2.2.2.2

Claims for damages are excluded unless the EPO has caused the damage wilfully or through gross negligence, or the damage consists of an injury to life, limb or health, or the

obligation breached is of a fundamental nature. In the latter case, if the claimant is not a consumer (within the meaning of Article 13 of the German Civil Code), the EPO's liability shall be limited to typical and foreseeable damages.

2.2.3 The law governing the EPO's liability

Without prejudice to the governing law provision (2.4.1), liability claims against the EPO shall be governed by Article 9 EPC. For the purposes of the application of Article 9(1) and (2) EPC, the applicable law shall be German law.

2.2.4 Subscriber and Relying Party liability

Subscriber Agreements and Relying Party Agreements shall reflect the EPO's limited liability as laid down in section 2.2 of the CP, and these agreements shall, where applicable, require Subscribers/Relying Parties to warrant that they comply with the obligations set out in sections 2.1.3 and 2.1.4 respectively.

2.3 Financial responsibility

2.3.1 Indemnification by Relying Parties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall require Subscribers/Relying Parties to indemnify the EPO for any consequences resulting from failure to comply with the requirements laid down in such agreements or elsewhere in the EPO PKI documentation.

2.3.2 Fiduciary relationships

The issuance of certificates shall not make the CA for the EPO an agent, fiduciary, trustee or other representative of Subscribers or Relying Parties.

2.3.3 Administrative processes

No stipulation.

2.4 Interpretation and enforcement

2.4.1 Governing law

2.4.1.1 Governing law

The governing law shall be as laid down in the European Patent Convention and the rules and regulations based thereon. The PCT, the rules and other regulations based thereon are applicable to the extent foreseen in or under the EPC or in the CP. Subsidiarily, German law shall apply, to the exclusion of recourse to the German law of conflicts.

This governing law provision shall apply to the CP and other documents relating to the EPO PKI based on the CP, such as the CPS, Subscriber Agreements and Relying Party Agreements, unless indicated otherwise in such documents.

This governing law provision shall not preclude the applicability of other national law provisions in the relationship between Relying Parties on the one hand and Subscribers on the other hand. The latter sentence does not apply to the EPO.

This governing law provision is based on the principle that uniform procedures and interpretation must be ensured for all parties involved in the EPO PKI, no matter where they are located.

2.4.1.2 Privileges and immunities accorded to the EPO

The CP shall be interpreted in such a way that the rights of the European Patent Organisation as described in the EPC, including the Protocol on Privileges and Immunities of the European Patent Organisation, signed in Munich on 5 October 1973, are in all cases preserved.

2.4.2 Miscellaneous

In the event that any one or more of the provisions of the CP shall for any reason be held to be invalid, illegal or unenforceable at law, such unenforceability shall not affect any other provision, but the CP shall then be construed as if such unenforceable provision or provisions had never been contained herein and, insofar as possible, construed to maintain the original intent of the CP.

No term or provision of the CP may be amended, waived, supplemented, modified or terminated, except in accordance with the procedures as set forth in the CP.

Any notice, consent, request or other communication by the CA for the EPO under the CP shall be in paper or electronic form.

2.4.3 Dispute resolution procedures

If a dispute arises in connection with the operation of the EPO PKI, the CP, the CPS or any other document relating to the EPO PKI, the parties shall undertake in good faith to use all reasonable endeavours to settle the dispute by negotiation.

Any dispute arising out of or in connection with the operation of the EPO PKI and in which the EPO is a party shall be finally settled by binding arbitration with one single arbitrator in accordance with the provisions of the German Code of Civil Procedure (ZPO). The venue for arbitration shall be Munich.

Notwithstanding the aforementioned, if the EPO waives its immunity from national jurisdiction, the courts of Munich shall have jurisdiction for any such dispute.

Where under applicable patent law an event arising out of the operation of the EPO PKI allows a party to seek resolution, the judicial means provided there under shall take precedence over the above-indicated dispute resolution procedures. Section 2.4.1.2 applies.

Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause, which shall include the above-mentioned principles unless specific circumstances necessitate deviation there from.

2.5 Fees

The fees for Subscribers and Relying Parties for using the EPO PKI, performing certificate management actions, using the smart card and any other component or service mentioned

in the CP or the CPS, shall be included in the fees for the services rendered by the EPO or mentioned separately.

2.5.1 Certificate issuance or renewal fees

Smart cards, certificates and supporting software shall normally be available to Subscribers free of charge. However, the EPO reserves the right to charge a fee under certain circumstances.

2.5.2 Certificate access fees

The EPO shall not normally charge a fee for making certificates available to Relying Parties.

2.5.3 Revocation or status information access fees

Revocation information shall be available free of charge.

2.5.4 Fees for other services such as policy information

The EPO shall not charge a fee for access to policy information such as that in the CP or the CPS.

2.5.5 Refund policy

No stipulation.

2.6 Publication and repository

2.6.1 Publication of CA for the EPO information

The EPO shall publish (as a minimum by means of a website accessible via the Internet) the following information:

- *EPO Certificate Policy*
- *EPO Certification Practice Statement*
- *CA for the European Patent Organisation certificate (root certificate)*
- *Relying Party Agreement*
- *Subscriber Agreement*
- *CA for the EPO certificate*
- *CRL repository*

2.6.2 Frequency of publication

The CA for the EPO shall publish the information stipulated in section 2.6.1 above as soon as said information becomes available to it.

2.6.3 Access controls

The CA for the EPO shall control access to its repositories to prevent the updating or deletion of the information they contain by any other party.

2.6.4 Repositories

The CA for the EPO shall maintain repositories for the publication of Subscriber certificates, CRLs and documents relating to the EPO PKI.

2.7 Compliance audit

2.7.1 Frequency of entity compliance audit

The EPO shall carry out periodic and ad hoc inspections and audits of its site and operations to check that they are functioning in accordance with the security practices and procedures set forth or referenced in its CPS. It shall also contract with an external auditor to conduct an independent annual audit.

2.7.2 Identity/qualifications of auditor

An external auditor shall conduct an independent audit once a year. The auditor shall be an employee of a competent professional firm that complies with appropriate national and international standards and codes of practice.

2.7.3 Auditor's relationship to audited party

The performance and reporting of the audit shall be governed by a contract between the auditor and the audited party.

2.7.4 Topics covered by audit

The audit shall determine the compliance of EPO PKI systems and processes with the EPO CP and CPS. It shall determine the business risks of non-compliance with the CP and CPS in accordance with the identified control objectives.

2.7.5 Actions taken as a result of deficiency

The EPO shall take such action as it deems necessary and appropriate to resolve deficiencies resulting from the audit.

2.7.6 Communication of results

The EPO shall be responsible for operating the EPO PKI in accordance with the applicable requirements and controls. The detailed audit report will therefore be issued to the EPO only.

2.8 Confidentiality

2.8.1 Types of information to be kept confidential

- *The EPO shall protect the contents of any certificate application or revocation request, whether successful or unsuccessful, as confidential to the CA for the EPO and the Subscriber/requester, except in the circumstances mentioned in 2.8.2 to 2.8.7.*
- *The EPO shall keep detailed security and operations documentation confidential to Subscribers and Relying Parties. The EPO shall, however, disclose these documents to the appointed auditor on request.*

2.8.2 Types of information not considered confidential

The EPO shall not consider any information contained in a certificate, CRL or the CP as confidential.

2.8.3 Disclosure of certificate revocation/suspension information

CRL contents as well as the individual status of any certificate shall be freely disclosed to any Relying Party.

2.8.4 Release to law enforcement officials

The EPO shall be entitled to disclose information it holds in its capacity as CA or RA or otherwise in connection with the execution of the EPO PKI, to the extent that such disclosure is allowed by the law governing the CP, and is based on verifiable and appropriate legal instruments (such as court orders). The aforementioned shall be without prejudice to the EPO's privileges and immunities.

2.8.5 Release as part of civil discovery

The EPO shall be entitled to disclose any confidential information relating to a particular Subscriber as required by civil discovery to the extent that such disclosure is allowed by the law governing the CP, and is based on a verifiable and appropriate legal basis. The aforementioned shall be without prejudice to the EPO's privileges and immunities.

2.8.6 Disclosure upon owner's request

The EPO shall undertake to disclose to a Subscriber on request any confidential information relating to that Subscriber.

2.8.7 Other information release circumstances

No stipulation.

2.9 Intellectual property rights

All intellectual property rights relating to Subscriber certificates and the CP belong to and shall remain the property of the EPO.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial registration

3.1.1 Types of name

The CA for the EPO uses the X.501 distinguished names in the issuer and subject fields as shown in Table 1:

Attribute	Value
Country (C)=	NL
Organisation (O)=	European Patent Office
Organisational Unit (OU)=	Not used
State or Province (S)=	Not used
Locality (L)=	Not used
Common Name (CN)	European Patent Office CA

Table 1 - Distinguished name attributes in the CA for the EPO certificate

Subscriber certificates issued by the CA for the EPO contain an X.501 distinguished name in accordance with section 7.1

3.1.2 Need for names to be meaningful

The RA for the EPO shall ensure that the set of attributes uniquely identifies each Subscriber and has meaningful values by adding a unique four-digit ID.

3.1.3 Rules for interpreting various name forms

No stipulation.

3.1.4 Uniqueness of names

The CA for the EPO shall allocate the set of names according to 3.1.1 and 3.1.2 in such a way that they are unambiguous. The CA for the EPO shall reject certificate applications where the name does not sufficiently distinguish the certificate requester from an existing Subscriber's DN.

3.1.5 Name claim dispute resolution procedure

The CA for the EPO shall resolve any disputes that may arise over the allocation of names by allocating a unique number to each certificate requester, thereby ensuring that the CN, and therefore the DN, is always unique.

3.1.6 Recognition, authentication and role of trade marks

The CA for the EPO shall not be required to seek any evidence of trade marks.

3.1.7 Method to prove possession of private key

Not applicable as Subscriber keys are generated by the CA for the EPO.

3.1.8 Authentication of organisation identity

The RA for the EPO shall check whether the applicant's organisation is included in the EPO's Client Data System (CDS).

3.1.9 Authentication of individual identity

Where the EPO has already assigned an FREP number to a new Subscriber, the identity of the requester shall be authenticated by the RA for the EPO by means of a check on the credentials of the Subscriber in the CDS.

Where the applicant has no reference in the CDS, his identity must be authenticated by the RA for the EPO by means of a check on the following credentials:

- first name(s)
- surname
- address
- e-mail address
- passport or ID card
- signature of Subscriber on faxed enrolment form

The RA for the EPO shall validate the certificate request by uploading the 'new Subscriber file' into the card management system.

3.2 Routine rekey

If a Subscriber's certificates have not been revoked, sixty days before the expiration of the certificate the CA for the EPO shall send him an e-mail inviting him to renew his certificates. The Subscriber will be directed to the enrolment web page and, once his identity has been verified, he will be able to request new certificates. The Subscriber's identity shall be verified using his current certificate.

The CA for the EPO shall generate new keys on a new smart card and send the Subscriber the new smart card with the certificates together with an acceptance letter. The Subscriber shall return the acceptance letter to the RA for the EPO and, upon receipt, the CA and RA for the EPO shall take action to activate the certificates.

3.3 Rekey after revocation

The identification and authentication process for rekeying after revocation shall be the same as the process for initial registration.

Rekey after revocation is not allowed if

- the revoked certificate was issued to another person
- the RA of the EPO has reason to believe that the credentials are false.

3.4 Revocation request

Before a certificate is revoked, the identity of the requester shall be authenticated by the RA for the EPO by means of a check on:

- the credentials of the requester (who may be the Subscriber or the Subscriber’s employer)

4. OPERATIONAL REQUIREMENTS

4.1 Certificate application

For each certificate application requesters shall:

- *authenticate themselves to the RA for the EPO in accordance with the requirements specified in section 3.*
- *apply for a (new) private key generated and protected according to this policy or present a public key and prove possession of the corresponding private key together with proof that it has been generated and protected in accordance with this policy.*
- *present personal information to be certified and/or filed along with the certificate application.*

The CA for the EPO and RA for the EPO shall take all reasonable care in accepting and processing certificate applications. The CA for the EPO shall document detailed procedures for processing certificate applications.

4.2 Certificate issuance

The issuance of a certificate by the CA for the EPO shall indicate complete and final approval of the certificate application by the CA for the EPO.

The production process for certificates and the private keys and tokens associated with the certificate consists of five clearly distinguishable parts (or functions) with their corresponding separate subsystems.

The five functions are:

1. *Key generation*
2. *Storage in token*
3. *Creation of certificates*
4. *Generation of PINs*
5. *Distribution and delivery*

4.2.1 Key generation

Keys are generated within a smart card in accordance with this CPS, Section 6.1.

4.2.2 Storage in token

Keys are stored in the personalised smart card of the Subscriber.

4.2.3 Creation of certificates

After the 'new Subscriber file' has been uploaded into the card management system (CMS), a PKCS#10 certificate request is generated and submitted to the CA for the EPO. Upon receipt of a PKCS#7 certificate response from the CA for the EPO, the card management system will write the certificate into the smart card.

4.2.4 Generation of PINs

Once the certificate has been written into the smart card the user PIN is set to a randomised value.

4.2.5 Distribution and delivery

The CA for the EPO will send a package containing a personalised smart card, smart card reader, Online Services starter kit CD, acceptance letter and other EPO printed material to the new Subscriber within 10 days of approval of the request.

4.3 Certificate acceptance and activation

Subscribers must acknowledge receipt of their smart card by signing and faxing the acceptance letter to the CA for the EPO. This acknowledgement shall be deemed as conveying acceptance of the certificate.

Once the signed acceptance letter has been received, the Subscriber is sent their corresponding PIN, and an LDIF file is sent via a secure connection to the RA for the EPO. The RA for the EPO activates the certificate by uploading it via this LDIF file into the repository. Once the Subscriber certificate has been uploaded into the repository the Subscriber can use the EPO's online services.

The CMS administrator shall cancel the card request of any Subscriber who has not returned the acceptance letter within 8 weeks.

4.4 Certificate revocation

Certificates shall be revoked when they become invalid or are no longer trustworthy.

4.4.1 Circumstances for revocation

4.4.1.1 Subscriber certificates

Subscribers (or others in accordance with 4.4.2) may request revocation of their certificates. Reasons for revoking a certificate include, but are not limited to, the following circumstances:

- *Theft, loss, disclosure, modification or other compromise or suspected compromise of the Subscriber's private key, PIN or smart card.*
- *Deliberate misuse of keys and/or certificate(s) by the Subscriber.*
- *Substantial non-observance of operational requirements laid down in the CP or other relevant documents (e.g. Subscriber Agreements).*
- *Certificate information becomes or is found to be inaccurate (e.g. change of name on marriage).*
- *Improper (e.g. certificate information is not correct) or faulty issuance of a certificate;*
- *Denial by the EPO to the Subscriber of access rights to any product or service.*
- *Departure of the Subscriber from the company or organisation.*

4.4.1.2 CA certificates

The EPO shall revoke a CA certificate under its control if:

- it discovers, or has reason to believe, that the private key of that CA has been compromised.
- authorised EPO staff request revocation of the certificate.

4.4.2 Who can request revocation

The following entities shall be authorised to request revocation of a Subscriber certificate:

- *the holder of the certificate (Subscriber)*

- *the employer of the Subscriber*
- *the RA for the EPO*
- *the CA for the EPO*
- *other parties authorised by the EPO*

Requests for revocation of CA certificates shall only be accepted from parties so authorised by the EPO*.*

4.4.3 Procedure for revocation request

Revocation requests shall be submitted to the RA for the EPO (by e-mail, fax or letter) by a Subscriber (or the Subscriber's employer). The RA for the EPO shall check whether the revocation request has been submitted by an authorised party for the certificate concerned and in turn initiate a revocation request to the CA for the EPO.

The CA for the EPO shall process the request during office hours and publish the revoked certificate in the CRL. The RA for the EPO shall then inform the Subscriber of the revocation by e-mail.

4.4.4 Revocation request grace period

The RA for the EPO shall take all reasonable care to process certificate revocation requests within a reasonable time.

4.4.5 Circumstances for suspension

Suspension is not supported within the EPO PKI.

4.4.6 Who can request suspension

Suspension is not supported within the EPO PKI.

4.4.7 Procedure for suspension request

Suspension is not supported within the EPO PKI.

4.4.8 Limits on suspension period

Suspension is not supported within the EPO PKI.

4.4.9 CRL issuance frequency (if applicable)

- *The CA for the EPO shall re-issue its CRL for Subscriber certificates every 24 hours, even if no changes to the CRL have been made*.
- *Every CRL shall denote the time for the next CRL issue in accordance with ITU-T X.509. A new CRL may be published before the stated time.*
- The CA for the European Patent Organisation shall re-issue its CRL every three months or when the certificate of one of its sub-CAs is revoked.

4.4.10 CRL checking requirements

Relying Parties shall check for certificate revocation or suspension (for the complete certificate chain) prior to accepting verification of a certificate, in accordance with the Relying Party obligations set out in the Relying Party Agreement [RPA].

4.4.11 Online revocation/status checking availability

No stipulation.

4.4.12 Online revocation checking requirements
No stipulation.

4.4.13 Other forms of revocation advertisement available
No stipulation.

4.4.14 Checking requirements for other forms of revocation advertisement
No stipulation.

4.4.15 Special requirements regarding key compromise
No stipulation.

4.5 Security audit procedures

The CA for the EPO shall manually or automatically log the following events:

4.5.1 Types of event recorded
- CA key life-cycle management events, including:
  - key generation, backup, storage, recovery, archiving and destruction
  - cryptographic device life-cycle management events

- CA and Subscriber certificate life-cycle management events, including:
  - certificate applications, renewal, rekey, and revocation
  - successful or unsuccessful processing of requests
  - generation and issuance of certificates and CRLs

- Security-related events, including:
  - successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed by Getronics PinkRoccade (GPR) personnel
  - security-sensitive files or records read, written or deleted
  - security profile changes
  - system crashes, hardware failures and other anomalies
  - firewall and router activity
  - CA facility visitor entry/exit

Log entries shall include the following elements:
- date and time of entry
- serial or sequence number of entry, for automatic journal entries
- identity of the entity making the journal entry
- kind of entry.

RA for the EPO and administrators shall log certificate enrolment information, including:
- kind of identification document(s) presented by the Subscriber
- record of unique identification data, numbers or a combination thereof (e.g., driver's licence number) of identification documents, where applicable
- storage location of copies of applications and identification documents
- identity of entity accepting the application

- method used to validate identification documents, if any
- name of receiving CA or submitting RA, where applicable

In addition, the CMS shall provide full operational and audit log files detailing all operations performed, and identifying the user that requested that the operation be performed. Reports can be generated to obtain the following information:

- general data - allows browsing of the audit trail via search criteria
- list devices - displays a printable list of who has what device
- certificate requests - review requests for certificates sent to the CA for the EPO
- issued certificates - review and revoke issued certificates
- revoked certificates - review certificate revocation requests
- add/modify/remove users
- issue/change/cancel cards
- modify system configuration

4.5.2 Frequency of processing log

Online logs shall be processed every working day to identify actual or suspected security breaches.

4.5.3 Retention period for audit log

Logs shall be retained for at least seven years.

4.5.4 Protection of audit log

Online logs shall be protected against modification, e.g. by write-protecting relevant media as appropriate, and audit records shall be protected so that only authorised personnel can access them.

When subjected to external audit, data will not leave the premises, and review of the data shall only be allowed under the supervision of EPO staff or staff of a third party under contract to the EPO.

Electronically archived data is protected against unauthorised viewing, modification, deletion or other tampering by way of the implementation of physical and logical access controls.

4.5.5 Audit log backup procedures

- *A copy of each online log shall be kept at an off-site secure location.*
- *It shall be possible to examine logs during their retention period*.

4.5.6 Audit collection system (internal vs. external)

Audit logs shall be created on all EPO PKI systems.

4.5.7 Notification to event-causing subject

No stipulation.

4.5.8 Vulnerability assessments

The EPO shall perform vulnerability assessments of its CA and RA systems on a periodic basis. Policies, practices and system configurations shall be updated as appropriate, based upon the results of the assessment.

4.6 Archiving records

4.6.1 Types of event archived

Records shall include all relevant evidence in the CA for the EPO's possession, including:

- certificate applications and any related messages
- correspondence and contracts with other parties
- CA for the EPO rekeying information, including key identifiers and CA for the EPO certificates
- revocation requests and messages exchanged with the originator of the request and/or the Subscriber
- audit journals, including records of annual auditing of the CA for the EPO
- all types of event listed in section 4.5.1

4.6.2 Retention period for archive

- All audit records created shall be maintained for a total number of seven years after generation.
- If the original media cannot retain the data for the required period, the CA for the EPO shall operate procedures to ensure archived data is periodically moved to new media.
- The CA for the EPO shall maintain the applications required to process archive data for as long as may be needed.

4.6.3 Protection of archive

The CA for the EPO shall ensure that no entity can modify or delete the archive.

4.6.4 Archive backup procedures

The CA for the EPO shall ensure that archive data is stored off-site in a segregated, secure facility.

4.6.5 Archive collection system (internal or external)

Archives shall be collected internally.

4.6.6 Procedures to obtain and verify archive information

The CA for the EPO shall ensure that only authorised personnel may obtain archive information.

4.7 Key changeover

- The CA for the EPO shall generate a new certificate signing and verification key pair, employing a key splitting/sharing scheme, and a CA for the EPO certificate at least three months prior to the expiration of the old private CA for the EPO key.
- Changing a CA for the EPO key pair shall involve the same security procedures as during the original creation.
- The CA for the EPO shall ensure that key changeover causes minimal disruption to any subordinate entities in the CA for the EPO chain of trust.

4.8 Compromise and disaster recovery

The EPO has implemented application- and system-specific business continuity and disaster recovery plans in order to assure continued operation without compromise in the event of disaster. Reference should be made to the Service Continuity Plan for Principal Directorate Information Management.

4.8.1 Key compromise

In the event of actual or suspected compromise of the CA for the EPO's private key, the EPO shall immediately notify all subordinate entities within the CA for the EPO's chain of trust. Where the CA for the EPO certificate is revoked, all subordinate certificates shall also be revoked.

4.8.2 Disaster recovery

The CA for the EPO has implemented a remote disaster recovery site. To ensure recovery, the following measures have been put in place:

- Fully documented system, including design, configuration files and detailed installation scripts of the systems, hardware and software.
- Procedures for backup and restore; backups are stored in two different locations.
- Clones of cryptographic hardware - two clones are live backups of each other in separate signing servers..

4.9 CA for the EPO termination

The CA for the EPO shall notify its Subscriber community of the expiry of the CA for the EPO certificate at least six months prior to its expiry.

Termination of the CA for the EPO is defined as when all service associated with the CA for the EPO ceases permanently. It does not apply when the service is transferred from one organisation to another, or when an old CA for the EPO key pair is changed for a new CA for the EPO key pair.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical controls

The CA for the EPO, including smart card processing (with the card management system - CMS) is located within a secure, non-EPO facility in The Netherlands.

The RA for the EPO is located within the facilities of the EPO's offices in Munich. This CPS supports the security requirements of the EPO Certification Policy. All CA and RA operations shall be conducted within a physically protected environment designed to deter, prevent and detect covert or overt penetration.

5.1.1 Site location and construction

The site location and construction information shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

CA for the EPO operations shall be conducted within the GPR facilities in Apeldoorn. All operations for the CA for the EPO and for processing smart cards for the EPO shall be conducted within the physically protected environment of GPR designed for these operations.

The CA for the EPO has up to six physical security tiers. They are described in paragraph 5.1.2 and consist of:

- issuing smart cards (Tier 3)
- CA functions (Tier 4)
- online CA cryptographic modules for the CA for the EPO (Tier 5)
- offline CA cryptographic modules for the CA for the European Patent Organisation (Tier 7)

The CA for the EPO shall take reasonable steps to locate its site in secure accommodation such that any party or exterior walls and any ceilings and roofs that could otherwise afford unauthorised access are at least of brick, tile, concrete or aggregate construction. Walls must connect at both top and bottom with floors and ceilings/roofs (i.e. they must penetrate suspended ceilings or floors that could afford access via void spaces).

RA for the EPO operations, including validation operations, shall be conducted within the eBusiness User Support facilities at the EPO's offices in Munich.

5.1.2 Physical access

Information about physical access shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

The characteristics for physical access to the CA for the EPO are as follows:

- Access to Tier 1 at GPR requires the use of a proximity card employee badge.

- Tier 2 requires individual access control for all persons entering the common areas of the CA for the EPO through the use of a proximity card employee badge.
- Tier 3 requires individual access control through the use of two-factor authentication, including biometrics.
- The Tier 4 data centre requires individual access control and the key ceremony room requires dual control, each through the use of two-factor authentication, including biometrics.
- Tiers 5-7: online cryptographic security units (CSUs) are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with GPR segregation of duties requirements.
- All physical access to the tiers described above is automatically logged.

The characteristics for physical access to the RA for the EPO are as follows:
- The eBusiness User Support of the EPO is guarded by security personnel.
- The eBusiness User Support of the EPO is open to employees of the EPO during opening hours.
- Outside opening hours the eBusiness User Support is locked.
- All the RA for the EPO's information is protected through the use of locked cabinets.

5.1.3 Power and air conditioning
The CA and the RA for the EPO secure facilities are equipped with primary and back-up for:
- power systems to ensure continuous, uninterrupted access to electric power
- heating/ventilator/air conditioning systems to control temperature and relative humidity

5.1.4 Water exposure
The CA for the EPO shall take reasonable measures to protect its site from exposure to flooding (including both external incursion and leakage of water coolant and/or heating systems) within its site that could affect critical processing operations (choice of geographical location of the CA above sea level).

5.1.5 Fire prevention and protection
The CA for the EPO shall take reasonable measures to protect its site from fire that could affect computers, media, equipment or paper records.

5.1.6 Media storage
Information about media storage shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

The CA for the EPO shall store its removable media securely within the EPO/GPR facilities or in a secure off-site location.

5.1.7 Waste disposal

Information about waste disposal shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

Sensitive documents and materials shall be shredded prior to disposal. Cryptographic devices shall be physically destroyed or reset to zero in accordance with the manufacturer's guidelines for disposal. Other waste shall be disposed of in accordance with standard EPO and GPR waste disposal requirements.

5.1.8 Off-site backup

The CA and the RA for the EPO shall perform routine off-site backups of critical system data, audit log data and other sensitive information.

5.2 Procedural controls

5.2.1 Trusted roles

Information about trusted roles shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

Trusted persons include all employees, contractors and consultants of both the GPR and the EPO who have access to or control authentication or cryptographic operations that may materially affect the:

- validation of information in certificate applications
- acceptance, rejection or other processing of certificate applications, revocation requests or renewal requests or enrolment information
- issuance or revocation of certificates, including personnel having access to restricted portions of its repository
- handling of Subscriber information or requests

Trusted persons include, but are not limited to:

- customer service personnel
- cryptographic business operations personnel
- security personnel
- systems administration personnel
- designated engineering personnel
- executives designated to manage infrastructural trustworthiness

Persons seeking to become trusted persons by obtaining a trusted role must successfully complete the screening requirements described in the following paragraphs. All staff shall sign a security declaration.

5.2.2 Number of persons required per task

Information about the number of persons required per task shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

The most sensitive tasks within the CA for the EPO, such as access to and management of CA for the EPO cryptographic modules and associated key material, shall require at least two trusted persons.

The RA role at the RA for the EPO requires one employee for processing the application, revocation and renewal requests, and enrolment information.

5.3 Personnel controls

5.3.1 Background, qualifications, experience and clearance requirements

Information about background qualifications, experience and clearance requirements shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

Personnel seeking to become trusted persons must present proof of the background, qualifications and experience required for them to perform their job responsibly and satisfactorily.

5.3.2 Background check procedures

Information about background check procedures shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

Prior to commencement of employment in a trusted role, the CA for the EPO shall conduct background checks which shall include the following:

- confirmation of previous employment
- check of professional reference
- confirmation of the highest or most relevant educational qualification obtained
- background check

The factors arising from a background check that may be considered grounds for rejecting candidates for trusted roles include the following:

- misrepresentations made by the candidate
- highly unfavourable or unreliable personal references
- certain criminal convictions

5.3.3 Training requirements

Personnel supporting the EPO PKI shall be provided with training upon hire, plus the requisite on-the-job training needed for personnel to perform their job responsibilities competently and satisfactorily.

Training programs shall include the following:

- basic PKI concepts
- job responsibilities
- security and operational policies and procedures
- use and operation of deployed hardware and software
- incident and compromise reporting and handling

- disaster recovery and business continuity procedures

5.3.4 Retraining frequency and requirements
Personnel shall be provided with refresher training. Periodic security awareness training shall be provided on an ongoing basis.

5.3.5 Job rotation frequency and sequence
Information about job rotation frequency and sequence shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

5.3.6 Sanctions for unauthorised actions
The CA for the EPO shall take disciplinary action against any personnel who violate the terms of the CP, its CPS, or other policies and procedures. Disciplinary action may include measures up to and including termination of employment, depending on the frequency and severity of the unauthorised actions.

5.3.7 Contract personnel requirements
Information about contract personnel requirements shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

In limited cases, independent contractors or consultants may be used to fill trusted roles. Contractors and consultants shall comply with the same functional and security requirements that apply to EPO and GPR employees.

5.3.8 Documentation supplied to personnel
All personnel involved with the RA for the EPO and the CA for the EPO shall be required to read this CPS, the CP for the EPO and the applicable security policies.

6. TECHNICAL SECURITY CONTROLS

The CA for the EPO is a sub-CA of the CA for the European Patent Organisation (see also 1.3.1). This chapter describes the security controls for the CA for the EPO and the Subscriber keys issued by the CA for the EPO.

6.1 Key pair generation and installation

6.1.1 Key pair generation

Information about key pair generation shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

The CA for the EPO and the CA for the European Patent Organisation use separate hardware cryptographic modules that have been certified as meeting the FIPS PUB 140-1 standard Security Level 3 to generate certificate signing and verification key pairs.

Generation of RA for the EPO key pairs is performed by the RA for the EPO using a FIPS 140-1 level 1 certified cryptographic module provided with their browser software.

Subscriber key pair generation is performed within the Subscriber smart card. As a result, the keys will never leave the card. The card itself is protected by a PIN that is known only to the Subscriber.

6.1.2 Private key delivery to entity

Subscriber private keys are stored on the Subscriber smart card and delivered to the Subscriber by the CA for the EPO.

6.1.3 Public key delivery to certificate issuer

Information about public key delivery to certificate issuer shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

Subscriber public keys are generated by the CA for the EPO within the Subscriber smart card. The card management system (CMS) generates a PKCS#10 certificate request for each certificate, and submits it to the CA for the EPO for processing. Upon receipt of a PKCS#7 certificate response from the CA for the EPO, the CMS writes the certificate to the Subscriber card. As soon as the certificate is written into the smart card, the Subscriber PIN is set to a randomised value. GPR will then send this PIN in a PIN mailer to the Subscriber in accordance with section 4.3.

6.1.4 CA for the EPO public key and CRL delivery to permitted users

The CA for the EPO public key is available to permitted users and is distributed as a self-signed certificate on the CD. The CRL is published by Getronics PinkRoccade at http://www.megasign.nl/crl/EuropeanPatentOfficeepoline/LatestCRL.crl.

6.1.5 Key sizes

- The CA for the EPO keys have a length of 2048 bits.
- Subscriber keys have a length of 1024 bits.

6.1.6 Public key parameter generation

No stipulation

6.1.7 Parameter quality checking

No stipulation

6.1.8 Hardware/software key generation

The CA for the EPO key generation is performed in a cryptographic module that complies with FIPS PUB 140-1 level 3.

Subscriber key generation is performed within the user's smart card.

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

For ITU-T X.509 Version 3 certificates, the KeyUsage extension of certificates is used in accordance with RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

6.2 Private key protection

6.2.1 Standards for cryptographic module

The CA for the EPO employs a hardware cryptographic module that has been certified as meeting the FIPS PUB 140-1 Security Level 3 to protect the CA for the EPO private key.

The Subscriber private key is stored on a smart card that meets the requirements of FIPS PUB 140-1.

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

Information about private key (n out of m) multi-person control shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

The CA for the EPO has implemented technical and procedural mechanisms requiring the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. A minimum of three secret shares out of the total number of nine secret shares created and distributed for the cryptographic module of the CA for the EPO are required to activate the private key of the CA for the EPO stored on this module.

The Subscriber key is stored on a smart card and the card itself is protected by a PIN known only to the Subscriber.

6.2.3 Private key escrow

Keys within the EPO PKI are not escrowed.

6.2.4 Private key backup

The CA for the EPO creates back-up copies of CA private keys for routine recovery and disaster recovery procedures. These keys are stored in encrypted form within cryptographic modules and associated key storage devices.

The CA for the EPO does not back up copies of RA for the EPO or Subscriber private keys.

6.2.5 Private key archival

Expired, inactive private signing keys will not be archived, but will be destroyed in accordance with section 6.2.9.

The CA for the EPO does not archive copies of RA for the EPO and Subscriber private keys.

6.2.6 Private key entry into the cryptographic module of the CA for the EPO

Information on private key entry into the cryptographic module of the CA for the EPO shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

The CA for the EPO generates CA key pairs on the hardware module in which the keys will be used. In addition, the CA for the EPO makes copies of these keys for routine recovery and disaster recovery purposes. Where the CA for the EPO is backed up to another hardware cryptographic module, the key pairs are transported between modules in encrypted form.

6.2.7 Method of activating private keys

Information about the method of activating private keys shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

The private key for the CA for the European Patent Organisation is activated only to sign the certificate of the CA for the EPO, after which it is deactivated and the security module returned to secure storage.

The RA for the EPO administrator private keys are stored on a smart card and are activated with a PIN code known to the administrator.

Subscriber key pair generation is performed within the Subscriber smart card. Consequently, the keys never leave the card. The Subscriber private keys are activated by a PIN code that is known only to the Subscriber.

6.2.8 Method of deactivating private keys

RA for the EPO administrator private keys are deactivated upon system log-off. The RA for the EPO is required to log off the workstation when leaving the work area.

Subscriber private keys are deactivated upon removal of the smart card from the reader.

6.2.9 Method of destroying private keys

The CA for the EPO deactivates the CA for the EPO private key by destroying the key irrevocably.

Subscriber keys cannot be destroyed, but the corresponding certificate can be revoked to prevent misuse of a private key (see 4.4.1). The replacement card has new keys and certificates.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The CA for the EPO certificate, the RA for the EPO certificate and the Subscriber certificates are backed up and archived as part of the CA for the EPO routine back-up procedure.

6.3.2 Usage periods for public and private keys

CA for the European Patent Organisation keys have a usage period of 20 years. CA for the EPO keys have a usage period of 10 years. Subscriber keys have a usage period of 3 years.

6.4 Activation data

6.4.1 Activation data generation and installation

Information about activation data generation and installation shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO’s Security and Audit directorate.

The CA for the EPO employs strong passwords to protect private keys. The selection guidelines stipulate that passwords should:

- be generated by the user
- have at least eight characters
- have at least one alphabetic and one numeric character
- have at least one lower-case character
- not contain excessive occurrences of the same character
- not be the same as the operator's profile name
- not contain a long substring of the use's profile name

The RA for the EPO uses strong authentication for activating private keys: smart card and PIN code.

Subscribers also use strong authentication for activating private keys: smart card and PIN code (see also 6.1.3).

6.4.2 Activation data protection

The CA for the EPO administrators are required to safeguard their secret shares and sign an agreement acknowledging their responsibilities.

The RA for the EPO administrators are required to store the administrator private keys in encrypted form on a smart card.

6.4.3 Other aspects of activation data
No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements
The RA and CA for the EPO shall employ computer security controls to identify individual personnel. A smart card and PIN shall be required for access to the RA for the EPO and CMS equipment. Additionally, the CA for the EPO shall limit access to data and functions in accordance with the user's role and privileges, and record access by means of an online log (audit trail) of security-relevant events.

6.5.2 Computer security rating
Not applicable. See section 6.1.1.

6.6 Life cycle technical controls

6.6.1 System development controls
The CA for the EPO shall employ development controls where appropriate to ensure all software and hardware is created, integrated, tested, configured, installed, commissioned and maintained in accordance with the CA for the EPO's business objectives. It shall employ appropriate goods-inwards procedures for bought-in items.

6.6.2 Security management controls
The CA for the EPO shall establish a security organisation and shall manage and control all security activities associated with system development and operation.

6.6.3 Life cycle security ratings
Not applicable.

6.7 Network security controls

Information about network security controls shall be recorded separately. This information shall not be disclosed publicly for security reasons. Access to this information may be granted to eligible parties following a reasoned request to the EPO's Security and Audit directorate.

The CA for the EPO shall protect its internal communications networks from unauthorised access, including access via any connected external networks. It shall employ a firewall to protect each such connection. Each firewall shall be configured with an appropriate security policy restricting the passage of data between the networks to the minimum necessary to accomplish its business objectives, and analysing incoming data for virus

contamination as appropriate. It shall conduct routine and ad hoc analyses of firewall operation to detect actual or suspected breaches of security.

The link connecting the RA of the EPO with the CMS (card management system) shall be encrypted and use mutual authentication.

All communication between the CMS registration component and the CA for the EPO shall be digitally signed. For that purpose, the CMS server shall use:
- a unique RA for the EPO certificate and matching private key
- the public CA for the EPO certificate

All request operations shall be digitally signed using the RA for the EPO certificate. This will enable the CA for the EPO to validate them as having come from the registered RA for the EPO only.

All responses from the CA for the EPO to the RA for the EPO shall be signed using the CA for the EPO private key. This will enable the CMS to validate them as legitimate responses from the CA for the EPO.

6.8 Cryptographic module engineering controls

See section 6.2.1.

7. CERTIFICATE AND CRL PROFILES

Certificates provided to Subscribers are defined, in accordance with the definition in Annex F to the PCT, as low-level certificates.

7.1 Certificate profile

Subscriber certificates shall conform to RFC 2459.
The certificate profile contains the following values or value constraints:

Field	Value or value constraint
Version	See CPS § 7.1.1
Serial number	Unique value per user DN (MD5 hash of public key)
Signature algorithm	SHA1 RSA
Issuer DN	See section 7.1.4
Valid from	Issue date (Coordinated Universal Time (UTC) base. Encoded in accordance with RFC 2459).
Valid to	Issue date + 3 years (UTC base. Encoded in accordance with RFC 2459.)
Subject DN	C: Country of Subscriber
	O: Company of Subscriber
	CN: <First letter of first name> + <.>+ <-> +<First letter of second name> + <*space*> + <surname> + <space> + <EPO ID>
Subject public key	Encoded in accordance with RFC 2459 using algorithms specified in CPS section 7.1.3 and key length specified in CPS section 6.1.5
Signature	Generated and encoded in accordance with RFC 2459

Table 2 Certificate profile

7.1.1 Version number(s)

The CA for the EPO and Subscriber certificates are X.509 Version 3 certificates.

7.1.2 Certificate extensions

The CA for the EPO has implemented a single non-critical Certificate Policy certificate extension in accordance with RFC 2459 with policy qualifiers on each certificate..

7.1.3 Algorithm object identifiers

Subscriber certificates are signed with SHA-1 with RSA encryption (1 2 840 113549 1 1 5) in accordance with RFC 2459.

7.1.4 Name forms

See 3.1.1

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate Policy object identifier

See section 1.2.

7.1.7 Usage of policy constraints extension
No stipulation.

7.1.8 Policy qualifiers syntax and semantics
No stipulation.

7.1.9 Processing semantics for critical Certificate Policy extensions
No stipulation.

7.2 CRL profile

The CRL profile contains the basic fields and contents specified in the table below:

Field	Value or value constraint
Version	See CPS section 7.2.1
Signature algorithm	Md5RSA or md2RSA
Issuer	Issuer of the CRL. The issuer name is in accordance with section 7.1.4.
Effective date	Issue date of the CRL.
Next update	Date by which the next CRL will be issued. The next update date is three months from the effective date for the CRL of the CA for the European Patent Organisation. CRL issuance frequency for Subscriber certificates is in accordance with the CPS, section 4.4.9.
Revoked certificates	Listing of revoked certificates, including serial number of the revoked certificate and revocation date.
Signature	Generated and encoded in accordance with RFC 2459

Table 3 CRL profile basic fields

7.2.1 Version number(s)
The CA for the EPO issues X.509 version 1 CRL.

7.2.2 CRL and CRL entry extensions
No stipulation.

8. SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

Amendments shall be in the form of either a document containing an amended form of the CPS or an update.

8.2 Publication and notification policies

See 1.4 for details.

8.3 CP approval procedures

The EPO's Security and Audit directorate shall be responsible for maintenance of the CP document.