CCBE

Représentant les avocats d'Europe
Representing Europe's lawyers

TECHNICAL STANDARDS FOR INTEROPERABILITY OF ELECTRONIC ID CARDS

Conseil des barreaux européens – Council of Bars and Law Societies of Europe
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail ccbe@ccbe.eu – www.ccbe.eu

Technical standards for interoperability of electronic ID cards

1. Introduction

1.1. Overview

1.1.1 The role of the CCBE

The Council of Bars and Law Societies of Europe (CCBE) represents, through its member bars and law societies of the European Union and the European Economic Area, more than 700,000 European lawyers. In addition to membership from EU bars, it has also associate representatives (from EU candidate countries) and observer representatives from further European countries' bars.
The objectives of the CCBE are:

1. To represent the Bars and Law Societies of its Members, whether full, associate or observer members, on all matters of mutual interest relating to the exercise of the profession of the lawyer, the development of the law and practice pertaining to the rule of law and administration of justice and substantive developments in the law itself, both at a European and international level.
2. To act as a consultative and intermediary body between its Members, whether full, associate or observer members, and between the Members and the institutions of the European Union and the European Economic Area on all cross border matters of mutual interest as listed under a) above.
3. To monitor actively the defence of the rule of law, the protection of the fundamental and human rights and freedoms, including the right of access to justice and protection of the client, and the protection of the democratic values inextricably associated with such rights.

As the representative organ of National Bar Councils in Europe, CCBE is the most qualified body for setting up the common/minimum standards to be followed for the identification of lawyers on the Internet.

This document specifies the minimum requirements that should be observed by national Bar Certification Authorities which identify those lawyers registered with them on the Internet through qualified Certificates. This Policy is called "Digital Qualified Certificate for Lawyers".

The present document will observe the requirements of *The Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures* (hereinafter referred to as "the Directive") and the standard requirements of RCF 2527 – *Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework,* and will be based on the Technical Specification of the ETSI TS 101 456 V1.2.1 (2004-2004) Policy Requirements for certification authorities issuing qualified certificates.

The ownership of all trademarks and proprietary names belonging to third parties are acknowledged, when used in this document.

1.1.2. Principal concept of the CCBE Policy

As already indicated in the CCBE Framework proposal of which this policy forms an annex, the CCBE promotes the insertion of chips to be used for the creation of digital signatures in its own European card for European Lawyers, and promotes the use of electronic ID cards at European level. In order to make electronic ID cards interoperational at European level, the CCBE would be constituted as a competent authority that oversees that the national conditions of emitted electronic ID cards are in accordance with European standards and can be recognised for cross-border practice[1]. One of the key functions of electronic ID cards are digital certificates, for which this policy sets a common technical standard.

[1] The expression "competent authority" is not meant to say that the CCBE should issue any Digital Certificate. "Comptetent authority" as used in this document is referring to a technical rather than a legal role for the CCBE. The CCBE with the approval of this policy would only create common technical standards for evaluating and checking national policies of the National Certification Authority. This would allow a French lawyer with a French certificate to have the guarantee that his/her policy complies with the CCBE standards and therefore would trust in another country that CCBE has entrusted in the framework of its European policy.

An introductory tutorial, which summarises the CCBE Policy and which does not go into the complete technical details, is given in the following paragraphs[2]. Some of the terms used are specifically explained further in the document (please see the table of contents).

The use of digital certificates and digital signatures are supported generally by a **public key infrastructure (PKI)**. A PKI is a system of hardware, software, people, processes, and policies supporting the use of **public key cryptography** (described below) to provide various security services or assurances. Specifically, a PKI seeks to create secure electronic communications, transactions, and/or records by providing assurances that may include:

- reliable methods for authenticating the identity and authority of individuals and organisations communicating electronically or their attributes[3]
- reliable methods for providing assurances of the integrity of electronic communications and records and detecting corruption or unauthorised modifications to them
- reliable methods for the protection of electronic messages and records against interception, unauthorised access, and the disclosure of confidential or sensitive information within them
- reliable methods for controlling access to sensitive information and ensuring that only certain parties, certain properly authorised parties, or parties with certain attributes have such access
- the collection of persuasive significant evidence for the purpose of preventing parties from successfully repudiating electronic transactions
- the adequacy of particular technologies, including PKI technology, to comply with emerging legal mandates.

Digital signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use what is known as **public key cryptography** which uses two keys:

1. the **private key** (known only to the signer and used to create the signature) and
2. the **public key** (known more widely and used by the relying party to verify the signature).

Due to the principle of irreversibility, it is computationally infeasible to derive the private key from the knowledge of the public key. Thus, though many people may know the public key of a given signer and use it to verify that signer’s signature, they cannot discover that signer’s private key and use it to forge digital signatures.

In order to verify digital signatures, the verifier must have access to the signer’s public key and have assurance that it corresponds to a signer having a certain identity and/or attributes, as well as that signer’s private key. However, a public and private key pair has no intrinsic association with any person; it is simply a pair of numbers. Some reliable method is necessary to associate a particular person or entity to the key pair. The solution to this problem is the use of one or more **trusted third parties** to associate an identified signer and/or signer with specific attributes with a specific public key. That trusted third party is referred to as a **Certification authority (CA) or National certification authority (NCA)** in most technical standards and in this policy.

To associate a public key with a prospective signer, a **(National) Certification authority** first authenticates a person, organisation, or device. It then issues a certificate, an electronic record which contains the public key and lists the authenticated person, organisation, or device as the subject of the

[2] This introductory tutorial has used the « Digital Signature Guidelines (1996)» and the « PKI Assessment Guidelines (2003)» published by the Information Security Committee, Section of Science and Technology Law, American Bar Association, as a basis for the description of the technology here. The CCBE especially thanks Stephen S. Wu, PKI Assessment Guidelines Co-Rapporteur, former Information Security Committee Co-Chair and partner of Cooke Kobrick & Wu LLP, Cupertino, CA for his comments.

[3] Attributes are characteristics of an individual or organisation. In the case of an individual, examples of attributes may include an office or role he or she holds, organizational affiliation, membership in a group, specific authorities held by the individual, or licensure or other professional status. A PKI may also support the authentication of devices, such as specific servers used to conduct ecommerce.

certificate holding that public key. As part of the issuance process, it confirms that the prospective signer identified in the certificate holds the private key corresponding to the public key to be placed in the certificate.

The prospective signer who receives a certificate is termed a **subscriber**. A certificate's principal function is to bind a key pair with a particular subscriber. A recipient of the certificate desiring to rely upon a digital signature created by the subscriber named in the certificate (called a **relying party**) can use the public key listed in the certificate to verify that the digital signature was created with the corresponding private key. In other words, if a relying party receives a digitally signed message purporting to come from a given person, the relying party will want to make sure he or she has the purported signer's real public key before attempting to verify the signature.

Certificates are themselves digitally signed record. To assure both the integrity and identity of the source of the certificate, the (National) Certification authority digitally signs it. A digital signature, whether created by a subscriber to authenticate a message or by a (National) Certification Authority to authenticate its certificate should be reliably time-stamped to allow the relying party to determine reliably whether the digital signature was created during the operational period stated in the certificate, which is a condition upon verifiability of a digital signature under this policy. The (National) Certification Authority therefore has an important role to **suspend** (temporarily invalidate) or **revoke** (permanently invalidate) the certificate, for example because of a compromise in the security of the subscriber's private key. The conditions for suspension or revocation are further described in this policy. Immediately upon suspending or revoking a certificate, the (National) Certification Authority must **publish notice of revocation or suspension** or notify persons who inquire or who are known to have received a digital signature verifiable by reference to the unreliable certificate.

1.2. Identification

The identifiers for qualified certificate Policy for Lawyers should be:

Name	CP_CCBE_05
O.I.D.	CCBE would need to obtain an Object identifier number by IANA (http://www.iana.org/cgi-bin/enterprise.pl) which aims at identifying entities which act on internet.
Description:	Certification Policy (CP) Digital Qualified Certificate for lawyers
Version	003.0
Issuing Date	
Localization	URL

1.3. User Community and Applicability

1.3.1. Certification Authority (CA)

The Certification Authority should be an entity, or a legal or a natural person, which issues certificates.

It is a trusted third party of confidence that provides assurances of the connection between the public key contained in the certificate and its owner, the person or corporation named in the certificate.

The CA manages the certificate life cycle: issuance, distribution, revocation, and renewal of certificates, and issues periodically public Certificate Revocation Lists.

1.3.2. Registration Authority (RA)

The Registration Authority (RA) is an entity which is authorised by the CA and which is responsible for the identification and authentication of subscribers. The RA identifies the use through:

Verification of Registry information (certificate requests, revocation, suspension and changes)

The RA in the context of this PC should be:

- The Bar or
- National Bar

1.3.3. The Subscriber (or signatory)

Under this policy the Subscriber should be a natural person who holds a signature creation device and is authorised to pursue his professional activities under one of the professional titles established by article 2 of the Directive 98/5/EC (OJ No L 77 of 14 March 1998) and its revised versions.

1.3.4. User

The User is a Natural or legal person who trusts in the digital certificate created in the context of this policy.

1.3.5. User Community and applicability

Digital certificates issued by this Policy should identify a natural person who acts as a lawyer in his/ her profession.

Digital Certificates issued by this policy should comply with the standard RFC3280 (X.509)

Digital Certificates issued by this policy should be Qualified Certificates according to Directive 1999/93/CE and national law.

Digital Certificates issued by this policy should be created by a Secure Signature Creation Device.

1.4. Contact details

Organisation name:	CCBE
Contact Person:	Birgit Beger
E-mail:	beger@ccbe.eu
Phone	+32 2 234 6510
Direction	

2. General Concepts

2.1. Obligations

2.1.1. Certification authority (CA)/ National Certification Authority (NCA)

The Certification authority (CA) or National Certification Authority (NCA) that issues certificates according to this policy should apply a reasonable level of skills in its activities as a CA, according to Directive 1999/93/CE and the respective national law.

The NCA should ensure that all requirements on CAs are implemented as applicable to this Policy.

NCAs which want to appear as “recognised” CAs on the CCBE Web-site should inform the CCBE about their compliance status.

2.1.2. Registration Authority (RA)

If there are Registration Authorities (RAs) which are delegated to act by the NCA, the RAs should act according this Certification Policy.

2.1.3. Subscriber

A Subscriber shall read and sign a Subscriber Agreement to ensure that he/she fulfils the following obligations:

1. Submit accurate and complete information to the NCA in accordance with the requirements of this PC, particularly with regard to the registration.
2. To only use the Key pair for electronic signatures in accordance with this PC.
3. He/she should avoid unauthorised use of the certificate
4. Only his/her private key once delivered to him/her should be used.
5. To notify the NCA, within a reasonable delay, if there are any changes of his/her person or professional activities before the end of the validity period indicated in the certificate.

2.1.4. User

The user should verify the following:

1. To check the validity of the digital certificate by requesting the current Status information on any revocation of the certificate.
2. To take into account the limitation on the usage of the digital certificate indicated in this PC.

2.1.5. Repository obligations

To be determined by the NCAs (National Certification Authorities).

2.2. Liability

NCAs issuing qualified certificates under this Policy are liable as specified in Article 6 of the Directive 1999/93/CE and the respective national law.

2.3. Financial Liability

To be determined by the NCAs.

2.4. Interpretation and Enforcement

2.4.1. Governing law

NCAs issuing qualified certificates under this Policy should comply with the Directive 1999/93/CE and its legal transposition into national law.

2.4.2. Severability, survival, merger and notice

In the event that any part of this Certificate Policy is found to be unenforceable or invalid pursuant to the applicable law, that part will be enforced to the maximum extent possible so as to give effect to its intention. The remaining terms and conditions will continue in full force and with full effect.

Each NCA shall ensure that any agreements it enters into contain appropriate provisions governing severability, survival, merger and notice as applicable.

2.4.3. Dispute resolution procedures

Any dispute arising out of, or relating to, this Certificate Policy should be resolved using an appropriate dispute settlement mechanism.

2.5. Fees

To be determined by NCAs.

2.6. Publication and Repository

2.6.1. Publication of CA information

2.6.1.1. Certification Policy (CP) and Certificate Practices Statement (CPS)

NCAs which act according to this Certificate Policy (CP) should ensure that their CP and the Certificate Practices Statement (CPS) are available to all subscribers and relying parties.

2.6.1.2. Certificate Status information

NCAs should ensure that the certificate status information is made available to all subscribers and relying parties.

2.6.1.3 Other information

NCAs should ensure that the information about their compliance with this Policy is available to all subscribers and relying parties. Each NCA will decide about the way to inform about their compliance.

NCAs should create an e-mail function by which the user is informed that the certificate is in compliance with the Certification Policy (CP), create an optional filed on the chip of the electronic card or any other method at their discretion.

The CCBE will list “recognised” NCAs on the CCBE Web-site which include all those member bars which comply with the Certification Policy and which have informed the CCBE respectively.

The CCBE would not take any responsibility of the actual status of the NCAs’ compliance.

2.6.2. Frequency of publication

The Certificate Policy should be published immediately within normal business hours, on issuance, and whenever updates are made.

Certificate Revocation Lists (CRLs) must be issued and published periodically, even if there is no change to the certificate status information, or more frequently when subscribers’/end entities’ certificates are suspended or revoked.

Certificates will be published to the NCAs repository as soon as they are issued.

2.6.3. Access controls

NCAs do not impose any access control on their Policy, its issued certificates, and its CRLs. In the future, NCAs may impose access controls on issued certificates, their status information and CRLs at their discretion.

2.7 Compliance Audit

Each NCA shall ensure that their CP is in accordance to the guidelines specified in the present CP.

2.8. Confidentiality and protection data

The NCA issuing qualified certificates under this Policy should comply with the Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and its legal transposition into national law.

2.8.1. Types of information not considered confidential

CPs, CPS, Certificates, Certification Revocation Lists (CRLs), and personal or corporate information appearing on them are not considered confidential and are therefore deemed to be in the public domain.

2.8.2. Disclosure of certificate revocation/suspension information

CRLs will be published periodically, with revoked and suspended certificates

2.8.3. Release to law enforcement officials

NCAs shall respect Privacy rights subject to the applicable laws.

2.9. Intellectual Property Rights

This Policy, its OID and the CCBE Logo are the intellectual property of CCBE, protected by trademark, copyright and other laws regarding intellectual property, and may be used only pursuant to a license or other express permission from CCBE and only in accordance with the provisions of this Policy. Any other use of the above mentioned items without the express written permission of the owner is expressly prohibited.

3. Identification and Authentication

3.1. Initial registration

3.1.1. Type of name

Each certificate issued under this policy should have a distinguished name (here in after DN) in accordance with the standard X.501.

The DN should include as minimum requirements the following components, each component should be identified by NCAs:

- **Common Name – CN**: this component will contain the full name (given name and Surname) of the subscriber as stated in the proof-of identity documents.
- **E-mail –E**: this component will be the email of the subscriber.
- **Organization –O;** this is the official name of the institution the subscriber is affiliated with and indicates that the subscriber is a lawyer.
- **Unit Organization –OU:** this component will contain de name of the NCA or the Bar.
- **Title-T**: This component will identify the professional title of the lawyer.
- **State –ST:** This component should indicate the state of the NCA. It is an optional component for NCAs.
- **Country-C:** This component will be the country of the NCA.

3.1.2. Need for names to be meaningful

NCAs shall issue their own policy on the usage of names which are meaningful according to the respective national law.

3.1.3. Rules for interpreting various name forms

To be determined by NCAs.

3.1.4. Uniqueness of names

NCAs shall enforce uniqueness within the X.500 name space for which they have been authorised to issue names.

3.1.5. Name claim dispute resolution procedure

To be determined by NCAs.

3.1.6. Recognition, authentication and role of trademarks

To be determined by NCAs.

3.1.7. Method to prove possession of Private Key

The private Key shall be created by the subscriber and has to be exclusively in his/her possession.

Proof of possession of the Private Key shall be achieved by signing the certificate request using a recognised standard protocol, ie, PKCS#10.

3.1.8. Authentication of organization identity

The NCAs should verify the identity of the subscriber. It will be necessary that the subscriber presents him/herself personally and that he/she proves his/her identity personally in the presence of the authorised person. The personal presence shouldn't be necessary if the subscriber uses an electronic identity card admitted under the respective national law as a method of identify proof on the internet.

NCAs should verify in it own Data Bases the attributes of the subscriber.
NCAs issuing qualified certificates under this Policy should comply with the Directive 1999/93/CE and its legal transposition into national law.

3.2. Routine Rekey

To be determined by NCAs.

3.3. Rekey after Revocation

To be determined by NCAs.

3.4. Revocation Request

In accordance with section 4.

4. Operational Requirements

4.1. Certificate Request

This Policy is not intended to impose implementation requirements on the issuing NCAs or Subscribers/End Entities. However, this Policy does identify the required information and procedures that constitute assurance and support trust in the NCA.

Each NCA should define the request procedure, which should describe the following:

1. Procedure of request (ie, online or personal presence)
2. Who will be the person authorised to identify the subscriber
3. Proof of the subscriber's identity
4. The information to be submitted by the subscriber/end entity before the creation of a digital Certificate

4.2. Certificate Issuance

NCAs should carefully check the compliance and validity of documents presented by the subscriber. After the authentication is accomplished with the methods specified in Section 3.1, the NCA should issue the certificate.

In the case of issuance the NCA must notify the requester. If for any reasons the CA decides not to issue the certificate (even if the checks and the authentication were correct) it should notify the requesters by giving the reason for this decision.

4.3. Certificate Acceptance

With the delivery of the secure signature creation device, the subscriber accepts the private Key custody.

4.4. Certificate Suspension and Revocation

NCAs issuing qualified certificates under this Policy should comply with the Directive 1999/93/CE and its legal transposition into national law.

4.4.1. Circumstances for Revocation

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

- The subscriber's private key is lost or suspected to be compromised
- The information in the subscriber's certificate is suspected to be inaccurate
- The subscriber no longer needs the certificate to access Relaying Parties' resources
- The subscriber is no longer entitled

4.4.2. Procedure for Revocation Request

NCAS should describe the procedure for revocation in the CPS, which shall include:

- An identification of the certificate to be revoked;
- A clear statement of the reasons for revocation; and
- The authentication of the requester of the revocation, as described in Section 3.4.

4.4.3. Who Can Request Revocation

A certificate revocation can be requested by the holder of the certificate to be revoked or by any other entity presenting proof of knowledge of a circumstance for revocation.

4.4.4. Circumstances for suspension

NCAs should specify in their CPs if they support Certificate Suspension. If this is the case, NCAs should comply with the Directive 1999/93/CE and its legal transposition into national law.

4.4.5. Who can request suspension

NCAs should specify in their CP or Certification Practice Statements (CPSs) who can request certificate suspension.

4.4.6. Procedure for suspension request

NCAs should specify in their CP or CPSs the procedure for a Certificate suspension request. Suspension requests must be authenticated, accountable and auditable.

NCAs should notify the subscribers, if his/her digital certificate has been suspended, giving the following information:

- An identification of the certificate which is to be suspended
- Date and time of the suspension request
- A clear statement of reasons for suspension
- The period of time (if it is indicated in the CP or CPS) of the suspension

4.5. Security Audit Procedures

This policy recognises the importance of security audit procedures suggesting that a conforming NCA specifies all this kind of provisions in their CPS.

4.6. Records archival

To be determined by NCAs.

4.7 Key Change over

To be determined by NCAs.

4.8. Compromise and Disaster Recovery

To be determined by NCAs.

4.9. CA Termination

NCAs should specify in their CPs the procedure of CA termination and the way to inform the subscribers.

5. Physical, Procedural and Personnel Security Controls

NCAs should stipulate the security requirements required in their own CPS.

NCAs should implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or Tokens) used in connection with providing CA services. Access to such hardware and software will be limited to the personnel performing in a trusted role.

6. Technical Security Controls

6.1. Key pair generation and installation

6.1.1. Key pair generation

NCAs should assure in their CP and CPS that the subscriber's private key and the CA's Private keys is generated by using a Secure Device Signature Creation (ie, CC EAL4+, FIPS 140-1 level 2, ITSEC High4).

The Secure Device Signature Creation used by NCAs will comply with the Directive 1999/93/CE, its legal transposition into national law and the CEN CWA 14169.

6.1.2. Public key delivery to certificate issuer

To be determined by NCAs.

6.1.3. CA public key delivery to users

To be determined by NCAs.

6.1.4. Key size

6.1.4.1. CA Key Size

NCAs should use a key size of a minimum length of 2048 bits.

6.1.4.2. Subscriber key size

NCAs will comply with the Directive 1999/93/CE, its legal transposition into national law regarding the validity of the subscriber's key.

The Keys should be generated using RSA algorithm for public keys and should have a minimum of Length 1024 bits.

6.1.5 Public key parameters generation

To be determined by NCAs.

6.1.6. Parameter quality checking

To be determined by NCAs.

6.1.7. Hardware/software key generation

NCAs should assure in their CP and CPS that the Subscriber's private key and the CA's Private keys are generated by using a Secure Device Signature Creation (ie, CC EAL4+, FIPS 140-1 level 2, ITSEC High4).

The Secure Device Signature Creation used by NCAs will comply with the Directive 1999/93/CE, its legal transposition into national law and the CEN CWA 14169.

6.1.8. Key usage purposes

The purposes for which a key can be used should be restricted by the NCA through the key usage and key usage 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 should have the extension of the key usage flagged as a critical step of procedure. This means that the certificate shall be used only for the purpose for which the corresponding key usage bit was originally intended.

6.2. Private Key Protection

6.2.1. CA private key

NCAs should assure in their CP and CPS the procedure regarding the protection of the CA private key according to the provisions on Qualified Digital Certificates in Directive 1999/93/CE and its transposition into national law.

6.2.2. Subscriber private key

The Subscriber's private key will be issued through Secure Signature Creation Device according to the provisions on Qualified Digital Certificates in Directive 1999/93/CE and its transposition into national law.

6.3. Other Aspects of Key Pair Management

6.3.1. Validity Period

NCAs should include in their CP and CPS the validity period of private and public keys according to Directive 1999/93/CE and its legal transposition into national law.

6.4. Activation data

To be determined by NCAs.

6.5. Computer security controls

NCAs should stipulate in their CP and CPS the procedure undertaken on the computer for security controls.

6.6 Life cycle security controls

NCAs should stipulate in their CP and CPS the procedure for the control of the certificate's life cycle.

6.7. Cryptographic Module Engineering Controls

To be determined by NCAs.

7. Certificate and CRL Profiles

7.1. Certificate profile

Digital Certificates issued under this Policy, should be in accordance with the standard X.509 V3, RFC3280 "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*", ETSI TS 101 862 "*European profile for Qualified Certificates"* and the RFC 3739 "*Qualified Certificates Profile*".

Digital Certificates issued under this Policy are qualified certificates according to Directive 1999/93/EC, Annex I and its legal transposition into national law, and the European Technical Specification TS 101 456.

Digital Certificates issued under this Policy, should include at least the following fields:

- The specification that they are qualified Certificates
- An unique serial number for the Certificate
- An issued CA signature to authenticate the Certificate
- Name of the issuing CA
- Subscriber identification according to the name of the issuing CA as described in Section 3.1.
- Activation and expiry date for the Certificate

7.1.1. Description of the Certificate's Profile

The use of certificate extensions shall comply with the specifications in RFC 3280. Digital certificate should also comply with the standard X509:

Fields	
Version	V3
Serial Number	unique serial number for Certificate
Signature Algorithms	Sha1WithRSAEncryption
issuer	
Not before	Activation certificate
Not after	Expiry certificate
Subject	(As Described in Section **3.1.1**)
Public key	RSA (1024 bits)

7.1.2. Certificate Extension/ Additions to the Certificate

The following extensions could be included in the Digital Certificates:

Fields	
Issuer Alternative Name	To be determined by NCAS
Subject Alternative Name	To be determined by NCAS
Key Usage	To be determined by NCAS
Extended Key Usage	To be determined by NCAS
Netscape Certification Type	To be determined by NCAS
Netscape-ca-policy-url	To be determined by NCAS
Netscape Comment	To be determined by NCAS
Authority Key Identifier	To be determined by NCAS
(Subject Key Identifier)	To be determined by NCAS
Subject Statement	To be determined by NCAS
(CRL Distribution Point)	To be determined by NCAS
Basic Constraints	To be determined by NCAS
Authority Information Access	To be determined by NCAS

1.3.6.1.5.5.7.1.3 Qc Statements x.509v3 certificate extension from RFC 3039	To be determined by NCAS

7.1.3. Algorithm object identifiers

The identifier for the object algorithm signature should be:
1. 2. 840. 113549. 1. 1. 5 SHA-1 with RSA Encryption

The identifier for the object algorithm public key should be:
1.2.840.113549.1.1.1 rsa Encryption

7.1.4. Name forms

To be determined by NCAs.

7.1.5. Name constraints

NCAs should avoid any accents or Umlaut in the names included in the certificate.

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. 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 Constraints extension

To be determined by NCAs.

7.1.8. Policy qualifiers syntax and semantics

To be determined by NCAs.

7.1.9. Processing semantics for the critical certificate policy extension

To be determined by NCAs.

7.2. CRL Profile

7.2.1. Version number

The version number shall be 2 (two), as defined in RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

7.2.2. Publication

CRLs must be issued and published periodically, even if there is no change to the certificate status information, or more frequently when end entity certificates are suspended or revoked.

7.2.3. CRL Profile

The CRLs should include, at least, the following options for extension:

Fields
Version
Validity not after
Validity not before
Signature Algorithms
Serial
CRL distribution point

8. Specification administration

8.1. Specification change procedures

The CCBE can make changes to this policy. In case of substantial changes of the policy all NCAs and users shall be notified in advance. Moreover, NCAs update the policy in accordance with the policy changes.

Also policy changes that imply only minor technical adjustments shall be notified in advance.

8.2. Publication and notification policies

An electronic copy of this document, digitally signed by an authorised representative of the CCBE, is available in electronic form on the Internet.

Annex 1 ACRONYMS

CA	*Certification Authority*
CCBE	*Council of Bars and Law Societies of Europe*
CP	*Certification Policy*
CPS	*Certification Practice Statement*,
CRL	*Certificate revocation list*,
CSR	*Certificate Signing request*,
DES	*Data Encryption Standard*.
DN	*Distinguished Name*,
DSA	*Digital Signature Algorithm*.
FIPS	*Federal information Processing Standard publication*
IETF	*Internet Engineering task force*
ISO	*International Organisation for Standardization*.
ITU	*International Telecommunications Union.*
LDAP	*Lightweight Directory Access Protocol*.
NCA	*National Certification Authority*
OCSP	*On-line Certificate Status Protocol.*
OID	*Object identifier*.
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
RA	*Registration Authority*
RFC	*Request For Comments*
RSA	*Rivest-Shimar-Adleman*.
SHA-1	*Secure Hash Algorithm*.
SSCD	*Secure Signature Creation Device*