Allianz Managed Operations & Services SE

Certification Practice Statement for Allianz Group Root Certification Authority

Information Owner: Allianz Managed Operations & Services SE
Version 3.3 / 17.02.2012
Document-ID: AZ-RCACPS
Classification: public

Change management

Version	Description	Date	Author
0.1	Preliminary CPS	1.10.2002	S. A. Guenther
0.2	Minor Changes, First Publishing	21.11.02	SAG
1.0	Certificate Application; PAC	06.12.2002	Heyden/Westebbe
1.1	Complete Review	18.2.2004	GIM
1.5	Review subject to RFC 3647	31.08.2005	Secaron AG
2.0	New Version	31.12.2005	Group IT
2.1	Review CS 4D	1.6.2006	Westebbe
3.0	New Version	22.01.07	Group IT
3.1	Review AG6DCI07	15.12.2010	Andre Witwer
3.2	Review A-ITNCV04	27.12.2011	Andre Witwer
3.3	Classification change to public; NCV04 change to CCN03	17.02.2012	Andre Witwer.

Content

1 Introduction 12

1.1 Overview 12

1.2 Document Name and Identification 13

1.3 PKI Participants 13

1.3.1 Certification Authorities 13

1.3.2 Registration Authorities 13

1.3.3 Subscribers 13

1.3.4 Relying parties 14

1.4 Certificate Usage 14

1.4.1 Allowed Certificate Usage 14

1.5 Policy Administration 15

1.5.1 Organization administering the document 15

1.5.2 Contact person 15

1.5.3 Entity determining CPS suitability for the policy 15

1.5.4 CPS approval procedures 15

1.6 Definitions and Acronyms 15

2 Publication and Repository Responsibilities 16

2.1 Repositories 16

2.2 Publication of certification information 16

2.3 Time or frequency of publication 16

2.4 Access controls on repositories 16

3 Identification and Authentication 17

3.1 Naming 17

3.1.1 Types of names 17

3.1.2 Need for names to be meaningful 17

3.1.3 Anonymity or pseudonymity of subscribers 17

3.1.4 Rules for interpreting various name forms 17

3.1.5 Uniqueness of names 17

3.1.6 Recognition, authentication, and role of trademarks 17

3.2 Initial Identity Validation 17

3.2.1 Method to prove possession of private key 17

3.2.2 Authentication of organization identity 18

3.2.3 Authentication of individual identity 18

3.2.4 Non-verified subscriber information 18
3.2.5 Validation of authority 18
3.2.6 Criteria for interoperation 18

3.3 Identification and Authorization for Re-key Requests 18
3.3.1 Identification and authentication for routine re-key 18
3.3.2 Identification and authentication for re-key after revocation 18

3.4 Identification and Authorization for Revocation Requests 18

4 Certificate Life-Cycle Operational Requirements 20

4.1 Certificate Application 22
4.1.1 Who can submit a certificate application? 22
4.1.2 Enrolment process and responsibilities 22

4.2 Certificate Application Processing 22
4.2.1 Performing identification and authentication functions 22
4.2.2 Approval or rejection of certificate applications 23
4.2.3 Time to process certificate applications 23

4.3 Certificate Issuance 23
4.3.1 Certificate Requests 23
4.3.2 Verification and Rejection of Certificate Requests 23
4.3.3 CA actions during certificate issuance 23
4.3.4 Notification to subscriber by the CA of issuance of his certificate 24

4.4 Certificate Acceptance 24
4.4.1 Conduct constituting certificate acceptance 24
4.4.2 Publication of the certificate by the CA 24
4.4.3 Notification of certificate issuance by the CA to other entities 24

4.5 Key Pair and Certificate Usage 24
4.5.1 Subscriber private key and certificate usage 25
4.5.2 Relying party public key and certificate usage 26

4.6 Certificate Renewal 26
4.6.1 Circumstance for certificate renewal 26
4.6.2 Who may request renewal 26
4.6.3 Processing certificate renewal requests 26
4.6.4 Notification of new certificate issuance to subscriber 26
4.6.5 Conduct constituting acceptance of a renewal certificate 27
4.6.6 Publication of the renewal certificate by the CA 27
4.6.7 Notification of certificate issuance by the CA to other 27

4.7 Certificate Re-key 27

4.7.1 Circumstance for certificate re-key 27
4.7.2 Who may request certification of a new public key 27
4.7.3 Processing certificate re-keying requests 27
4.7.4 Notification of new certificate issuance to subscriber 27
4.7.5 Conduct constituting acceptance of a re-keyed certificate 28
4.7.6 Publication of the re-keyed certificate by the CA 28
4.7.7 Notification of certificate issuance by the CA to other entities 28

4.8 Certificate Modification 28
4.8.1 Circumstance for certificate modification 28
4.8.2 Who may request certificate modification 28
4.8.3 Processing certificate modification requests 28
4.8.4 Notification of new certificate issuance to subscriber 28
4.8.5 Conduct constituting acceptance of modified certificate 28
4.8.6 Publication of the modified certificate by the CA 28
4.8.7 Notification of certificate issuance by the CA to other 28

4.9 Certificate Revocation and Suspension 28
4.9.1 Circumstances for revocation 28
4.9.2 Who can request revocation 29
4.9.3 Procedure for revocation request 29
4.9.4 Revocation request grace period 29
4.9.5 Time within which CA must process the revocation request 29
4.9.6 Revocation checking requirement for relying parties 30
4.9.7 CRL issuance frequency (if applicable) 30
4.9.8 Maximum latency for CRLs (if applicable) 30
4.9.9 On-line revocation checking requirements 30
4.9.10 Other forms of revocation advertisements available 30
4.9.11 Special requirements re key compromise 30
4.9.12 Circumstances for suspension 30
4.9.13 Who can request suspension 30
4.9.14 Procedure for suspension request 30
4.9.15 Limits on suspension period 30

4.10 Certificate Status Services 30
4.10.1 Operational characteristics 31
4.10.2 Service availability 31
4.10.3 Optional features 31

4.11 End of Subscription 31

4.12 Key Escrow and Recovery 31

4.12.1 Key escrow and recovery policy and practices 31
4.12.2 Session key encapsulation and recovery policy and practices 31
5 Facility, Management, and Operational Controls 32
5.1 Physical Security Controls 32
5.1.1 Site location and construction 32
5.1.2 Physical access 32
5.1.3 Power and air conditioning 32
5.1.4 Water exposures 32
5.1.5 Fire prevention and protection 32
5.1.6 Media storage 32
5.1.7 Waste disposal 32
5.1.8 Off-site backup 32
5.2 Procedural Controls 32
5.2.1 Trusted roles 33
5.2.2 Number of persons required per task 33
5.2.3 Identification and authentication for each role 33
5.3 Personnel Controls 33
5.3.1 Qualifications, experience and clearance requirements 33
5.3.2 Recruitment and Qualification of Personnel 34
5.3.3 Background check procedures 34
5.3.4 Training requirements 34
5.3.5 Retraining frequency and requirements 34
5.3.6 Job rotation frequency and sequence 34
5.3.7 Sanctions for unauthorized actions 34
5.3.8 Independent contractor requirements 34
5.3.9 Documentation supplied to personnel 34
5.4 Audit Logging Procedures 35
5.4.1 Types of events recorded 35
5.4.2 Frequency of Processing Log 35
5.4.3 Retention period for Audit Log 35
5.4.4 Protection of Audit Log 35
5.4.5 Audit log backup procedures 35
5.4.6 Audit collection system (internal vs. external) 35
5.4.7 Notification to event-causing subject 36
5.4.8 Vulnerability assessments 36
5.5 Records Archival 36
5.5.1 Types of records archived 36

5.5.2 Retention period for archive 37
5.5.3 Protection of archive 37
5.5.4 Archive backup procedures 37
5.5.5 Archive collection system (internal or external) 37
5.5.6 Procedures to obtain and verify archive information 37

5.6 Key Changeover 37

5.7 Compromise and Disaster Recovery 38

5.7.1 Incident and compromise handling procedures 38
5.7.2 Computing resources, software, and/or data are corrupted 38
5.7.3 Entity private key compromise procedures 39
5.7.4 Business continuity capabilities after a disaster 39

5.8 CA or RA Termination 39

5.8.1 Keys and Certificates 39

6 Technical Security Controls 41

6.1 Key Pair Generation and Installation 41

6.1.1 Key pair generation 42
6.1.2 Private key delivery to subscriber 42
6.1.3 Public key delivery to certificate issuer 42
6.1.4 CA public key delivery to relying parties 42
6.1.5 Key sizes 42
6.1.6 Public key parameters generation and quality checking 43
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 43

6.2 Private Key Protection and Cryptographic Module Engineering Controls 43

6.2.1 Cryptographic module standards and controls 43
6.2.2 Private key (n out of m) multi-person control 43
6.2.3 Private key escrow 43
6.2.4 Private key backup 43
6.2.5 Private key archival 43
6.2.6 Private key transfer into or from a cryptographic module 43
6.2.7 Private key storage on cryptographic module 43
6.2.8 Method of activating private key 44
6.2.9 Method of deactivating private key 44
6.2.10 Method of destroying private key 44
6.2.11 Cryptographic Module Rating 44

6.3 Other Aspects of Key Pair Management 44

6.3.1 Public Key Archival 44
6.3.2 Usage Periods for the Public and Private Keys 44

6.4 Activation Data 44
6.4.1 Activation data generation and installation 44
6.4.2 Activation data protection 44
6.4.3 Other aspects of activation data 44
6.5 Computer Security Controls 45
6.6 Life Cycle Security Controls 45
6.6.1 System Development Controls 45
6.6.2 Security Management Controls 45
6.6.3 Life cycle security controls 45
6.7 Network Security Controls 45
6.8 Timestamping 45
7 Certificate, CRL, and OCSP Profiles 46
7.1 Certificate Profile 46
7.1.1 Key Usage 46
7.1.2 Certificate Policies 46
7.1.3 Version number(s) 46
7.1.2 Certificate extensions 46
7.1.3 Algorithm object identifiers 47
7.1.4 Name formats 47
7.1.5 Name constraints 47
7.1.6 Certificate policy object identifier 47
7.1.7 Usage of Policy Constraints extension 47
7.1.8 Policy qualifiers syntax and semantics 47
7.1.9 Processing semantics for the critical Certificate Policies extension 47
7.2 CRL Profile 47
7.2.1 Version number(s) 47
7.2.2 CRL and CRL entry extensions 47
7.3 OCSP Profile 48
7.3.1 Version number(s) 48
7.3.2 OCSP extensions 48
7.3.3 Reference 48
8 Compliance Audit and Other Assessment 49
8.1 Frequency or circumstances of assessment 49
8.2 Identity/qualifications of assessor 49
8.3 Assessor's relationship to assessed entity 49

8.4 Topics covered by assessment 49
8.4.1 Initial compliance audit 49
8.4.2 Ongoing compliance audit 49
8.5 Actions taken as a result of deficiency 50
8.6 Communication of results 50
9 Other Business and Legal Matters *51*
9.1 Fees 51
9.1.1 Certificate issuance or renewal fees 51
9.1.2 Certificate access fees 51
9.1.3 Revocation or status information access fees 51
9.1.4 Fees for other services 51
9.2 Financial Responsibility 51
9.2.1 ***Insurance*** coverage 51
9.2.2 Other assets 51
9.2.3 Insurance or warranty coverage for end-entities 52
9.3 Confidentiality of Business Information 52
9.3.1 Allianz Group RCA Documentation 52
9.3.2 Scope of confidential information 52
9.3.3 Types of Information in particular considered confidential 52
9.3.4 Information not within the scope of confidential information 53
9.3.5 Responsibility to protect confidential information 53
9.4 Privacy of Personal Information 53
9.4.1 Privacy plan 53
9.4.2 Information treated as private 53
9.4.3 Information not deemed private 53
9.4.4 Responsibility to protect private information 53
9.4.5 Notice and consent to use private information 53
9.4.6 Disclosure pursuant to judicial or administrative process 53
9.4.7 Other information disclosure circumstances 53
9.5 Intellectual Property Rights 53
9.5.1 Property in Certificates 53
9.5.2 Certificate 53
9.5.3 Distinguished Names 54
9.5.4 Copyright 54
9.6 Representations and Warranties 54
9.6.1 CA representations and warranties 54

9.6.2 RA representations and warranties 54
9.6.3 Subscriber representations and warranties 54
9.6.4 Relying party representations and warranties 54
9.6.5 Representations and warranties of other participants 54
9.7 Disclaimers of Warranties 54
9.8 Limitations of Liability 54
9.8.1 Safeguards 54
9.9 Indemnities 55
9.10 Term and Termination 55
9.10.1 Term Allianz Group Root certificate 55
9.10.2 Termination 55
9.10.3 Effect of termination and survival 56
9.11 Individual Notices and Communications with Participants 56
9.12 Amendments 56
9.12.1 Notification mechanism and period 56
9.12.2 Circumstances under which OID must be changed 56
9.13 Dispute Resolution Procedures 56
9.14 Governing Law 56
9.15 Compliance with Applicable Law 56
9.16 Miscellaneous Provisions 56
9.16.1 Entire agreement 56
9.16.2 Assignment 57
9.16.3 Severability 57
9.16.4 Enforcement (attorneys' fees and waiver of rights) 57
9.16.5 Force Majeure 57
9.16.6 Other Provisions 57
10 Appendix 58
10.1 Root CA Signing Key Certificate Profile 58
10.2 Participant CA Key Signing Certificate Profile 59
10.3 Definitions and Acronyms 61

References

[AZ-SP]	Allianz Group IT Security Policy
[AZ-BCM]	Allianz Group Business Continuity Management Policy and Standards
RFC 3647	Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework

1 Introduction

1.1 Overview

This Certification Practice Statement (CPS) is written to support the use of all types of certificates under the Allianz Group Root Certification Authority (Allianz Group RCA).

The Allianz Group RCA system is designed and is operated to comply with the broad strategic direction of the existing international standards for the establishment and operation of a Public Key Infrastructure (PKI) for members of Allianz worldwide. Certificate services are to be considered as one of many elements in an framework of mechanisms, controls and procedures that protect and facilitate an organisation's electronic business. Allianz Group RCA's certificate services provide a range of security and assurance levels to support the use of various certificates created under the Allianz Group RCA System.

Allianz Group RCA has established the Root CA under which a number of subordinate entities operate. The Root CA provides the subordinate entities with Issuer Certificates enabling them to issue Identity and Utility Certificates to their subscribers. The operating model of the Allianz Group RCA includes three primary parties: Allianz Group RCA, participating organisation and related participants, i.e. systems, employees, and customers. Cf. Figure 1 for the resulting trust relationships.

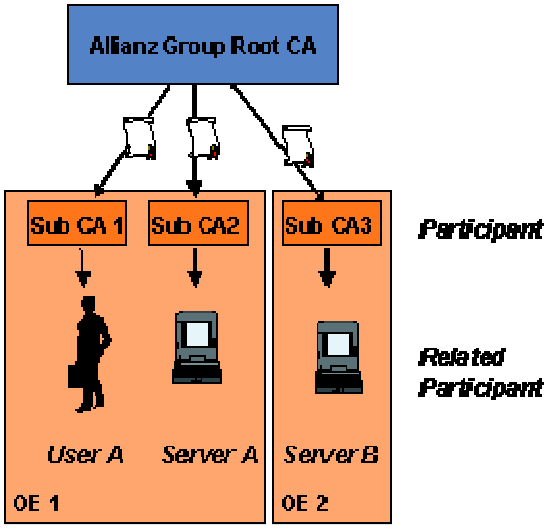

Figure 1: Allianz Group RCA Operating Model

The practices in this CPS:

1. Focus primarily on the operations of the Allianz Group RCA;
2. Accommodate the diversity of the community and the scope of applicability within the Allianz Group RCA chain of trust;
3. Adhere to the primary purpose of the CPS, of ensuring the uniformity and efficiency of practices throughout the PKI. In keeping with their primary purpose, the practices in this CPS are the minimum requirements necessary to ensure that participating organisations have the highest possible level of assurance and that critical functions are provided at appropriate levels of trust.

The structure of this CPS is based on Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC3647].

All certificate operations comply with:

1. The policy requirements of:
   - this CPS;
   - the Allianz Group Security Policy [AZ-SP]
2. The technology requirements of:
   - Relevant internal guidelines for the physical protection of technology assets;
   - X.500 directory services;
   - X.509 certificate format;
   - X.509 CRL format;
   - X.500 Distinguished name standards;
   - PKCS#7 format for Digital Encryption and Digital Signatures;
   - PKCS#10 certificate request format;
   - Recognised PKI conventions and standards.
3. Legal requirements of domestic and, where applicable, international privacy legislation;
4. Appropriate international and domestic standards relevant to PKI operations;
5. Audit requirements for certificate operations.

1.2 Document Name and Identification

The CPS at hand is referred to as the “Allianz Group Root Certification Authority Certification Practice Statement”, or abbreviated “Allianz Group RCA CPS”.

The structure of this CPS is based on Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC3647].

The OID of the CPS at hand is 1.3.6.1.4.1.7159.30.1

1.3 PKI Participants

1.3.1 Certification Authorities

Allianz Group RCA logical architecture consists of

- Allianz Group Root Certification Authority, RCA
- Sub CAs operated by the participating organisations;

1.3.2 Registration Authorities

- Registration Authorities are handling incoming certification requests for the respective CA; They can be located inside or outside of RCA or the participating organisations.

1.3.3 Subscribers

Subscribers of RCA are Sub CAs with commitment to the contract with RCA and provided with a certificate from Allianz Group RCA.

Each participating Sub CA consists of at least the following components:

- Documentation

An entity seeking to become a participating organisation shall provide to Allianz Group RCA documentation satisfying to enable Allianz Group RCA to undergo the acceptance procedure. Allianz Group RCA in its sole discretion determine whether an entity satisfies such conditions of eligibility.

Documentation in particular include the Certification Practise Statement of the Sub CA, and a compliance statement concerning Allianz Group Security Policy [AZ-SP].

- Registration Authority, RA

  The interface to submit certificate requests to and to obtain digital certificates from the respective Sub CA.

- Certificates

  Each participating Sub CA issues digital certificates for (a) subscriber identity keys, or (b) utility keys. The use of all digital certificates must conform to the Allianz Group RCA operating requirements and rules as stipulated in chapter 4 of this CPS.

- Directory Service

  A repository, which stores digital certificates and CRLs issued by the participating Sub CA.

- Certificate Status Information

  A component which provides status information on all digital certificates issued by the respective Sub CA. This functional requirement does not impose a requirement to implement a CRL mechanism. Each participating organisation will be responsible for maintaining an appropriate mechanism to ensure that it is able to supply timely digital certificate status.

- Secure Key Storages

  Key generation and storage must be compliant to the minimum operational requirements of Allianz Group RCA published in this CPS.

1.3.4 Relying parties

Customers and employees of the participating organisations.

1.3.5 Other participants

No external certificate manufacturing authorities or providers are part of RCA PKI architecture.

1.4 Certificate Usage

1.4.1 Allowed Certificate Usage

Certificates issued by the Allianz Group RCA are used to support secure communication and the secure exchange of information between organisational entities operating within the Allianz Group. The practices described in this CPS support a large, diverse and widespread community of users who require PKI services in support of subscriber identification and secured transactions.

A subscriber of Allianz Group RCA **must** provide the supported applications and certificate usages as part of his CPS. Most relevant are the key usages of issued certificate profile.

1.4.2 Prohibited certificate usage

As Allianz Group RCA does not support applications directly, a description of supported applications is given in the CPS of the participating Sub CAs.

1.5 Policy Administration

1.5.1 Organization administering the document

Responsible for this CPS is

Allianz Managed Operations & Services SE

A-IT05CCN03 – Network Management & PKI Services

Gutenbergstrasse 8

85774 Unterföhring

Germany

1.5.2 Contact person

Inquiries or other communications about this document should be addressed to:

Allianz Managed Operations & Services SE

A-IT05CCN03 – Network Management & PKI Services

Gutenbergstrasse 8

85774 Unterföhring

Germany

or to

rootca@allianz.com

1.5.3 Entity determining CPS suitability for the policy

Within the Allianz Group RCA the Policy Approval Council (PAC) has been established to maintain the integrity of the policy infrastructure in the Allianz Group RCA System. PAC determines CPS suitability to the policy infrastructure. In addition, a subscriber contract between SUB CAs and Allianz Group RCA is concluded. The contract defines the legal basis between subscriber and Allianz Group RCA internally and adjusts the disclaimer of warranties for Allianz Group RCA and subscriber.

1.5.4 CPS approval procedures

An entity seeking to become a participating organisation shall provide to Allianz Group RCA documentation satisfactory to enable Allianz Group RCA to undergo the acceptance procedure. Allianz Group RCA in its sole discretion determine whether any entity satisfies such conditions of eligibility.

Documentation in particular include the Certification Practise Statement of the Sub CA and a compliance statement concerning Allianz Group Security Policy [AZ-SP].

1.6 Definitions and Acronyms

Definitions and Acronyms are part of the appendix 10.5 to this CPS.

2 Publication and Repository Responsibilities

Information relating to Allianz RCA policies for PKI participants is available at the Allianz Group RCA Internet Site: http://rootca.allianz.com. The access to this information is not limited to participating members only.

2.1 Repositories

All confidential information disclosed hereunder shall remain the property of the informant. No recipient shall disclose any information for any purpose. The degree of care required of the recipient regarding the prevention of disclosure of the informant's confidential information shall be at least the degree of care the recipient uses to protect its own similar confidential information, but in no event shall the recipient exercise less than reasonable care.

Confidential information shall include any and all information disclosed by Allianz Group RCA or a participating organisation (each an “Informant”) to a participant of the Allianz Group PKI (each a “Recipient”). Confidential information of Allianz Group shall include any information concerning the Allianz Group RCA Services or the Allianz Group RCA System or technology and information belonging to Allianz Group RCA, which are marked “confidential” or “proprietary”.

Participants **must** provide access to revocation information data. The participant guarantees the correct supply of this service and **must** assure that personal data are not published via the RCA communication channels.

2.2 Publication of certification information

New or amended policies are published on the internet web site nominated for Allianz Group RCA documentation. Subordinate parties are notified by the appropriate certification authority of changes to a policy as and when they are approved. Sub CAs are advised of the changes a minimum of one week prior to publication.

2.3 Time or frequency of publication

The CRLs created by the Allianz Group RCA will be issued to the web server at a minimum once every three month and whenever a change in the CRL occurred.

The central repository for the Allianz Group RCA System is the Allianz Group Directory (GD).

The Allianz Group RCA promptly publishes new certificates and changes in certificate status, including revocation and expiry to its repository.

2.4 Access controls on repositories

The subscriber or operating company of the revocation service warrants a duly operated access control avoiding all uncontrolled changes of all revocation information.

3 Identification and Authentication

A fundamental concept underpinning the operation of Allianz Group RCA's PKI is **trust**. Trust must be realised in each and every aspect of the service operation. At Allianz Group RCA's discretion, other trustworthy parties are permitted to operate Certification Authority and Registration Authority services within Allianz Group RCA's chain of trust.

To ensure the integrity and trustworthiness of operations throughout the PKI hierarchy, participating Sub CAs and their related RAs must agree during registration to comply with the practices of Allianz Group RCA defined in this CPS and the Allianz Group Security Policy [AZ SP].

3.1 Naming

3.1.1 Types of names

All certificate holders require a Distinguished Name that is in compliance with the X.501 standard for Distinguished Names. The attribute CommonName (CN) must be part of Subject DN and Issuer DN.

3.1.2 Need for names to be meaningful

Distinguished Names are to be unambiguous and unique.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

Certificates issued by participants and used for secure email must contain the email address of the Certificate holder.

3.1.5 Uniqueness of names

The Allianz Group RCA approves naming conventions for the creation of distinguished names for certificate applicants.

3.1.6 Recognition, authentication, and role of trademarks

No Stipulation.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

The registrar takes appropriate steps to ensure the subscriber is the true owner of the key pairs. Such steps typically consist of:

1. The Registration Authority checking its records to ensure that public keys are not already listed against any current operational or revoked certificate;
2. Additionally, if deemed appropriate, obtaining a document from the subscriber that it is the true owner of the key pairs;

3. Finally, the RCA has the option of exchanging signed and encrypted messages with the PKI participants, to verify use of new keys. If any doubt exists, the RCA is not to perform certification of the key.

3.2.2 Authentication of organization identity

The subscriber's identity is to be authenticated during an interview with an authorised registrar of the respective RA.

3.2.3 Authentication of individual identity

The RA warrants the reliable identification and checking of application data within the scope of the Allianz Group RCA security policy.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

The process of checking that the applicant is allowed to apply for certificates **must** be documented.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and Authorization for Re-key Requests

3.3.1 Identification and authentication for routine re-key

Allianz Group RCA's keys are not re-keyed or rolled-over. When root keys expire, a complete new set of root keys is generated.

3.3.2 Identification and authentication for re-key after revocation

Subscribers may request certificate re-issue provided that after investigation into the reason for the revocation of any certificate, Allianz Group RCA may issue a replacement for a revoked certificate, if it concludes in its discretion it is consistent with the preservation of the integrity of the Allianz Group RCA System.

In any other case, the subscriber must apply for a new certificate, providing all information and documentation required at an initial registration interview. Key pairs must always expire at the same time as the associated certificate. When a subscriber requests certificate renewal, new key pairs have to be generated.

3.4 Identification and Authorization for Revocation Requests

A request to revoke keys and certificates, if initiated by an authorised PKI participant (i.e. the subscriber itself or the issuing CA), constitutes a valid revocation request. Only a subscriber or a participating organisation can generate a valid revocation request for the respective certificates.

- Each participating organisation may only request revocation for certificates issued by any of the Sub CAs operated by it.
- Each subscriber may only request revocation of certificates assigned to it during the registration process.

- Certificates issued by the Allianz Group RCA are revoked by the RCA itself.

The revocation request **should** be preferentially sent via email, digitally signed with the certificate whose respective public key needs to be revoked.

4 Certificate Life-Cycle Operational Requirements

The purpose of this chapter is to identify the Allianz Group RCA Certificate Management Life Cycle.

This includes the two different certificate states as part of the certificate life cycle and the certificate types supported by the Allianz Group RCA System.

The responsibility for defining, creating and providing operational support for the certificate states described here rests with the Reviewing Officer of Allianz Group RCA. This responsibility may be delegated to nominated persons.

Authority for approving new certificate types and Certificate Policies (CPs) rests with the Allianz Group RCA Policy Council (PAC).

All certificate operations will comply with the requirements of:

- an applicable certificate policy (CP);
- an applicable CPS
- the minimum operational requirements and operating rules of Allianz Group RCA system and
- legal requirements of domestic and, where applicable, international privacy legislation.

Appropriate operational and audit records will be maintained for all certificate states.

The life cycle of an Allianz Group RCA certificate starts when a certificate is requested and generated, and ends when the certificate expires or is revoked. During this time, a certificate can move through a number of different states. The Allianz Group RCA Certificate Life Cycle in figure 2 below illustrates the states that may apply to an Allianz Group RCA certificate during its life cycle. Note that the diagram applies to all types and grades of certificates issued in the Allianz Group RCA System, although not all certificates will traverse all state changes.

These are the states a certificate undergoes as part of its normal lifecycle (primary states):

- Generation;
- Operational Use;
- Expiry; and
- Archive.

Allianz Group RCA certificates may be revoked before the end of their regular lifetime when the private key related to a certificate is suspected of, or is compromised or for other reasons that may be determined by the issuer (secondary state).

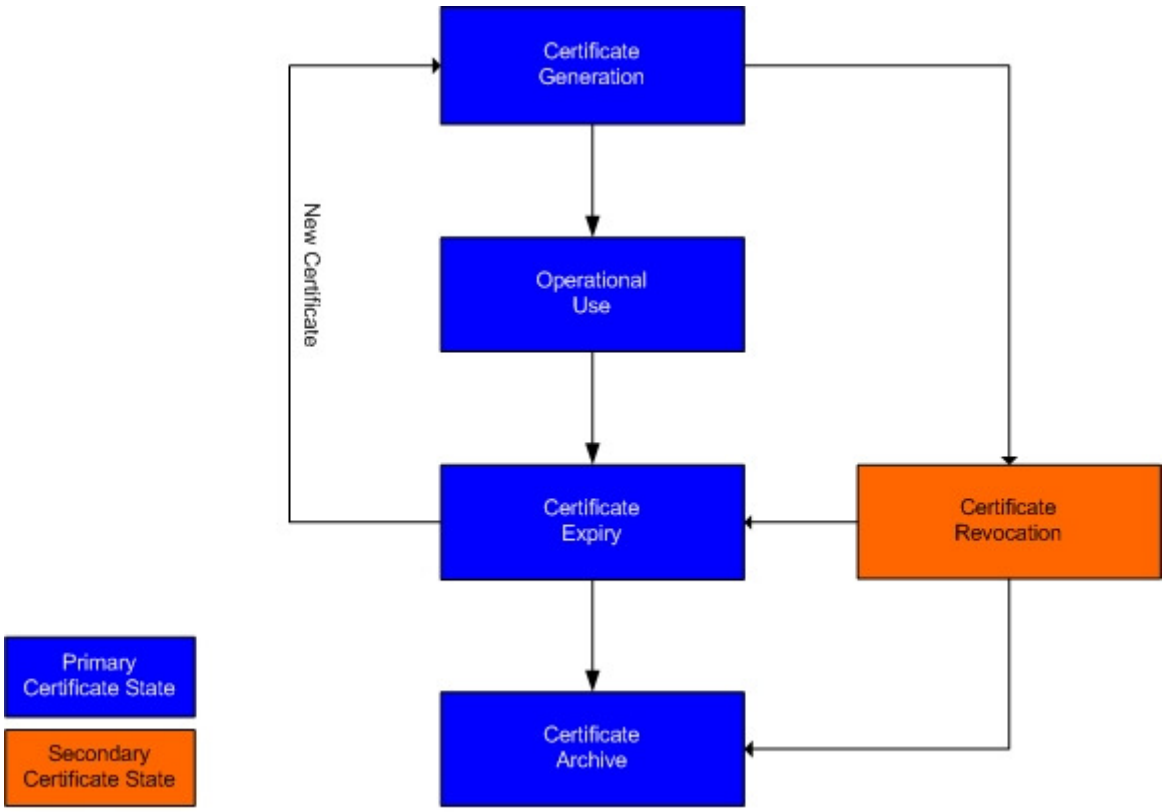

Figure 2: Allianz Group RCA Certificate Life Cycle

All certificates within the Allianz Group RCA system, after completing their primary life cycle may require re-issuance. This rollover has to be conducted in a manner that does not halt or interrupt any certificate based operations. This section provides details of the Allianz Group RCA certificate life cycle including the time at which a new replacement certificate is introduced within the system. Figure 3 depicts the typical rollover for the Allianz Group RCA certificate roll-over of the Root CA and the participating Sub CAs.

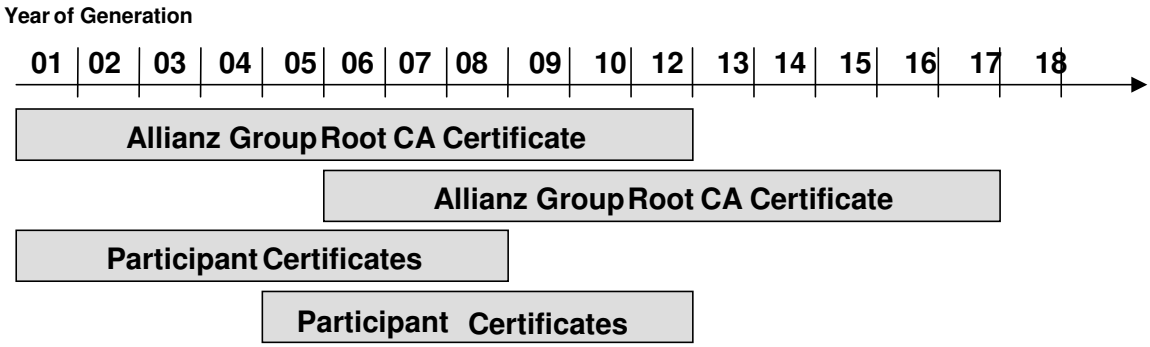

Figure 3: Allianz Group RCA Certificate Rollover

To prevent problems with nested certificates, each 5 years a new Root CA is created. After a new Root CA has been created, the old Root CA must no longer issue any certificates but may continue with generating CRLs until the respective CRL signing certificate expires.

The same applies for each Sub CA. 4 years before the respective certificate signing certificate expires, a new Sub-CA is installed by the responsible participating organisation. From the

moment on, the new Sub-CA is in place, the old Sub CA must no longer issue any certificates but may continue with generating CRLs until the respective CRL signing certificate expires.

All CAs must thus determine the process for key rollover ensuring minimal disruption to subscribers and relying parties.

4.1 Certificate Application

Allianz Group RCA provides the participating organisations with issuer certificates for their respective Sub CAs by request.

4.1.1 Who can submit a certificate application?

Requests can only be submitted by authorized personnel of organisations that have prior be accepted as participating organisations, cf. section 1.3. The enrolment process is describes in section 4.2.

RCA requires that such Sub CAs must not be subordinate to any other certification authority.

4.1.2 Enrolment process and responsibilities

For the enrolment process each participant will request certification electronically by sending an email to Allianz Group RCA (*rootca@allianz.com*). Only one email per certification is permitted.

The participants presents the CPS to Allianz Group RCA Policy Council (PAC). PAC is responsible for approving CPS of participant CA, new certificate types and Certificate Policies. After attesting the conformity of the CPS of the participating Sub CA to Allianz Group Root CA CPS, the certificate request of the Sub CA can be submitted.

4.2 Certificate Application Processing

Allianz Group RCA will follow the procedures specified here as part of the certificate management lifecycle described in chapter 4 to confirm that the process has been adhered by the participating Sub CA.

4.2.1 Performing identification and authentication functions

Allianz Group RCA participating Sub CAs do generate their own keys. Thereby, key generation and storage in hardware is the preferred way.

Each participant will request certification electronically by sending an email to Allianz Group RCA (*rootca@allianz.com*). Only one email per certification is permitted.

The issued request has to contain (at least) the following extensions:

- Basic Constraints = CA (critical)
- PathLenConstraint - Where it appears, the pathLenConstraint field MUST be a fixed integer value defined by the PAC defining the maximum number of SUB-CAs allowed.
- Key Usage (keyCertSign and/or cRLSign) (critical).
- Subject Key ID (calculated using a 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (issuing certificate)).

Procedures have been established within Allianz Group RCA to ensure the authenticity and security of certificate requests. Further extensions must be approved by PAC.

4.2.2 Approval or rejection of certificate applications

Allianz Group RCA carries out the following checks:

1. Check email to confirm that it was transmitted by a member of Allianz Group.
2. The integrity of the message has not been compromised.
3. The content of the request file is correct (all fields and extensions are complete and conforming to naming conventions).
4. Ensure the certificate request has not been tampered.

4.2.3 Time to process certificate applications

Allianz Group RCA informs the applicant about the actual status of processing the request.

4.3 Certificate Issuance

Allianz Group RCA acts as the central certification authority for all participating subordinate CAs operated by Allianz Group RCA participating organisations.

The Allianz Group RCA takes reasonable care in accepting and processing certificate requests. It complies with the practices described in this CPS and with any requirements imposed by this CPS. In particular, care is taken to ensure certificate information does not contain any factual misrepresentations and that no data entry errors are made when accepting an application or generating a certificate.

4.3.1 Certificate Requests

Certificate requests are usually generated by the respective Sub CA, applying a PKCS#10 request to Allianz Group RCA. Other formats may be supported by Allianz Group RCA as well.

4.3.2 Verification and Rejection of Certificate Requests

Certificates of RCA are issued at the discretion of Allianz Group RCA. The Allianz Group RCA has the right to verify and to possibly reject a certificate request. If a certificate request is rejected, Allianz Group RCA must promptly inform the applicant.

4.3.3 CA actions during certificate issuance

The Allianz Group RCA is not responsible for monitoring, investigating or confirming the accuracy of certificate information after a certificate has been issued. Where advice is received that certificate information is inaccurate or no longer applicable, the certificate may be revoked and a new certificate applied for.

Issuance of certificate by RCA is performed only for valid certificate applications. It is documented and ensured that there exist an unambiguous correlation between subscriber and key pairs.

The main CA activities with regard to certification are to

- bind the private/public key pair associated with the certificate to customer or participant; and
- allow the certificate to be issued and used in accordance with the purposes specified in a recognised and relevant CPS.

Certificates are generated as a result of new certificate applications or certificate renewal requests.

Certificate generation involves creating, signing and issuing a certificate. It is performed in a physically secure facility on the receipt of a properly authorised digital request.

4.3.4 Notification to subscriber by the CA of issuance of his certificate

After certificate generation, the Allianz Group RCA returns the signed public key of the requesting CA in PKCS#7 format to the responsible participating organisation.

During the registration process, the Allianz Group RCA will contact the requesting participating organisation in order to verify the correctness of the certificate request.

4.4 Certificate Acceptance

A participant's receipt of a certificate, and its subsequent use of its keys and certificates, constitutes certificate acceptance.

4.4.1 Conduct constituting certificate acceptance

Before using a Sub CA certificate, the responsible participating organisation has to:

1. Confirm the continuous responsibilities, obligations and duties imposed by the General Operating Rules and the Allianz Group RCA operational requirements defined in this CPS (cf. section 4 and 6);
2. Represent and warrant that to its knowledge no unauthorised person has access to the private key associated with the Sub CA's certificate;
3. Represents and warrants that the certificate information it has supplied during the registration process is truthful and has been accurately and fully published within the certificate.

4.4.2 Publication of the certificate by the CA

Certificates are published in the Allianz Group Directory (GD). Cf. section 2.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key Pair and Certificate Usage

Understanding the life cycle of an Allianz Group RCA key supports the understanding of the Allianz Group RCA compliance requirements. Figure 4 shows the typical life cycle of an Allianz Group RCA Key Pair which equally applies to subordinate key pairs. This document will cover each activity/process shown in the lifecycle model and will be applicable to all subordinate CAs within the Allianz Group RCA System.

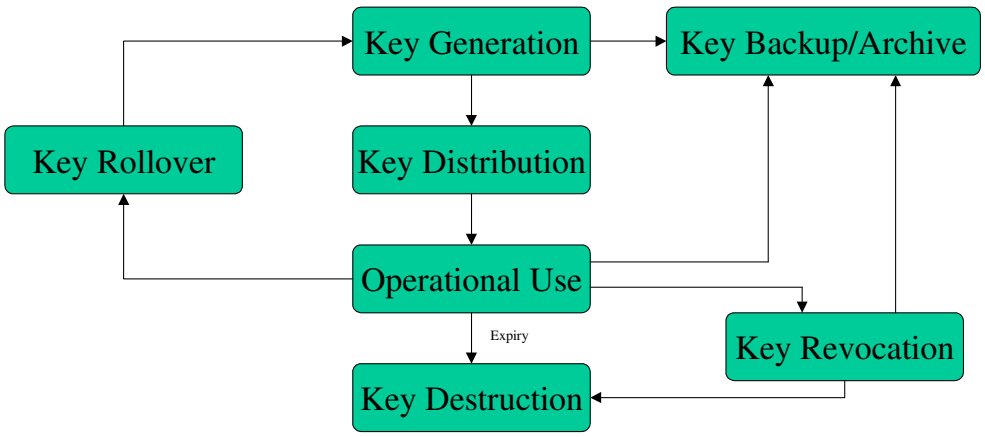

Figure 4: Allianz Group Key Life Cycle

The life cycle starts with key pair generation, which for the purposes of Allianz Group RCA is limited to generation of asymmetric cryptographic keys in hardware. At this stage the key pair, depending on its use, may be backed up. Before the key can be used, a process of secure key distribution takes place allowing the key pair to enter the operational use stage. If the key pair is compromised, the certificate related to that key pair shall be revoked. The key pair may then be archived.

Under normal circumstances, the key pair expires with the life of the associated X.509 certificate, thus ending the usable period of the keys and after which they are securely destroyed or if required archived. The user usually obtains a replacement key pair prior to its expiry. In effect, key rollover is the process by which a new key is generated prior to expiry of the current key.

Allianz Group RCA participating Sub CAs and related subscribers generate their own keys.

4.5.1 Subscriber private key and certificate usage

Allianz Group RCA certificates are used to support the Allianz Group RCA system, to enable secure electronic commerce and the secure exchange of information by electronic means, between organisational units. Certificates can only be used during their lifetimes, but cannot be used during this time if they are revoked.

Allianz Group RCA uses a number of key pairs for designated purposes. Typically, these keys fall into the types set out below:

- CA certificate and CRL signing key pairs related to either RCA or a Sub CA.
- End entity keys

All keys used in the Allianz Group RCA System are RSA keys:

Allianz Group RCA Participant Keys	Maximum Operational Life	Minimum Key Length (bits)
Allianz Group RCA Keys	12 Years	2048
Participant CA Keys	8 Years	1024

Operational life of end entity keys should be adapted to the actual technical standard and can not be longer than operational life of participant CA key.

Each Allianz Group RCA certificate has an associated CPS, which specifies the certificate's operational purpose. Before being relied on, the certificate must be processed in compliance

with RFC 3647[1] by the relying party. Any certificate issued by the RCA must be in the repository until the expiration of the certificate.

4.5.2 Relying party public key and certificate usage

The private key of the participant documented by the issued certificate can only be used for applications in accordance with the key usages given in the certificate. End entity keys can only be used for certificate based authentication, encryption and digital signing. Those keys are related to subscribers such as systems, employees or customers.

The relating private keys of any Sub CA or systems provided with a certificate by RCA has to be protected against compromise.

All certificates have a maximum fixed lifetime set by the Allianz Group RCA PAC and as indicted in Appendix A. At the end of which time they must expire. The primary reasons for having certificates expire are to:

- Guard against the possibility of long-term cryptographic attack; and
- Ensure the integrity of the Allianz Group RCA System.

A certificate is deemed to have expired when it reaches or has exceeded its expiry date. A certificate can be in any of the following states when it is due to expire:

- Operational Use; or
- Revoked.

In each case, the certificate must expire on its expiry date. When a certificate expires the certificate is archived and another certificate may be issued to the participant.

Cf. section 6.1 for details.

4.6 Certificate Renewal

Public key re-certification is currently not supported by the Allianz Group RCA System.

Key pairs must always expire at the same time as the associated certificate. When a subscriber requests certificate renewal, new key pairs have to be generated.

4.6.1 Circumstance for certificate renewal

No stipulation

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

[1] Until this CPS becomes effective, RFC 2459 was relevant.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other

No stipulation.

4.7 Certificate Re-key

The Allianz Group RCA public key is conveyed in a self-signed certificate, but the customer must gain trust in the Allianz Group RCA public key through some out-of-band means because the signature only provides integrity, not authentication.

4.7.1 Circumstance for certificate re-key

Key rollover is a condition that may be applied to any valid key. In effect, key rollover is the process by which a new key is generated prior to the expiry of the current key. All new certificates are issued with the new key; however existing keys remain operational until expiry of the related certificate.

4.7.2 Who may request certification of a new public key

Key rollover shall be conducted by Allianz Group RCA or the participating Sub CAs with the least possible impact on subscribers and relying parties. Re-keying of a Sub CA certificate is not permitted after certificate revocation. Participating Sub CAs requiring a replacement certificate after revocation must complete the complete initial registration process in order to apply for a new certificate.

4.7.3 Processing certificate re-keying requests

To prevent problems with nested subsidiary certificates, 5 years before expiry of the Allianz Group RCA Certificate, a second Root Certificate will be created.

To allow for a smooth enrolment of a new Root CA, Allianz Group RCA issues two additional cross certificates:

1. The old Allianz Group RCA public key, signed with the new private key, with validity interval the same as the old self-signed certificate; and
2. The new RCA public key, signed with the old private key, with the validity interval starting at the same time as the new self-signed certificate, and ending whenever all entities are expected to have the new self-signed certificate (at worst, the ending date on the old self-signed certificate).This will be a ‘Parallel Root Certificate' and all new participant certificates will be issued under the new Root Certificate. Once the new participant certificate is issued, the participant must not issue any new end entity certificates under the old participant certificate.

4.7.4 Notification of new certificate issuance to subscriber

Participants will be provided the new Root Certificate to include in any new certificate issued.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

For RCA initiated key roll-over no constituting acceptance is required. The process of certificate delivery to participants is the same as for initial certificate application.

4.7.6 Publication of the re-keyed certificate by the CA

RCA provides for publishing the re-keyed certificate. The certificates are stored in the Allianz Group RCA repository and accessed like any other certificate.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate Modification

4.8.1 Circumstance for certificate modification

Certificate modification is possible under the following restrictions:

a) the name in the certificate is no longer bound to the certificate holder

b) The Email address from the certificate is no longer bounded to the certificate holder

4.8.2 Who may request certificate modification

Requesting is only possible for Sub CAs under Allianz Group RCA PKI.

4.8.3 Processing certificate modification requests

Participating Sub CAs requiring a modified certificate must complete the complete initial registration process in order to apply for a new certificate.

4.8.4 Notification of new certificate issuance to subscriber

Notification is performed following the documented processes of Allianz Group RCA.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

The participating organisation is notified about publication of any related Sub CA certificate.

4.8.7 Notification of certificate issuance by the CA to other

If certificates are modified by a participating SUB CA. Notification to RCA is required.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

The purpose of revoking a certificate is to permanently prevent the future use of the certificate and its associated private/public key pair, due to a compromise in the private key, the misuse of or errors in the certificate. Each participant will establish the circumstances under which, and

manner in which, the certificates that it issues may be revoked. The circumstances under which participant's issuer certificate may be revoked are

- the security or confidentiality of the participant's private key or the root key has been compromised or is at material risk of being compromised,
- the revocation is necessary to avoid an immediate and material threat to the safe and sound operation of the Allianz Group RCA System
- the participant has terminated its participation in the Allianz Group RCA System.

Once a certificate has been revoked, it cannot revert back to operational use (valid status). If a replacement certificate is required, the respective subscriber has to apply for a new certificate. Revoked certificates should be archived to tamper evident media. All types of certificates can be revoked.

While the Allianz Group RCA does not perform suspension for their certificates.

There are no variations to the described certificate revocation procedures when the revocation is due to private key compromise.

4.9.2 Who can request revocation

Certificate revocation can be initiated by:

1. Allianz Group RCA (on behalf of Allianz Group Board), under the circumstances specified in this CPS.
2. The owner of the certificate or the issuing CA.
3. Certificate revocation information is provided via CRL, where the status response information depends on the CRL type in use.

4.9.3 Procedure for revocation request

1. The Allianz Group RCA receives a digitally signed certificate revocation request;
2. The Allianz Group RCA verifies the revocation request and revokes the certificate. Notice: Revoked Certificates are not deleted from the Allianz Group RCA's repository;
3. The Allianz Group RCA adds the revoked certificate to its list of revoked certificates. A new CRL is published at the next scheduled update to the corresponding repository;
4. The Allianz Group RCA sends a notice containing the certificate details and the date and time of revocation to the owner of the certificate. The notice must not include the reason for revocation.

The owner of a revoked certificate must continuously safeguard the private key associated to the revoked certificate, at least until the expiration date of the revoked certificate.

4.9.4 Revocation request grace period

Once a certificate has been revoked, it cannot revert back to operational use (valid status). If a replacement certificate is required, the respective subscriber has to apply for a new certificate.

4.9.5 Time within which CA must process the revocation request

The CRLs created by the Allianz Group RCA will be issued to the web server at a minimum once every three month and whenever a change in the CRL occurred. Revoked certificates must remain within the certificate repository until they expire, after which they may be archived.

4.9.6 Revocation checking requirement for relying parties

Each participating CA establishes its own technical and organisational framework in which the certificates issued by it may be revoked. This framework has to be compliant with the Allianz Group RCA operating rules.

4.9.7 CRL issuance frequency (if applicable)

See 4.10.2

4.9.8 Maximum latency for CRLs (if applicable)

Allianz Group Root CA has a maximum latency between revocation and CRL issuing of 24h. The time frame for Sub CAs may depend on the operation area and conditions.

The CRLs created by the Allianz Group RCA will be issued to the web server at a minimum once every three month and whenever a change in the CRL occurred.

4.9.9 On-line revocation checking requirements

It is required, that the relying parties must check the validity of the issuer certificate with respect to every action signed with that issuer certificate.

Allianz Group RCA provides a web page hosted CRL for verifying the status of all certificates issued by RCA. The same applies to the responsible participating organisations for the respective Sub CAs.

4.9.10 Other forms of revocation advertisements available

No stipulation.

4.9.11 Special requirements re key compromise

No stipulation.

4.9.12 Circumstances for suspension

No stipulation.

4.9.13 Who can request suspension

No stipulation.

4.9.14 Procedure for suspension request

No stipulation.

4.9.15 Limits on suspension period

No stipulation.

4.10 Certificate Status Services

Allianz Group RCA provides a web page hosted CRL for verifying the status of all certificates issued by RCA. The same applies to the responsible participating organisations for the respective Sub CAs.

4.10.1 Operational characteristics

The certificate status service of Sub CAs should be inter-operational to CRL service of Allianz Group RCA. It is required, that the Relying Parties must check the validity of the issuer certificate with respect to every action signed with that issuer certificate.

4.10.2 Service availability

The CRLs created by the Allianz Group RCA will be issued to the web server at a minimum once every three month and whenever a change in the CRL occurred. The IT Service Provider guarantees high availability of service subject to specification of SLA.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

In the event that a CA terminates operation permanently, all subscribers and participants, and all relying parties are promptly notified of the termination. Revocation of Subscriber CA is required.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

Allianz Group RCA private key escrow and recovery is not permitted.

All private keys used within the Allianz Group RCA are backed up.

All Certificates (and hence the public keys contained in them) shall be archived.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

There exist one secured CA production environment. The site will house the complete production PKI, including the CA (offline), Registration Authority, Key Generation, Web server, and value added services in a highly secured facility on two different localities. There exist a backup system. The production CA updates the CRLs. In the event that the CA becomes unavailable, the backup CA will be in place.

5.1.1 Site location and construction

The secured CA environment consists of two separated facilities. The Root Certification Authority, Registration Authority and Backup Systems operate within physically secured areas that meet the standards identified in the Allianz Group Security Policy [AZ-SP].

5.1.2 Physical access

Physical access is controlled by distributed smart cards. The CA system is in addition protected in a safe with gain access only for CA personnel.

5.1.3 Power and air conditioning

Conditions meet the standards identified in the Allianz Group Security Policy [AZ-SP].

5.1.4 Water exposures

Conditions meet the standards identified in the Allianz Group Security Policy [AZ-SP].

5.1.5 Fire prevention and protection

Conditions meet the standards identified in the Allianz Group Security Policy [AZ-SP].

5.1.6 Media storage

Conditions meet the standards identified in the Allianz Group Security Policy [AZ-SP].

5.1.7 Waste disposal

Conditions meet the standards identified in the Allianz Group Security Policy [AZ-SP].

5.1.8 Off-site backup

Conditions meet the standards identified in the Allianz Group Security Policy [AZ-SP].

5.2 Procedural Controls

Access controls and procedures are set in place to ensure that one person acting alone cannot circumvent the entire system (dual control principle). Oversight may be in the form of a person who is not directly involved in issuing certificates examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security policy. Individual threat and risk assessments are required at each subordinate entity level e.g. approved CA.

5.2.1 Trusted roles

The root functions are performed centrally. The operation of the Allianz Group RCA itself will be carried out by authorised personnel from a centralised location.

For the Allianz Group Root CA the following roles apply:

- Allianz Group RCA Registrar

  The Registrar shall be an Allianz Group employee who will process certificate requests in the Certification authority.

  Suggested level: Officer or equivalent

- Allianz Group RCA System Administrator

  The System Administrator shall be an Allianz Group employee managing the RCA systems and its databases providing functions such as (a) defining and maintaining information about participants, (b) performing backups, (c) update CRLs.

  Suggested level: Officer or equivalent

- Allianz Group RCA Auditor

  The Root Certification Authority Auditor shall be an Allianz Group employee who will be responsible for reviewing the Certification authority records to ensure that the PKI has not been compromised and procedures are being followed. This review entails verifying the audit records, validating the information in the audit records and making sure that none are missing.

  Suggested level: Vice President or equivalent

The Allianz Group RCA mandates that certain functions within the RCA System are controlled to such a level that multiple persons must be present when these functions are carried out.

5.2.2 Number of persons required per task

At least two smartcard holders are required for a task

5.2.3 Identification and authentication for each role

Deployment of Allianz Group RCA PKI system is always documented. It is always reproducible who the smartcard holders are and what kind of action have been performed on the PKI system by administrators.

5.3 Personnel Controls

The Allianz Group RCA System has adopted and employs personnel and management practices to ensure the trustworthiness, integrity and professional conduct of its staff. The personnel standards described below are applied.

5.3.1 Qualifications, experience and clearance requirements

Persons filling trusted roles (cf. section 5.2) must undergo an appropriate security screening procedure, designated “Position of Trust”.

All Allianz Group RCA operations staff:

1. are evaluated before employment to assess their suitability;
2. enter into non-disclosure agreements to protect against the unauthorised disclosure of confidential information;

3. are trained in (a) basic PKI concepts, (b) the use and operation of Certification authority software, (c) documented Certification authority procedures, (d) computer security awareness and procedures, and (f) this CPS.

5.3.2 Recruitment and Qualification of Personnel

The recruitment and selection practices for Sub CAs personnel operating under the Allianz Group RCA System take into account the background, qualifications, experience and clearance requirements of each position, which are compared against the profiles of potential candidates.

5.3.3 Background check procedures

Background checks are conducted on all persons selected to take up a trusted role in accordance with the designated security screening procedure, prior to the commencement of their duties. Operations personnel must notify their security administrator when a process or action causes a critical security event or discrepancy.

5.3.4 Training requirements

Allianz Group RCA will ensure that all staff is briefed immediately on any changes which affect current operations. Operational personnel will be trained immediately if any applications that affect operations have been either upgraded or modified due to the natural upgrade cycle or program error.

All staff of the Allianz Group RCA shall be trained in:

1. Basic PKI concepts;
2. The use and operation of certification authority software;
4. Documented procedures;
5. Computer security awareness and procedures;
6. The meaning and effect of relevant CPs, this CPS.

5.3.5 Retraining frequency and requirements

Retraining will occur at least once a year based on the necessary measurements.

5.3.6 Job rotation frequency and sequence

No stipulation.

5.3.7 Sanctions for unauthorized actions

Unauthorised actions by Allianz Group RCA System staff are submitted to appropriate authorities including, but not limited to, the Security Administrator.

5.3.8 Independent contractor requirements

No stipulation.

5.3.9 Documentation supplied to personnel

Allianz Group RCA System staff has access to all training documentation.

5.4 Audit Logging Procedures

The Allianz Group RCA and all approved Sub CAs are obliged to maintain adequate records and archives of information pertaining to the operation of the PKI. The CA software automatically preserves an audit trail for the primary states in the Allianz Group RCA certificate life cycle, i.e., generation, operational use, expiry and archive.

5.4.1 Types of events recorded

The minimum audit records to be kept include all:

1. Types of registration records, including records relating to rejected applications;
2. Certificate generation requests, whether or not certificate generation was successful;
3. Certificate issuance records, including CRLs;
4. Audit records, including security related events.

5.4.2 Frequency of Processing Log

Audit logs are processed on a daily, weekly, monthly and annual basis.

5.4.3 Retention period for Audit Log

Audit logs are retained for a minimum of seven years.

5.4.4 Protection of Audit Log

Audit logs are encrypted using a key and certificate specifically generated for the purpose.

5.4.5 Audit log backup procedures

Each service provider in the Allianz Group RCA hierarchy is to establish and maintain a backup procedure for audit logs.

5.4.6 Audit collection system (internal vs. external)

The Allianz Group RCA System audit collection system is a combination of automated and manual processes performed by the Certification authority Operating System platform (OS), the Certification authority software, and by operational personnel.

Type of event	**Collection System**	**Recorded by**
Successful and failed attempts to change operating system security parameters	Automatic	OS
Application start up and shutdown	Automatic	OS
Successful and failed login and log-off attempts	Automatic	OS, Certification authority Software
Successful and failed attempts to create, modify, or delete system accounts	Automatic	OS, Certification authority Software
Successful and failed attempts to create, modify or delete authorised system users	Automatic	OS, Certification authority Software

Type of event	Collection System	Recorded by
Successful and failed attempts to request, generate, sign, issue or revoke keys and certificates	Automatic	Certification authority Software
Successful and failed attempts to create, modify or delete Certificate Holder information	Automatic	Registration Authority Software
Backup, archiving and restoration	Automatic and Manual	OS, Certification authority Software and Operations Personnel
System configuration changes	Manual	Operations Personnel
Software and hardware updates	Manual	Operations Personnel
System maintenance	Manual	Operations Personnel
Personnel changes	Manual	Operations Personnel

5.4.7 Notification to event-causing subject

Operations personnel must notify their security administrator when a process or action causes a critical security event or discrepancy

5.4.8 Vulnerability assessments

Individual threat and risk assessments are required at each subordinate entity level e.g. approved CA.

5.5 Records Archival

Each CA in the Allianz Group RCA hierarchy maintains an archive of relevant records. This section details the RCA's records archiving procedures. Expired certificates (and CRLs if used) are archived because digitally signed or encrypted documents often outlast the validity period of the certificate used to sign or encrypt the document. Certificates whose validity period has expired must continue to be accessible to allow the certificate to be used to prove the authenticity of, a document. Archived certificates can only be accessed in authorised circumstances, for example at the participant's request or where a properly constituted subpoena or warrant is produced.

Archived certificates are to be:

- archived on tamper evident media;
- archived for a minimum period of seven years from the date of expiry, unless another period is specified in a relevant CP; and
- securely destroyed at the end of the archive period.

5.5.1 Types of records archived

The following types of information are to be recorded and archived by the Allianz Group RCA:

1. Audit logs;
2. Certificate request information;

3. Certificates, including CRLs generated;
4. Complete back up records;
5. Copies of e-mail logs;
7. Formal correspondence;
8. Application records.

5.5.2 Retention period for archive

Certificates issued by the Allianz Group RCA are archived for a minimum period of 10 years beginning with the date of expiration, unless another period is specified in the CPS of the respective Sub CA.

5.5.3 Protection of archive

Archive media is protected either by physical security or a combination of physical security and cryptographic protection. It is also protected from environmental factors such as temperature, humidity, and magnetism. Records maintained and accessed under dual control.

5.5.4 Archive backup procedures

Certificates issued by the RCA are archived for a minimum period of 10 years beginning with the date of expiration, unless another period is specified in the CPS of the respective Sub CA. Certificates are archived securely on an archive medium.

Expired certificates (and CRLs if used) are archived because digitally signed or encrypted documents often outlast the validity period of the certificate used to sign or encrypt the document. Certificates whose validity period has expired must continue to be accessible to allow the certificate to be used to prove the authenticity of a document.

Access to archived certificates is under control of Allianz Group RCA.

5.5.5 Archive collection system (internal or external)

Audit trail information is kept for a minimum period of ten years from the date of generation, unless another period is specifically required. Audit logs are archived by the Allianz Group RCA securely on an archive medium.

The Allianz Group RCA has established archive backup procedures to ensure and enable complete restoration of archived records in the event of a disaster situation.

5.5.6 Procedures to obtain and verify archive information

The integrity of the Allianz Group RCA's archives are verified:

1. At the time the archive is prepared;
2. Periodically at the time of a programmed security audit;
3. At any other time when a full security audit is required.

5.6 Key Changeover

Key changeover does not apply to end entity certificates since RCA and Sub CAs are not rolled-over but replaced by new key CA instances, cf. section 4.7.

5.7 Compromise and Disaster Recovery

The purpose of such a plan is to restore core business operations as quickly as practicable when systems operations have been significantly and adversely impacted by fire, strikes, etc. The plan acknowledges that any impact on system operations will not cause a direct and immediate operational impact within the PKI due to designed in redundancy and resilience. This means that the plan's primary goal is to reinstate the Root Certification Authority in order to make accessible the logical records kept within the software.

The Allianz Group RCA as well as any Sub CA:

1. Has to establish and maintain detailed documentation covering:
   - Contingency & disaster recovery plan, including key compromise, hardware, software and communications failures, and natural disasters such as fire and flood. See also Allianz Group Business Continuity Management Policy and Standards [AZ-BCM].
   - Configuration baseline, including operating software, and PKI specific application programs.
   - Backup, archiving and offsite storage procedures.
2. Provides the above documentation on the request of persons conducting a security, compliance or CPS practices audit;
3. Provides appropriate training to all relevant staff in contingency and disaster recovery procedures;
4. Periodically tests the Allianz Group RCA System with the minimum test activity being the full restoration of operational services as follows:
   - the current operational platforms are shut down and disconnected from the communications links;
   - system operating software, application programs and operational data is restored onto new hardware platforms, solely from backup media and in compliance with the configuration baseline;
   - the restored service is connected to the communications links and the correct operation of its certificate services tested;
   - service operations are resumed using the original operational platform. All files on the hard disk of the test platform are securely deleted.

Generating a compromise and disaster recovery plan, the following use cases have to be taken into account:

- Allianz Group RCA's certificate is revoked

  The Allianz Group RCA has established a key and user compromise plan that addresses the actions to be taken in the event that the Allianz Group RCA's signing certificate is revoked. Subordinate Certificate Authorities are to promptly advise of any compromise or suspected compromise of the Allianz Group RCA private keys.

5.7.1 Incident and compromise handling procedures

Incident and compromise handling are part of Allianz Disaster Recovery Plans and Business Continuity Management plan.

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

For all computing resources backup for hardware and software is kept ready.

5.7.3 Entity private key compromise procedures

The Allianz Group RCA has established a key and Sub CA compromise plan that addresses the actions to be taken in the event that the private signing key of one of the participating Sub CAs is compromised.

5.7.4 Business continuity capabilities after a disaster

Therefore the Allianz Group RCA has:

1. Identified individuals authorised to initiate disaster recovery action;
2. Identified major elements at risk, for example;
   - Operational hardware;
   - Certification authority software application;
   - Logical records;
   - Registration records;
3. Identified criteria that might prompt disaster recovery initiation;
4. Considered secondary precautionary measures that may be required, such as:
   - a backup site;
   - trained backup staff;
5. Developed recovery actions and timeframes;
6. Prioritised recovery actions from most significant to least significant;
7. Maintained a record of the hardware and software configuration baseline;
8. Maintained records of the necessary equipment and procedures required to recover from an unexpected event such as a hardware failure, including the intended maximum period that the system is to be down.

5.8 CA or RA Termination

When it is necessary to terminate the Allianz Group RCA service, the impact of the termination is to be minimised as much as possible in light of the prevailing circumstances. The Allianz Group RCA shall at least provide as much prior notice as is practicable and reasonable to all PKI participants and relying parties.

Notice

In the case of the programmed termination of the Allianz Group RCA, it has to provide Sub CAs with a minimum of 120 days notice of the proposed shut down. In the event of an emergency shut down of the Allianz Group RCA, e.g. due to the compromise of its private key, the Allianz Group RCA will provide Sub CAs with as much notice as is practical and reasonable under the prevailing circumstances. All keys and certificates are to be revoked by the Allianz Group RCA immediately and prior to the emergency shut down. Services should be recommenced by the same (or a successor Root Certification Authority) as quickly as possible after the shut down has been effected.

5.8.1 Keys and Certificates

In the event that it becomes necessary to terminate the Allianz Group RCA:

1. All Sub CA certificates may need to be revoked prior to the shutdown; or

2. All Sub CA certificates may need to be transferred to a replacement Allianz Group RCA, provided the transferred certificates do not become operational within the chain of trust of the replacement Allianz Group RCA Service until after the shutdown of the terminating Allianz Group RCA or
4. All Sub CA certificates may need to be revoked prior to the shutdown of the terminating Allianz Group RCA service, and the keys may be transferred to the replacement Allianz Group RCA service for the issue of new certificates, provided that such new certificates are not generated until after the shutdown of the terminating Allianz Group RCA service.
5. The last act of the terminated certification authority is to issue a CRL with all certificates revoked. The Allianz Group RCA will include revocation of its own certificate as well. Where practical, key and certificate revocation should be timed to coincide with the progressive and planned rollout of new keys and certificates by a successor Allianz Group RCA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

It is a fundamental principle of Allianz Group RCA that a certificate may only be issued for a public key in the situation where the corresponding private key has been generated in a secure environment.

Allianz Group RCA uses a number of key pairs for designated purposes and therefore the is a variety of keys. Typically, these keys fall into the types set out below:

- Allianz Group RCA participant keys are keys issued for or generated by the CAs within the Allianz Group RCA System. They may be related to Allianz Group RCA or participant.
- Infrastructure keys are keys issued for or generated by infrastructure nodes. They may be related to Allianz Group RCA or a participant. (*not applicable at the moment)*

The following RSA key pairs are used in the Allianz Group RCA System:

Allianz Group RCA Participant Keys	**Operational Life**	**Minimum Key Length (bits)**
Allianz Group RCA Keys	12 Years	2048
Allianz Group RCA CRL Signing Keys	12 Years	2048
Participant CA Keys	8 Years	1024
Participant CA CRL Signing Keys	8 Years	1024

Infrastructure Keys	***Operational Life***	***Key Length (bits)***
Root Responder Inter-Participant OCSP Keys	*<= 2 Years*	*1024*
Root SSL OCSP Keys	*<= 2 Years*	*1024*
Participant Inter- Participant OCSP Keys	*<= 2 Years*	*1024*
Participant SSL OCSP Keys	*<= 4 Years*	*1024*

The Allianz Group RCA's keys are exclusively generated by the Hardware Security Module (HSM) as part of the Allianz Group RCA systems. All subscribers shall generate keys in secure environments like HSM or smartcards.

Where cryptographic modules are used, the private keys must be generated in them and remain there in both encrypted and decrypted forms, and be decrypted only at the time at which it is being used.

Allianz Group RCA has established HSM compliance criteria that ensure the quality and requirements from an HSM are uniform and consistent. All keys used within the Allianz Group RCA System shall be generated in hardware.

Key generation in software and hardware are equally supported by Allianz Group RCA, but it may be necessary to apply different security measurements related to the environment. It is suggested to generate the private key on a HSM or a smart card.

If the private key is generated extern of a secure environment, it must be encrypted prior to leaving the device on which it was generated.

6.1.1 Key pair generation

It is a fundamental principle of Allianz Group RCA that a certificate may only be issued for a public key in the situation where the corresponding private key has been generated in a secure environment.

Key generation in software and hardware are equally supported by Allianz Group RCA, but it may be necessary to apply different security measurements related to the environment. It is suggested to generate the private key on a HSM or a smart card.

If the private key is generated extern of an secure environment, it must be encrypted prior to leaving the device on which it was generated.

Key generation on a HSM is mandated for the Allianz Group RCA Signing Key and all other Allianz Group RCA keys.

The HSM must:

1. Comply at least with the FIPS 140-1 Level 2 (Federal Information Standards, NIST, 140-2: Security Requirements for Cryptographic Moduls) specifications,
2. Export the keys securely (if required); and
3. Destroy the keys if they have been expired.

Migration of the private key to and from a cryptographic module must:

1. Be encrypted during the course of the transfer;
2. Use a Triple DES Key of at least 112 Bits or other encryption algorithm of equal or greater strength;
3. In the case of CA keys, be undertaken with the supervision of a Senior Management personnel of either:
   - Allianz Group RCA or
   - A person, who has been specifically authorised by Sub CA owner.

Key generation on smart card is optional. Where smart card based key generation is supported it must comply with the provisions of this policy.

6.1.2 Private key delivery to subscriber

No stipulation. All private keys are generated locally and thus do not require delivery.

6.1.3 Public key delivery to certificate issuer

It is preferred that all form of deliverance should be performed via encrypted and signed emails.

6.1.4 CA public key delivery to relying parties

The Allianz Group RCA public signing keys are distributed as certificates to all PKI participants and accepted relying parties.

6.1.5 Key sizes

Generally the Allianz Group RCA Root keys are 2048 bit RSA keys.

6.1.6 Public key parameters generation and quality checking

No stipulation.

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

Keys may be used for the purposes and in the manner described in the relevant CPS. Any restrictions described in the section must be observed.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Private keys shall be protected using adequate processes and measurements and hardware support wherever possible.

6.2.1 Cryptographic module standards and controls

A FIPS 140-1 Level 3 Cryptographic Module including card management are in use. Hardware security moduls are also recommended to be used by Sub CAs for private key protection. The Allianz Group RCA Operating Rules mandate that each subscriber is responsible for the safekeeping of its private key(s). The safekeeping of private keys must be achieved in accordance with the standards set down in this CPS.

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

The n out of m rule allows a private key to be split into multiple parts (m), where a smaller number of those parts (n) are required to fully restore the key. Any number of parts below (n) however, (for example n --1) are not sufficient to obtain any information about the key. Allianz Group RCA does not mandate the use of n out of m multi-person control. Subscribers, in particular participating Sub CAs, may, however, choose to use n out of m multi-person control as a result of their system risk review.

6.2.3 Private key escrow

Private key escrow is not supported.

6.2.4 Private key backup

The Allianz Group RCA's private keys shall be stored in encrypted form, which is backed up under further encryption with backup copies maintained on site and in secure off site storage. Allianz Group RCA is responsible for the safekeeping of the root key in accordance with the standards set forth in this CPS.

6.2.5 Private key archival

The private key is archived in a backup FIPS 140-1 Level 3 module locally separated on different sites.

6.2.6 Private key transfer into or from a cryptographic module

FIPS 140-1 Level 3 permits private key import to HSM modules. Export is only possible from one HSM to the backup HSM. Private key generation is only performed on hardware security modules.

6.2.7 Private key storage on cryptographic module

Allianz Root RCA stores private key in HSM modules

6.2.8 Method of activating private key

It is the n out of m multi-person control in use.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

No stipulation.

6.2.11 Cryptographic Module Rating

The nCipher Fips 140-1 Level 3 compliant module is in use.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

All public keys are archived by the certifying Certification authority.

Expired certificates (and CRLs if used) are archived because digitally signed or encrypted documents often outlast the validity period of the certificate used to sign or encrypt the document. Certificates whose validity period has expired must continue to be accessible to allow the certificate to be used to prove the authenticity of, a document. Archived certificates can only be accessed in authorised circumstances, for example at the participant's request or where a properly constituted subpoena or warrant is produced.

Archived certificates are to be:

- Archived on tamper evident media;
- Archived for a minimum period of seven years from the date of expiry, unless another period is specified in a relevant CP; and
- securely destroyed at the end of the archive period.

6.3.2 Usage Periods for the Public and Private Keys

The usage periods are prescribed within this CPS.

6.4 Activation Data

No activation data other than access control mechanisms is required to operate cryptographic modules.

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

Allianz Group RCA has established the Allianz Group Security Policy [AZ-SP] that incorporates computer security technical requirements that are specific to Allianz Group RCA's operations.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

If applications are developed by Allianz Group RCA or other PKI participants, this takes place in controlled environments employing appropriate quality controls. All applications are required to meet accreditation by Allianz Group RCA before they are used within the Allianz Group RCA System.

6.6.2 Security Management Controls

System security management is controlled by the privileges assigned to operating system accounts, and by the trusted roles described in section 5.2 of this document.

6.6.3 Life cycle security controls

Only certified software components are in use as operational environment. The software development obeys the software development procedures forced by Allianz Group IT Security. The Allianz Group RCA as well as any participating Sub CA shall maintain contingency plans in force, including adequate back up and recovery procedures, to ensure that the participant can continue to meet its obligations under these operating rules without material interruption in the event of the failure or shut down of the relevant primary computer facilities or other operating facilities. All contingency plans shall meet the minimum requirements set forth in this CPS.

6.7 Network Security Controls

Network security controls are highlighted in the Allianz Group Security Policy [AZ-SP].

6.8 Timestamping

No stipulation.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificates issued by Allianz Group RCA participating Sub CAs are expected to comply with:

- All certificates are IETF-PKIX certificates in accordance with RFC2459. The use of certificate extensions (critical / non-critical) will be governed by RFC2459. Certain extensions within the standard may be set to critical or non-critical. Any Sub CA wishing to implement critical extensions other than those defined here must first seek approval of Allianz Group RCA so that an investigation can be carried out to ensure full interoperability between all PKI participants and relying parties.
- There are no constraints on the size of the serial number.
- The public key in a certificate must be unique. No party, be it an end-entity or a Sub CA, may have it's public key signed by more than one Certification Authority.
- Identifiers
    - All certificates must not contain Issuer and Subject Unique ID.
    - Subject and Authority Key identifiers shall be used.
    - KeyID method based on 160bit hash of subject public key as per RFC2459.
- RFC 283 algorithms are supported.
- Constraint Extensions
- OIDs
    - OIDs are not allocated to algorithms supported and used within the Allianz Group RCA System.
    - CP OIDs are carried in the standard extension field of X.509 Certificates and published in the relevant CP.

7.1.1 Key Usage

Key usage in all certificates (as defined in the individual certificate profiles in the appendix):

- keyCertSign for CA Certificates
- cRLSign for CRL Signing Certificates
- digitalSignature and nonRepudiation for Identity
- keyEncipherment or dataEncipherment as required for Utility Certificates

7.1.2 Certificate Policies

Certificate policies shall be present and contain an Allianz Group RCA Object Identifier at a minimum.

7.1.3 Version number(s)

Certificates must comply to X.509 v3 standard

7.1.2 Certificate extensions

The certificate extensions are defined by Allianz Group RCA and Sub CAs. Basic constraints shall be present in all CA certificate. Basic constraints will be used to differentiate between CA

and End-Entity certificates. Certificate extensions both private and registered are used within Allianz Group RCA certificates.

Signature algorithm for all Allianz Group RCA Certificates is RSA with SHA1

- The root shall have 2048 bit RSA keys
- All other CAs shall have 1024 bit RSA keys, at a minimum

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name formats

Distinguished Name:

Certificates issued by the Allianz Group RCA System contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields.

All certificates must have non-null Issuer DN.

All Certificates must contain a Subject DN.

Note: There are no constraints on the relationship between issuer and subject DNs.

7.1.5 Name constraints

Name constraints shall not be used.

7.1.6 Certificate policy object identifier

It is recommended that the OID of this CPS should be non-critical extension of the attribute certificatePolicies.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

Certificate policies shall be present and contain an Allianz Group RCA Object Identifier at a minimum.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL Profile

Only X509 Version 2 CRLs are supported. Certificate validity checking must be performed in accordance to the operating rules of Allianz Group RCA System.

7.2.1 Version number(s)

At least revocation lists of version 1 or higher are supported. For interoperability reasons revocation lists of version 2 are preferred.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP Profile

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

7.3.3 Reference

More details specifically detailing technical compliance can be found in the Allianz Group RCA Certificate Profiles Document [AZ-CP]. The Allianz Group RCA System supports and uses X.509 Version 3 Certificates.

8 Compliance Audit and Other Assessment

Allianz Group RCA shall conduct, at Allianz Group RCA's expense, an internal or external audit of its compliance with the operating rules.

All participants utilising the Allianz Group RCA System will be subject to minimum audit requirements necessary to demonstrate compliance with the Allianz Group RCA Operating Rules and to ensure that proper control procedures have been implemented and are operating. Allianz Group RCA has established auditing requirements and other standards to further the safety and soundness of the system's operations. The audit requirements consist of two distinct phases.

If a participant chooses to outsource any of the related functions to a third party, the third party must also be bound the same system rules and audit requirements that bind the participant. The Allianz Group RCA Audit/Review procedures will need to be extended to the Third Party by the participant. The ultimate responsibility for ensuring compliance with the operating rules will rest with the participant.

8.1 Frequency or circumstances of assessment

The audit shall be conducted on at least an annual basis. Allianz Group RCA shall, at its expense, remedy any deficiencies revealed by any audit conducted pursuant to this section within the time period specified in the audit results, or if no such time period is specified within a reasonable time period. Applying and participating Sub CAs will provide Allianz Group RCA with copies of all audits and reviews on a timely basis (within 30 days). Allianz Group RCA will also be informed about interim reviews and follow up conducted on all significant audit / review issues.

8.2 Identity/qualifications of assessor

The assessment is to be conducted by qualified internal or external audit personnel, with the results of such reviews reported to Allianz Group RCA.

8.3 Assessor's relationship to assessed entity

Allianz Group RCA may initiate third party audits.

8.4 Topics covered by assessment

8.4.1 Initial compliance audit

Each participating Sub CA is required to conduct the Allianz Group RCA initial compliance audit process prior to issuing certificates. The purpose of the Allianz Group RCA initial compliance audit process is to determine that the Sub CA complies with the minimum eligibility, operational and technical requirements of the Allianz Group RCA.

8.4.2 Ongoing compliance audit

The assessment is to be conducted by qualified internal or external audit personnel, with the results of such reviews reported to Allianz Group RCA. After acceptance as participant of Allianz Group RCA system the participant will be required to conduct the Allianz Group RCA review process in conjunction with any significant changes to the deployment of their system, but in no event less than at least annually.

8.5 Actions taken as a result of deficiency

Allianz Group PAC decides in each individual case of deficiency what kind of actions should be taken in order that the security of the RCA security infrastructure can be guaranteed continuously in all cases.

8.6 Communication of results

Applying and participating Sub CAs will provide Allianz Group RCA with copies of all audits and reviews on a timely basis (within 30 days). Allianz Group RCA will also be informed about interim reviews and follow up conducted on all significant audit / review issues.

9 Other Business and Legal Matters

9.1 Fees

In particular, no fees are charged for the issuance, access, revocation, suspension and validation of issuer certificates and no fees are charged for the usage of the offered directory services. This arrangement is only suitable to the PKI participants named in section 1.3.

Fees may occur concerning the services of subordinate CAs as defined in the relevant CPS' of the Sub CAs.

Notwithstanding the above financial implications may occur especially related to hardware/software licenses at the PKI participants' sites.

Cross-certification agreements with other organisations, may result in additional fees and will be addressed in the specific cross-certification agreements themselves and are outside the scope of this CPS.

9.1.1 Certificate issuance or renewal fees

No fees are taken for issuance or renewal services provided by Allianz Group RCA. Fees may occur concerning the services of subordinate CAs as defined in the relevant CPS' of the Sub CAs.

9.1.2 Certificate access fees

No fees are taken for access to PKI services provided by Allianz Group RCA. Fees may occur concerning the services of subordinate CAs as defined in the relevant CPS' of the Sub CAs.

9.1.3 Revocation or status information access fees

No fees are taken for certificate status information services provided by Allianz Group RCA. Fees may occur concerning the services of subordinate CAs as defined in the relevant CPS' of the Sub CAs.

9.1.4 Fees for other services

No fees are taken for other services provided by Allianz Group RCA. Fees may occur concerning the services of subordinate CAs as defined in the relevant CPS' of the Sub CAs.

9.2 Financial Responsibility

The scope of this CPS does not include commercial issues such as the financial viability or stability of Allianz Group RCA participating organisations operating Sub CA services within the Allianz Group PKI.

Participating organisations who manage Certification Authority and/or Registration Authority services within the Allianz Group RCA System may be requested by Allianz Group RCA to provide supporting documentation during initial registration.

9.2.1 ***Insurance*** coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Allianz Group RCA Documentation

All documentation provided by Allianz Group RCA, that is deemed to be confidential shall be labelled “ALLIANZ GROUP RCA CONFIDENTIAL”. Each PKI participant shall treat all information as confidential and proprietary. A PKI participant shall use at least the same degree of care to protect the confidentiality of the confidential information as the PKI participant uses to protect its own similar confidential information, which degree of care shall be no less than reasonable care.

9.3.2 Scope of confidential information

Confidential Information include all information disclosed by Allianz Group RCA or a PKI participant (each an “Informant”) to another PKI participant (each a “Recipient”). Confidential information of Allianz Group RCA shall include any information concerning the Allianz Group RCA Services or the Allianz Group RCA System or technology and information belonging to Allianz Group RCA, which are marked “confidential” or “proprietary”.

“Confidential Information” also includes the results of compliance audits provided to Allianz Group RCA, cf. section 8.

9.3.3 Types of Information in particular considered confidential

1. **Personal Information**

   Information supplied to Allianz Group RCA as a result of the practices described in this CPS may be covered by national government or other privacy legislation or guidelines.

   Access to confidential information by operational staff is on a need-to-know basis. Paper-based records and other documentation containing confidential information is to be kept in secure and locked containers or filing systems, separate from all other records.

2. **Registration Information**

   All registration records are considered to be confidential information, including:

   a) Certificate applications, whether approved or rejected;

   b) Proof of identification documentation and details;

   c) Certificate information collected as part of the registration records, but this does not act to prevent publication of certificate information in the certificate repository;

   d) Any information requested by Allianz Group RCA when it receives an application from a third party to operate a CA within the Allianz Group RCA chain of trust.

3. **Certificate and Revocation Information**

   The reason for a certificate being revoked is considered to be confidential information, with the sole exception of the revocation of an issued certificate due to the compromise of its private key, in which case a disclosure must be made that the private key has been compromised.

9.3.4 Information not within the scope of confidential information

Certificate information published in the Allianz Group RCA certificate repository is not confidential and is considered to be public knowledge.

9.3.5 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

The collection, processing and use of personal data SHALL be admissible only if permitted or prescribed by the "German Federal Data Protection Act" or any other legal provision or if the subscriber has consented.

9.4.3 Information not deemed private

All information out of the scope of 9.4.2.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual Property Rights

Allianz Group RCA warrants that it is in possession of or holds licenses for the use of hardware and software required in support of this CPS.

9.5.1 Property in Certificates

All intellectual property rights, including all copyright, in all certificates belong to and will remain the property of the issuing certification authority.

9.5.2 Certificate

The Allianz Group RCA reserves the right at any time to revoke any certificate in accordance with the procedures and policies set out in this CPS.

9.5.3 Distinguished Names

Intellectual property rights in Distinguished Names vest in the assigning subscriber.

9.5.4 Copyright

Copyright in the Object Identifiers (OID) for the Allianz Group RCA System vests solely in Allianz Group RCA. OIDs are not to be copied, used or otherwise dealt with in any way except as provided for in the operation of the Allianz Group RCA infrastructure, or in accordance with the relevant this CPS.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

Allianz Group RCA makes no representations and give no warranties regarding the financial efficacy of any transaction completed utilizing a certificate or any services provided by the Allianz Group RCA in relation to the certificates.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

Allianz Group RCA disclaims all warranties of any kind unless stated otherwise within the Allianz Group RCA PKI agreements, whether express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, non-infringement, title, satisfactory title, and also including warranties that are statutory or by usage of trade.

9.8 Limitations of Liability

In no event shall a Allianz Group RCA be liable to any participant, customer or other entity or person for any loss, claim, damage or expense arising from Allianz Group RCA.

9.8.1 Safeguards

Allianz Group RCA has introduced a number of measures to reduce or limit its liabilities in the event that the safeguards in place to protect its resources fail to:

- inhibit misuse of those resources by authorised personnel;
- prohibit access to those resources by unauthorised individuals;
- prevent system failures (i.e., other than as a result of abuse).

These measures include but are not limited to:

1. Testing of the Allianz Group RCA Disaster Recovery Plans;
2. Performing regular system data backups;
3. Performing a backup of the current operating software and certain software configuration files;
4. Storing all backups in secure local and offsite storage;
5. Maintaining secure offsite storage of other material needed for disaster recovery;
6. Periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure;
7. Periodically reviewing its Disaster Recovery Plan, including the identification, analysis, evaluation and prioritisation of risks.

9.9 Indemnities

Cf. Section 9.8.

9.10 Term and Termination

9.10.1 Term Allianz Group Root certificate

Validity	
Not Before	Friday, 28. July 2006 10:12:27
Not After	Sunday, 29. November 2026 10:12:27

9.10.2 Termination

a) Termination by Participant

A participating organisation may at any time voluntarily terminate its participation in the Allianz Group RCA System. It shall provide at least 180 days prior written notice of such termination, unless otherwise agreed by Allianz Group RCA.

b) Termination by Allianz Group RCA

Allianz Group RCA may, in accordance with the procedures described in this CPS, cf. chapter 4, revoke the certificate of a Sub CA and may terminate the participation of the responsible participating organisation from the Allianz Group PKI if

1. Allianz Group RCA reasonably determines that the respective organisation failed to disclose or wilfully misrepresented information in its application to become a participating organisation origin subsequent filings, which in the reasonable judgement of Allianz Group RCA, has a material adverse impact upon Allianz Group RCA, or
2. the Allianz Group RCA System, any participants, or any of their customers or the participant no longer qualifies as an eligible entity, or
3. Allianz Group RCA is precluded for any reason from operating, or
4. otherwise determines to discontinue provision of the Allianz Group RCA System.

Allianz Group RCA shall provide the participating organisation at least thirty (30) days prior written notice of Allianz Group RCA's intention to terminate the participant, and shall include in such notice a summary of the reasons for such termination. Upon a decision by Allianz Group RCA to terminate the participant, Allianz Group RCA shall provide notice of the termination to the participant stating the reasons for and the effective date of the termination.

9.10.3 Effect of termination and survival

After termination, Allianz Group RCA revokes all certificates issued to the corresponding participating organisation, e.g. the Sub CA certificates.

After revocation, the respective CA informs its subscribers and the relevant relying parties as soon as reasonably possible that they shall cease at once to use for any purpose their digital certificates that are digitally identified with the revoked certificate.

9.11 Individual Notices and Communications with Participants

Upon receipt of a participant, Allianz Group RCA shall confirm whether the Issuer Certificate of the participant is valid.

Allianz Group RCA agrees that the records maintained by it in connection with the operation of the Allianz Group RCA System shall be available for examination and audit at the location at which Allianz Group RCA maintains such records.

9.12 Amendments

If a new CPS is approved, signed and distributed by Allianz Group RCA, all earlier versions of the CPS will expire.

9.12.1 Notification mechanism and period

All changes made by Sub CA must be announced to Allianz Root RCA.

9.12.2 Circumstances under which OID must be changed

For all CPS there MUST be assigned a unique OID. Used OIDs MUST NOT be reused for a new version of the CPS.

9.13 Dispute Resolution Procedures

No stipulation.

9.14 Governing Law

The enforceability, construction, interpretation and validity of this CPS and all agreements related to Allianz Group RCA SHALL be governed by German law. This applies to all participants.

9.15 Compliance with Applicable Law

Cf. sections 9.4 and 9.5.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

In the event of a conflict between the provisions of this CPS and any related agreement, the terms of the related agreement shall take precedence. This in particular includes (a) the CPS of any subordinate CA of the Allianz Group RCA, (b) an agreement with a third party CA.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

In the event that these operating rules are translated into a language other than English, the English version provided by Allianz Group RCA of this CPS shall govern

9.16.5 Force Majeure

A participant shall maintain contingency plans in force, including adequate back up and recovery procedures, to ensure that the participant can continue to meet its obligations under the Operating rules without material interruption in the event of the failure or shut down of the participant's primary computer facilities or other operating facilities.

9.16.6 Other Provisions

Sub CAs of the Allianz Group RCA are subordinate exclusively to the Allianz Group RCA and may not be certified by any other authority within or outside the Allianz Group RCA PKI. A participant CA may not use a self-signed certificate. As a consequence, Sub CAs are not permitted to perform cross-certification with any other CA.

Each participant will be required to conduct the Allianz Group RCA initial compliance audit process prior to issuing certificates. The purpose of the Allianz Group RCA initial compliance audit and ongoing review process is to determine that the participant complies with the minimum eligibility, operational and technical requirements of the Allianz Group RCA. The assessment is to be conducted by qualified internal or external audit personnel, with the results of such reviews reported to Allianz Group RCA.

Each participant has to confirm both the Allianz Group Participant Agreement (RCA PA) and the minimum security provisions stated by Allianz Group RCA.

10 Appendix

There are a number of different types of certificates currently issued by Allianz Group RCA.Their profiles are defined in this Appendix. Every effort is made to match these profiles to RFC 3647. The following certificate types are profiled:

- Root CA Key Signing Certificate
- Participant CA Key Signing Certificate

10.1 Root CA Signing Key Certificate Profile

This certificate is the self-signed certificate generated by Allianz Group RCA which is used to sign all other RCA certificates and all participant CA certificates.

Field	Content	Critical*
1. X.509v1 Field		
1.1. Version	v3	
1.2. Serial Number	01	
1.3. Signature Algorithm	SHA-1 with RSA Signature	
1.4. Issuer Distinguished Name		
1.4.1. Country (C)	DE	
1.4.2. Organization (O)	“Allianz Group”	
1.4.3. Common Name (CN)	“Allianz Group Root CA”	
1.5. Validity		
1.5.1. Not Before	e.g., “13:13:13 13 December 2002”	
1.5.2. Not After	e.g., “23:59:59 31 December 2012”	
1.6. Subject		
1.6.1. Country (C)	DE	
1.6.2. Organization (O)	“Allianz Group”	
1.6.3. Common Name (CN)	“Allianz Group Root CA”	
1.7. Subject Public Key Info	99 51 32 e8 bf f2 99 2a 50 06 dd 84 4d 67 a4 ed ff 41 f5 45	
2. Key	RSA 2048bit	
3. X.509v3 Extensions		
3.1. Authority Key Identifier		n
3.1.1. Key Identifier	99 51 32 e8 bf f2 99 2a 50 06 dd 84 4d 67 a4 ed ff 41 f5 45	
3.1.2. AuthorityCertIssuer	cn=Allianz Group Root CA, o=Allianz Group, C=DE	
3.1.3. AuthorityCertSerialNumber	01	
3.2. Subject Key Identifier	99 51 32 e8 bf f2 99 2a 50 06 dd 84 4d 67 a4 ed ff 41 f5 45	n
3.3. Key Usage		y
3.3.1. Digital Signature	Selected	
3.3.2. Non Repudiation	Not selected	
3.3.3. Key Encipherment	Not selected	
3.3.4. Data Encipherment	Not selected	
3.3.5. Key Agreement	Not selected	

Field	Content	Critical*
3.3.6. Key Certificate Signature	Selected	
3.3.7. CRL Signature	Selected	
3.4. Certificate Policies		n
3.4.1. Policy Identifier	1.3.6.1.4.1.7159.30.1	
3.4.2. Policy Qualifier ID	1.3.6.1.5.5.7.2.2	
3.4.2.1. User Notice	This Certificate is issued by Allianz Group Root CA by Allianz Group Germany	
3.4.2.2. URL	http://rootca.allianz.com/cps/	
3.5. Subject Alternate Names		n
3.5.1. rfc822Name	Not present	
3.6. Basic Constraints		y
3.6.1. Subject Type	CA	
3.6.2. Path Length Constraint	None	
3.7. Netscape Extensions		n
3.7.1. Base URL	http://rootca.allianz.com	
3.7.2. CertType	SslCA, smime-CA, Codesign CA	
3.7.3. PolicyURL	/cps/	
3.7.4. Comment	This Certificate is issued by Allianz Group Root CA by Allianz Group Germany	
3.8. CRL Distribution Point		n
3.8.1. 1st URL	http://rootca.allianz.com/rootca.crl	
Fingerprint	a8 2a 05 d7 a2 2a 34 8a be 1e 01 11 6e ca f1 18 d2 2a 67 ff	

10.2 Participant CA Key Signing Certificate Profile

This certificate is signed by the Allianz Group RCA Key Signing Certificate and is used to sign both Identity and Utility Certificates, if a single certificate-signing key is used; or the certificate signing key used to sign subordinate Identity Certificates, if dual certificate-signing keys are used.

Field	Content	Critical*
1. X.509v1 Field		
1.1. Version	v3	
1.2. Serial Number	01	
1.3. Signature Algorithm	SHA-1 with RSA Signature	
1.4. Issuer Distinguished Name		
1.4.1. Country (C)	DE	
1.4.2. Organization (O)	“Allianz Group”	
1.4.3. Common Name (CN)	“Allianz Group Root CA”	
1.5. Validity		
1.5.1. Not Before	Tbd.	
1.5.2. Not After	Tbd. max., “23:59:59 31 December 2012”	
1.6. Subject		
1.6.1. Country (C)	Tbd	
1.6.2. Organization (O)	Tbd	

Field	Content	Critical*
1.6.3. Common Name (CN)	Tbd	
1.7. Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1	
2. Key	Tbd, Min RSA 1024bit	
3. X.509v3 Extensions		
3.1. Authority Key Identifier		n
3.1.1. Key Identifier	99 51 32 e8 bf f2 99 2a 50 06 dd 84 4d 67 a4 ed ff 41 f5 45	
3.1.2. AuthorityCertIssuer	cn=Allianz Group Root CA, o=Allianz Group, C=DE	
3.1.3. AuthorityCertSerialNumber	01	
3.2. Subject Key Identifier	Public key encoded in accordance with RFC2459 & PKCS#1	n
3.3. Key Usage		y
3.3.1. Digital Signature	Selected	
3.3.2. Non Repudiation	Not selected	
3.3.3. Key Encipherment	Not selected	
3.3.4. Data Encipherment	Not selected	
3.3.5. Key Agreement	Not selected	
3.3.6. Key Certificate Signature	Selected	
3.3.7. CRL Signature	Selected	
3.4. Certificate Policies		n
3.4.1. Policy Identifier	1.3.6.1.4.1.7159.30.1.x	
3.4.2. Policy Qualifier ID	1.3.6.1.5.5.7.2.2	
3.4.2.1. User Notice	This Certificate is issued by Allianz Group Root CA by Allianz Group Germany	
3.4.2.2. URL	http://rootca.allianz.com/cps/	
3.5. Basic Constraints		y
3.5.1. Subject Type	CA	
3.5.2. Path Length Constraint	Not empty	
3.6. Netscape Extensions		n
3.6.1. Base URL	http://rootca.allianz.com	
3.6.2. CertType	SslCA, smime-CA, Codesign CA	
3.6.3. PolicyURL	/cps/	
3.6.4. Comment	This Certificate is issued by Allianz Group Root CA by Allianz Group Germany	
3.7. CRL Distribution Point		n
3.7.1. 1st URL	http://rootca.allianz.com/rootca.crl	
3.8. Special extensions of CA	tbd	n
Fingerprint	Public key encoded in accordance with RFC2459 & PKCS#1	

10.3 Definitions and Acronyms

Authentication	The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.
CA-certificate	A certificate for one CA's public key issued by another CA.
Certificate policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.
Certification path	An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Practice Statement (CPS)	A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.
CPS Abstract	A subset of the provisions of a complete CPS that is made public by a CA.
CPS Summary	Cf. "CPS Abstract".
Identification	The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and (2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.
Issuing certification authority (issuing CA)	In the context of a particular certificate, the issuing CA is the CA that issued the certificate.
PKI Participant	An organization (or individual) that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

PKI Disclosure Statement (PDS)	An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.
Policy qualifier	Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information.
Registration authority (RA)	An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Related Participants of a Sub CA	The term includes all relying parties as well as all subscribers of the respective Sub CA; in particular subscribing employees and customers of the participating organisation operating the respective Sub CA.
Relying party	A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate.
Relying party agreement (RPA)	An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.
Set of provisions	A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework.
Subscriber	A subject of a certificate who is issued a certificate
Subscriber Agreement (SA)	An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.
Validation	The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants.

For more definitions refer to [RFC 3647].