Allianz Technology SE

Certification Practice Statement
for Allianz
Root Certification Authority

Information Owner: Allianz Technology SE

Version 1.5 / 22.06.2022

Document-ID: AZ-RCA-CPS

Classification : Public

Change Management

Version	Description	Date	Author
0.1	Preliminary CPS	20.01.2014	Aditya Kumar Yellai
1.0	Final Release	28.04.2015	Aditya Kumar Yellai
1.1	Validity of External Participant CA	06.05.2015	Helmut Buss
1.2	Review	19.11.2015	Vera Kloepper
1.3	OID Update – Final	10.05.2016	Aditya Kumar Yellai
1.4	• Changed company name to Allianz Technology SE • Updated references to new Allianz security policies, practical rules and practices • Updated trusted roles • Added Computer Emergency Response Team	28.04.2022	Thi Hang Nguyen
1.5	Review	22.06.2022	Helmut Buss

Content

1 Introduction 16

1.1 Overview 16

1.2 Document Name and Identification 17

1.3 PKI Participants 17

1.3.1 Certification Authorities 17

1.3.2 Registration Authorities 18

1.3.3 Subscribers 18

1.3.4 Relying parties 19

1.4 Certificate Usage 19

1.4.1 Allowed Certificate Usage 19

1.5 Policy Administration 19

1.5.1 Organization administering the document 19

1.5.2 Contact person 19

1.5.3 Entity determining CPS suitability for the policy 20

1.5.4 CPS approval procedures 20

1.6 Definitions and Acronyms 20

2 Publication and Repository Responsibilities 21

2.1 Repositories 21

2.2 Publication of certification information 21

2.3 Time or frequency of publication 21

2.4 Access controls on repositories 21

3 Identification and Authentication 22

3.1 Naming 22

3.1.1 Types of names 22

3.1.2 Need for names to be meaningful 22

3.1.3 Anonymity or pseudonymity of subscribers 22

3.1.4 Rules for interpreting various name forms 22

3.1.5 Uniqueness of names 22

3.1.6 Recognition, authentication, and role of trademarks 23

3.2 Initial Identity Validation 23

3.2.1 Method to prove possession of private key 23

3.2.2 Authentication of organization identity 23

3.2.3 Authentication of individual identity 24

3.2.4 Non-verified subscriber information 24

3.2.5 Validation of authority 24

3.2.6 Criteria for interoperation 24

3.3 Identification and Authorization for Re-key Requests 24

3.3.1 Identification and authentication for routine re-key 24

3.3.2 Identification and authentication for re-key after revocation 24

3.4 Identification and Authorization for Revocation Requests 24

4 Certificate Life-Cycle Operational Requirements 26

4.1 Certificate Application 28

4.1.1 Who can submit a certificate application? 28

4.1.2 Enrolment process and responsibilities 28

4.2 Certificate Application Processing 28

4.2.1 Performing identification and authentication functions 28

4.2.2 Approval or rejection of certificate applications 29

4.2.3 Time to process certificate applications 29

4.3 Certificate Issuance 29

4.3.1 Certificate Requests 29

4.3.2 Verification and Rejection of Certificate Requests 29

4.3.3 CA actions during certificate issuance 29

4.3.4 Notification to subscriber by the CA of issuance of his certificate 30

4.4 Certificate Acceptance 30

4.4.1 Conduct constituting certificate acceptance 30

4.4.2 Publication of the certificate by the CA 30

4.4.3 Notification of certificate issuance by the CA to other entities 30

4.5 Key Pair and Certificate Usage 30

4.5.1 Subscriber private key and certificate usage 31
4.5.2 Relying party public key and certificate usage 32
4.6 Certificate Renewal 32
4.6.1 Circumstance for certificate renewal 32
4.6.2 Who may request renewal 33
4.6.3 Processing certificate renewal requests 33
4.6.4 Notification of new certificate issuance to subscriber 33
4.6.5 Conduct constituting acceptance of a renewal certificate 33
4.6.6 Publication of the renewal certificate by the CA 33
4.6.7 Notification of certificate issuance by the CA to other 33
4.7 Certificate Re-key 33
4.7.1 Circumstance for certificate re-key 33
4.7.2 Who may request certification of a new public key 33
4.7.3 Processing certificate re-keying requests 33
4.7.4 Notification of new certificate issuance to subscriber 34
4.7.5 Conduct constituting acceptance of a re-keyed certificate 34
4.7.6 Publication of the re-keyed certificate by the CA 34
4.7.7 Notification of certificate issuance by the CA to other entities 34
4.8 Certificate Modification 34
4.8.1 Circumstance for certificate modification 34
4.8.2 Who may request certificate modification 34
4.8.3 Processing certificate modification requests 35
4.8.4 Notification of new certificate issuance to subscriber 35
4.8.5 Conduct constituting acceptance of modified certificate 35
4.8.6 Publication of the modified certificate by the CA 35
4.8.7 Notification of certificate issuance by the CA to other 35
4.9 Certificate Revocation and Suspension 35
4.9.1 Circumstances for revocation 35
4.9.2 Who can request revocation 36
4.9.3 Procedure for revocation request 36

4.9.4 Revocation request grace period 36
4.9.5 Time within which CA must process the revocation request 36
4.9.6 Revocation checking requirement for relying parties 37
4.9.7 CRL issuance frequency (if applicable) 37
4.9.8 Maximum latency for CRLs (if applicable) 37
4.9.9 On-line revocation/status checking availability 37
4.9.10 On-line revocation checking requirements 37
4.9.11 Other forms of revocation advertisements available 37
4.9.12 Special requirements re key compromise 37
4.9.13 Circumstances for suspension 37
4.9.14 Who can request suspension 37
4.9.15 Procedure for suspension request 37
4.9.16 Limits on suspension period 37
4.10 Certificate Status Services 38
4.10.1 Operational characteristics 38
4.10.2 Service availability 38
4.10.3 Optional features 38
4.11 End of Subscription 38
4.12 Key Escrow and Recovery 38
4.12.1 Key escrow and recovery policy and practices 38
4.12.2 Session key encapsulation and recovery policy and practices 38
5 Facility, Management, and Operational Controls 39
5.1 Physical Security Controls 39
5.1.1 Site location and construction 39
5.1.2 Physical access 39
5.1.3 Power and air conditioning 39
5.1.4 Water exposures 39
5.1.5 Fire prevention and protection 40
5.1.6 Media storage 40
5.1.7 Waste disposal 40

5.1.8 Off-site backup 40

5.2 Procedural Controls 40

5.2.1 Trusted roles 40

5.2.2 Number of persons required per task 42

5.2.3 Identification and authentication for each role 42

5.3 Personnel Controls 43

5.3.1 Qualifications, experience and clearance requirements 43

5.3.2 Recruitment and Qualification of Personnel 43

5.3.3 Background check procedures 43

5.3.4 Training requirements 43

5.3.5 Retraining frequency and requirements 44

5.3.6 Job rotation frequency and sequence 44

5.3.7 Sanctions for unauthorized actions 44

5.3.8 Independent contractor requirements 44

5.3.9 Documentation supplied to personnel 44

5.4 Audit Logging Procedures 44

5.4.1 Types of events recorded 44

5.4.2 Frequency of Processing Log 44

5.4.3 Retention period for Audit Log 45

5.4.4 Protection of Audit Log 45

5.4.5 Audit log backup procedures 45

5.4.6 Audit collection system (internal vs. external) 45

5.4.7 Notification to event-causing subject 46

5.4.8 Vulnerability assessments 46

5.5 Records Archival 46

5.5.1 Types of records archived 46

5.5.2 Retention period for archive 46

5.5.3 Protection of archive 46

5.5.4 Archive backup procedures 47

5.5.5 Archive collection system (internal or external) 47

5.5.6 Procedures to obtain and verify archive information 47

5.6 Key Changeover 47

5.7 Compromise and Disaster Recovery 47

5.7.1 Incident and compromise handling procedures 49

5.7.2 Computing resources, software, and/or data are corrupted 49

5.7.3 Entity private key compromise procedures 49

5.7.4 Business continuity capabilities after a disaster 49

5.8 CA or RA Termination 49

5.8.1 Keys and Certificates 50

6 Technical Security Controls 51

6.1 Key Pair Generation and Installation 51

6.1.1 Key pair generation 51

6.1.2 Private key delivery to subscriber 52

6.1.3 Public key delivery to certificate issuer 52

6.1.4 CA public key delivery to relying parties 52

6.1.5 Key sizes 52

6.1.6 Public key parameters generation and quality checking 52

6.1.7 Key usage purposes (as per X.509 v3 key usage field) 52

6.2 Private Key Protection and Cryptographic Module Engineering Controls 53

6.2.1 Cryptographic module standards and controls 53

6.2.2 Private key (n out of m) multi-person control 53

6.2.3 Private key escrow 53

6.2.4 Private key backup 53

6.2.5 Private key archival 53

6.2.6 Private key transfer into or from a cryptographic module 53

6.2.7 Private key storage on cryptographic module 53

6.2.8 Method of activating private key 54

6.2.9 Method of deactivating private key 54

6.2.10 Method of destroying private key 54

6.2.11 Cryptographic Module Rating 54

6.3 Other Aspects of Key Pair Management 54

6.3.1 Public Key Archival 54

6.3.2 Usage Periods for the Public and Private Keys 54

6.4 Activation Data 54

6.4.1 Activation data generation and installation 54

6.4.2 Activation data protection 55

6.4.3 Other aspects of activation data 55

6.5 Computer Security Controls 55

6.6 Life Cycle Security Controls 55

6.6.1 System Development Controls 55

6.6.2 Security Management Controls 55

6.6.3 Life cycle security controls 55

6.7 Network Security Controls 55

6.8 Timestamping 55

7 Certificate, CRL, and OCSP Profiles 56

7.1 Certificate Profile 56

7.1.1 Key Usage 56

7.1.2 Certificate Policies 56

7.1.3 Version number(s) 56

7.1.2 Certificate extensions 57

7.1.3 Algorithm object identifiers 57

7.1.4 Name formats 57

7.1.5 Name constraints 57

7.1.6 Certificate policy object identifier 57

7.1.7 Usage of Policy Constraints extension 57

7.1.8 Policy qualifiers syntax and semantics 57

7.1.9 Processing semantics for the critical Certificate Policies extension 57

7.2 CRL Profile 57

7.2.1 Version number(s) 58

7.2.2 CRL and CRL entry extensions 58

7.3 OCSP Profile 58

7.3.1 Version number(s) 58

7.3.2 OCSP extensions 58

7.3.3 Reference 58

8 Compliance Audit and Other Assessment 59

8.1 Frequency or circumstances of assessment 59

8.2 Identity/qualifications of assessor 59

8.3 Assessor's relationship to assessed entity 59

8.4 Topics covered by assessment 59

8.4.1 Initial compliance audit 59

8.4.2 Ongoing compliance audit 59

8.5 Actions taken as a result of deficiency 60

8.6 Communication of results 60

9 Other Business and Legal Matters 60

9.1 Fees 60

9.1.1 Certificate issuance or renewal fees 60

9.1.2 Certificate access fees 60

9.1.3 Revocation or status information access fees 60

9.1.4 Fees for other services 61

9.2 Financial Responsibility 61

9.2.1 ***Insurance*** coverage 61

9.2.2 Other assets 61

9.2.3 Insurance or warranty coverage for end-entities 61

9.3 Confidentiality of Business Information 61

9.3.1 Allianz RCA Documentation 61

9.3.2 Scope of confidential information 61

9.3.3 Types of Information in particular considered confidential 61

9.3.4 Information not within the scope of confidential information 62

9.3.5 Responsibility to protect confidential information 62

9.4 Privacy of Personal Information 62

9.4.1 Privacy plan 62

9.4.2 Information treated as private 62

9.4.3 Information not deemed private 62

9.4.4 Responsibility to protect private information 63

9.4.5 Notice and consent to use private information 63

9.4.6 Disclosure pursuant to judicial or administrative process 63

9.4.7 Other information disclosure circumstances 63

9.5 Intellectual Property Rights 63

9.5.1 Property in Certificates 63

9.5.2 Certificate 63

9.5.3 Distinguished Names 63

9.5.4 Copyright 63

9.6 Representations and Warranties 64

9.6.1 CA representations and warranties 64

9.6.2 RA representations and warranties 64

9.6.3 Subscriber representations and warranties 64

9.6.4 Relying party representations and warranties 64

9.6.5 Representations and warranties of other participants 64

9.7 Disclaimers of Warranties 64

9.8 Limitations of Liability 64

9.8.1 Safeguards 64

9.9 Indemnities 65

9.10 Term and Termination 65

9.10.1 Term Allianz Root certificate 65

9.10.2 Termination 65

9.10.3 Effect of termination and survival 66

9.11 Individual Notices and Communications with Participants 66

9.12 Amendments 66

9.12.1 Notification mechanism and period 66

9.12.2 Circumstances under which OID must be changed 66

9.13 Dispute Resolution Procedures 66

9.14 Governing Law 67

9.15 Compliance with Applicable Law 67

9.16 Miscellaneous Provisions 67

9.16.1 Entire agreement 67

9.16.2 Assignment 67

9.16.3 Severability 67

9.16.4 Enforcement (attorneys' fees and waiver of rights) 67

9.16.5 Force Majeure 67

9.16.6 Other Provisions 67

10 Appendix 69

10.1 Root CA Signing Key Certificate Profile 69

10.2 Participant CA Key Signing Certificate Profile 71

10.3 Definitions and Acronyms 73

References

[AZ-BCMG]	Allianz Business Continuity Management Recovery Strategy Guide
[AZ-ITISP]	Allianz Group Information Technology and Information Security Policy Version 2.0 Effective: 22.06.2021
[AZ-AFRIS]	Allianz Functional Rule for Information Security (AFRIS) version 1.0 Effective: 01.07.2020
[AZ-ISPE]	Information Security Practice 02 – Encryption Version 1.0 Effective: 01.03.2021
[AZ-ISPN]	Allianz Information Security Practice 05 - Network Security Version 1.0 Effective: 01.12.2020
[AZ-GPS]	Guideline for Physical Security version 1.0 Effective: 08.11.2021
[AZ-ASIDM]	Allianz Standard for Information and Document Management (ASIDM) with regard to de- and encryption (see B. VI. 5. ASIDM)
[RFC-2119]	Key Words for use in RFCs to Indicate Requirement Level, IETF (Bradner), March 1997, http://www.ietf.org/rfc/rfc2119.txt
[RFC-5280]	Internet X.509 PKI Certificate and Certification Revocation List (CRL) Profile, IETF (Cooper, Santesson, Farrell, Boeyen, Housley, and Polk), May 2008, http://www.ietf.org/rfc/rfc5280.txt
[RFC-3647]	Internet X.509 PKI Certificate Policy and Certification Practices Framework, IETF (Chokhani, Ford, Sabett, Merrill, and Wu), November 2003, http://www.ietf.org/rfc/rfc3647.txt
[RFC-2459]	Internet X.509 Public Key Infrastructure Certificate and CRL Profile http://www.ietf.org/rfc/rfc2459.txt
[RFC-2560]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF (Myers, Ankney, Malpani, Galperin, Adams), June 1999, http://www.ietf.org/rfc/rfc2560.txt
[RFC-5019]	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, IETF (Deacon, Hurst), September 2007, http://www.ietf.org/rfc/rfc5019.txt
[RFC-2986]	PKCS #10: Certification Request Syntax Specification , IETF (Nystrom, Kaliski, November 2000, https://tools.ietf.org/html/rfc2986

[BSI TR-02102]	BSI - BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (bund.de)
[EN319411]	Policy and security requirements for Trust Service Providers (aka CI) issuing certificates

1 Introduction

1.1 Overview

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

The Allianz RCA system is designed and 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 RCA's certificate services provide a range of security and assurance levels to support the use of various certificates created under the Allianz RCA System.

Allianz RCA has established the Root CA for a number of subordinate entities. 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 RCA includes three primary parties: Allianz RCA, participating organisation and related participants, i.e. systems, employees, and customers. Cf. Figure 1 for the resulting trust relationships.

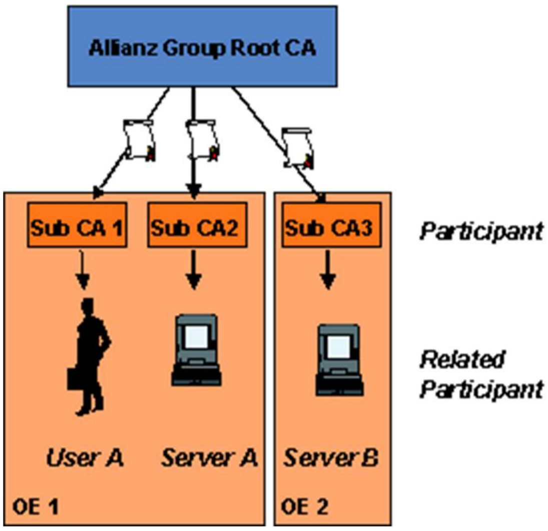

Figure 1: Allianz RCA Operating Model

The practices in this CPS:

1. Focus primarily on the operations of the Allianz RCA
2. Accommodate the diversity of the community and the scope of applicability within the Allianz 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 [RFC-3647].

All certificate operations comply with:

1. The requirements of:
    - this CPS
    - the Allianz Group Information Technology and Information Security Policy [AZ-ITISP]
2. The technology requirements of:
    - Relevant internal guidelines for the physical protection of technology assets [AZ-GPS]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 Root Certification Authority Certification Practice Statement”, or abbreviated “Allianz RCA CPS”.

The OID of the CPS at hand is 1.3.6.1.4.1.7159.30.30.1

1.3 Conventions

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

1.4 PKI Participants

1.4.1 Certification Authorities

Allianz RCA logical architecture consists of:

- Allianz Root Certification Authority (RCA)

- Sub CAs operated by the participating organisations

1.4.2 Registration Authorities

- Registration Authorities (RA) are handling incoming certification requests for the respective CA they can be located inside or outside of RCA or the participating organisations.

1.4.3 Subscribers

Subscribers of RCA are Sub CAs with commitment to the contract with RCA and provided with a certificate from Allianz 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 RCA documentation satisfying to enable Allianz RCA to undergo the acceptance procedure. Allianz 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 Information Technology and Information Security Policy [AZ-ITISP]

- Registration Authority (RA)
  The interface to submit certificate requests and 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 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 RCA published in this CPS.

1.4.4 Relying parties

Customers and employees of the participating organisations.

1.4.5 Other participants

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

1.5 Certificate Usage

1.5.1 Allowed Certificate Usage

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

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

1.5.2 Prohibited certificate usage

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

1.6 Policy Administration

1.6.1 Organization administering the document

The maintain of this CPS is under the responsibility of Allianz PKI Team. Please see section 1.6.2 for contact information.

1.6.2 Contact person

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

Allianz Technology SE
Allianz PKI Team
pki-support@allianz.com

1.6.3 Entity determining CPS suitability for the policy

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

1.6.4 CPS approval procedures

The CPS approval procedure of Allianz RCA and its Sub CAs follow Allianz Group Information Technology and Information Security Policy [AZ-SP] approval processes.

1.7 Definitions and Acronyms

Definitions and Acronyms are part of the appendix 10.3 of this CPS.

2 Publication and Repository Responsibilities

2.1 *Repositories*

The Allianz RCA make publicly available following information on its repository:

- The current and all previous version of CP/CPS
- The current certificates
- The current version of CRLs.

The public repository can be accessible at http://rootca.allianz.com

2.2 *Publication of certification information*

Allianz RCA provides certificates and certificate status updates on its repository. Sub CAs are notified by the Allianz RCA certification authority about changes when practical one week prior to publication.

In regard of Sub CA, CRLs and OCSP responses are available through online service of the respective CAs.

End entity certificates are not publicly available.

2.3 *Time or frequency of publication*

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

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

2.4 *Access controls on repositories*

There is no read access limitation to the public repository. However, unauthorized write access **must** be prevented by implementation of strict logical and physical access control.

3 Identification and Authentication

A fundamental concept underpinning the operation of Allianz RCA's PKI is **trust**. Trust **must** be realised in each and every aspect of the service operation. At Allianz RCA's discretion, other trustworthy parties are permitted to operate Certification Authority and Registration Authority services within Allianz 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 RCA defined in this CPS and the Allianz Group Information Technology and Information Security Policy [AZ SP].

3.1 Naming

3.1.1 Types of names

All certificate subscriber requires a distinguished name listed in the certificate subject, that is in compliance with the X.501 standard and follows ASN.1 syntax structures. The attribute common name (CN) **shall** be part of Subject DN and Issuer DN.

3.1.2 Need for names to be meaningful

The identification and authentication of subscriber can be carried only when the distinguished names (DN) are clearly understood and provide an irreversible association with the authenticated identity of the subscriber. Therefore distinguished names need to be unambiguous and unique.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

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

Before issuing a certificate the Allianz RCA has to prove the correctness and uniqueness of the DN because every DN **shall** be linked to exactly one single Subscriber.

3.1.6 Recognition, authentication, and role of trademarks

Allianz RCA and its subsidiary CAs provide only certificates, which are used in direct context of Allianz product business and service. The issuance of certificates, that infringe upon Intellectual Property Right and Trademark of another company, is prohibited.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

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

1. Checking its records to ensure that public keys are not already listed in any current operational or revoked certificate
2. Additionally, if deemed appropriate, obtaining a document from the subscriber that proves he/she is the true owner of the key pairs
3. Finally, the RCA has the option of exchanging signed and encrypted messages with the subscriber, to verify use of new keys. If any doubt exists, the RCA **must** not 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 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 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

After revocation subscribers **may** request certificate re-issue. Allianz RCA will investigate the reason for the revocation. When the integrity of Allianz RCA systems can be preserved, a replacement for a revoked certificate can be issued.

In any other case, the subscriber **shall** apply for a new certificate, providing all information and documentation required as 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, which 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** request revocation for certificates which were issued by its Sub CAs.
- Each subscriber **may** request revocation of certificates assigned to it during the registration process.
- Certificates issued by the Allianz RCA are revoked by the RCA itself.

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

4 Certificate Life-Cycle Operational Requirements

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

This includes the primary and secondary certificate states as part of the certificate life cycle and the certificate types supported by the Allianz RCA System.

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

The Allianz Root CA Owner is authorized for approving new certificate types and CPs/CPSs.

All certificate operations at Allianz RCA will comply with the requirements of:

- an applicable security policy [AZ-ITISP]
- this CPS
- the minimum operational requirements and operating rules of Allianz 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 RCA certificate starts when a certificate is 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 RCA Certificate Life Cycle in figure 2 below illustrates the states that **may** apply to an Allianz RCA certificate during its life cycle. Note that the diagram applies to all types and grades of certificates issued in the Allianz 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
- Archive.

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

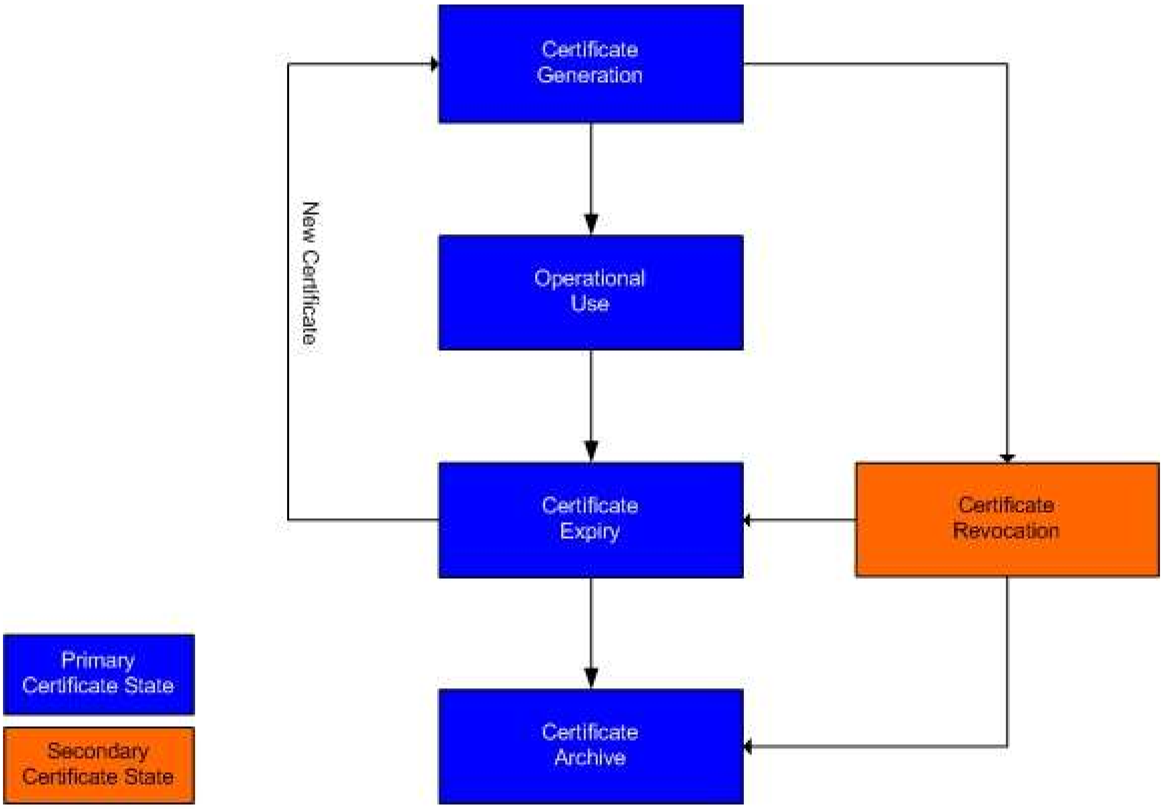
Certificate Generation
Operational Use
Certificate Expiry
Certificate Archive
Certificate Revocation
New Certificate
Primary Certificate State
Secondary Certificate State

Figure 2: Allianz RCA Certificate Life Cycle

All certificates within the Allianz 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 RCA certificate life cycle including the time at which a new replacement certificate is introduced within the system. Figure 3 depicts the typical rollover certificate of the Allianz Root CA and the participating Sub CAs.

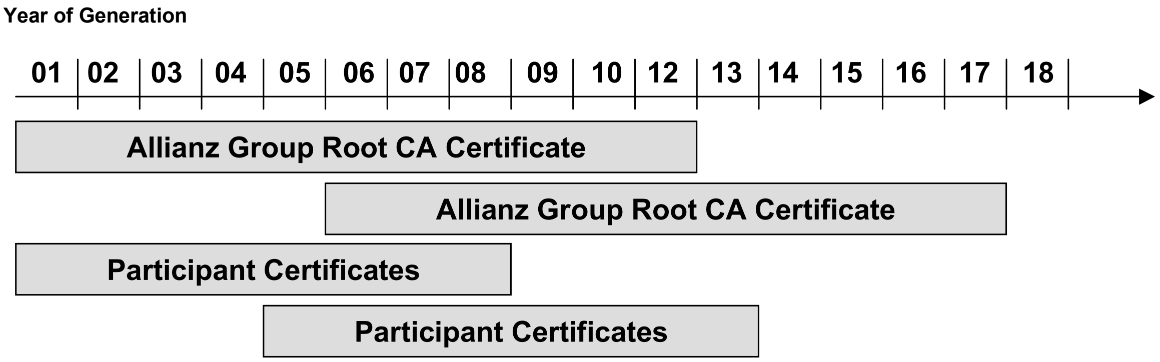
Year of Generation
01
02
03
04
05
06
07
08
09
10
12
13
14
15
16
17
18
Allianz Group Root CA Certificate
Allianz Group Root CA Certificate
Participant Certificates
Participant Certificates

Figure 3: Allianz RCA Certificate Rollover

To prevent problems with nested certificates, 5 years before the expiration of the current Root CA, a new Root CA will be created. After that, 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 RCA issues Sub CA certificates for the participating organisations 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 1.4. The enrolment process is describes in section 4.2.

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

4.1.2 Enrolment process and responsibilities

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

The participants presents the CPS to Allianz Root CA Owner. After attesting the conformity of the participating Sub CA CPS to Allianz policy, the enrolment process can be established.

4.2 Certificate Application Processing

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

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

The issued request **must** enclose (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 Root CA Owner defining the maximum number of SubCAs allowed.
- Key Usage (keyCertSign and/or cRLSign) (critical).
- Subject Key ID (calculated using a 256-bit SHA-256 hash of the value of the bit string subjectPublicKey (issuing certificate)).

Procedures have been established within Allianz RCA to ensure the authenticity and security of certificate requests. Further extensions **shall** be approved by Root CA Owner.

4.2.2 Approval or rejection of certificate applications

Allianz RCA carries out the following checks:

1. Check email to confirm that it was transmitted by a member of Allianz.
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 RCA informs the applicant about the actual status of processing the request.

4.3 Certificate Issuance

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

The Allianz 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, it is essential to ensure that certificate information does not enclose any factual misrepresentations and no data entry errors are made when accepting an application or generating a certificate.

4.3.1 Certificate Requests

Certificate requests in format PKCS#10 are usually generated by the respective Sub CA. Other formats **may** be supported by Allianz RCA as well.

4.3.2 Verification and Rejection of Certificate Requests

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

4.3.3 CA actions during certificate issuance

The Allianz 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 activity with regard to certification is 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 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 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 Allianz Information Security Practice 02 – Encryption [AZ-ISPE] and the Allianz 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 which was 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 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 RCA key supports the understanding of the Allianz RCA compliance requirements. Figure 4 shows the typical life cycle of an Allianz RCA Key Pair which can equally apply to subordinate key pairs. This document will cover every activity/process shown in the lifecycle model and will be applicable to all subordinate CAs within the Allianz RCA System.

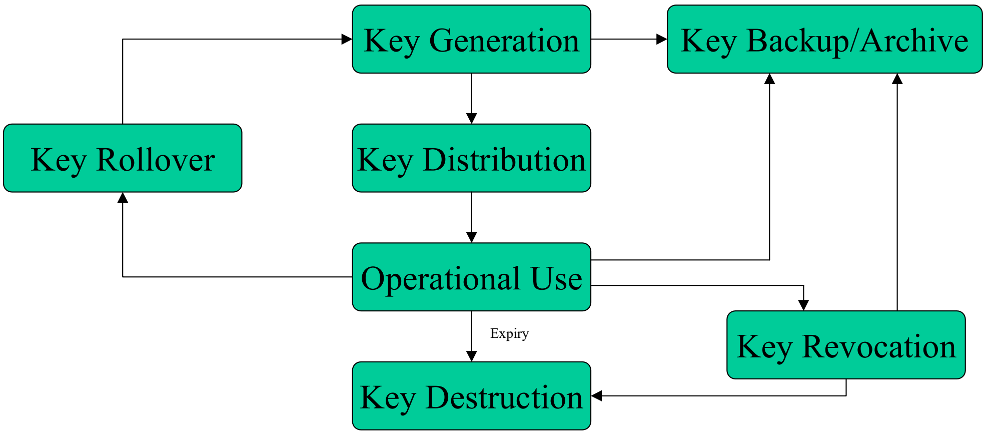

Figure 4: Allianz Key Life Cycle

The life cycle starts with key pair 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 when the associated X.509 certificate reaches the end of its life time. After that the keys **shall** not be used and **shall** be securely destroyed or if required archived. The user usually obtains a new key pair prior to the expiration date of the current key pair. This process is known as key rollover process.

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

4.5.1 Subscriber private key and certificate usage

Allianz RCA certificates are used to support the Allianz RCA system, to enable secure electronic commerce and the secure exchange of information by electronic means, between organisational units. Certificates **shall** only be used during their lifetimes. Revoked certificates **must** not be used.

Allianz RCA uses a number of key pairs for designated purposes. Typically, these keys fall into following types:

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

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

Allianz RCA Participant Keys	Maximum Operational Life	Minimum Key Length (bits)
Allianz RCA Keys	25 Years	4096
Sub CA Keys	15 Years	2048

External Sub CA Keys	10 Years	2048

Operational life of end entity keys **should** be adapted to the actual technical standard and cannot be longer than operational life of associated CA key.

Each Allianz RCA certificate has an CPS, which specifies the certificate's operational purposes and requirements. Before being relied on, the certificate **must** be processed in compliance with [RFC-3647].[RFC-2119]

Any certificate issued by the RCA **must** be published in the repository until the expiration of the certificate.

4.5.2 Relying party public key and certificate usage

The private key of the issued certificate **shall** only be used 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 Participant Agreement (RCA PA) and as indicted in Appendix. At the end of which time they **must** expire. The primary reasons for having certificates expired are to:

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

A certificate is deemed to be 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 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.

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 RCA public key is conveyed in a self-signed certificate, but the customer **shall** gain trust in the Allianz 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 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** conduct 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 expiration of the Allianz RCA Certificate, a new Root Certificate will be created.

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

1. The old Allianz 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 rollover 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

The re-keyed certificates are published in the Allianz RCA repository and can be 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:

1. the name in the certificate is no longer bound to the certificate holder
2. 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 RCA PKI.

4.8.3 Processing certificate modification requests

Participating Sub CAs requiring a modified certificate **shall** 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 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 key pair due to one of the following reasons:

- The security or confidentiality of the private 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 RCA System.
- Loss of private key
- Errors in the certificate
- Change of certificate content
- Certificate misuse
- Cryptographic algorithms become insecure and do not protect the target business or customer data as required.
- The affected CA terminates its operation permanently.
- The participant has terminated its participation in the Allianz 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 **must** be archived to tamper evident media. All types of certificates can be revoked.

While the Allianz 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 RCA (on behalf of Allianz 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 the Certificate Revocation List (CRL), in which the serial numbers of revoked certificates of affected CA are listed.

4.9.3 Procedure for revocation request

4. The Allianz RCA receives a digitally signed certificate revocation request
5. The Allianz RCA verifies the revocation request and revokes the certificate. Notice: Revoked Certificates are not deleted from the Allianz RCA's repository
6. The Allianz 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
7. The Allianz RCA sends a notice including 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 of 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 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 RCA operating rules.

4.9.7 CRL issuance frequency (if applicable)

Not applicable.

4.9.8 Maximum latency for CRLs (if applicable)

Not applicable.

4.9.9 On-line revocation/status checking availability

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

4.9.10 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 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.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

No stipulation.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate Status Services

Allianz RCA provides a web page hosted CRL for verifying the status of revoked 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 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 RCA will be issued to the web server at a minimum once every three month and whenever a change in the CRL occurred.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

In the event that a CA terminates operation permanently, all subscribers, participants and 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 RCA private key escrow and recovery is not permitted.
All private keys used within the Allianz 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 CA environment is hosted in two geographical redundant secure facilities for HA and disaster recovery. The Root Certification Authority, Registration Authority and Backup Systems operate within physically secured areas that meet the standards identified in the Allianz Functional Rule for Information Security [AZ-AFRIS] and Guideline for Physical Security [AZ-GPS].

5.1.2 Physical access

Identification for access to Allianz Group buildings is by means of access system badges or smart cards combined with building access. Access and exit to Allianz Group's buildings is monitored and recorded by the access system. Visitors **must** sign a visitor document with name, company, department, date and time and are handed a badge.

On top of the building access control, the PKI operation room has additional physical security layer. Access to this room is limited only for authorized personnel. No visitors or guests are allowed. Camera surveillance is implemented.

The CA system is in addition protected in a safe with gain access only for CA personnel.

The data centers where CA systems, hardware are located, are ISO 27001 certified.

Physical access control system of data centers follows ISO 27001 – Annex A.11: Physical & Environmental Security implementation guides.

All access systems are armed continuously (24 hours/day, 7 days/week).

5.1.3 Power and air conditioning

Conditions meet the standards identified in the Allianz Guideline for Physical Security [AZ-GPS].

5.1.4 Water exposures

Conditions meet the standards identified in the Allianz Guideline for Physical Security [AZ-GPS].

5.1.5 Fire prevention and protection

Conditions meet the standards identified in the Allianz Guideline for Physical Security [AZ-GPS].

5.1.6 Media storage

Conditions meet the standards identified in the Allianz Guideline for Physical Security [AZ-GPS].

5.1.7 Waste disposal

Conditions meet the standards identified in the Allianz Guideline for Physical Security [AZ-GPS].

5.1.8 Off-site backup

Conditions meet the standards identified in the Allianz Guideline for Physical Security [AZ-GPS].

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 performed by a person who does not directly involved in RCA PKI operations. Issuing certificates system records or audit logs **should** be examined for ensuring that all RCA operators act within the realms of their responsibilities and 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 keys and certificates management tasks are performed centrally. The operation of the Allianz RCA itself will be carried out by authorised personnel from a centralised location.

With reference to personnel aspect, the secure and robust Certificate Authority (CA) operation is based on following essential security principles:

- Least privilege
- Four-eyes/ dual control
- Avoid single source of knowledge

A clear definition of trusted roles helps preventing the conflict during role assignment process.

The following roles have been defined to interact in the Allianz Root CA operational processes. One CA personnel can be assigned to more than one role when the basic security principles described above are not be violated.

Roles	Responsibilities
CA Owner	• Owns the CA • Fully responsible for the whole CA business • Approve high risk tasks like revoke CA certificates
CA Manager	• Organize, lead CA events like key ceremony • Maintenance and create CA process, procedures & operational documentation • Monitor CA events to ensure each participant follows documented procedures. • Organize CA operator and key custodians • User management including roles and access rights (technical and organizational) • Manage inventory of CA assets (hardware, software, key material). Conduct inventory check every six months.
CA Operator	Setup/configure/operate/ manage CA components, which include RA, CA, CRL, and OCSP services: • Generate CA keys and CA certificates • Revoke CA certificates • Update CRL • Manage registration data including suspension and revocation information • Generate OCSP keys, OCSP updates, request OCSP certificates, update OCSP information, revoke OCSP certificates, configure online OCSP functions and application features • Configure offline/online CA, OCSP functions and application features • Perform backup tasks
Key Custodian	• Not key owners, hold normally key component, handle cryptographic key material for CA services, which includes

	keys for RA, CA, OCSP and other cryptographic enabled services. • Enable RA, CA, OCPS keys and support backup and recovery services, using dual controls with split knowledge.
System Administrator	• Setup, configure and maintain the CA IT structure, including networks, databases and server
Security Officer	• Create CA policy, functional practices • Review and approve CA process, procedures & operational documents • Provide physical security controls for all CA related services, applications, systems or network components • Annual or ad hoc security and risk assessments of any or all CA components/services.
Auditor	• Review annually CA documents including process documents, CA event protocol and log data • Conduct physical security inspection of all CA (offline/online CA systems + OCSP) related services, application, system or network components • Inspect the management of cryptographic material to ensure security policies, practices, and procedures are followed.
Safe User	• Owns the safe PIN and/or key

5.2.2 Number of persons required per task

At least two RCA personnel authenticated by smart card are required for a task

5.2.3 Identification and authentication for each role

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

5.3 Personnel Controls

The Allianz RCA System has adopted the personnel 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 0) **must** undergo an appropriate security screening procedure, designated “Position of Trust”.

All Allianz 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 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 RCA personnel who are 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 Allianz Computer Emergency Response Team (CERT) when a process or action causes a critical security event or discrepancy.

5.3.4 Training requirements

Allianz RCA will ensure that all staff is briefed immediately on any changes which affect current operations. Operational personnel will be trained without delay 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 RCA **shall** be trained in:

a. Basic PKI concepts
b. The use and operation of certification authority software
c. Documented procedures

d. Computer security awareness and procedures
e. The meaning and effect of this CPS and relevant CPs.

5.3.5 Retraining frequency and requirements

Retraining is performed at least once a year based on and include the necessary quality controls.

5.3.6 Job rotation frequency and sequence

No stipulation.

5.3.7 Sanctions for unauthorized actions

Unauthorised actions by Allianz RCA System staff are submitted to appropriate authorities including, but not limited to, the Computer Emergency Response Team(CERT) .

5.3.8 Independent contractor requirements

No stipulation.

5.3.9 Documentation supplied to personnel

Allianz RCA System staff has access to all documentation of RCA system and training material.

5.4 Audit Logging Procedures

The Allianz RCA and all approved Sub CAs are obliged to maintain adequate records and archives of operative information of the PKI. The CA software automatically preserves an audit trail for the primary states of the Allianz 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:

4. Types of registration records, including records relating to rejected applications
5. Certificate generation requests, whether or not certificate generation was successful
6. Certificate issuance records, including CRLs
7. 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 RCA hierarchy is to establish and maintain a backup procedure for audit logs.

5.4.6 Audit collection system (internal vs. external)

The Allianz 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
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

Type of event	Collection System	Recorded by
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 the Computer Emergency Response Team (CERT) 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 RCA hierarchy maintains an archive of relevant records. This section details the RCA's records archiving procedures.

5.5.1 Types of records archived

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

1. Audit logs
2. Certificate request information
3. Certificates, including CRLs generated
4. Complete back up records
5. Copies of e-mail logs
6. Formal correspondence
7. Application records.

5.5.2 Retention period for archive

Certificates issued by the Allianz 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

No stipulation.

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 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 RCA securely on an archive medium.

The Allianz 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 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 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 Business Continuity Management Recovery Strategy Guide [AZ-BCMG].
   - 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 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 RCA's certificate is revoked
  The Allianz RCA has established a key and user compromise plan that addresses the actions to be taken in the event that the Allianz RCA's signing certificate is revoked. Subordinate Certificate Authorities are to promptly advise of any compromise or suspected compromise of the Allianz RCA private keys.
- Key compromise
- Natural or other type of disaster

5.7.1 Incident and compromise handling procedures

Incident and compromise handling are part of Allianz IT DRP and BCM plans, cf. [AZ-BCMG].

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

Computing resources are always hardware and software backed up.

5.7.3 Entity private key compromise procedures

The Allianz 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 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 **may** prompt disaster recovery initiation
4. Considered secondary precautionary measures that **may** be required, such as:
    a. a backup site
    b. 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 RCA service, the impact of the termination is to be minimised as much as possible in light of the prevailing circumstances. The Allianz 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 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 shutdown of the Allianz RCA, e.g. due to the compromise of its private key, the Allianz 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 RCA immediately and prior to the emergency shutdown. Services **should** be recommenced by the same (or a successor Root Certification Authority) as quickly as possible after the shutdown has been effected.

5.8.1 Keys and Certificates

In the event that it becomes necessary to terminate the Allianz 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 RCA, provided the transferred certificates do not become operational within the chain of trust of the replacement Allianz RCA Service until after the shutdown of the terminating Allianz RCA or
3. All Sub CA certificates **may** need to be revoked prior to the shutdown of the terminating Allianz RCA service, and the keys **may** be transferred to the replacement Allianz RCA service for the issue of new certificates, provided that such new certificates are not generated until after the shutdown of the terminating Allianz RCA service.
4. The last act of the terminated certification authority is to issue a CRL with all certificates revoked. The Allianz 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 RCA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

Allianz 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 RCA participant keys are keys issued for or generated by the CAs within the Allianz RCA System. They **may** be related to Allianz RCA or participant.

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

Allianz RCA/Participant Keys	Maximum Operational Life	Minimum Key Length (bits)
Allianz RCA Keys	25 Years	4096
Participant CA Keys	15 Years	2048
External Participant CA Keys	10 Years	2048

The Allianz RCA's keys are exclusively generated by the Hardware Security Module (HSM) as part of the Allianz 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 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 RCA System **shall** be generated in hardware.

6.1.1 Key pair generation

It is a fundamental principle of Allianz 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 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.

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

The HSM **must**:

1. Comply at least with the FIPS 140-2 Level 2 (Federal Information Standards, NIST, 140-2: Security Requirements for Cryptographic Module) 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. AES 256 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 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 CPS.

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

6.1.5 Key sizes

Generally the Allianz RCA Root keys are 4096 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, measurements and hardware support wherever possible.

6.2.1 Cryptographic module standards and controls

A FIPS Level 3 Cryptographic Module including card management are in use. Hardware security module are also recommended to be used by Sub CAs for private key protection. The Allianz RCA 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 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 RCA’s private key backup **shall** be encrypted. Backup copies are maintained securely on onsite and offsite storage. Allianz 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 keys are archived in FIPS 140-2 Level 3 HSMs, which are stored on different locally separated sites.

6.2.6 Private key transfer into or from a cryptographic module

FIPS 140-2 Level 3 permits private key import to HSM. Export is only possible from one HSM to the backup HSM. Private key generation is only performed on HSM.

6.2.7 Private key storage on cryptographic module

6.3 Indemnities

6.3.1 Method of activating private key

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

6.3.2 Method of deactivating private key

No stipulation.

6.3.3 Method of destroying private key

No stipulation.

6.3.4 Cryptographic Module Rating

The HSM, FIPS 140-2 Level 3 compliant, is in use.

6.4 Other Aspects of Key Pair Management

6.4.1 Public Key Archival

All public keys are archived by the Certificate 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 with expired validity period **must** continue to be accessible in order 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.

6.4.2 Usage Periods for the Public and Private Keys

The usage periods are prescribed within this CPS.

6.5 Activation Data

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

6.5.1 Activation data generation and installation

No stipulation.

6.5.2 Activation data protection

No stipulation.

6.5.3 Other aspects of activation data

No stipulation.

6.6 Computer Security Controls

Allianz RCA has established the Allianz Group Information Technology and Information Security Policy [AZ-ITISP]

that incorporates computer security technical requirements that are specific to Allianz RCA's operations.

6.7 Life Cycle Security Controls

6.7.1 System Development Controls

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

6.7.2 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.

6.7.3 Life cycle security controls

Only certified software components are in use in operational environment. The software development obeys the software development procedures forced by Allianz IT Security. The Allianz RCA as well as any participating Sub CA **shall** maintain contingency plans in force, including adequate backup 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.

6.8 Network Security Controls

Network security controls are highlighted in the Allianz Information Security Practice 05 - Network Security [AZ-ISPN].

6.9 Timestamping

No stipulation.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

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

- All certificates are IETF-PKIX certificates in accordance with [RFC-2459]. The use of certificate extensions (critical / non-critical) will be governed by [RFC-2459]. 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 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, if it is an end-entity or a Sub CA, **shall** have its public key signed by more than one Certification Authority.
- Identifiers
    - All certificates **must** not contain Issuer Unique ID and Subject Unique ID.
    - Subject and Authority Key identifiers **shall** be used.
    - KeyID method based on 256 bits hash of subject public key as per [RFC-2459].
- Constraint Extensions
- OIDs
    - OIDs are not allocated to algorithms supported and used within the Allianz 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 and/or certificate practices statement **shall** be present and enclose an Allianz RCA Object Identifier at a minimum.

7.1.3 Version number(s)

Certificates **must** comply with X.509 v3 standard

7.1.2 Certificate extensions

The certificate extensions are defined by Allianz 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 RCA certificates.

- Signature algorithm for all Allianz RCA Certificates is RSA with SHA256
- The root **shall** have 4096 bit RSA keys, at least
- All other CAs **shall** have 2048 bit RSA keys, at least

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name formats

Certificates issued by the Allianz 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** consist of a non-null Issuer DN and a Subject DN.
Note: There are no constraints on the relationship between issuer and subject DNs.

7.1.5 Name constraints

Name constraints **muss** 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 consist of an Allianz 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 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

No stipulation.

8 Compliance Audit and Other Assessment

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

All participants utilising the Allianz RCA System will be subject to minimum audit requirements necessary to demonstrate compliance with the Allianz Information Security Practice 02 – Encryption [AZ-ISPE]. Allianz 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 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 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 RCA with copies of all audits and reviews on a timely basis (within 30 days). Allianz 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 RCA.

8.3 Assessor's relationship to assessed entity

Allianz 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 RCA initial compliance audit process prior to issuing certificates. The purpose of the Allianz RCA initial compliance audit process is to determine that the Sub CA complies with the minimum eligibility, operational and technical requirements of the Allianz 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 RCA. After acceptance as participant of Allianz

RCA system the participant will be required to conduct the Allianz 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 Root CA Owner 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 RCA with copies of all audits and reviews on a timely basis (within 30 days). Allianz RCA will also be informed about interim reviews and follow up conducted on all significant audit / review issues.

Other Business and Legal Matters

9 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 1.4 1.4.

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 Certificate issuance or renewal fees

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

9.2 Certificate access fees

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

9.3 Revocation or status information access fees

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

9.4 Fees for other services

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

9.5 Financial Responsibility

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

9.5.1 ***Insurance*** coverage

No stipulation.

9.5.2 Other assets

No stipulation.

9.5.3 Insurance or warranty coverage for end-entities

No stipulation.

9.6 Confidentiality of Business Information

9.6.1 Allianz RCA Documentation

All documentation provided by Allianz RCA, that is deemed to be confidential **must** be labelled “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 **must** be no less than reasonable care.

9.6.2 Scope of confidential information

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

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

9.6.3 Types of Information in particular considered confidential

1. **Personal Information**

   Information supplied to Allianz 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 including 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 RCA when it receives an application from a third party to operate a CA within the Allianz 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.

9.6.4 Information not within the scope of confidential information

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

9.6.5 Responsibility to protect confidential information

No stipulation.

9.7 Privacy of Personal Information

9.7.1 Privacy plan

No stipulation.

9.7.2 Information treated as private

The collection, processing and use of personal data **shall** be admissible only if permitted or prescribed by the **General Data Protection Regulation** (Regulation (EU) 2016/679) ('GDPR') or any other legal provision or if the subscriber has consented.

9.7.3 Information not deemed private

All information out of the scope of 9.4.2.

9.7.4 Responsibility to protect private information

No stipulation.

9.7.5 Notice and consent to use private information

No stipulation.

9.7.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.7.7 Other information disclosure circumstances

No stipulation.

9.8 Intellectual Property Rights

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

9.8.1 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.

9.8.2 Certificate

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

9.8.3 Distinguished Names

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

9.8.4 Copyright

Copyright of the Object Identifiers (OID) for the Allianz RCA System vests solely in Allianz 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 RCA infrastructure, or in accordance with the relevant CPS.

9.9 Representations and Warranties

9.9.1 CA representations and warranties

Allianz 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 RCA in relation to the certificates.

9.9.2 RA representations and warranties

No stipulation.

9.9.3 Subscriber representations and warranties

No stipulation.

9.9.4 Relying party representations and warranties

No stipulation.

9.9.5 Representations and warranties of other participants

No stipulation.

9.10 Disclaimers of Warranties

Allianz RCA disclaims all warranties of any kind unless stated otherwise within the Allianz 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.

9.11 Limitations of Liability

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

9.11.1 Safeguards

Allianz 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 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

9.12 Indemnities

Cf. Section 9.11.

9.13 Term and Termination

9.13.1 Term Allianz Root certificate

Validity	
Not Before	e.g. “Wednesday, April 29, 2015 10:41:30 AM”
Not After	e.g. “Sunday, April 22, 2040 10:41:30 AM”

9.13.2 Termination

a) Termination by Participant

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

b) Termination by Allianz RCA

Allianz 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 PKI if

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

4. otherwise determines to discontinue provision of the Allianz RCA System.

Allianz RCA **must** provide the participating organisation at least thirty (30) days prior written notice of Allianz 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 RCA to terminate the participant, Allianz RCA **shall** provide notice of the termination to the participant stating the reasons for and the effective date of the termination.

The relevant CA **should** notify their subscriber about the CA termination before the due date.

9.13.3 Effect of termination and survival

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

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

9.14 Individual Notices and Communications with Participants

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

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

9.15 Amendments

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

9.15.1 Notification mechanism and period

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

9.15.2 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.

9.16 Dispute Resolution Procedures

No stipulation.

9.17 Governing Law

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

9.18 Compliance with Applicable Law

Cf. sections 9.7 and 9.8.

9.19 Miscellaneous Provisions

9.19.1 Entire agreement

No stipulation.

9.19.2 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 RCA, (b) an agreement with a third party CA.

9.19.3 Severability

No stipulation.

9.19.4 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 RCA of this CPS **shall** govern

9.19.5 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.

9.19.6 Other Provisions

Sub CAs of the Allianz RCA are subordinate exclusively to the Allianz RCA and **may** not be certified by any other authority within or outside the Allianz 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 RCA initial compliance audit process prior to issuing certificates. The purpose of the Allianz 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 RCA. The assessment is to be conducted by qualified internal or external audit personnel, with the results of such reviews reported to Allianz RCA.

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

10 Appendix

There are a number of different types of certificates currently issued by Allianz 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 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-256 with RSA Signature	
1.4. Issuer Distinguished Name		
1.4.1. Country (C)	DE	
1.4.2. Organization (O)	“Allianz”	
1.4.3. Common Name (CN)	“Allianz Root CA III”	
1.5. Validity		
1.5.1. Not Before	Apr 29, 2015 10:41:30 AM CEST	
1.5.2. Not After	Apr 22, 2040 10:41:30 AM CEST	
1.6. Subject		
1.6.1. Country (C)	DE	
1.6.2. Organization (O)	“Allianz”	
1.6.3. Common Name (CN)	“Allianz Root CA III”	
1.7. Subject Public Key Info	D7:02:1E:73:8A:AF:08:22:A4:BB:39:4E:7D:66:55:F2 7C:BE:AD:DA:A9:F7:24:94:0F:09:DA:69:17:AD:D5:34 1C:9A:40:5E:F4:16:9C:E8:2B:2F:C4:0B:53:6F:99:21 F0:ED:18:EE:96:85:29:E6:2E:0C:B5:38:D2:1A:AF:26 2A:BA:6B:C9:E5:7B:06:00:80:C2:B1:EC:7E:44:4D:13 60:2D:39:1B:2D:B2:DD:25:60:D6:90:45:34:60:BF:46 47:3A:7B:EA:84:E0:BC:41:57:10:D8:7E:9B:C5:01:16 82:CD:AE:9F:EC:CC:7D:93:AC:21:B5:5E:2D:EC:10:20 01:74:F2:1F:7B:E7:72:87:21:B9:7D:30:44:0E:EB:92 23:57:8A:FA:BE:4B:32:C5:BC:D2:40:75:81:BD:D8:21 31:49:96:48:0A:17:21:CA:BC:79:D5:E8:A1:DA:FC:7E 09:47:18:75:CB:5D:91:5B:B5:1C:B4:D7:B3:72:60:18 76:D7:CC:82:F4:C2:18:1C:97:3F:7B:75:1E:29:B3:BF C4:0C:FF:B7:1D:76:A7:08:E6:F5:B7:D8:4D:7F:59:52 A5:99:1F:3D:68:18:CA:BF:91:16:19:A2:19:15:8D:90 22:D1:FE:AC:88:79:AC:D2:3E:1E:4F:AC:4C:45:C4:ED	

Field	Content	Critical*
	1A:EB:21:24:85:8C:E2:E5:81:B5:4D:0E:B6:2D:7E:0E 67:BF:81:CA:74:85:D6:1B:C3:97:E6:B5:DF:73:B5:B9 65:4D:56:C9:62:EF:17:57:C1:D2:77:91:C0:03:02:F1 B2:C9:F2:56:90:1C:97:4E:AE:B2:13:3E:08:83:9B:BA 30:8A:28:BC:42:57:6E:46:34:89:C8:3B:F3:48:3C:47 1F:F5:82:03:84:9D:7D:BD:B4:B5:3F:6F:F7:2C:99:2C 93:2C:2E:A4:72:14:BC:51:4E:B9:E1:A0:65:11:CB:7F C8:89:86:34:E3:DE:6E:AC:D6:02:59:C9:BD:2B:79:1A 8D:FF:A9:B2:03:E0:48:C7:62:47:CF:E8:E0:E0:97:43 71:87:7C:F6:0C:04:C0:EE:3C:3A:87:2E:4D:7A:67:A5 B1:5C:9D:BA:06:DD:60:C2:2F:6A:87:BE:7A:48:79:63 C9:F3:02:6C:78:8B:15:17:60:E7:6E:62:BC:73:D7:3F 73:FB:0D:76:80:7C:D7:A0:26:6C:A8:F9:F4:3E:C8:94 88:67:96:DB:D3:09:55:A8:AB:4C:35:FA:C5:31:B7:CE 98:C2:7D:0A:75:3C:B3:A8:EE:98:E1:68:61:36:DD:44 F2:AC:83:2C:21:54:F7:1A:35:91:31:35:1D:AB:1A:47	
2. Key	RSA 4096bit	
3. X.509v3 Extensions		
3.1. Authority Key Identifier		n
3.1.1. Key Identifier	1a 57 d8 63 81 b1 9f 1a fe 8b 36 6c d0 a7 80 68 47 2e 7a f9	
3.2. Subject Key Identifier	1a 57 d8 63 81 b1 9f 1a fe 8b 36 6c d0 a7 80 68 47 2e 7a f9	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	1.3.6.1.4.1.7159.30.30.3	
3.4.2. Policy Qualifier ID	CPS	
3.4.2.1. User Notice (Organiz.)	Allianz Germany	
3.4.2.2. User Notice (notice No.)	1	
3.4.2.3. User Notice (Display Text)	This Certificate is issued by Allianz Root CA III, by Allianz Germany	

Field	Content	Critical*
3.4.2.4. URL (ia5String)	http://rootca.allianz.com/cps3/	
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	1	
3.7. Netscape Extensions		n
3.7.1. CertType	SSL CA, SMIME CA, Signature CA	
3.8. CRL Distribution Point		n
3.8.1. 1st URL	http://rootca.allianz.com/rootca3.crl	
Fingerprint	1c4229d2b1cf4e2fee5c6564bb8647910163e2ab	

*not used for attributes, only extensions

10.2 Participant CA Key Signing Certificate Profile

This certificate is signed by the Allianz 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*
4. X.509v1 Field		
4.1. Version	v3	
4.2. Serial Number	01	
4.3. Signature Algorithm	SHA-256 with RSA Signature	
4.4. Issuer Distinguished Name		
4.4.1. Country (C)	DE	
4.4.2. Organization (O)	“Allianz”	
4.4.3. Common Name (CN)	“Allianz Root CA III”	
4.5. Validity		
4.5.1. Not Before	tbd	
4.5.2. Not After	Tbd max. ., “23:59:59 31 December 2026”	
4.6. Subject		
4.6.1. Country (C)	DE	
4.6.2. Organization (O)	Allianz	
4.6.3. Common Name (CN)	tbd	
4.7. Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1	
5. Key	Min RSA 2048bit	

Field	**Content**	**Critical***
6. X.509v3 Extensions		
6.1. Authority Key Identifier		n
6.1.1. Key Identifier	Hash Value of Certificate	
6.2. Subject Key Identifier	Hash Value of Certificate	n
6.3. Key Usage		y
6.3.1. Digital Signature	Selected	
6.3.2. Non Repudiation	Not selected	
6.3.3. Key Encipherment	Not selected	
6.3.4. Data Encipherment	Not selected	
6.3.5. Key Agreement	Not selected	
6.3.6. Key Certificate Signature	Selected	
6.3.7. CRL Signature	Selected	
6.4. Certificate Policies		n
6.4.1. Policy Identifier	1.3.6.1.4.1.7159.30.x	
6.4.2. Policy Qualifier ID	1.3.6.1.5.5.7.2.2	
6.4.2.1. User Notice (Organiz.)	Allianz Germany	
6.4.2.2. User Notice (notice No.)	1	
6.4.2.3. User Notice (Display Text)	This Certificate is issued by Allianz Root CA III, by Allianz Germany	
6.4.2.4. URL (ia5String)	https://rootca.allianz.com/cps3/	
6.5. Basic Constraints		y
6.5.1. Subject Type	CA	
6.5.2. Path Length Constraint	Not empty	
6.6. CRL Distribution Point		n
6.6.1. 1st URL	https://rootca.allianz.com/crl/rootca3.crl	
6.7. Special extensions of CA	tbd	n
Fingerprint	Public key encoded in accordance with RFC2459 & PKCS#1	

*not used for attributes, only extensions

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 **may** 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.
Computer Emergency Response Team (CERT)	A specialist unit of the technical information security department that is contact for topics related to the technical aspect of information security and takes care of the analysis and defense against hacking attacks and security-related incidents on the Allianz Technology SE.
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.
HSM	Hardware Security Module

For more definitions refer to [RFC-3647].

10.4 Abbreviations

ADS	Active Directory Service
BGU	Betriebsgebäude Unterföhring (Data Centre)
CA	Certification Authority
CMLC	Certificate Management Life Cycle
CN	Common Name
CPS	Certification Practise Statement
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DCOM	Distributed Component Object Model
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name Service
FIPS	Federal Information Processing Standard
GISF	Allianz Group Information Security Framework
HSM	Hardware Security Module
ISIS-MTT	Interoperability Standard (ISIS – Mail Trust)
ISO	Information Security Officer
OCSP	Online Certificate Status Protocol
OE	Organisational Entity
OID	Object Identifier
OS/390	Operating System 390
OU	Organisational Unit
PAC	Policy Approval Council
RA	Registration Authority
RCA	Root Certification Authority
RFC	Request for Comment
SCEP	Simple Certificate Enrollment Protocol
TSM	Tivoli Storage Management
VPN	Virtual Private Network