Certification Practice Statement for Allianz Smartcard Certification Authority V (SC-CA V)

Information Owner: Allianz PKI Team

Version 1.2 / 18.07.2022

Document-ID: SC-CA V CPS

Classification: Public

Change Log

Version	Description	Date	Author
0.9	Initial Draft	27.04.2015	Helmut Buss
0.9.1	Allianz Group to Allianz, Root CA II removal. Contact details updated.	28.04.2015	Sinu Joseph
0.9.2	Chapter numbers, Certificate profile	13.05.2015	Helmut Buss
0.9.3	Review	19.11.2015	Vera Kloepper
1.0	Final with OIDs	10.05.2016	Aditya Kumar Yellai
1.1	• Changed company name to Allianz Technology SE • Updated references to new security policies, practical rules and practices • Removed CRL information • Added OCSP information • Updated trusted roles • Added document OID • Added Computer Emergency Response Team	31.06.2022	Thi Hang Nguyen
1.2	Review	18.07.2022	Helmut Buss

1 Introduction

1.1 Overview

Allianz has established a SmartCard Infrastructure (SCI) that supports authentication services for a variety of access scenarios such as Single Sign-On (SSO) to Allianz Windows Domains or Remote Access to the Allianz Corporate Network or Logon to Intranet Applications by providing authentication tokens to subscribers.

As central architectural components, it comprises a Card Management System (CMS) and the "Allianz Smartcard CA V" (SC-CA V) Certification Authority, referred to as SC-CA-V hereafter, which is part of the Allianz's PKI landscape and chains up to Allianz Root CA. The RCA Certification Practice Statement is published under http://rootca.allianz.com/cps3.

The SCI is capable of issuing smartcards with different key pairs so that separate certificates can be loaded onto a card each with distinct purposes (e.g. one for encryption and one for authentication and digital signing).

This Certification Practice Statement (CPS) describes the practices that Allianz adopts in its approach to Certification Authority (CA) operations regarding SC-CA V.

The SCI manages registration, issuance, renewal, management, reinstatement, and revocation of digital certificates under an X.509 certificate-based Public Key Infrastructure (PKI) for subscribers defined in section 1.3.3.

The SC-CA V service is intended for business use. The subscriber certificates will be issued to Allianz employees, Allianz field agents and employees from other Allianz OE or external staff, which are not employees but in a contractual relationship.

1.1.1 Aim of the policy

This CPS describes the policies, practices and procedures that SC-CA V **may** employ for issuing certificates to eligible subscribers. It stipulates legitimate certificate use in terms of who **may** use SC-CA V Certificates and in terms of the specific purposes that SC-CA V certificates **may** be used for.

This CPS assumes that the reader is generally familiar with PKI. Allianz top-level security policies do apply and are described in Allianz Security Policy.

1.1.2 RFC 3647 Structure

This document is structured in accordance with [RFC-3647] and follows the outline therein provided.

The formal structure, based on the internationally accepted framework, enhances the transparency and comparability compared to common practice. This transparent structure aims at achieving a better comparability of the policies and, thus, of the security levels.

1.1.3 Validation

From the date of publication on Allianz RCA Internet Site: http://rootca.allianz.com is this policy for this SC-CA V binding for all of its subscribers and their relying parties.

1.2 Document Name and Identification

This CPS is referred to as the “Certification Practice Statement for Allianz Smartcard Certification Authority V”.

Object Identifier (OID) for this document is: 1.3.6.1.4.1.7159.30.34

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

PKI Participants are persons involved in the operations or use of the SC-CA PKI but also technical infrastructure and automated procedures in as far as they implement Registration Authority or Certification Authority functionality.

1.4.1 Certification Authorities

Within the 2-tier trust hierarchy of the Allianz PKI, SC-CA V is the Sub-CA of Allianz RCA that has been specifically created to issue X.509 end-entity certificates for smartcards.

The SC-CA V relies on a highly-available physical infrastructure comprising a Certificate Management System, Hardware Security Modules (HSM) and a Card Management System (CMS) offering a rich functionality of card life cycle management.

1.4.2 Registration Authorities

Registration authorities (RAs) are authorities dealing with registrations for subscribers. They are entrusted to ensure the identification of subscribers based on personal appearance and the presentation of credentials (ID card, passport, etc.).

Being an Allianz internal CA, it is permitted for SC-CA V to rely on internal corporate directories for the purpose of subscriber identity verification. A subscribers’ organizational entity (OE) is responsible for delivering valid subscriber data to corporate directories and keeping this data up-to-date. Before delivering the data, the initial subscriber identification has to be passed the applicable provision process of this OE. SC-CA V is not in charge of the legitimacy of directory data.

The SC-CA V RA process is by default initiated through a card request for a specific subscriber. The request has to be trigged by an authorized person, who is typically a person designated a Rights Administrator Role with respect to the subscriber. Depending on the circumstances, e.g. for the issuance of temporary cards, this can also be ID-Card-Centre or security guard reception.

In order to issue card request, authorized persons are required to authenticate to Identity Management (IDM) Tools. The IDM Tools in turn authenticate against the CMS. The communication is secured via SSL channels. The CMS will always accept a card request for a subscriber from an authorized IDM Tool if relevant subscriber data can be verified electronically against corporate directories.

The RA process concludes with the registration of the approved card request in the system. In the specific case of certificate renewal, the RA process can be implemented as an automated scheduling on the CSM without involvement of any IDM Tool but still relying on identity verification against directories. RA procedures are described in detail in section 3 of this CPS.

1.4.3 Subscribers

SC-CA V issues End-Entity certificates only. Certificate subscribers are natural persons working for organizational entities (OE) within Allianz. Such persons can be internal staff, sales representative or external consultants in a contractual relationship with an Allianz OE.

1.4.4 Relying parties

Relying parties are the certificate subscribers, recipients or senders of secure E-Mail and IT-systems, which authenticate subscriber of the corresponding OE.

1.4.5 Other participants

No external certificate authorities or PKI service providers are part of SC-CA V PKI architecture.

1.5 Certificate Usage

1.5.1 Appropriate Certificate Usage

Certificates issued by the SC-CA V are used to support authentication of subscribers by relying parties, as well as secure communications and the secure exchange of information between subscribers and relying parties

Certificate usage is intended to the services described above and Key Usages specified in the SC-CA V certificates. Certificate usage is restricted to the x509 standard.

The following certificate key usages have been approved for SC-CA V:

- Digital Signature
- Key Encipherment
- Data Encipherment

1.5.2 Prohibited certificate usage

Certificates issued by SC-CA V **may** only be used for the purposes listed in Appropriate Certificate Usage above. Other usages **may** be approved in advance in written by SC-CA V administration.

1.6 Policy Administration

1.6.1 Organization administering the document

This CPS is published and administered by Allianz PKI Team from Allianz Technology SE.

1.6.2 Contact person

Comments, feedback, and requests for further help and information are welcome. PKI Team makes every effort to respond promptly to inquiries. Please address your correspondence to :

Allianz Technology SE

Allianz PKI Team

Email: *pki-support@allianz.de*

1.6.3 Person determining CPS suitability for the policy

The Allianz Root CA Owner **shall** govern the enforceability, construction, interpretation, and validity of this CPS.

1.6.4 CPS approval procedures

Allianz Root CA Owner determines the suitability of this CPS and its compliance with other Allianz policies.

It is the final approval authority of any proposed changes to this CPS.

Documentation of SC-CA V in particular includes this Certification Practice Statement and a compliance statement in respect to Allianz Group Information Technology and Information Security Policy [AZ-ITISP]

1.7 Definitions and Acronyms

This CPS assumes that the reader is familiar with basic PKI concepts, including:

- The use of digital signatures for authentication, integrity and non-repudiation
- The use of encryption for confidentiality
- The principles of asymmetric encryption, public key certificates and key pairs and
- The role and function of Certificate Authorities (CAs).

Definitions and Acronyms are part of the appendix “A. Definitions and Acronyms” of this CPS.

2 Publication and Repository Responsibilities

2.1 Repositories

The Allianz RCA make publicly available following information of all Allianz RCA participants included SC-CA V on its repository:

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

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

SC-CA V distributes end entity certificates and certificate information to internal directory services like Allianz Global Directory, Corporate Active Directory and RACF (for reference by IBM Hosts). Those repositories are private, not publicly available and operated by Allianz Technology SE.

2.2 Publication of certification information

Certificate status information is available in both forms: regularly updated Certificate Revocation Lists at the Allianz RCA Internet Site http://rootca.allianz.com and OCSP service accessible at http://rootca.allianz.com/ocsp/ .

2.3 Time or frequency of publication

Changes to this CPS are published as soon as they are approved.

End-Entity Certificates and Certificate fingerprints are published directly after certificate issuance.

The SC-CA V CRL is updated at an interval of two weeks with a validity of four weeks. If necessary, the CRL can be published manually by support staff.

Certificate status information provided via OCSP services is always up-to-date as the SC-CA's internal data repository is consulted the current information at the time of OCSP request.

2.4 Access controls on repositories

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

The private repositories where SC-CA V end entity PKI data like certificates, certificate status, certificate revocation etc. underlie a strict access control as stipulated by the Allianz Group Information Technology and Information Security Policy [AZ-ITISP]

3 Identification and Authentication

Identification and Authentication performed by SC-CA V Registration Services are in compliance with Allianz RCA provisions. Identification and authentication are required in the events of card enrollment, card delivery and card unlock.

SC-CA's RA accepts card / certificate requests for subscribers if they are trigged by authorized persons, transmitted through authorized IDM systems and if a defined set of subscriber's data can be verified against corporate directories. SC-CA V thereby relies on the fact that Allianz's organizational entities (OEs) fulfills their obligation to provide valid subscriber data to corporate directories.

Authorized persons who request smartcards for a subscriber can only send request if relevant data for this person is present in corporate directories.

After provisioning, the smartcard can be handed over to a subscriber in person by authorized persons or sent via internal post to subscriber's office address.

Persons who is authorized to personally hand-over smartcard including ID-Card-Centre staff will always perform proper subscriber identification by checking personal ID documents or aligning with the subscriber's rights administrator and line manager

Subscribers have to sign a document to confirm receipt of their smartcard.

3.1 Naming

3.1.1 Types of names

All certificate holders require a Distinguished Name that is in compliance with the X.501 ITU-T recommendation for Distinguished Names. The attribute Common Name (CN) is part of Subject DN and Issuer DN.

The subscriber certificates issued by the SC-CA V use the following DN name format:

- Country (C) = DE
- Organization (O) = ALLIANZ AG
- E-Mail (E) = e-mail address which complies with [RFC-822], listed and managed by the Allianz internal Mail-System
- Common Name (CN) = 'first name surname'.

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

SC-CA V does not issue certificates to anonymous identities. The use of pseudonyms by subscribers is not permitted. Only the subscribers' real names can be used to verify against corporate directories..

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The uniqueness of the Distinguished Name (DN) is established by the inclusion of a subscriber's unique e-mail address in the DN. Every DN **shall** be linked to exactly one single Subscriber.

3.2 Initial Identity Validation

The subscriber's OE is accountable for the initial identity registration of every subscriber and the delivery of correct identity information to corporate directories in upfront.

SC-CA V RA will check subscriber information included in certification request against corporate directories.

3.2.1 Method to prove possession of private key

SC-CA V only signs public keys, like their associated private keys, which have been generated either on a smartcard (permitted by this CPS but not currently practiced) or centrally on the CMS. The CMS controls the creation of the private key, the calculation of the public key from the private key and the construction of the CSR and the submission of CSR to SC-CA V.

Subscribers typically gain possession of their private key only after receiving their smartcard. In the special cases of online certificate renewal or online rekey, private key possession of the legitimate subscriber is ensured by the card holder's physical possession of the card along with the knowledge of the card PIN.

3.2.2 Authentication of organization identity

SC-CA V certificates can only be issued for subscribers whose affiliation with an Allianz Organizational Entity is verified through corporate directory lookup. The value of the organization (currently 'O=Allianz AG' for all certificates issued) is prescribed only by SC-CA V via the applicable certificate template. Applicant can not submit this information by subject a subsequent authentication.

3.2.3 Authentication of individual identity

Individual identity authentication is required in the events of card enrollment, card delivery and card unlock.

Only authorized persons can request card enrollment via authenticated, authorized IDM Tools. During this process, the subscriber's individual identity is verified against corporate directories.

3.2.4 Non-verified subscriber information

There is no non-verified user provided data. All certified content **may** be looked up and verified in appropriate corporate directories.

3.2.5 Validation of authority

Certificate requests (implied in smartcard requests) are not raised by subscribers themselves but by authorized personnel on their behalf. The authorized personnel was assigned with the right in IDM to create smartcard request and need to authenticate with the IDM Tools by presenting their own smartcard.

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

Routine re-key will be carried out when subscribers' encryption certificate is about to expire. The rekey-request will be scheduled on the CMS.

3.3.2 Identification and authentication

Identification for re-key is no different from identification for initial enrollment and is performed against corporate directories.

3.4 Identification and Authorization for Revocation Requests

Card and Certificate Revocation are part of the smartcard replacement process. A subscriber is authorized to initiate replacement of a damaged, lost or stolen smartcard. The subscriber **may** request replacement by reporting the damage, lost or theft immediately to their rights administrator (who will have to verify the subscriber's identity in a reliable way) or to ID-Card-Centre staff (subscriber appears in person and provides personal identification).

The replacement and revocation of the current smartcard can only be performed by authorized personnel (rights administrators, ID-Card-Centre staff), who are identified and authorized via IDM Tools.

Card and Certificate Revocation without card replacement is carried out when the subscriber's affiliation with Allianz terminates. In that case, competent HR personnel and the subscriber's line manager are authorized and obligated to inform the subscriber right's administrator about this event. She/he is obligated to revoke all valid cards of the subscriber.

4 Certificate Life-Cycle Operational Requirements

Operation of SC-CA V **may** comply with rules laid out in the Allianz Root CA CPS and Allianz Group Information Technology and Information Security Policy [AZ-ITISP]

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

The CMS is the only trusted entity that is authorized to submit a certificate request to Allianz Smartcard CA.

On the CMS side, Rights Administrators or personnel with analogous organizational role are entitled to trigger certificate requests for subscribers.

4.1.2 Enrollment process and responsibilities

Certificate requests are implicit in smartcard requests initiated by authorized persons (e.g. a subscriber's rights administrator) via IDM Tools that interface with the CMS and upon authentication are authorized to submit card requests.

The CMS will only authenticate the IDM Tool. It is the OE's responsibility to model the rights administrator role in their respective IDM Tool and assign it to the persons it selected to perform this role.

4.2 Certificate Application Processing

Certificate application processing is carried out by automated procedures and authorized ID-Card-Center staff.

4.2.1 Performing identification and authentication functions

Identification and authentication of subscriber are described in chapter 3 "Identification and Authentication"

4.2.2 Approval or rejection of certificate applications

Certificate applications are approved automatically when the verification of subscriber data against corporate directories is successful. The other way around, failure to confirm subscriber data via directory lookup results in the rejection of a certificate request without any exception whether the certificate application is filed by a rights administrator or generated automatically on the CMS as part of a renewal or re-key process.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

SC-CA V issues a certificate upon receiving an authenticated request by the CMS. Request submission by the CMS always presupposes that proper certificate application checking has been performed and the application has been approved.

The issued certificate is returned to the CMS and published to corporate directories as stipulated section 2.2 “Publication of certification information”.

4.3.2 Notification to subscriber by the CA about certificate issuance

In regard to certificate issuance, no express notification is required. SC-CA V certificates are typically delivered to subscribers on smart cards. The card delivery implies logically a certificate issuance notification.

If the smartcard is not provisioned in subscriber’s presence, she/he will either receive their card via internal mail or be notified via e-mail that a smartcard is ready for pickup at a ID-Card-Centre.

In the event of a scheduled online certificate renewal or re-key, subscribers will be informed about the impending renewal or rekey and their approval for the process to go ahead will be prompted.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

A subscriber's receipt of a card or consent to a scheduled renewal or rekey, and the subsequent use of the keys and certificates residing on the card, constitutes certificate acceptance.

Certificates and private keys are delivered on a smart card, which needs to be unlocked prior to first use. Authorized staff (Help Desk) perform unlocking after authenticating the subscriber in accordance with stipulated identification requirements.

Subscribers once they have their smartcard unlocked are obligated (by section 4.5.1 of this CPS) to verify the contents of their certificate and bring objections to the attention of their Rights Administrator. Failure to raise objections implicitly constitutes acceptance of the certificate

4.4.2 Publication of the certificate by the CA

All valid smartcard end-user certificates are published in the Allianz Corporate Directory, Corporate Active Directory and RACF (for lookup by IBM Hosts) upon creation. At the same time, the certificate’s fingerprint as SHA-256 is written to the subscriber’s Active Directory account.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

SC-CA V certificates are used to support authentication processes within Allianz OEs and to secure the exchange of electronic information both within Allianz as well as between Allianz entities and third parties.

Certificates can only be used during their lifetime as long as they are not revoked prior to expiration.

The participant’s private key **may** only be used in accordance with the key usage field extensions included in the certificate.

The following certificate usages are permitted:

- Client Authentication (1.3.6.1.5.5.7.3.2)
- Secure Email (1.3.6.1.5.5.7.3.4)
- IP security end system (1.3.6.1.5.5.7.3.5)
- IP security user (1.3.6.1.5.5.7.3.7)
- Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
- Digital Signature (80)

Subscribers **may** adequately protect their smart card and token PIN from unauthorized physical access at all times.

Subscribers **shall** notify the appropriate ID-Card-Center immediately upon loss of their card or any suspected or actual compromise of their private keys.

Subscribers agree to be bound by all terms and conditions specified within this CPS.

Subscribers **may** verify the contents of their certificate upon receipt of the smartcard and notify their Rights Administrator in case of objections.

Subscribers accept that their certificate is published to corporate directory services and thus made publicly available within Allianz corporate networks.

4.5.2 Relying party public key and certificate usage

The public key of the subscriber described by the issued certificate can only be used for applications in accordance with the key usages given in the certificate. This means end entity certificates can only be used for certificate based authentication, encryption, Smartcard Logon and VPN connection establishment.

4.6 Certificate Renewal

SC-CA V supports certificate renewal for authentication certificates.

For authentication certificates, which are about to expire, the Card Management System can automatically schedule renewal. The subscriber will be requested to prove the certificate renewal when log on to a client computer during the pending scheduled renewal. After the approval is granted, the certificate renewal will be proceed automatically through secure communications with the SCI. In this case, the existing key pair on the smartcard will be re-used. No new private key is generated. The certificate renewal process requires no interaction of authorized persons. The subscriber's data in corporate directories can be reconfirmed.

4.6.1 Circumstance for certificate renewal

Certificate Renewal is allowed for authenticated certificates, which is about to expire (i.e. as of 90 days prior to expiration). The subscriber data on the certificate can be verified against valid person's entries in corporate directories.

4.6.2 Who may request renewal

Renewal is triggered automatically via scheduled tasks on the Card Management System.

4.6.3 Processing certificate renewal requests

Certificate renewal requests are processed through secure communications between a subscriber's logon client and the Card Management System following the subscriber's approval to the renewal process.

4.6.4 Notification of new certificate issuance to subscriber

Certificate renewal occurs as part of an interactive dialogue involving the subscriber. Certificate issued immediately after the subscriber's approval to certificate renewal and is confirmed in the dialogue. There is no separate notification.

4.6.5 Conduct constituting acceptance of a renewal certificate

Subscriber who allows a scheduled renewal will have the renewal certificate automatically written to their card. They are obligated by this CPS (section 4.5.1) to review their certificate contents and report any objections to the attention of their Rights Administrator. Failure to raise objections implicitly constitutes the certificate acceptance.

4.6.6 Publication of the renewal certificate by the CA

Procedures as stipulated in section 4.4.2 of this CPS apply.

4.6.7 Notification of certificate issuance by the CA to other entities

No other entity **may** be notified about certificate issuance.

4.7 Certificate Re-key

Certificate re-key is the process by which a new (sequent) certificate is issued to replace an expired (or expiring) certificate. Certificate renewal requires the creation of a new private and public key pair.

Re-key is allowed by this CPS for encryption certificates.

In the current operation mode, SC CA does not issue encryption certificates and thus no re-key is practiced. The stipulations hereafter (sections 4.7.1 through 4.7.7) apply when the mode of operation include the issuance of encryption certificates.

4.7.1 Circumstance for certificate re-key

The circumstance for certificate re-key is the pending expiry of a subscriber's existing encryption certificate.

4.7.2 Who may request certification of a new public key

Re-key requests are generated automatically via scheduled tasks on the Card Management System when an encryption certificate is nearing expiration and the subscriber data can be verified against corporate directories.

4.7.3 Processing certificate re-keying requests

Re-key requests differ from the initial certificate requests in that they are generated automatically relying on the data quality maintained by the respective data owners (OEs).

On successful verification of subscriber data against corporate directories the new key pair will be generated centrally by the CMS who will then submit the CSR to SC CA and retrieve a new certificate. A key store including both the private key and the certificate will be downloaded onto

the card and the private key will be stored in a central encrypted database. On the smart card, the subscriber's previous encryption certificates will be retained.

4.7.4 Notification of new certificate issuance to subscriber

Certificate re-key occurs as part of an interactive dialogue involving the subscriber. Certificate issued immediately after the subscriber's approval to certificate re-key and is confirmed in the dialogue. There is no separate notification.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Subscriber who allows a scheduled re-key will have the re-key certificate automatically written to their card. They are obligated by this CPS (section 4.5.1) to review their certificate contents and report any objections to the attention of their Rights Administrator. Failure to raise objections implicitly constitutes the certificate acceptance.

4.7.6 Publication of the re-keyed certificate by the CA

Procedures as stipulated in section 4.4.2 of this CPS apply.

4.7.7 Notification of certificate issuance by the CA to other entities

No other entity **may** be notified about certificate issuance.

4.8 Certificate Modification

Certificate modification refers to the issuance of a new certificate in order to reflect changes in subscriber data (other than then the public key) that do not match to the information in the existing certificate any more.

4.8.1 Circumstance for certificate modification

Certificate modification of SC-CA's subscriber certificates is part of the smart card change process and does not differ from the process of issuing new certificates.

Certificate modification **may** be possible under the following circumstances:

- The subscriber's name no longer corresponds to the name in the certificate
- The subscriber's e-mail address no longer corresponds to the e-mail address in the certificate

4.8.2 Who may request certificate modification

Section 4.1.1 of this CPS applies, i.e. the CMS will accept any card request submitted via an authorized IDM Tool and the provided subscriber data can be verified by directory lookup. This implies that an update of subscriber information in corporate directories (pursuant to the applicable processes in the subscriber's OE) has to precede the card request.

4.8.3 Processing certificate modification requests

The processing of certificate modification requests does not differ from the processes applicable to the issuance of new cards.

4.8.4 Notification of new certificate issuance to subscriber

The stipulations made in sections 4.3.2 apply.

4.8.5 Conduct constituting acceptance of modified certificate

The stipulations made in sections 4.4.1 apply.

4.8.6 Publication of the modified certificate by the CA

Procedures as stipulated in section 4.4.2 of this CPS apply.

4.8.7 Notification of certificate issuance by the CA to other entities

No other entity **may** be notified about certificate issuance.

4.9 Certificate Revocation and Suspension

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

4.9.1 Circumstances for revocation

The following events will result in the revocation of a certificate:

- Termination of the subscriber's relationship with Allianz
  (departure or dismissal of internal staff; end of contract with external staff).
- Suspected or known compromise of private keys (exclusive control of the smartcard by the subscriber not guaranteed at all times owing to (temporary) loss, theft, etc.)
- Replacement of the subscriber's smartcard.

If one of the above circumstances occurs, the smartcard and the associated certificate(s) **may** be revoked and the certificates placed on the CRL. Revoked certificates remain on the CRL until they expire.

4.9.2 Who can request revocation

Revocation of a subscriber’s smartcard and the associated certificates can be initiated by the subscriber’s HR department, by an Allianz ID-Card-Centre, by the subscriber’s Rights Administrator and by the subscriber himself.

While Rights Administrator and ID-Card-Centers are legitimated and technically empowered to perform revocation themselves, a subscriber’s HR department and the subscriber himself will have to contact the subscriber’s Rights Administrator in order to request revocation.

In the case of card replacement, revocation of the predecessor card (of the same card profile) and its associated certificates is an automated part of the replacement process that does not need to be requested expressly.

4.9.3 Procedure for revocation request

Revocation orders can effectively be performed only by Rights Administrator or ID-Card-Centre staff using the tools and authorizations that are granted to them to fulfill their role (IDM Tool Dialogues and CMS Client respectively). They **shall** state a reason for the revocation which is logged by the CMS together with the time of revocation.

If the subscriber’s contractual relationship with Allianz is terminated, the departing employee or external employee will generally hand in their card to ID-Card-Centre staff, who will revoke the smartcard after properly identifying the subscriber (return to the card office).

The subscriber's Rights Administrator, upon receipt of a written notification about the termination by authorized Human Resources personnel or the Subscriber's line manager, **may** verify the status of the Subscriber's smart cards and revoke valid cards using the appropriate dialog in an IDM tool.

In the event of suspected or known compromise of private keys (e.g. card loss, card theft), subscribers **may** report this incident as soon as possible either to ID-Card-Centre staff or to their Rights Administrator either in person or via telephone. The Rights Administrator will order a replacement card and implicitly revoke the compromised card.

In the case of a card malfunction (physical damage), the subscriber contacts ID-Card-Centre or their Rights Administrator, who will order a replacement card and implicitly revoke the compromised card.

Rights Administrator or ID-Card-Centre staff who perform revocation at request of another person **may** always verify this person's identity and legitimacy when submitting the request.

Corporate ID-Card-Centre employees and Rights Administrator will notify subscribers about the revocation of their cards and associated certificates if the revocation was not initiated by the subscriber himself.

4.9.4 Revocation request grace period

There is no revocation request grace period.

4.9.5 Time within which CA **may** process the revocation request

Revocation requests are processed within one regular business day.

4.9.6 Revocation checking requirement for relying parties

Relying parties **shall** check the validity of a subscriber certificate and the CA certificates included in its chain of trust every time the certificate is relied for any of its legitimate usages.

SC-CA V provides OCSP Services and CRLs, each accessible via http protocol on the internet and the Allianz Intranet, to enable certificate status checking by relying parties.

4.9.7 CRL issuance frequency (if applicable)

CRLs are issued with a validity period of 4 weeks and updated at a minimum of once every 2 weeks.

4.9.8 Maximum latency for CRLs (if applicable)

CRL are published to the repository within 15 minutes after generation.

4.9.9 On-line revocation/status checking availability

Status information on certificates issued by SC-CA V is available online via OCSP service at http://rootca.allianz.com/ocsp/ and via regularly updated CRL at http://rootca.allianz.com/crls/smartcard5.crl.

4.9.10 On-line revocation checking requirements

A relying party **may** verify the validity of a certificate prior to any transaction that relies on the certificate or a digital signature created therewith. The relying party can perform this check either by consulting the latest CRL or alternatively by using the SC-CA V OCSP Responder.

4.9.11 Other forms of revocation advertisements available

There is no other revocation advertisement from SC-CA.

4.9.12 Special requirements regarding 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

SC-CA V supports certificate status verification for all certificates it has issued and that have not yet expired by providing a regularly updated Certificate Revocation List available at http://rootca.allianz.com/crls/smartcard5.crl and by providing an OCSP Responder service accessible at http://rootca.allianz.com/ocsp/.

Both verification methods are available to relying parties inside the Allianz Corporate Network and on the Internet.

4.10.1 Operational characteristics

SC-CA V uses CRL publishing and OCSP to allow relying parties checking the status of all certificate issued by SC-CA. The CRL encloses the serial numbers of all non-expired certificates that were revoked up to the creation time of the CRL was created. The OCSP responder provides up-to-date status information on every non-expired certificate at the time of the OCSP request.

4.10.2 Service availability

SC-CA's CRL and the SC-CA V OCSP are accessible and available 24x7.
Both services are under the operational responsibility of Allianz Technology PKI Support.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

In the event of the termination of a subscriber's affiliation with Allianz, his subscription to certificates issued by SC-CA V will also be terminated and the entire subscriber's cards and associated certificates **shall** be revoked.

Should SC-CA V terminate its operation prematurely, i.e. before expiry date consist of in its own CA Certificate, all subscribers, participants and relying parties will receive timely notification of the termination.

In that case, on the day of operation cessation, the serial number of the SC-CA V CA certificate **shall** be put on the Allianz Root CA revocation list, which implicitly invalidates all subscriber certificates issued by SC-CA V that have not yet expired and have not yet been revoked.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

Key escrow is not permitted.

Key backup for signing keys is not allowed.

The SC-CA's signing key is securely stored in a clustered FIPS 140-2 Level 3 compliant Hardware Security Module.

Subscribers' signing key is created and stored only on the same smartcard.

This CPS authorizes the issuance of encryption certificates to subscribers even though in its current mode of operation no encryption certificates are issued.

Should SC-CA V issue encryption certificates to subscribers, the central backup of the private keys is permitted and mandatory. The keys **shall** be created centrally on the CMS and encrypted copies thereof stored in a central key recovery database.

The key recovery database **shall** be archived pursuant to the standard processes defined for data backup services within Allianz.

The SC-CA's internal repository, which includes all certificates it has issued (and hence the public keys they include) is archived according to the standard processes defined for data backup services within Allianz.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 Facility, Management, and Operational Controls

5.1.1 Physical Security Controls

Physical security of the SC-CA V is conducted in accordance with the Allianz Guideline for Physical Security [AZ-GPS]

5.1.2 Site location and construction

SC-CAs production environment consists of components set up in different, sufficiently secured locations.

5.1.3 Physical access

Identification for access to Allianz buildings is via access system badges or smartcards with implemented support for physical access control.

Access and exit to Allianz's buildings is monitored and recorded by the access system. Visitors **may** sign a visitor document with name, company, department, date and time and are handed a badge.

Access to the server room is separately protected and access is recorded.

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

5.1.4 Power and air conditioning

All equipment in the server room is protected against power fluctuation and loss of power by uninterruptible Power Supplies (UPS).

The server room temperature and humidity are controlled by air conditioning. In case of excessive values, an alarm will be initiated.

5.1.5 Water exposures

Conditions meet the standards identified in the Allianz Group Information Technology and Information Security Policy [AZ-ITISP].

5.1.6 Fire prevention and protection

An automatic fire detection system has been installed in the server room. There is a fire extinguisher in the server room.

5.1.7 Media storage

Media is stored in a fire-rated safe located in a fire zone different from the server room zone. Access to media is limited to authorized personnel.

5.1.8 Waste disposal

Waste disposal is handled in compliance with Allianz Group Information Technology and Information Security Policy [AZ-ITISP].

Off-site backup

Conditions meet the standards identified in Allianz Group Information Technology and Information Security Policy [AZ-ITISP].

5.2 Procedural Controls

The Allianz SCI service is being operated in accordance with an approved Allianz policy, practices, and procedures regarding safe and trustworthy system operation.

5.2.1 Trusted roles

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 SC-CA V 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

As laid out in section 3 of this CPS, all non-automated RA functionality such as initial subscriber identification, card request issuance etc. is performed under the responsibility of a subscriber's OE. The OE in accordance with Allianz Group Information Technology and Information Security Policy [AZ-ITISP] defines provisions governing these processes. So are the trusted roles involved, which are thus not stipulated by this CPS.

5.2.1.1 SCI Administrator

SCI Administrators are trained technical staff in charge of maintaining and operating the Smartcard Infrastructure. They are not involved in any of the RA or Card Live Cycle Operations unless as part of test scenarios, centrally managed migration scenarios or of last level support solicited by incumbents of any of the other authorized roles via the official Incident Management Process.

5.2.2 Number of persons required per task

No stipulation.

5.2.3 Identification and authentication for each role

SC-CA V systems and processes use the corporate access control infrastructure based on smartcards, which provides strong authentication and role based access control. Granting and withdrawal of SC-CA V administrative roles require compliance with user access management

standard as laid out in Allianz Group Information Technology and Information Security Policy [AZ-ITISP].

5.3 Personnel Controls

The Allianz SC-CA V service is being operated in accordance with an approved Allianz security policy, functional rules, practices and procedures regarding safe and trustworthy system operation.

5.3.1 Qualifications, experience and clearance requirements

Staff selected for trusted roles **may** pass a security screening procedure appropriate to the designated "Position of Trust".

The same applies to external staff but this has to be assured by contractual arrangements.

5.3.2 Background check procedures

Background checks are conducted on all persons selected to take up a trusted role in accordance with the designated security screening procedure, prior to the commencement of their duties.

5.3.3 Training requirements

Operational personnel **may** possess sufficient skills to perform their duties in a responsible manner. All SC-CA V staff **shall** be trained in:

(1) Basic PKI concepts
(2) The use and operation of certification authority software and hardware
(3) Documented procedures
(4) Computer security awareness and procedures
(5) The meaning and effect of this CPS and relevant CPs

5.3.4 Retraining frequency and requirements

Retraining and appropriate quality controls is performed at least once a year as the need arises owing to personnel fluctuation and changes in technology and procedures.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Unauthorized actions by SC-CA V System staff are submitted to appropriate authorities including, but not limited to, the Corporate Security Officer.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

All required information is located within the “Smartcard CA Online Service Handbook”.

This document is maintained by the operations department in charge of the SCI and is available online at the official Allianz Online Repository for Service Documentation.

5.4 Audit Logging Procedures

SC-CA V maintains adequate records and archives of information pertaining to the operation of the PKI, specifically to the generation, operational use, expiry and archiving of certificates.

Audit events are forwarded to a central security logging facility.

5.4.1 Types of events recorded

The information recorded (audit log) include the following:

- Time and date the event occurred
- Person or entity initiating the event
- Reason for event
- Outcome of the event (successful/unsuccessful)

The following events are recorded by the SC-CA

- Issuance of certificates
- Revocation of certificates

5.4.2 Frequency of Processing Log

Log processing will be performed on demand by authorized roles (Information Security Officers, Internal Audit).

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 accessible for authorized personnel. Only CA Administrators are entitled to access the logs as part of their CA maintenance work. Audit logs **may** not be modified and **shall** be signed in order to facilitate the detection of audit log manipulation. It is acceptable for the system to over-write audit logs after they have been rolled-over and archived.

5.4.5 Audit log backup procedures

Audit logs are included in daily system backup procedures according to standard operations procedures.

5.4.6 Audit collection system (internal vs. external)

The SC-CA V audit collection is generated at the application and operating system level and is invoked at system start-up and only ceases at system shutdown.

5.4.7 Notification to event-causing subject

This CPS imposes no requirement to provide notice when an event was audited to the individual, entity or application that caused the event.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records Archival

All relevant data is archived according to Allianz System Operation Standard (Allianz Group Information Technology and Information Security Policy [AZ-ITISP]).

5.5.1 Types of records archived

The following data is recorded for archive during CA and SCI operation:

- SC-CA V Internal LDAP
- SC-CA V Logs (including audit log)

5.5.2 Retention period for archive

Standard controls according to Allianz policy apply to the retention of archiving data, which currently means 10 years at minimum.

5.5.3 Protection of archive

Standard controls according to Allianz policy apply to the protection of the archived data.

The backup files are stored in a secure place (fire-proof safe) in another fire zone. The access to the backups is protected by passwords. The security relevant data is protected by encryption in the database and in the backups.

5.5.4 Archive backup procedures

The backup files are stored in a secure place (fire-proof safe) in another fire zone. The access to the backups is protected by passwords. The security relevant data is protected by means of encryption in the database as well as in the backups.

5.5.5 Archive collection system (internal or external)

No stipulation.

5.5.6 Procedures to obtain and verify archive information

No stipulation.

5.6 Key Changeover

The validity period of the SC-CA V certificate is 15 years. Upon expiration of the certificate, a new key pair and certificate will be generated.

5.7 Compromise and Disaster Recovery

SC-CA V and every CA under RCA:

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 SC-CA V 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.

The above documentation has to be made available on request to authorized persons tasked with conducting a security, compliance or CPS practices audit.

In addition, appropriate training **may** be provided to all relevant staff involved in contingency and disaster recovery procedures.

5.7.1 Incident and compromise handling procedures

In general, incidents within the SC-CA V are handled according to the Allianz Information Security Practice for Incident Handling [AZ-ISINC].

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

The general disaster recovery plan of Allianz applies.

5.7.3 Entity private key compromise procedures

In case of compromise of the SC-CA V private key, the following measures **may** be taken:

- Inform Root CA Council
- Revoke SC-CA V certificate
- Inform subscribers via intranet and e-mail
- Generate new SC-CA V key pair and certificate
- Publish new certificate
- Issue new cards to subscribers

5.7.4 Business continuity capabilities after a disaster

The purpose of this 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 systems operations will not cause a direct and immediate operational impact within the PKI due to designed resilience. This means that the plan's primary goal is to reinstate the SC-CA V in order to make accessible the logical records kept within the software. Therefore the SC-CA V 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 backup site
   - trained backup staff
5. Developed recovery actions and timeframes
6. Prioritised recovery actions from most significant to least significant
7. Maintained a record of the hardware and software configuration baseline
8. Maintained records of the necessary equipment and procedures required to recover from an unexpected event such as a hardware failure, including the intended maximum period that the system is down.

5.8 CA or RA Termination

Should it become necessary to terminate the SC-CA V service before its expiration, the impact of the termination is to be minimized as much as possible in light of the prevailing circumstances. The SC-CA **shall** at least provide as much prior notice as is practicable and reasonable to participants and relying parties.

SC-CA's last action will be to revoke all valid certificates issued by it and publish a final CRL. The SC-CA V signing certificate will be revoked by Allianz Root CA III. 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 of Allianz SC-CA V.

6 Technical Security Controls

SC-CA V applies technical security controls complying with all requirements as laid out by Allianz Group Information Technology and Information Security Policy [AZ-ITISP]

6.1 Key Pair Generation and Installation

Technical security controls are carried out on the basis of documented processes and stipulations following the status quo of technology. These security controls are duly fulfilled by Allianz SC-CA V in order to meet the operation requirements explained in chapter **Error! Reference source not found.**. The cryptographic procedures and records **may** correspond to the status quo of security measures of cryptographic procedures and to the respectively valid legal stipulations.

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.

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

Key generation in software and hardware are equally supported by SC-CA V, but it **may** be necessary to apply different security measures related to the environment.

6.1.1 Key pair generation

A properly initialized random number generator is used to generate the random data required for key generation.

6.1.1.1 CA Key Pair Generation

In the case of CA keys, the key generation **may** be undertaken under the supervision of either a Senior Manager of the Allianz OE which retains the ownership and administrative control of Allianz RCA or a person specifically authorized by Senior Management to oversight this task.

It is permitted to generate the CA key as a software token instead of creating it inside a HSM.

In that case, the token **may** subsequently be transferred into an HSM for operational use.

The private key **may** not remain on any system other than the HSM and **may** be stored in encrypted form on storage media that **may** be securely kept in a safe. Access to the safe **may** be restricted to trusted SCI security personnel. The symmetric encryption key, which is used to encrypt the CA key, **may** be split and possession of the key components **may** be distributed among at least three trusted persons as defined in 5.2.1 Trusted roles .

6.1.1.2 Subscriber Key Pair Generation

For end-entity keys, key generation on the smartcard itself is the preferred and recommended method that is practiced unless a specific compliance requirement (e.g. central storage of encryption certificates) mandates a centralized key generation in the form of soft tokens. Whatever key generation method chosen **may** comply with the provisions of this CPS.

6.1.2 Private Key delivery to subscriber

Private keys **may** be delivered to subscriber on personalized smartcards only. If the private key was generated outside the smartcard, it **may** be transferred to smartcard via an adequately encrypted transport within the SCI.

6.1.3 Public key delivery to certificate issuer

Public keys are transferred to the CMS and submitted by the CMS to SC-CA V for signing by the via adequately encrypted communication channels.

6.1.4 CA public key delivery to relying parties

The SC-CA V certificate is transferred via individual communication and can be verified using the RCA certificate published at http://rootca.allianz.com.

6.1.5 Key sizes

The SC-CA V requires the minimum of 2048 bit RSA keys for certification. Exceptions are possible in well-founded circumstances.

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)

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Private key Protection

6.2.1.1 CA Private Key

The SC-CA V private key is stored securely in a HSM. An encrypted backup copy of it is kept in a safe. Access to the safe is restricted to CA personnel with trusted roles. The encryption key is split and distributed among at least three key custodian.

6.2.1.2 SCI Personnel Private Keys

The private keys of the SCI personnel are stored securely on a smartcards that provide physical protection. Logical protection is provided by the necessity to enter a PIN in order to use the keys on the smartcard.

6.2.1.3 Subscriber Private Keys

The subscriber private keys are stored securely on a smartcard which provides physical protection. Logical protection is by a PIN.

If the SC-CA V issues encryption certificates to subscribers, encrypted copies of the respective private keys will be stored in a central key recovery database.

6.2.1.4 Key Recovery

Key recovery will be used for all those private keys generated by the SCI that are associated to encryption certificates. The key recovery database is encrypted. Key recovery of historic encryption keys will be performed when a new smartcard for an existing subscriber is issued.

6.2.2 Cryptographic module standards and controls

Not applicable.

6.2.3 Private Key (n out of m) multi-person control

No stipulation.

6.2.4 Private Key escrow

Private key escrow is not supported.

6.2.5 Private key backup

Key recovery will be used for all private keys generated by the SCI. The key recovery database is encrypted.

6.2.6 Private key archival

The key recovery database and the certificates will be archived due to the processes defined for Allianz backup service.

6.2.7 Private key transfer into or from a cryptographic module

No stipulation.

6.2.8 Private key storage on cryptographic module

No stipulation.

6.2.9 Method of activating private key

No stipulation.

6.2.10 Method of deactivating private key

No stipulation.

6.2.11 Method of destroying private key

No stipulation.

6.2.12 Cryptographic Module Rating

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

SC-CA V archives all certifies that include the public keys..

Expired certificates (and CRLs if used) are archived because digitally signed or encrypted documents often outlast the validity period of the certificate, which was used to sign or encrypt the document. Expired certificate **may** still be accessible so that it can be used to prove the authenticity of a document. Archived certificates can only be accessed under legitimate circumstances, such as at the request of the participant or a duly drafted subpoena or warrant will be presented.

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
- Securely destroyed at the end of the archive period.

6.3.2 Usage Periods for the Public and Private Keys

The usage periods for public and private keys are as follows:

- CA key and certificate: 15 years
- SCI personnel keys and certificates: up to 5 years
- Subscriber keys and certificates: up to 5 years (internal staff), 6 months to 5 years (external staff)

6.4 Activation Data

The private key on smartcard is protected by a PIN and can be activated by entering the PIN.

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

The following computer security controls have been implemented and are enforced by the SCI servers' operating systems and the SCI applications:

- Access control to SCI services
- Use of tokens to store private keys
- Encrypted Key Recovery database
- Encrypted communication between all entities of the SCI
- Recovery mechanisms for keys and the SCI applications.

The SCI applications are installed on clustered (CMS) or load-balanced (SC-CA V) Linux systems.

The operating systems are hardened according to Allianz standard guidelines for server systems.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The SCI application was developed and tested in all conscience by a professional security software developing firm following a proven design methodology.

A manufacturer's declaration on the security of the system and its configuration was presented to Allianz.

6.6.2 Security Management Controls

Allianz PKI Team establishes a change management system to control, monitor the configurations of the systems and prevent unauthorized modification.

6.6.3 Life Cycle Security Controls

Any configuration modifications or upgrades of the SCI (including SC-CA) **may** be tested, documented and approved in advance.

A contingency plan is in force, which includes adequate redundancy, back-up and recovery procedures.

6.7 Network Security Controls

The SCI is an online system. Access to the SCI servers is safeguarded by firewalls. Only the CMS is accessible from within Allianz internal networks. Only the CMS and SCI Administrators can access SC-CA.

All communications involving SCI clients are encrypted and authenticated.

The Allianz Internal Network is protected by firewalls. No direct connection to the Internet is permitted. Only Allianz Organization Units are connected to this network, with all traffic controlled by firewalls.

6.8 Time stamping

Not applicable.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

For detailed information, refer to 10. Smartcard CA V Certificate Profile.

7.1.1 Version numbers

SC-CA V issues X.509 version 3 certificates in accordance with ITU-T Rec. X.509 (1997).

This standard is identical to ISO/IEC 9594-8 (1997).

7.1.2 Certificate Extensions

SC-CA V subscriber certificates **may** include extensions as specified in sections 7.1.2.1 through 7.1.2.6.

7.1.2.1 Authority Key Identifier

This extension **shall** be included marked non-critical and be set to the value corresponding to the Subject Key Identifier of SC-CA V, i.e. the 256-bit SHA256 hash of the SC-CA V public key.

7.1.2.2 KeyUsage

This extension **may** be included and marked critical following the stipulations of the Common PKI Profile (see Common PKI Version 2.0 Part 1).

It is configured with bits set or cleared as specified in the table below:

0	digitalSignature	**true**
1	nonRepudiation	false
2	keyEncipherment	false
3	dataEncipherment	false
4	keyAgreement	false
5	keyCertSign	false
6	CRLSign	false
7	encipherOnly	false
8	decipherOnly	false

7.1.2.3 Extended Key Usage

This extension **may** be present marked non-critical and including the following OIDs:

1.3.6.1.5.5.7.3.2	Client Authentication

1.3.6.1.5.5.7.3.4	Email Protection
1.3.6.1.5.5.7.3.5	IPSec End System
1.3.6.1.5.5.7.3.7	IPSec User
1.3.6.1.4.1.311.20.2.2	Microsoft Smart Card Logon

7.1.2.4 CRL Distribution Points

This extension **may** be included, marked non-critical and set to the value:

```
Number of Points: 1
Point 0
   Distribution Point: [URIName: http://rootca.allianz.com/scca/azsccav.crl]
```

7.1.2.5 Netscape Certificate Type

This extension **shall** be included marked non-critical and set to the value:

```
Certificate Usage:
          SSL Client
          Secure Email
```

7.1.2.6 Subject Alternative Name

This extension **may** be included marked non-critical and include as the following 2 values:

```
OtherName: (UTF8String)1.3.6.1.4.1.311.20.2.3,<UPN>
RFC822Name: <E-Mail Address>
```

with `<UPN>` to be replaced by a subscriber's User Principal Name as a ASN1 encoded UTF8 string and `<E-Mail Address>` by the subscriber's e-mail address in internet format.

7.1.3 Algorithm Object Identifiers (OIDs)

No stipulation.

7.1.4 Name forms

Certificates issued by the SC-CA V System **may** enclose the full X.500 distinguished names (DN) of both the certificate issuer and the certificate subject. It is mandatory that the subject-DN be composed of the common name (CN), e-mail in internet format, organization and country (CN, E, O and C) attributes.

All certificates **may** have non-null Issuer DN and/or a Subject DN.

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

7.1.5 Name constraints

No stipulation

7.1.6 Certificate policy object identifier

No stipulation.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL Profile

SC-CA V issues X.509 version 2 CRLs in accordance with ITU-T Rec. X.509 (1997).

CRLs are published by SC-CA V to the Allianz RCA Website.

They include the basic fields and contents specified in the table below:

Version	V2 for Version 2 as stipulated in Section 7.2.1
Issuer	DN of Issuer i.e. DN of SC-CA
Effective date	Date from which CRL is valid
Next update	Date of next scheduled CRL update
Signature Algorithm	Sha256RSA
X509v3 CRL Number	number of the revocation list that is incremented with each update
Revoked Certificates	List including for each revoked certificate the serial number and the revocation date and a revocation reason

7.2.1 Version number(s)

SC-CA V issues X.509 Version 2 CRLs compliant to [RFC-5280]

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP Profile

The SC-CA V supports Online Certificate Status Protocol (OCSP) to allow reliant parties to obtain timely status information on any certificate issued by SC-CA. The formats for OCSP request and response **may** be compliant with RFC 2560. SC-CA V does not use a nonce in the response to a request that contains a nonce. Instead, clients should use the local clock to check for response freshness.

7.3.1 Version Number(s)

Version 1 of the OCSP specification in [RFC-2560]

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audit and Other Assessment

SC-CA V operation is subject to RCA and corporate technical and organizational audits.

8.1 Frequency or circumstances of assessment

The audit by Allianz RCA is performed at least annually.

8.2 Identity/qualifications of assessor

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

The initial compliance audit by RCA showed that SC-CA V 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 SC-CA V security infrastructure can be guaranteed continuously in all cases.

8.6 Communication of results

Results of audits and reviews are communicated within 30 days to Allianz RCA. Allianz RCA will also be informed about interim reviews and follow up conducted on all significant audit / review issues.

9 Other Business and Legal Matters

No stipulation.

9.1 Fees

No stipulation.

9.2 Financial Responsibility

No stipulation.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

All data owned by SC-CA V is classified and marked with the data classification level in compliance with Allianz Information Security Framework.

Confidential Information on the CIS is stored encrypted and is decrypted by the CIS Application on the CIS Environment itself.

“Confidential Information” also includes the results of compliance audits provided by SC-CA, cf. section 8.

9.3.2 Types of Information in particular considered confidential

The following types of information are classified as confidential:

- Personal information is treated according to the rules of Corporate Privacy
- Key information and passwords stored in the CIS TODO
- Personal Identification Numbers (PINs)

9.3.3 Information not within the scope of confidential information

Certificate Revocation Information (CRL-Files) are classified as public and intended for publication via Allianz websites.

9.3.4 Responsibility to protect confidential information

9.4 Privacy of Personal Information

9.4.1 Privacy plan

Use of personal information has been reviewed and approved by the respective department of Allianz.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual Property Rights

SC-CA V warrants that it is in possession of, or holds licenses for the use of hardware and software required in support of this CPS.

9.5.1 Property in Certificates

All intellectual property rights, including all copyright, in all certificates belong to and will remain the property of SC-CA.

9.5.2 Certificate

SC-CA V reserves the right at any time to revoke any certificate in accordance with the procedures and policies set out in this CPS.

9.5.3 Distinguished Names

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

9.5.4 Copyright

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

9.6 Representations and Warranties

9.6.1 CA representations and warranties

SC-CA V **shall** not be responsible for any breach of warranty, delay, or failure in performance that results from events beyond its control, such as acts of God, acts of war, power outages, fire, earthquakes, and other disasters.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

SC-CA V makes every effort to provide a secure and reliable PKI service to its subscribers. However, SC-CA V assumes no liability related to the SC-CA V PKI service.

9.8.1 Safeguards

Allianz SC-CA V utilizes 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 authorized personnel;
- Prohibit access to those resources by unauthorized individuals;
- Prevent system failures (i.e., other than as a result of abuse).

These measures include but are not limited to:

- Testing of the Allianz RCA Disaster Recovery Plans;
- Performing regular system data backups;
- Performing regular backups of the current operating software and certain software configuration files;
- Storing all backups in secure local and offsite storage;
- Maintaining secure offsite storage of other material needed for disaster recovery;
- Periodical testing of local and offsite recovery to ensure that the information is retrievable in the event of a failure;
- Periodical reviewing its Disaster Recovery Plan, including the aspects identification, analysis, evaluation and prioritization of risks.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term SC-CA V

The SC-CA V operational period is currently not limited.

9.10.2 Termination

9.10.2.1 Termination by Participant

Not applicable.

9.10.2.2 Termination by Allianz RCA

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

1. Allianz RCA reasonably determines that the respective organization failed to disclose or willfully misrepresented information in its application to become a participating organization or in subsequent filings, which in the reasonable judgment 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 **shall** provide the participating organization at least thirty 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.

9.10.3 Effect of termination and survival

After termination, SC-CA V revokes all certificates issued to the corresponding participating organization, e.g. the subscriber's certificates.

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

9.11 Individual Notices and Communications with Participants

9.12 Amendments

If a new CPS is approved, signed and distributed by Allianz PKI Team, all earlier versions of the CPS for the SC-CA V are superseded.

9.12.1 Notification mechanism and period

Changes made by SC-CA V are announced to Allianz Root RCA.

9.12.2 Circumstances under which OID **may** be changed

No stipulation.

9.13 Dispute Resolution Procedures

No stipulation.

9.14 Governing Law

The enforceability, construction, interpretation and validity of this CPS and all agreements related to SC-CA V **shall** be governed by German law.

9.15 Compliance with Applicable Law

Cf. sections 9.4 and 9.5.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

In the event of a conflict between the provisions of this CPS and RCA CPS, RCA provisions **shall** take precedence.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

In the event that these operating rules are translated into a language other than English, the English version of this CPS SC-CA V **shall** govern.

9.16.5 Force Majeure

SC-CA V maintains contingency plans in force, including adequate backup and recovery procedures, to ensure SC-CA V can continue to meet its obligations under the Operating rules without material interruption in the event of the failure or shut down of the SC-CA's primary computer facilities or other operating facilities.

9.16.6 Other Provisions

No stipulation.

10. Smartcard CA V Certificate Profile

This certificate is a Root CA signed certificate, which is used to sign all Smartcard Certificates.

Field	Content	Critical*
1. X.509v1 Field		
1.1. Version	v3	
1.2. Serial Number	0a	
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	“11:13:18 29 April 2015”	
1.5.2. Not After	“11:13:18 25 April 2030”	
1.6. Subject		
1.6.1. Country (C)	DE	
1.6.2. Organization (O)	“Allianz”	
1.6.3. Common Name (CN)	“Allianz Smartcard CA V”	
1.7. Subject Public Key Info	30 82 01 0a 02 82 01 01 00 ba 0e d5 9d b3 e3 28 50 2f b2 95 7c 3e 6d 95 3a 06 ce 3e e4 af 6e 18 06 d5 36 04 29 cd c9 7a 2a 01 80 3b b8 aa dd 0b 54 2a 51 c1 58 8c 03 4d 87 1d 9d c3 a7 26 b6 e3 9d af 10 f7 85 f1 9b 18 b3 50 69 fa 11 fc 48 53 6c 9c 8f c4 2d f9 95 0d 20 28 dd a2 8b d5 8c 61 a6 e7 61 b7 4b c6 b2 d7 58 e6 67 fc 8d 6b ab 53 83 8e ae ca 9b a3 1b 3e 05 94 ff 9a 0e 0e 53 fe 34 51 c2 1b 72 a8 4c 52 91 47 51 6d 3d 3f a1 be 59 29 09 8c b0 3b b3 9a 55 93 47 39 3a ec b7 d2 c7 20 19 af d0 12 99 0b 44 56 a6 a0 24 f3 07 55 81 71 6b 96 e6 d9 a4 9e 33 a7 8a 8d 76 c3 52 d7 fa f3 91 46 1a 56 d2 01 f1 8f 0e 24 05 51 f9 4a 3b da 4d 0f ba d4 61 47 ac 94 fd 44 2e dc 0e 15 b5 50 03 1c 1f 5a 17 93 e5 bc 9a 78 74 d7 5d d2 cf a9 29 40 4c bf e8 c6 70 11 6d a2 58 57 f6 6e 9f 7f c5 9c d4 35 5d 7b bf 02 03 01 00 01	
2. Key	RSA 2048bit	
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	

Field	Content	Critical*
3.2. Subject Key Identifier	9d 0c 81 9c b8 af f2 87 e3 75 3f c6 7a c2 5e 49 71 35 c7 48	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	1.3.6.1.4.1.7159.30.34	
3.4.2. Policy Qualifier ID	1.3.6.1.5.5.7.2.2	
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	
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	None (empty for maximum)	
3.7. Netscape Extensions		n
3.7.1. CertType	SslCA, smime-CA, Codesign CA	
3.8. CRL Distribution Point		n
3.8.1. URL	http://rootca.allianz.com/crl/rootca3.crl	
Fingerprint	99 b6 6e 23 a6 a5 cd 4f 16 6f 4c f3 9c 4e 3d 69 55 da c2 16	

*not used for attributes, only extensions

Appendix

A. 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	An entity that is responsible for one or more of the following functions: the

(RA)	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

B. Abbreviations

ADS	Active Directory Service
ASD	Allianz Service Desk
CA	Certification Authority
CMLC	Certificate Management Life Cycle
CMS	Card Management System
CN	Common Name
CPS	Certification Practice Statement
CRL	Certification Revocation List
CSP	Cryptographic Service Provider
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name System
FIPS	Federal Information Processing Standard
GISF	Group Information Security Framework
GSS-API	Generic Security Services – Application Programming Interface
HSM	Hardware Security Module
ISIS-MTT	Interoperability Standard (ISIS – Mail Trust)
ISO	Information Security Officer
IDM	Identity Management
IDM Tool	Identity (and Access) Management Tool, in the context of this CPS any such Tool authorized to interface with the CMS
IP	Internet Protocol
ITSEC	Information Technology Security Evaluation Criteria
ITU-T	International Telecommunications Union - Telephony
KEK	Key Encryption Key
LA	Local Assistant
LDAP	Lightweight Directory Access Protocol
Rights Administrator	Organizational Role tasked with Identity and Access Management for employees and external staff
OCSP	Online Certificate Status Protocol
OID	Object Identifier

OU	Organizational Unit
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
PSE	Personal Secure Environment
PW	Password
RA	Registration Authority
RCA	Root CA as in Allianz Root CA
RFC	Request for Comment
SC	Smartcard with Crypto processor
SC-CA	Smartcard CA
SCEP	Simple Certificate Enrollment Protocol
SCI	Smartcard Infrastructure
SSO	Single Sign-on
SSO-card	Single Sign-on card (term used for smartcard)
TCSEC	Trusted Computer System Evaluation Criteria
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
VPN	Virtual Private Network

C. 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]	Allianz 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-ISINC]	Allianz Information Security Practice #09 IS Incident Handling Version 1.0 Effective: 01.09.2021
[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)
[AZ-APS]	Allianz Privacy Standard version 4.0 Effective: 01.01.2022
[AZ-RCA]	http://rootca.allianz.com/de/rootca3_cp.htm Allianz Root CA III CPS: http://rootca.allianz.com/download/Allianz_Root_CA_III_CPS.pdf
[BSI TR-02102]	BSI - BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (bund.de)
[EN319411]	Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Trust Service Providers issuing certificates Part 1: General requirements ETSI EN 319 411-1 V1.3.0 (2021-02)
[ITU-T]	Rec. X.500, International Telecommunications Union, Geneva, 1997
[ISIS/MTT]	Teletrust: Common industrial Signature Interoperability Specifications. ISIS Mail Trust, Specifications for interoperable PKI applications July 2002
[OHBID]	Allianz Organisationshandbuch interne Dienste
[PDOKSP]	Allianz Projektdokumentation „Prozessbeschreibung Mitarbeiterausweis mit SSO-Funktion“. Version 0.86
[RFC-822]	STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES, David H. Crocker, August 13, 1982 https://www.ietf.org/rfc/rfc822.txt
[RFC-2119]	Key Words for use in RFCs to Indicate Requirement Level, IETF (Bradner), March 1997, http://www.ietf.org/rfc/rfc2119.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-2986]	PKCS #10: Certification Request Syntax Specification , IETF (Nystrom, Kaliski, November 2000, https://tools.ietf.org/html/rfc2986
[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-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-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
[X.500]	X.500 Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services
[X.501]	Information technology - Open Systems Interconnection - The Directory: Models ITU-T Recommendation X.501 was revised by ITU-T Study Group 7 (2001-2004) and approved on 2 February 2001. An identical text is also published as ISO/IEC 9594-2.)
[X.509]	ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology - Open Systems Interconnection: The Directory: Authentication Framework,"