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

Information Owner: A-IT02WPL02 SC-CA
Version 1.4 / 17.07.2013
Document-ID: AZ-SC-CA CPS
Classification: public

Change Log

Version	Description	Date	Author
0.9	Initial Draft	20.10.2006	Actisis GmbH
0.91	Review AGIS	26.10.2006	AG2IAM03, André Witwer
0.92	Modification Organization	27.10.2006	AG2IAM03, André Witwer
0.93	Update according to comments by S. Günther	10.12.2007	AG2IAM04, David Kaluza
1.1	Review	15.12.2010	AG6DCI07, André Witwer
1.2	Review	27.12.2011	A-IT05NCV04, Andre Witwer
1.3	Classification and Owner of this document changed	17.02.2012	A-IT05CCN03, Andre Witwer
1.4	Adaptations reflecting changes in card management, certificate profiles and introduction of OCSP service	17.07.2013	A-IT02WPL02, Michael May

Content

1 Introduction

1.1 Overview

Allianz has established a smartcard infrastructure (SCI), that by providing authentication tokens to subscribers supports authentication services for a variety of access scenarios such as SingleSignOn Logon to Allianz Windows Domains or Remote Access to the Allianz Corporate Network or Logon to Intranet Applications.

As central architectural components it comprises a Card Management System (CMS) and the "Allianz Smartcard CA" (AZ-CA) certification authority which is part of the Allianz Group's PKI landscape and chains up to Allianz Group Root CA II (Allianz RCA II). (The RCA II Certification Practice Statement is published under http://rootca.allianz.com/).

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 Group adopts in its approach to Certification Authority (CA) operations regarding SC-CA.

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 service is intended for business use. The subscriber certificates will be issued to Allianz employees, Allianz field agents and employees from other Allianz Group 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 must employ for issuing certificates to eligible subscribers. It stipulates legitimate certificate use in terms of who may use SC-CA certificates and in terms of the specific purposes that SC-CA certificates may be used for.

This CPS assumes that the reader is generally familiar with PKI. Allianz Group top-level security policies do apply and are described in Allianz Group 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 02.08.2006 on, this policy is binding for SC-CA, all of its subscribers and their relying parties.

1.2 Document Name and Identification

The title of this certification practice statement is:
Certification Practice Statement for Allianz Group Smartcard Certification Authority.

1.3 PKI Participants

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

1.3.1 Certification Authorities

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

The SC-CA 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.

1.3.2 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 Group internal CA, it is permitted for SC-CA to rely on internal corporate directories for the purpose of subscriber identity verification. A subscribers' organizational entity (OE) is responsible for delivering validated subscriber data to corporate directories and keeping this data up-to-date. The initial subscriber identification required prior to data delivery has to be carried out by the OE pursuant to the provisions applicable for this process in the OE. It is not incumbent on SC-CA who is legitimated to rely on directory data as is.

The SC-CA RA process is by default initiated through a card request for a specific subscriber. The request has to be made 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 reception security staff.

In order to issue card requests authorized persons are required to authenticate with and use Identity Management (IDM) Tools. The IDM Tools in turn authenticate and communicate with the CMS via SSL secured channels. The CMS will always accept a card request for a subscriber from an authorized IDM Tool if relevant items of subscriber data can be verified electronically against corporate directories. The RA process concludes with the approved card request registered 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)

1.3.3 Subscribers

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

1.3.4 Relying parties

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

1.3.5 Other participants

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

Certificates issued by the SC-CA 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 restricted to the x509 standard and Key Usages specified in the SC-CA certificates.

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

- Digital Signature
- Key Encipherment
- Data Encipherment

(See section 4.5.1 for a detailed description in terms of x509 key usage OIDs.)

1.4.2 Prohibited certificate usage

Certificates issued by SC-CA must only be used for the purposes listed above (Appropriate Certificate Usage). Other usages must be approved in advance by written permission of SC-CA administration.

1.5 Policy Administration

1.5.1 Organization administering the document

This CPS is administered by and published by:

Allianz Managed Operations & Services SE

A-IT02WPL02 – IAM, PKI & Workplace Projects ,

Fritz-Schäffer-Str. 9 D-8137 München, Germany

1.5.2 Contact person

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

Allianz Managed Operations & Services SE

A-IT02WPL02 – IAM, PKI & Workplace Projects ,

Fritz-Schäffer-Str. 9 D-8137 München, Germany

E-Mail: rootca@allianz.com

1.5.3 Person determining CPS suitability for the policy

The Allianz Group RCA Approval Council, referred to as PAC hereafter, shall govern the enforceability, construction, interpretation, and validity of this CPS.

1.5.4 CPS approval procedures

Allianz Group RCA Approval Council determines the suitability of this CPS and its compliance with other Allianz Group policies.

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

Documentation of SC-CA in particular includes this Certification Practice Statement and a compliance statement in regard to Allianz Group Security Policy [AZ-SP].

1.6 Definitions and Acronyms

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

2 Publication and Repository Responsibilities

Information relating to SC-CA policies, the SC-CA and other Allianz Group RCA participants, is available at the Allianz Group RCA Internet Site: http://rootca.allianz.com.

The SC-CA CPS is publicly made available at the Allianz Group RCA Internet Site: http://rootca.allianz.com

2.1 Repositories

SC-CA uses internal directory services as repositories for certificates and certificate information.

The repositories used to make certificate information available to relying parties include Allianz Group Global Directory, Corporate Active Directory and RACF (for reference by IBM Hosts). (see section 2.2).

Certificate status information is made available both in the form of regularly updated Certificate Revocation Lists at the Allianz RCA Internet Site http://rootca.allianz.com and by a an OCSP services accessible at http://ocsp.allianz.com.

All above mentioned repositories and services are operated by *Allianz Managed Operations & Services SE* for Allianz Group.

2.2 Publication of certification information

SC-CA publishes all issued authentication certificates to the Allianz Group Global Directory for reference by relying parties in order to support authentication services.

It publishes all authentication certificates to RACF for reference by relying IBM Hosts.

It publishes the SHA1 fingerprint of each authentication certificate issued to the subscriber's Active Directory Account in order to support SingleSignOn functionality.

In case SC-CA issues encryption certificates in the future (not practiced in the current mode of operation) such certificates will be published to Allianz Group Global Directory for reference by relying mail clients.

The SC-CA Certificate Revocation List (CRL) is published periodically to the RCA Internet Site. (Certificate Revocation is treated in detail is section 4.9 of this CPS)

New policies added or amendments applied to the Group Information Security Framework are published at the appropriate intranet location.

This CPS is published on the Allianz RCA Internet website at http://rootca.allianz.com.

2.3 Time or frequency of publication

Changes to Group Policies or this CPS are published as and when they are approved.

End-Entity Certificates and Certificate fingerprints are published at the moment of certificate issuance.

The SC-CA CRL is updated at an interval of 14 days. If necessary the CRL can be published manually by support staff. The validity of the CRL is 1 month.

Certificate status information provided via OCSP Services is always up-to-date as the SC-CA's internal data repository is consulted directly for current information at the moment of an OCSP request.

2.4 Access controls on repositories

Any repository populated with data (certificates, certificate status, certificate revocation lists etc.) from SC-CA are subject to strict access control as stipulated by the Allianz Group IT-Security Policy [AZ-SP].

Equally any SC-CA related documentation as this CPS, Policy Documentation within GISF and similar relevant documents can be modified published or substituted by authorized personnel only.

3 Identification and Authentication

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

SC-CA's RA accepts card / certificate requests for subscribers if they are made by authorized persons, transmitted through authorized IDM systems and if a defined set of subscriber data can be verified against corporate directories. SC-CA thereby relies on the Allianz Group's organizational entities (OEs) fulfilling their obligation to deliver validated subscriber data to corporate directories upon proper subscriber identification pursuant to the provisions governing this process in the respective OE.

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

They are either handed over to a subscriber in person by authorized persons or they are sent via office mail to a subscriber's office address. Persons authorized to personally hand-over smartcard include ID-Card-Centre staff, who will always perform proper subscriber identification involving tender of personal ID documents, and the subscriber's rights administrator and line manager for whom such rigorous identity verification may not be necessary depending on the degree of personal acquaintance with the subscriber.

Subscribers will 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 standard for Distinguished Names. The attribute Common Name (CN) is part of Subject DN and Issuer DN.

The names of the subscribers are entered as a Distinguished Name (DN) according to ITU-T

X.500 [4]. The subscriber certificates issued by the SC-CA use the following DN name format:

- Country (C) = DE
- Organization (O) = ALLIANZ AG
- E-Mail (E) = e-mail address in RFC 822 compliant format
- Common Name (CN) = 'first name surname'.

3.1.2 Need for names to be meaningful

For the creation of Distinguished Names (DN) rules must be employed that guarantee that the created DN is unique and unambiguous in identifying a certificate's subject.

3.1.3 Anonymity or pseudonymity of subscribers

SC-CA does not issue certificates to anonymous identities. The use of pseudonyms by subscribers is not permitted, only the subscribers' real names as verified against corporate directories are used in X.500 subject DN.

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 in the DN of a subscriber's unique e-mail address.

3.2 Initial Identity Validation

The SC-CA RA implicitly relies on the initial identity registration performed for any subscriber by the subscriber's OE following their provisions for this process and prior to delivering the identity information to corporate directories that is checked against by SC-CA RA and included in certification requests.

3.2.1 Method to prove possession of private key

SC-CA only signs public keys that like their companion private keys have been generated under full control of the CMS itself either on a smartcard or (permitted by this CPS but not currently practiced) centrally on the CMS. The CMS itself controls the creation of the private key, the calculation of the public key from the private key and the construction of the CSR and its submission to SC-CA for certification. Subscribers typically gain possession of their private key only after certification through delivery of their smartcard which involves proper subscriber authentication. 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 certificates can only be issued for subscribers whose affiliation with an Allianz Organizational Entity is verified trough corporate directory lookup. The value of the organization X.500 name component (currently 'O=Allianz AG' for all certificates issued) is not submitted by an applicant subject to subsequent authentication but is prescribed by SC-CA via the applicable certificate template.

3.2.3 Authentication of individual identity

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

For card enrollment (which can be requested from the CMS only by authenticated, authorized persons via authenticated, authorized IDM Tools) a subscriber's individual identity is verified against corporate directories, relying on the subscriber's OE that is obligated to perform initial identity registration and commit validated relevant data to corporate directories.

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of authority

Certificate requests (implied in card requests) are not made by subscribers themselves but by authorized persons on their behalf. These persons' authority to issue a card request for a specific subscriber is technically implemented in the form of rights assigned to them in the IDM tools they are required to use in order to create a valid card request for a subscriber. Their authority to create any such request is effectively validated as they will have to authenticate with the IDM Tool by presenting their own smartcard authentication certificate and their right to request a card for the subscriber must successfully be verified in order for the request to succeed.

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 is part of the smartcard replacement process. A subscriber is authorized to initiate replacement of a damaged card and obligated to initiate this replacement without delay in case of lost or stolen smartcard. A subscribers initiate card replacement by reporting the damage, lost or theft to their rights administrator (who will have to establish the subscriber's identity in a reliable way) or to ID-Card-Centre staff appearing in person and providing personal identification. The actual card replacement and revocation 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 in the event of the termination of a subscriber's affiliation with Allianz Group. In that case competent HR personnel and the subscriber's line manager are authorized and obligated inform the subscriber right's administrator of this event who in turn is obligated to revoke all valid cards of the subscriber.

4 Certificate Life-Cycle Operational Requirements

Operation of SC-CA must comply with rules laid out in the Allianz Root CA II CPS and Allianz Group Security Policy [AZ-SP].

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

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

On the CMS side certificate requests are implicit in card requests for subscribers that in turn can be issued only by authorized persons (Rights Administrators or analogous organizational role) using an authorized IDM tool. The CMS will accept any card request submitted via an authorized IDM Tool provided the subscriber data can be verified via corporate directory lookup.

No interaction of authorized persons is required for Certificate Renewal (replacement on a card of a certificate pending expiry with a new one) which is scheduled automatically by the card management system provided the subscriber's data in corporate directories can be reconfirmed.

4.1.2 Enrollment process and responsibilities

Certificate requests are implicit in card 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 processes and authorized ID-Card-Center staff.

4.2.1 Performing identification and authentication functions

Identification and authentication for all subscriber information is performed in terms of section 3 of this CPS.

4.2.2 Approval or rejection of certificate applications

Certificate applications are auto-approved following successful verification of subscriber data against corporate directories and denied if such verification fails. This holds no matter whether the certificate application is implicit in a card request issued by a rights administrator or generated automatically on the Card Management System as part of a renewal or re-key process. Failure to confirm subscriber data via directory lookup results in the rejection of a certificate request.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

SC-CA creates and issues a certificate upon receiving an authenticated request by the CMS and based on the information contained therein. Submission of a request by the CMS always presupposes that proper certificate application processing has been performed and the application been approved.

The certificate issued is returned to the CMS and published to corporate directories as stipulated section 2.2 of this CPS.

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

No express notification is made in regard to certificate issuance.
SC-CA certificates are typically delivered to subscribers on smart cards with card delivery logically implying a notification of certificate issuance. Subscribers for whom card requests have been approved and if card issuance is not performed in their presence, are either notified via e-mail advising that a smartcard is ready for collection at a ID-Card-Centre or sent their card via internal mail.

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

4.4 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.

4.4.1 Conduct constituting certificate acceptance

Certificates and private keys are delivered on a smart card which needs to be unlocked prior to first use. Unlocking is performed by authorized staff (Help Desk) 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 end-user authentication certificates are published in the Allianz Corporate Directory and RACF (for lookup by IBM Hosts) upon creation. Also upon creation an authentication certificate's SHA1 fingerprint is written to the subscriber's Active Directory account.

All valid end-user encryption certificates are published to an Allianz Corporate Directory upon creation.

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 certificates are used to support authentication processes within Allianz Group OEs and to secure the exchange of electronic information both within Allianz Group as well as between Allianz Group entities and 3rd parties.

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

The participant's private key must only be used in accordance with the key usage field extensions included in the certificate.

The following certificate usages are permitted:

- Authentication of users or application data and technical systems
  (Key Usage: digital signature, Extended Key Usage: SSL Client Authentication
- Decryption of user or application data or of symmetrical keys serving as a means for encryption of such data in the so-called hybrid method
  (Key Usages: DataEncipherment and KeyEncipherment, Extended Key Usage: Secure E-Mail)
- Active Directory Smartcard Logon
  (Extended Key Usage: Microsoft Smartcard Logon – Allianz uses the unique UPN attribute of the authentication certificate to match a subscriber's Active Directory account)
- Establishing of VPN connections to the corporate network
  (Extended Key Usages: IPSec end system, IPSec User)

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

Subscribers are obligated to notify the appropriate Help Desk 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 are obligated to verify the contents of their certificate upon receipt of the smartcard and the associated certificate information and notify their Rights Administrator in the case of objections.

Subscribers accept that their certificate is published to corporate directory services and thus made publicly available within Allianz Group 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, Active Directory Smartcard Logon and VPN connection establishment.

4.6 Certificate Renewal

Certificate renewal is supported by SC-CA for authentication certificates.

For authentication certificates pending expiry renewal can automatically be scheduled by the Card Management System. Such a scheduled renewal being pending, a subscriber logging on

to a client computer will be prompted for approval to the certificate renewal which, the approval being granted, will proceed automatically through secure communications with the SCI.

For authentication certificate renewal the existing key pair on the smartcard is re-used. No new private key is generated.

4.6.1 Circumstance for certificate renewal

Certificate Renewal is allowed for authentication certificates pending expiration (i.e. as of 90 days prior to expiration) provided that 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 requested automatically via scheduled tasks on the Card Management System that will determine that an authentication certificate is nearing expiration and that its subscriber data can consistently be verified against corporate directories.

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 issuance ensues immediately upon the subscriber's approval to certificate renewal and will be confirmed in the dialogue. No separate notification is sent.

4.6.5 Conduct constituting acceptance of a renewal certificate

Subscribers by allowing a scheduled renewal to proceed will automatically have the renewal certificate written to their card. They are obligated by this CPS (section 4.5.1) to verify the contents of their certificate and bring any objections to the attention of their Rights Administrator. Failure to raise objections implicitly constitutes acceptance of the certificate.

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 is notified of certificate issuance.

4.7 Certificate Re-key

Re-Key is the process by which prior to the expiry of an end-entity certificate, a new private key is generated and a new certificate for the entity is issued certifying the new companion public key.

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

In the current mode of operation SC CA does not issue encryption certificates and thus no re-keying is practiced.

The stipulations made in hereafter (sections 4.7.1 through 4.7.7) apply should the mode of operation changed in a way to 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 that will determine that an encryption certificate is nearing expiration and that the subscriber data can consistently be verified against corporate directories.

4.7.3 Processing certificate re-keying requests

Rekey 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.
Re-key and certificate re-issuance ensue immediately upon the subscriber's approval to the re-issuance of his/her encryption certificate and will be confirmed in the dialogue. No separate notification is send.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Subscribers by allowing a scheduled re-key/re-issuance to proceed will automatically have the new key and certificate written to their card. They are obligated by this CPS (section 4.5.1) to verify the contents of their certificate and bring any objections to the attention of their Rights Administrator. Failure to raise objections implicitly constitutes acceptance of the certificate.

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 is notified of 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 are no longer matched by the information in the existing certificate.

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 provided subscriber data can be verified by directory lookup. This implies that a 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 (new card), 4.6.7 (renewal), 4.7.7 (re-key) apply.

4.8.5 Conduct constituting acceptance of modified certificate

The stipulations made in sections 4.4.1 (new card), 4.6.5 (renewal), 4.7.5 (re-key) 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 entities are notified of 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 compromise in the private key, 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 Group (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 must and the associated certificate(s) must 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 privileges accorded to them to fulfill their role (IDM Tool Dialogues and CMS Client respectively). They will have to state a reason for the revocation which along with the time of the revocation will be logged by the CMS.

In the case of the termination of the subscriber's relationship with Allianz Group the departing employee or external staff member will typically hand his or her card in to ID-Card-Centre staff who upon due identification of the subscriber will revoke the card (return to badge office).

Also the subscriber's Rights Administrator on receiving written notice of the departure by authorized HR Staff or the subscriber's Line Manager is required to check the status of the subscriber's smartcards and revoke valid cards using the proper dialogue in an IDM Tool.

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

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

Rights Administrator or ID-Card-Centre staff performing revocation on request by another person will always have to verify this person's identity and legitimacy in making the request .

Corporate ID-Card-Centre staff and Rights Administrator notify subscribers of the revocation of their cards and associated certificates in cases where 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 must 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 contained in its chain of trust every time the certificate is relied upon for any of its legitimate usages.

SC-CA 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 1 month and updated at a minimum of once every 14 days.

4.9.8 Maximum latency for CRLs (if applicable)

CRL are published to the web distribution point within 15 minutes after generation.

4.9.9 On-line revocation/status checking availability

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

4.9.10 On-line revocation checking requirements

A relying party must verify the validity of a certificate on it wishes to prior to every transaction relying on the certificate or a digital signature made with it. The Relying Party can perform this verification either by consulting the most recent CRL or alternatively by using the SC-CA 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 supports certificate status verification for all certificates it has issued and that have not yet expired by making a regularly updated web page hosted Certificate Revocation List available at http://rootca.allianz.com/scca/azscca.crl and by providing an OCSP Responder service accessible at http://ocsp.allianz.com.

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

4.10.1 Operational characteristics

SC-CA utilizes both CRL Publishing and OCSP service to allow Relying Parties check the validity of a any non-expired certificate issued by SC-CA. The CRL contains the serial numbers of all non-expired certificates that had been revoked up to the creation time of CRL of the CRL. The OCSP Responder offers current status information on any non-expired certificate at the very moment of the OCSP Query.

4.10.2 Service availability

SC-CA's CRL and the SC-CA OCSP service are open to public inspection 24x7.
Both services are under the operational responsibility of AMOS A-IT05CES02 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 Group his subscription to certificates issued by SC-CA ends simultaneously and all of the subscriber's cards and associated certificates shall be revoked.

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

In that event on date of cessation of operation the serial number to the SC-CA CA certificate shall be put on the Allianz Group Root CA II revocation list thus invalidating implicitly all subscriber certificates issued by SC-CA that are still non-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 is not permitted for signing keys.

The SC-CA's signing key is securely stored in a clustered Hardware Security Module.

Subscribers' signing keys are stored only the smartcards they are created on.

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 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 containing all certificates issued by it (and hence the public keys contained in them) is archived pursuant 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

SC-CAs systems are secured in compliance with GISF 2.2 physical security standard.

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 Group buildings is carried out by means of access system badges or smartcards with support implemented for physical access control.

Access and exit to Allianz Group's buildings is monitored and recorded by the access system.

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

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

Visitors must sign a visitor document with name, company, department, date and time and are handed a badge. Visitors to the server room are escorted all the time.

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 Security Policy.

5.1.6 Fire prevention and protection

An automatic fire detection system has been installed in the server room causing an alarm. 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 Security Policy.

5.1.9 Off-site backup

Conditions meet the standards identified in the Allianz Group Security Policy.

5.2 Procedural Controls

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

5.2.1 Trusted roles

This CPS defines trusted roles are bundles of tasks and associated access privileges that, if assigned to a person, empower that person to perform tasks related to the operation of the smartcard infrastructure and certificate life cycle management.

Trusted persons are natural persons (employees, contractors and consultants) who, after having undergone proper background checks and having received proper training, are entrusted with one or more trusted roles.

The trusted roles and their obligations are described subsequently with reference to the technical components and procedures involved in their execution.

As laid out in section 3 of this CPS, all non-automated RA functionality such as initial subscriber identification, card request issuance and approval etc. is performed under the responsibility of a subscriber's OE. Provisions governing these processes are defined by the OE in accordance with GISF. 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 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 administrative roles require compliance with user access management standard as laid out in GISF 2.2.

5.3 Personnel Controls

Personnel serving in such trusted position must meet the Allianz Group personnel security requirements.

5.3.1 Qualifications, experience and clearance requirements

Staff selected for trusted roles must 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 must be trained sufficiently to perform their duties in a responsible manner.

5.3.4 Retraining frequency and requirements

Retraining and appropriate quality controls is performed regularly 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 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 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

Only SCI Administrators have access the audit logs that will be made available to authorized roles (5.4.2) on request. Audit logs must 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 audit collection is generated at the application and operating system level and is invoked at system start-up and ceases only at system shutdown.

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

No vulnerability assessment has been carried out.

5.5 Records Archival

All relevant data (see 4.4.1) is archived according to Allianz Group System Operation Standard (GISF 2.2).

5.5.1 Types of records archived

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

SC-CA Internal LDAP

SC-CA Logs (including audit log)

5.5.2 Retention period for archive

Standard controls according to Allianz Group 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 Group 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 means of encryption in the database as well as 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 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 Operations must establish and maintain detailed documentation covering:

- Contingency & disaster recovery plan, pertinent to the contingencies of key compromise of SC-CA (SC-CA signing certificate is revoked), key compromise of Allianz Root CA II (Allianz Group Root CA II certificate is revoked), hardware, software and communications failures, and natural disasters such as fire and flood. See also Allianz Group Business Continuity Management Policy and Standards.
- Configuration baseline, including operating software, and PKI specific application programs.
- Backup, archiving and offsite storage procedures.
- Tests conducted periodically to validate the procedures for a full restoration of operational services for each of the following scenarios:
  - the current operational platforms are shut down and disconnected from 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.

Also appropriate training must be provided to all relevant staff involved in contingency and disaster recovery procedures.

5.7.1 Incident and compromise handling procedures

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

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

The general disaster recovery plan of Allianz Group applies.

5.7.3 Entity private key compromise procedures

In case of compromise of the SC-CA Private Key the following measures must be taken:

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

5.7.4 Business continuity capabilities after a disaster

The general disaster recovery plan of Allianz Group applies.

Therefore the SC-CA has:

- Identified individuals authorized to initiate disaster recovery action
- identified major elements at risk, for example:
  - Operational hardware
  - Certification authority software application
  - Logical records
  - Registration records
- Identified criteria that might prompt disaster recovery initiation
- considered secondary precautionary measures that may be required, such as:
  - a backup site
  - trained backup staff
- developed recovery actions and timeframes
- prioritized recovery actions from most significant to least significant
- maintained a record of the hardware and a software configuration baseline
- maintained records of the necessary equipment and procedures required to recover from an unexpected event such as a hardware failure within a stipulated maximum time to recovery

5.8 CA or RA Termination

Should it become necessary to terminate the SC-CA service, the impact of the termination is to be minimized as much as possible in light of the prevailing circumstances. The SC-CA shall provide as much prior notice to all PKI participants as is practicable and reasonable..

5.8.1 Keys and Certificates

In the event that it becomes necessary to terminate the Allianz Group SC-CA prior to its expiration, SC-CA's last action will be to revoke all valid certificates issued by it and publish a final CRL. Also the SC-CA own signing certificate will be revoked by Allianz Group Root CA II. Where practical, key and certificate revocation should be timed to coincide with the progressive and planned rollout of new keys and certificates by a successor Allianz Group SC-CA.

6 Technical Security Controls

SC-CA applies technical security controls complying with all requirements as laid out by Allianz Group Information Security Framework 2.5.

6.1 Key Pair Generation and Installation

Technical security controls are carried out on the basis of documented processes and stipulations. These security controls are duly fulfilled by Allianz Group SC-CA administrators in order to meet the requirements laid out in chapter 4. The cryptographic procedures and records used must correspond to state-of-the-art of cryptographic technology and must be compliant to the applicable legal stipulations.

It is a fundamental principle of Allianz Group SC-CA that a certificate may only be issued for a public key if the corresponding private key has been generated in a secure environment. Where cryptographic modules are used, the private keys must be generated in them and remain there in both encrypted and decrypted forms, and be decrypted only at the time at which they are being used.

Key generation in software and hardware are equally supported by Allianz Group SC-CA.

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 their generation is has to be undertaken under the supervision of either a member of the Senior Management of the Allianz OE retaining ownership and administrative control of Allianz Group RCA or a person specifically authorized by this Management to perform this supervision 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 must subsequently be transferred into an HSM for operational use.

The private key must not remain on any system other than the HSM and must be stored in encrypted form on storage media that must be securely kept in a safe. Access to the safe must be restricted to trusted SCI security personnel and the symmetric encryption key used to encrypt the CA key must be split and possession of the key fragments distributed among at least 3 trusted persons each retaining a security role within Allianz.

6.1.1.2 Subscriber Key Pair Generation

For end-entity keys that will reside on smartcards for operational use, 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 must comply with the provisions of this CPS.

6.1.2 Private Key delivery to subscriber

Private keys must be delivered on personalized smartcards only and if generated outside the smartcard must be transferred to it 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 for signing by the via adequately encrypted communication channels.

6.1.4 CA public key delivery to relying parties

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

6.1.5 Key sizes

The SC-CA 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 private key is stored securely in an HSM. An encrypted backup copy of it is kept in a safe with access to the safe restricted to few trusted security staff and the encryption key split and distributed among at least 3 trusted persons.

6.2.1.2 SCI Personnel Private Keys

The private keys of the SCI personnel are stored securely on a smartcards which 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 case the SC-CA 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. TODO

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. TODO

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 archives all public keys it certifies.

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

Archived certificates are to be:

- Archived on tamper evident media;

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

6.3.2 Usage Periods for the Public and Private Keys

The usage periods 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 keys stored on the smartcards are protected by a PIN and are 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) 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

No stipulation.

6.6.3 Life Cycle Security Controls

The configuration of the SCI (including SC-CA) as well as any modifications and upgrades must 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 shielded against outside networks by firewalls. Only Allianz Group Organization Units are connected to this network with all traffic controlled by firewalls.

No direct connection to the Internet is permitted.

6.8 Time stamping

Not applicable.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

For detailed information refer to appendix C.

7.1.1 Version numbers

SC-CA 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 subscriber certificates must 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, i.e. the 160-bit SHA-1 hash of the SC-CA public key.

7.1.2.2 KeyUsage

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

```
Number of Points: 1
Point 0
    Distribution Point: [URIName: http://rootca.allianz.com/scca/azscca.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 must be included marked non-critical and contain 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 System must contain 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 must have non-null Issuer DN.

All Certificates must contain 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 issues X.509 version 2 CRLs in accordance with ITU-T Rec. X.509 (1997).

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

They contain 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	sha1RSA
X509v3 CRL Number	number of the revocation list that is incremented with each update
Revoked Certificates	List containing for each revoked certificate the serial number and the revocation date and a revocation reason

7.2.1 Version number(s)

SC-CA 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 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 must be compliant with RFC 2560. SC-CA 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 operation is subject to RCA II and corporate technical and organizational audits.

8.1 Frequency or circumstances of assessment

The audit by Allianz Group RCA II is performed at least annually.

8.2 Identity/qualifications of assessor

8.3 Assessor's relationship to assessed entity

Allianz Group RCA II may initiate third party audits.

8.4 Topics covered by assessment

8.4.1 Initial compliance audit

The initial compliance audit by RCA II showed that SC-CA complies with the minimum eligibility, operational and technical requirements of the Allianz Group RCA II.

8.4.2 Ongoing compliance audit

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

8.5 Actions taken as a result of deficiency

Allianz Group PAC decides in each individual case of deficiency what kind of actions should be taken in order that the security of the SC-CA 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 Group RCA II. Allianz Group RCA II 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 is classified and marked with the data classification level in compliance with Allianz Group 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 Group.

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 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 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 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 infrastructure, or in accordance with the relevant this CPS.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

SC-CA 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 disclaims all warranties of any kind unless stated otherwise within the SC-CA 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 makes every effort to provide a secure and reliable PKI service to its subscribers. However, SC-CA assumes no liability related to the SC-CA PKI service.

9.8.1 Safeguards

Allianz SC-CA 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 Group RCA II 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

The SC-CA 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 Group RCA II

Allianz Group RCA II 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 Group PKI if

1. Allianz Group RCA II 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 Group RCA II, has a material adverse impact upon Allianz Group RCA II, or
2. the Allianz Group RCA II System, any participants, or any of their customers or the participant no longer qualifies as an eligible entity, or
3. Allianz Group RCA II is precluded for any reason from operating, or
4. otherwise determines to discontinue provision of the Allianz Group RCA II System.

Allianz Group RCA II shall provide the participating organization at least thirty (30) days prior written notice of Allianz Group RCA II's intention to terminate the participant, and shall include in such notice a summary of the reasons for such termination. Upon a decision by Allianz Group RCA II to terminate the participant, Allianz Group RCA II 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 revokes all certificates issued to the corresponding participating organization, e.g. the subscriber's certificates.

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

9.11 Individual Notices and Communications with Participants

9.12 Amendments

If a new CPS is approved, signed and distributed by A-IT05CCN03 SC-CA, all earlier versions of the CPS are superseded.

9.12.1 Notification mechanism and period

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

9.12.2 Circumstances under which OID must 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 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 II CPS, RCA II 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 shall govern.

9.16.5 Force Majeure

SC-CA maintains contingency plans in force, including adequate backup and recovery procedures, to ensure SC-CA 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.

Appendix

A Definitions and Acronyms

ASD	Allianz Service Desk
CA	Certification Authority
CMS	Card Management System
CPS	Certification Practice Statement
CRL	Certification Revocation List
DN	Distinguished Name
DNS	Domain Name System
GISF	Group Information Security Framework
GSS-API	Generic Security Services – Application Programming Interface
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
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 Group Root CA
SC	Smartcard with Cryptoprocessor
SC-CA	Smartcard CA
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

B References

[1] Available at http://www.ietf.org/rfc/rfc2527.txt?number=2527

[2] [AZ-SP] Allianz Group Security Policy – GISF 2.2

[4] ITU-T Rec. X.500, International Telecommunications Union, Geneva, 1997

[5] Available at http://www.ietf.org/rfc/rfc0822.txt?number=822

[6] [AZ-RCACPS] Allianz Group Root CA CPS

[7] [OHBID] Allianz Organisationshandbuch interne Dienste.

[8] [PDOKSP] Allianz Projektdokumentation „Prozessbeschreibung Mitarbeiterausweis mit SSO-Funktion“. Version 0.86

C Cert Profiles

C.1 SC-CA User Signing Cert

```
Certificate:
        Data:
            Version:  v3
            Serial Number: 0xFFE2412
            Signature Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5
            Issuer: CN=Allianz Smartcard CA,O=Allianz AG,C=DE
            Validity:
                Not Before: Tuesday, August 6, 2013 7:34:52 AM CEST Europe/Berlin
                Not  After: Sunday, August 5, 2018 7:34:52 AM CEST Europe/Berlin
            Subject: CN=First Last,E=first.last@allianz.de,O=Allianz AG,C=DE
            Subject Public Key Info:
                Algorithm: RSA - 1.2.840.113549.1.1.1
                Public Key:
                    Exponent: 65537
                    Public Key Modulus: (2048 bits) :
                        8B:B4:CA:F2:52:65:D0:B3:AB:DD:37:55:65:53:94:86:
                        (…)
                        48:EF:BE:87:35:21:D8:8F:DB:C1:95:B5:DB:93:CC:1D
            Extensions:
                Identifier: Authority Key Identifier - 2.5.29.35
                    Critical: no
                    Key Identifier:
                        3C:2C:0E:8E:B9:13:0B:91:F2:D7:EA:9F:7F:35:3A:66:
                        1C:E1:40:85
                Identifier: Key Usage: - 2.5.29.15
                    Critical: yes
                    Key Usage:
                        Digital Signature
                Identifier: Extended Key Usage: - 2.5.29.37
                    Critical: no
                    Extended Key Usage:
                        1.3.6.1.5.5.7.3.2
                        1.3.6.1.5.5.7.3.4
                        1.3.6.1.5.5.7.3.5
                        1.3.6.1.5.5.7.3.7
                        1.3.6.1.4.1.311.20.2.2
                Identifier: CRL Distribution Points - 2.5.29.31
                   Critical: no
                    Number of Points: 1
                    Point 0
                  Distribution Point: [URIName: http://rootca.allianz.com/scca/azscca.crl]
                Identifier: Subject Alternative Name - 2.5.29.17
                    Critical: no
                    Value:
                     OtherName:
(UTF8String)1.3.6.1.4.1.311.20.2.3,5Lpy0Xi3XxroXgnJ@SC
                      RFC822Name: first.last@allianz.de
                Identifier: Netscape Certificate Type - 2.16.840.1.113730.1.1
                    Critical: no
                    Certificate Usage:
                        SSL Client
                        Secure Email
        Signature:
            Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5
            Signature:
                6E:BF:7F:6C:B8:3C:19:90:48:BF:6B:F0:56:22:D7:28:
                (…)
                1F:1D:8B:69:03:45:5D:25:7E:D0:00:8C:A7:86:D1:65
```

C.2 SC-CA Signing Cert

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Root CA II
        Validity
            Not Before: Aug  2 13:19:58 2006 GMT
            Not After : Jul 29 13:19:58 2021 GMT
        Subject: C=DE, O=Allianz AG, CN=Allianz Smartcard CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ba:06:1a:ef:fa:aa:99:d3:ad:ae:cf:d6:c1:ac:
                    (…)
                    f3:05
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
            3C:2C:0E:8E:B9:13:0B:91:F2:D7:EA:9F:7F:35:3A:66:1C:E1:40:85
            X509v3 Authority Key Identifier:
            keyid:C0:7D:0A:37:BC:D9:61:D5:D1:CB:B6:2C:F6:37:3A:09:3C:A2:4B:79

            X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:0
            Netscape Cert Type:
            SSL CA, S/MIME CA, Object Signing CA
            X509v3 CRL Distribution Points:
            URI:http://rootca.allianz.com/rootca2.crl

            X509v3 Certificate Policies:
            Policy: 1.3.6.1.4.1.7159.30.20.1
              CPS: http://rootca.allianz.com/cps2
              User Notice:
                Organization: Allianz Group Germany
                Numbers: 1, 1
                Explicit Text: This Certificate is issued by Allianz Group
Root CA II, by Allianz Group Germany

    Signature Algorithm: sha1WithRSAEncryption
        19:f9:c5:e0:10:7c:fb:16:23:8a:ea:a5:1a:59:ef:ef:ed:70:
        (…)
        44:21:a8:ad:be:46:0e:9d
```

C.3 RCA II Signing Cert

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Root CA II
        Validity
            Not Before: Jul 28 09:12:27 2006 GMT
            Not After : Nov 29 09:12:27 2026 GMT
        Subject: C=DE, O=Allianz Group, CN=Allianz Group Root CA II
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (4096 bit)
                Modulus (4096 bit):
                    00:98:3c:44:3a:51:1d:3e:3b:d3:e6:20:78:7e:63:
                    (…)
                    e7:49:8d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
            C0:7D:0A:37:BC:D9:61:D5:D1:CB:B6:2C:F6:37:3A:09:3C:A2:4B:79
            X509v3 Authority Key Identifier:
            keyid:C0:7D:0A:37:BC:D9:61:D5:D1:CB:B6:2C:F6:37:3A:09:3C:A2:4B:79

            X509v3 Basic Constraints: critical
            CA:TRUE
            Netscape Cert Type:
            SSL CA, S/MIME CA, Object Signing CA
            X509v3 CRL Distribution Points:
            URI:http://rootca.allianz.com/rootca2.crl

            X509v3 Certificate Policies:
            Policy: 1.3.6.1.4.1.7159.30.20.1
              CPS: http://rootca.allianz.com/cps2
              User Notice:
                Organization: Allianz Group Germany
                Numbers: 1, 1
                Explicit Text: This Certificate is issued by Allianz Group
                               Root CA II, by Allianz Group Germany

    Signature Algorithm: sha1WithRSAEncryption
        7b:8e:3f:33:f5:bc:a1:eb:5b:fc:bc:80:5d:f9:74:8b:0d:e0:
        (…)
        12:f4:55:f3:47:0a:8a:d5
```