Certification Practice Statement
for
Allianz User CA V

Information Owner: Allianz Technology SE

Version 1.3 / 09.03.2022

Document-ID: AZ-USER-CA V CPS

Classification: Public

Change Management

Version	Description	Date	Author
0.9	Final Draft	28.04.2015	Helmut Buss
1.0	Review	19.11.2015	Vera Kloepper
1.1	Final with OID Update	10.05.2016	Aditya Kumar Yellai
1.2	• 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 Computer Emergency Response Team	09.03.2022	Thi Hang Nguyen
1.3	Review	01.07.2022	Helmut Buss

1 Introduction

1.1 Overview

This CPS is specifically applicable to Allianz User CA V and its associated Certificate Infrastructure. The CPS governs the use of Allianz User CA V services within Allianz Group and its participation in Allianz Root CA schema. The practices in this CPS focus on the operations of the Allianz User CA V. The structure of this CPS is based on Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework **Error! Reference source not found.**.

All certificate operations comply with: The policy requirements of:

- this CPS
- the Allianz Group Security Policy [AZ-SP]

The technology requirements of:

- Relevant internal guidelines for the physical protection of technology assets
- X.500 directory services
- X.509 certificate format
- X.509 CRL format
- X.500 Distinguished name standards
- PKCS#7 format for Digital Encryption and Digital Signatures
- PKCS#10 certificate request format
- Recognized PKI conventions and standards.
- Legal requirements of domestic and, where applicable, international privacy legislation
- Appropriate international and domestic standards relevant to PKI operations
- Audit requirements for certificate operations.

1.2 Document Name and Identification

The CPS at hand is referred to as the “Allianz User CA V Certification Practice Statement”, or abbreviated “Allianz User CA V CPS”. The structure of this CPS is based on Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC3647]. The OID of the CPS at hand is 1.3.6.1.4.1.7159.30.33

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 **Error! Reference source not found.**

1.4 PKI Participants

1.4.1 Certification Authorities

In the trust hierarchy of the Allianz Group the Allianz User CA V is certified by Allianz Root CA. The Allianz User CA V is operated as an intermediate CA that issues X.509 end-entity certificates only.

1.4.2 Registration Authorities

A Registration Authority (RA) is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewing certificates on behalf of Allianz User CA V. The Allianz User CA V provides a web-based registration interface that accesses user data from the Allianz Global Directory (GD). Users applying for a certificate **must** select their user record and receive after proper two factor authentication their certificate automatically.

1.4.3 Subscribers

The Allianz User CA V issues end entity certificates only. Certificate subscribers are natural persons working for or being in contractual relationship with Allianz.

1.4.4 Relying parties

Relying parties are certificate subscribers, Allianz organizational entities (operating or being in charge of processes/IT-systems that authenticate subscribers using certificates of the Allianz User CA V) and recipients or senders of secure E-Mail (internal and external).

1.4.5 Other participants

Not applicable.

1.5 Certificate Usage

1.5.1 Allowed Certificate Usage

Certificates issued by the Allianz User CA V are used to support secure communication and the secure exchange of information between relying parties within the Allianz Group. Two specific Usages are implemented:

- Digital Signature
- Key Encipherment, Data Encipherment

1.5.2 Prohibited certificate usage

Certificates issued by Allianz User CA V **must** only be used for the purposes and applications enlisted above in 1.5.1 Allowed Certificate Usage. Other usages **must** be approved in advance by written permission of Allianz User CA V administration. The Certificates usage **shall** be consistent with applicable law and applicable export or import laws.

Allianz Certificates are not designed, intended or authorized for resale.

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. ASIC 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 Entity determining CPS suitability for the policy

Allianz RCA Policy Approval Council, referred to as PAC hereafter, determines the suitability of this CPS and its compliance with other Allianz policies.

The Allianz RCA Policy Approval Council **shall** govern the enforceability, construction, interpretation, and validity of this CPS.

1.6.4 CPS approval procedures

Allianz Group is the final approval authority of any proposed changes to this CPS. Documentation of the Allianz User CA V in particular includes this Certification Practice Statement and a compliance statement in regard to Allianz Group Information Technology and Information Security Policy.

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, acronyms and abbreviations which are used throughout this document can be found in the Appendix.

2 Publication and Repository Responsibilities

2.1 Repositories

The Allianz RCA make publicly available following information of all Allianz RCA participants included Allianz User 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

Subordinate parties are notified by the Allianz User CA V of changes to a policy as and when they are approved.

End entity certificates issued by AZ-USER-CA are published into Allianz private repositories and are not publicly available.

Allianz User CA V ensures not to publish private information underlying Allianz Privacy Standard **Error! Reference source not found.**.

2.2 Publication of certification information

Allianz User CA V provides certificates and certificate status updates to admitted requestors. Certificate status updates are provided though CRLs and OCSP responses as part of the validation service. End entity certificates are only available to certificate holders.

2.3 Time or frequency of publication

2.3.1 Certificate publication

After issuance a new certificate will be distributed directly into the Allianz Global Directory. Revoked certificates will be immediately unpublished from the Allianz Global Directory.

2.3.2 Certificate-Revocation-List publication

Certificate revocation data is published as a regularly updated CRL. New CRLs are published every three weeks with a validity of four weeks.

Newly revoked certificates are enlisted on the internal CRL regularly within 15 minutes. The CRL update is dependent on availability of underlying infrastructure services (network etc.). The Allianz User CA V promptly publishes new certificates and changes in certificate status, including revocation and expiry to its repository.

2.4 Access controls on repositories

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

The private repositories where Allianz User 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 **Error! Reference source not found.**

3 Identification and Authentication

Allianz User CA V Registration Authority carries out the identification and authentication relying on pre-registered user data stored in Allianz Global Directory.

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 names of the subscribers are entered as a Distinguished Name (DN). The subscriber certificates issued by the Allianz User CA V use the following DN name format:

- Country (C) = DE
- Organization (O) = ALLIANZ
- Organization (OU) = <optional>
- E-Mail (E) = e-mail address which complies with **Error! Reference source not found.**, listed and managed by the Allianz internal Mail-System
- Common Name (CN) = first name and surname of the Participant.

3.1.2 Need for names to be meaningful

Distinguished Names which are allowed by Allianz User CA V **must** include the subscribers name and email address as a meaningful part.

3.1.3 Anonymity or pseudonym of subscribers

Subscribers **must** not be anonymous or pseudonymous.

3.1.4 Rules for interpreting various name forms

Certificates issued by Allianz User CA V **must** be unique at least in regard to the Email Address of the certificate holder.

3.1.5 Uniqueness of names

The uniqueness of the DN is established by the use of the Allianz Group directory service (Group Directory) as a reliable data source for unique email addresses.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

Private key possession is proved by verification the association of the public key in certificate signing request and the private key, which was used to sign it.

Allianz User CA V RA checks its records to ensure that the public key to be certified does not already exist in the list of operational or revoked certificates. The OEs eligibility for requesting certificate services is determined by the responsible OE and enforced by control of write privileges to Allianz Global Directory.

3.2.2 Authentication of individual identity

Users requesting Allianz User CA V Certificates authenticate against the Allianz Global Directory. The user himself will be authenticated by an existing certificate, existing internal logon or a two factor authentication based on data of the internal Allianz Group Directory.

3.2.3 Non-verified subscriber information

Allianz User CA V employs policy filters to overwrite any data enclosed in the certificate request except the user name, the email-address and the public key.

3.2.4 Validation of authority

Authority of requestors is ensured by the certificate request process that requires authentication against the Allianz Global Directory. Any user listed in the Allianz Global Directory is entitled to request an Allianz User CA V Certificate.

3.2.5 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 is carried out when subscribers' keys are about to expire. The new certificate is issued using the pre-registered data. The re-key-request is initiated automatically by RA-systems. Key-pair generation, certification and private key activation are performed analogous to the initial issuing process.

3.3.2 Identification and authentication for re-key after revocation

Following a revocation no re-keying is possible. In case of a revocation a new certificate is issued and the processes enlisted for initial authentication apply as well.

3.4 Identification and Authorization for Revocation Requests

A request to revoke keys and certificates may be submitted by the Subscriber or the RA. The Subscriber **may** submit a revocation request by:

- using a request or email digitally signed by a valid private key and certificate that **shall** be revoked

- sending a signed document

4 Certificate Life-Cycle Operational Requirements

The purpose of this chapter is to identify the Allianz User CA V Certificate Management life cycle. The life cycle of an Allianz User CA V certificate starts when a certificate is generated and ends when the certificate expires or is revoked. During this time, a certificate can move through a number of different states. There are two main states of the certificate life cycle: primary and secondary certificate states.

The primary states are:

- Generation
  Certificate generation consists of
  - Receipt of an approved and verified certificate request.
  - Binding the key pair associated with the certificate to a certificate owner
  - Issuance of the certificate and the associated public key for operational use under a DN or distinguished name associated to the network connector, e.g. a server within Allianz.
- Operational use
  A certificate comes into operational use at the time of issuance, and remains in operational use until it expires or is revoked. Certificates have a maximum fixed operational lifetime that is determined by the Allianz RCA III and the specified AZ-USER-CA V life span. The AZ-USER-CA V certifies technical entities solely after request of trained Allianz Technology SE staff or their contactors responsible for correct application and use.
- Expiry
  Certificates expire automatically upon reaching the designated expiry date, at which time the certificate is archived. The life of a certificate cannot be extended. An expired certificate cannot be reissued.
- Archive
  Expired certificates are archived for a minimum period of 10 years from the date of expiry.
- All certificate types issued pass through these four primary states as part of their life cycle. The secondary state is revocation.

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

All certificate operations will comply with the requirements of:

- an applicable security policy **Error! Reference source not found.** this CPS
- the minimum operational requirements and operating rules of Allianz RCA system and
- legal requirements of domestic and, where applicable, international privacy legislation.

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

4.1 Certificate Application

Allianz User CA V provides the users of the Allianz with Authentication and Encryption certificates, whereas additionally group encryption certificates for shared email accounts are supported.

4.1.1 Who can submit a certificate application?

Any user of Allianz that is enlisted in Allianz Global Directory can submit certificate applications.

4.1.2 Enrollment process and responsibilities

The enrolment process for certificates issued by Allianz User CA V is web-based. Users access the Registration Authority interface with their web-browser. In the first step, the user is asked to enter his/her email address or user ID into a search form. As a result of the search action a list with matching user Ids and email-addresses is presented. The user has to select his/her entry from the list.

After selection of his/her data set from the Global Directory, the user proceeds with requesting a PIN. In combination with the PIN which is presented on the screen in the web-browser there is an email sent to the users email address. This email contains a Transaction Number (TAN) corresponding to the PIN. In order to proceed, the user **must** enter in the Registration Interface the received TAN that belongs to the shown PIN. If the email with the TAN is not received immediately, the user has to remember his PIN and accomplish this step at a later time.

After entering his credentials (PIN&TAN) the user accesses the Certificate Recovery Interface, where he **may** either recover an existing encryption certificate or request a new certificate. If the user did not yet own a certificate by Allianz User CA V he/she is headed directly to the Registration Interface, where again the authenticated data is presented. At this point the certificate request corresponding to the shown data can be submitted.

User authentication **may** be conducted by using valid certificates of predecessor CAs as long as those certificates provide equivalent assurance. If no valid certificate exists, NTLM authentication **may** surrogate authentication if user and system management provides equivalent security measures.

Certificates for group mailboxes **may** be issued to enable encryption. Those certificates **shall** not be issued for existing user mailboxes. The request for those special certificates requires use of a separate RA process ensuring Allianz Remote CSP Software usage for private key storage.

4.2 Certificate Application Processing

Certificate applications are processed by Allianz User CA V systems automatically. Certificate request approval is granted by Allianz User CA V support personal.

4.2.1 Performing identification and authentication functions

As part of the registration process, the registration authority approves or rejects the certification request based on the subscribers' authentication and identification data.

4.2.2 Approval or rejection of certificate applications

Certificate Applications are approved automatically after careful checks of the following:

- The integrity of the message has not been compromised.

- The content of the request file is correct (all fields and extensions are complete and conforming to naming conventions).
- Ensure the certificate request has not been tampered.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate Issuance

4.3.1 Certificate Requests

Allianz User CA V issues subscriber certificates based on the registration data delivered by the Registration Authorities respectively the Allianz Global Directory.

4.3.2 Verification and Rejection of Certificate Requests

The CA checks if the RA signed request is correct and if a profile with pertinent rights is assigned to it.

4.3.3 CA actions during certificate issuance

The CA signs the public key of the subscriber as requested. Completion confirmation is returned to the respective RA (the ActiveX Control that handles the Registration Procedure). Issued certificates are offered for download to the ActiveX Control.

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

The subscriber receives his/her newly issued certificate directly after finishing the registration procedure.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

The certificate is considered as accepted, when the applicant downloads it.

4.4.2 Publication of the certificate by the CA

All valid end-user certificates are published in the Allianz Global Directory (GD) 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

The Subscriber is responsible for taking sufficient measures to protect their own private key against any access by third parties. Allianz **must** be notified immediately if the Subscriber has any reasons to suspect that an unauthorized third party has access or has come into possession of their private key. In this case, the Registration Authority will revoke the certificate.

The Subscriber **must** discontinue the use of their private key after expiration or revocation of the certificate.

4.5.2 Relying party public key and certificate usage

The private key of the participant that associates with the public key in issued certificate can only be used for applications in accordance with the key usages given in the certificate. The permitted key usages are authentication, encryption and digital signing.

4.6 Certificate Renewal

Certificate renewal is the process by which a new (sequent) certificate is issued to replace an expired (or expiring) certificate. Certificate renewal reuses the existing private and public key pair of the old certificate of the Subscriber.

Allianz User CA V does not support certificate renewal as certificate re-key (see **Error! Reference source not found. Error! Reference source not found.**) is required by Allianz User CA V. Key pairs **must** always expire at the same time as the associated certificate. When a subscriber requests certificate renewal, new key pairs **must** be generated.

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other

No stipulation.

4.7 Certificate Re-key

4.7.1 Circumstance for 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 by the Subscriber. No certificate re-key will be performed for a key pair of an existing certificate. The Allianz User CA V issue only certificates with a new generated key pair.

4.7.2 Who may request certification of a new public key

Please see 4.1.1 “Who can submit a certificate application?”

4.7.3 Processing certificate re-keying requests

Please see 4.2 Certificate Application Processing

4.7.4 Notification of new certificate issuance to subscriber

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

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Please see 4.4 Certificate Acceptance

4.7.6 Publication of the re-keyed certificate by the CA

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

4.7.7 Notification of certificate issuance by the CA to other entities

Please see 4.4.3 Notification of certificate issuance by the CA to other entities

4.8 Certificate Modification

4.8.1 Circumstance for certificate modification

The Allianz User CA V does not support certificate modification. In cases where certificate information changes during the life span of a valid certificate, the existing certificate **shall** be revoked and a new certificate application is made using the modified information.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

The Allianz User CA V revokes certificates to permanently prevent the future use of the certificate and its associated key pair due to one of the following reasons:

- The termination of a business relationship between Allianz and the Subscriber
- The security or confidentiality of the private key has been compromised or is at material risk of being compromised.
- Loss of private key
- Errors in the certificate
- Change of certificate content
- Certificate misuse
- The issuing CA has ceased operation.
- Cryptographic algorithms become insecure and do not protect the target business or customer data as required.
- The affected CA terminates its operation permanently.
- The Certificate owner has submitted a valid revocation request.

A Subscriber can revoke his certificate at any time without warning.

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

4.9.2 Who can request revocation

Certificate revocation can be initiated by:

- The Registration Authority
- The Allianz User CA V
- The certificate subscriber

4.9.3 Procedure for revocation request

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

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

4.9.4 Revocation request grace period

The subscriber and other entities are obligated to request that the CA revoke the certificate as soon as possible after the need for revocation has been determined.

4.9.5 Time within which CA must process the revocation request

The revocation of a certificate **must** take place immediately.

4.9.6 Revocation checking requirement for relying parties

Allianz OEs that rely on certificates issued by Allianz User CA V are bound to check certificate status of subscriber and CA certificates prior to every use.

4.9.7 CRL issuance frequency (if applicable)

No stipulation.

4.9.8 Maximum latency for CRLs (if applicable)

No stipulation.

4.9.9 On-line revocation checking requirements

Status information on revoked certificates is available via the OCSP.

4.9.10 Other forms of revocation advertisements available

No stipulation.

4.9.11 Special requirements re key compromise

No stipulation.

4.9.12 Circumstances for suspension

Certificate suspension is not provided. Suspension will be handled by revoking the existing valid certificate and issuing a new certificate at the end of the suspension period.

4.9.13 Who can request suspension

No stipulation.

4.9.14 Procedure for suspension request

No stipulation.

4.9.15 Limits on suspension period

No stipulation.

4.10 Certificate Status Services

Allianz User CA V provides OCSP for verifying the status of all issued certificates.

4.10.1 Operational characteristics

The certificate status validation service is inter-operational to the OCSP service of Allianz RCA. It is required, that the Relying Parties check the validity of the issuer certificate (including the validity of the issuing CA certificate) with respect to every action signed with that issuer certificate.

4.10.2 Service availability

The provision of Certificate Status Information is an implicit part of service delivery and an essential feature of Allianz PKI design that **must** be available in a HA fashion. OCSP is monitored and any service discontinuity would trigger events that activate the responsible level support unit.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

Subscription ends with expiration of a certificate without renewal being requested or by revocation of a certificate.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

All secret keys of the CA-System used within the Allianz User CA V are backed up. All Certificates (and hence the public keys contained in them) **shall** be archived. The backup of the CA secret key will be operated under the same circumstances like the active CA secret key.

The secret key of the subscriber will not be stored for backup. Restore or escrow of the subscriber's secret key is not possible.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

Allianz User CA V systems are secured in compliance with the Allianz Guideline for Physical Security **Error! Reference source not found.**.

5.1.1 Site location and construction

The CA environment is hosted in two geographical redundant secure facilities for HA and disaster recovery. The Allianz User CA V Registration Authority and Backup Systems operate within physically secured areas that meet the standards identified in the Allianz Functional Rule for Information Security **Error! Reference source not found.** and Guideline for Physical Security **Error! Reference source not found.**.

5.1.2 Physical access

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

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

The data centers where CA systems, hardware are located, are ISO 27001 certified. Physical access control system of data centers follows ISO 27001 – Annex A.11: Physical & Environmental Security implementation guides.

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

5.1.3 Power and air conditioning

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.

5.1.4 Water exposure

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

5.1.5 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.

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Off-site backup

Allianz User CA V manages its backup, archive and offsite storage in accordance with Allianz Group Information Technology and Information Security Policy [AZ-ITISP].

5.2 Procedural Controls

The Allianz User CA V service is operated in accordance with Allianz approved policy, practices, and procedures regarding safe and trustworthy system operation. Access controls and procedures are set in place to ensure that one person acting alone cannot circumvent the entire system.

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 Allianz User CA operational processes. One CA personnel can be assigned to more than one role when the basic security principles described above are not be violated.

Roles	Responsibilities
CA Owner	• Owns the CA • Fully responsible for the whole CA business • Approve high risk tasks like revoke CA certificates
CA Manager	• Organize, lead CA events like key ceremony • Maintenance and create CA process, procedures & operational documentation • Monitor CA events to ensure each participant follows documented procedures. • Organize CA operator and key custodians • User management including roles and access rights (technical and organizational) • Manage inventory of CA assets (hardware, software, key material). Conduct inventory check every six months.
CA Operator	Setup/configure/operate/ manage CA components, which include RA, CA, CRL, and OCSP services:

	• Generate CA keys and CA certificates • Revoke CA certificates • Update CRL • Manage registration data including suspension and revocation information • Generate OCSP keys, OCSP updates, request OCSP certificates, update OCSP information, revoke OCSP certificates, configure online OCSP functions and application features • Configure offline/online CA, OCSP functions and application features • Perform backup tasks
Key Custodian	• Not key owners, hold normally key component, handle cryptographic key material for CA services, which includes keys for RA, CA, OCSP and other cryptographic enabled services. • Enable RA, CA, OCPS keys and support backup and recovery services, using dual controls with split knowledge.
System Administrator	• Setup, configure and maintain the CA IT structure, including networks, databases and server
Security Officer	• Create CA policy, functional practices • Review and approve CA process, procedures & operational documents • Provide physical security controls for all CA related services, applications, systems or network components • Annual or ad hoc security and risk assessments of any or all CA components/services.
Auditor	• Review annually CA documents including process documents, CA event protocol and log data • Conduct physical security inspection of all CA (offline/online CA systems + OCSP) related services, application, system or network components • Inspect the management of cryptographic material to ensure security policies, practices, and procedures are followed.
Safe User	• Owns the safe PIN and/or key

5.2.2 Number of persons required per task

All certification, administration and user administration tasks require compliance with multiple control requirements as laid out in the current Allianz Group Information Technology and Information Security Policy [AZ-ITISP]. Every task which requires a multiple control are administered with an m of n person doctrine (with m ≥ 2 and n > m).

5.2.3 Identification and authentication for each role

Allianz User CA V systems and processes use the corporate access control infrastructure based on smartcard and SSO mechanism which provides strong authentication and role based access control. Granting and withdrawal of Allianz User CA V administrative roles require compliance with user access management standard as laid out in the current Allianz Group Information Technology and Information Security Policy [AZ-ITISP].

5.3 Personnel Controls

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

5.3.1 Qualifications, experience and clearance requirements

Persons filling trusted roles (cf. section 5.2) **must** undergo an appropriate security screening procedure, designated “Position of Trust”. All Allianz User CA V operations staff:

- are evaluated before employment to assess their suitability
- enter into non-disclosure agreements to protect against the unauthorized disclosure of confidential information
- **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

5.3.2 Recruitment and Qualification of Personnel

The recruitment and selection practices for Allianz User CA V personnel take into account the background, qualifications, experience and clearance requirements of each position, which are compared against the profiles of potential candidates.

5.3.3 Background check procedures

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

5.3.4 Training requirements

Operational personnel is been trained sufficiently to perform their duties in a responsible manner.

5.3.5 Retraining frequency and requirements

Retraining is performed at least annually based on and include necessary quality controls.

5.3.6 Job rotation frequency and sequence

No stipulation.

5.3.7 Sanctions for unauthorized actions

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

5.3.8 Independent contractor requirements

No stipulation.

5.3.9 Documentation supplied to personnel

Allianz User CA V System staff has access to all documentation of CA system and training material.

5.4 Audit Logging Procedures

Allianz User CA V maintains adequate records and archives of information pertaining to the operation of the PKI, i.e., generation, operational use, expiry and archive of certificates.

5.4.1 Types of events recorded

Allianz User CA V manually or automatically logs the following significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
  - CA and Subscriber certificate life cycle management events, including: Certificate Applications, re-key and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.

- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed by Allianz User CA V personnel
  - Security sensitive files or records read, written or deleted
  - Security profile changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activity
  - CA facility visitor entry/exit

- The information recorded (audit log) include the following:
  - Type of event
  - Time and date the event occurred
  - Person or entity initiating the event
  - Reason for event
  - Outcome of the event (successful/unsuccessful)

5.4.2 Frequency of Processing Log

The Allianz User CA V audit log is reviewed periodically by the CA Administrators.

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

The audit logs are protected by smartcard authentication. Only authorized auditors **may** view the audit logs.

5.4.5 Audit log backup procedures

Log files are archived automatically by using the central archiving and backup system. Access control has to be configured to prevent unauthorized access and modification or deletion of audit logs.

5.4.6 Audit collection system (internal vs. external)

Automated audit data is generated and recorded at the application, network and operating system level internally.

5.4.7 Notification to event-causing subject

Operations personnel **must** notify their Allianz Computer Emergency Response Team (CERT) when a process or action causes a critical security event or discrepancy.

5.4.8 Vulnerability assessments

Vulnerability assessment is carried out as required by current operational IT standards of Allianz Group.

5.5 Records Archival

All relevant data (see 4.4.1) is archived according to Allianz Functional Rule for Information Security **Error! Reference source not found.**.

5.5.1 Types of records archived

The following operational records are archived by Allianz User CA V:

- Audit logs
- Certificate request information
- Certificates, including CRLs generated
- Complete back up records
- Copies of e-mail logs
- Formal correspondence
- Application records.

5.5.2 Retention period for archive

The retention period is chosen according to current IT operational standards.

5.5.3 Protection of archive

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

5.5.4 Archive backup procedures

Certificates issued by the Allianz User CA V are archived for a minimum period of 10 years beginning with the date of expiration. Certificates are archived securely on an archive medium. Access to archived certificates is under control of Allianz User CA V.

5.5.5 Archive collection system (internal or external)

The Allianz User CA V audit collection system is an automated processes performed by the Certification Management System and the Operating System (OS).

Access and verification of archived information is carried out by client software with the standards of the archiving and backup system.

The integrity of archived information is verified:

- upon creation
- upon retrieval
- at any other time when a full security audit is required.

5.6 Key Changeover

Key changeover is handled by setting up a new CA instance using new keys prior to expiration of the current Allianz User CA V instance.

5.7 Compromise and Disaster Recovery

Allianz User CA V **must** establish and maintain detailed documentation covering:

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 **Error! Reference source not found.**.
   - 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 INFRA-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.

5.7.1 Incident and compromise handling procedures

In general incidents within the Allianz User CA V are handled according to the Allianz Information Security Practice for Incident Handling **Error! Reference source not found.**. In addition the INFRA-CA-V has established a key compromise plan that addresses the actions to be taken in the event that its private key is compromised.

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

In the event of the corruption of computing resources, software and/or data, such an occurrence is reported and incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation and incident response. If necessary, key compromise or business continuity procedures will be enacted.

5.7.3 Entity private key compromise procedures

Upon the suspected or known Compromise of the Allianz User CA V, Key Compromise Response procedures are enacted by the Computer Incident Response Team (CIRT) as required by the Allianz Information Security Policy. If Allianz User CA V Certificate revocation is required, the CA Termination procedure will be enacted as described in section 5.8 CA or RA Termination.

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 Allianz User CA V in order to make accessible the logical records kept within the software. Therefore the Allianz User 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 might prompt disaster recovery initiation
4. Considered secondary precautionary measures that **may** be required, such as:
   - a backup site
   - trained backup staff
5. Developed recovery actions and timeframes
6. Prioritised recovery actions from most significant to least significant
7. Maintained a record of the hardware and software configuration baseline

8. Maintained records of the necessary equipment and procedures required to recover from an unexpected event such as a hardware failure, including the intended maximum period that the system is down.

5.8 CA or RA Termination

If it is necessary to terminate Allianz User CA V services, the impact of the termination **shall** be minimized as much as possible in light of the prevailing circumstances. The Allianz User CA V will at least provide as much prior notice as is practicable and reasonable to participants and relying parties.

5.8.1 Keys and Certificates

All keys and certificates will be revoked by Allianz User CA V immediately and prior to an emergency shut down. The last act of the terminated Allianz User CA V is to issue a CRL with all certificates revoked. The Allianz User CA V will include revocation of its own certificate as well. Where practical, key and certificate revocation **should** be timed to coincide with the progressive and planned rollout of new keys and certificates by a successor Allianz User CA V.

6 Technical Security Controls

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 User CA V members in order to meet the requirements explained in chapter 4 Certificate Life-Cycle Operational Requirements. The cryptographic procedures and records used correspond to the status quo of security measures of cryptographic procedures and to the respectively valid legal stipulations. The following RSA key pairs are used in the Allianz User CA V System: Allianz User CA V Keys - 5 Years - 2048 bit
- The Allianz User CA V keys are exclusively generated by the Hardware Security Module (HSM) as part of the Allianz User CA V systems.
- The Key Generation is described in the key ceremony document, part of the operation manual.

6.1.1 Key pair generation

It is a fundamental principle of Allianz User CA V that a certificate **may** only be issued for a public key which its corresponding private key has been generated in a secure environment. In case HSMs are used, the private keys are generated in HSM and remain there in both encrypted and decrypted forms, and will be decrypted only at the time when they are being used.

Allianz User CA V has established HSM compliance criteria that ensure the quality and requirements of HSMs are uniform and consistent. The keys used by Allianz User CA V Server (CA signing and server key) are generated using the HSM key generator. This integrates in Microsoft Enterprise Certification Authority 2003 Software via CSP. End entity keys are generated on the requestors systems with a minimum RSA key length of 2048 bit.

6.1.2 Private key delivery to subscriber

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

6.1.3 Public key delivery to certificate issuer

Subscribers submit their public key to Allianz User CA V for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) by an ActiveX Browser Plug-in in a session secured by Secure Sockets Layer (SSL). Allianz User CA V receives the public keys to be certified via signed certificate requests. Those requests are submitted by the subscriber using the RA web-interface via https.

6.1.4 CA public key delivery to relying parties

Allianz User CA V makes its CA Certificates and Allianz Root CA Certificates available to Subscribers and Relying Parties at the Allianz Root CA website. As new Allianz User CA V and Allianz Root CA Certificates are generated, Allianz provides such new Certificates at the Allianz Root CA website. Allianz generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance.

6.1.5 Key sizes

Generally, the Allianz User CA V and subscriber keys are 2048 bit RSA keys.

6.1.6 Public key parameters generation and quality checking

No stipulation.

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

Refer to User CA V Certificate Profile10 sample certificates for key usage settings that differ depending on the intended application. They are configured via certificate templates in the CA system.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Allianz User CA V secret signature key is stored in a FIPS 140-2 Level 3 compliant redundant Hardware Security Module and is not subject to automated backup procedures. End-entity private keys are stored in a secure way at the local key store on their individual computer. The subscriber is responsible for the secure storage of the secret key.

6.2.1 Cryptographic module standards and controls

For Allianz User CA V key pair generation and CA private key storage, Allianz User CA V uses HSMs that are certified at or meet the requirements of FIPS 140-2 Level 3.

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

Allianz has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. Allianz User CA V uses “Secret Sharing” to split the activation data needed to make use of a CA private key into separate parts called “Secret Shares” which are held by trained and trusted individuals called “Key custodians”. A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module. In order to export the private key encrypted, e.g. for transfer to a different HSM, multiple person control is implemented via the administrator cards required by the HSM.

6.2.3 Private key escrow

The CAs private key is stored in a HSM which prevents key escrow by design.

6.2.4 Private key backup

The CAs private key is kept redundantly on three HSM devices.

6.2.5 Private key archival

The CAs private key is not archived besides remaining on the HSM devices.

6.2.6 Private key transfer into or from a cryptographic module

FIPS 140-2 Level 3 permits private key import to HSM modules. Export is only possible from one HSM to the backup HSM. Private key generation is only performed on hardware security modules. Three persons are required to export the private key to a new HSM device (ISO,

Operator and Partition owner). The exported key can only operate under the same circumstances as the active key in the HSM.

6.2.7 Private key storage on cryptographic module

CA or RA private keys held on hardware cryptographic modules are stored in encrypted form.

6.2.8 Method of activating private key

Allianz User CA V protects the activation data for their private keys against loss, theft, modification, unauthorized disclosure or unauthorized use. The CA private key is activated using operator cards accessible for administrators of CA system only.

6.2.9 Method of deactivating private key

The CAs private key is deactivated by shutting down the CA server.

6.2.10 Method of destroying private key

The used HSM provides means to destroy the CAs private key together with the partition of the HSM which is used for the key storage. When conducting the destruction multiple controls apply. The private key on all redundant devices will be destroyed in succession.

6.2.11 Cryptographic Module Rating

Allianz User CA V secret signature key is stored in a FIPS 140-2 Level 3 compliant redundant Hardware Security Module.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Allianz User CA V, RA and Subscriber Certificates are backed up and archived as part of routine backup procedures. Expired certificates and CRLs 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:

- Archived on tamper evident media
- Archived for a minimum period of seven years from the date of expiry 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:

- CA key and certificate: 5 years
- Subscriber key and certificate: max. 2 years

6.4 Activation Data

6.4.1 Activation data generation and installation

Activation data for the Allianz User CA V key is generated at installation in form of administrator cards. Those cards **must** be initialized before they are used for private key generation and access in a specific HSM/partition (see 6.2.2).

6.4.2 Activation data protection

The HSM administration cards are stored securely by the respective card owners.

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 hosts' operating systems and the Allianz User CA V application:

- Access control to CA and RA services
- Use of HSM to store the CAs private keys
- Encrypted communication between all entities
- Backup and Recovery processes for Allianz User CA V systems including data.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The Allianz User CA V was setup 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 (including the key generator) and its configuration was presented to Allianz SE.

6.6.2 Security Management Controls

Allianz PKI Team control, monitor the configurations of the systems and prevent unauthorized modification.

6.6.3 Life cycle security controls

The configuration of the Allianz User CA V 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

Allianz User CA V follows to the requirements of the Allianz Network Security standard for the protection of its network infrastructure. Allianz User CA V is an online system. Access to the CA servers is protected by a firewall.

The Allianz Corporate Network is protected from outside networks by firewalls. Only Allianz Organizational Units are connected to this network by further firewalls. No direct connection to the internet is permitted.

6.8 Time stamping

No stipulation.

7 Certificate, CRL, and OCSP Profiles

End-Entity Certificates will be issued with the following profile parameters.

7.1 Certificate Profile

Certificates issued by Allianz User CA V comply with Allianz RCA requirements. For the detailed certificate profile refer to 10 User CA V Certificate Profile. The public key in a certificate **must** be unique. No party, if an end-entity or a Sub CA, **may** have its public key signed by more than one Certification Authority.

7.1.1 Key Usage

Key usage is present in all issued certificates as defined in the 10 User CA V Certificate Profile.

7.1.2 Certificate Policies

Certificate Profile Extension includes an individual Allianz OID: 1.3.6.1.4.1.7159.30.X

7.1.3 Version number(s)

Certificates comply with X.509 v3 standard.

7.1.4 Certificate extensions

Certificate extensions are used as described in the 10 User CA V Certificate Profile.

7.1.5 Algorithm object identifiers

No stipulation.

7.1.6 Name formats

All certificates **must** contain non-null Issuer DN and a Subject DN.

7.1.7 Name constraints

Name constraints **shall** not be used.

7.1.8 Certificate policy object identifier

The Certificate policy object identifier is for User CA V 1.3.6.1.4.1.7159.30.33

7.1.9 Usage of Policy Constraints extension

No stipulation.

7.1.10 Policy qualifiers syntax and semantics

No stipulation.

7.1.11 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL Profile

No stipulation.

7.2.1 Version number(s)

No stipulation.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP Profile

OCSP is used to check the revocation status of X509 certificates. OCSP provides revocation status on certificates in real time and is very useful in time-sensitive situations.

The revocation status of a certificate is checked by sending a request to an OCSP server. Based on the response from the OCSP-server, the access is allowed or denied.

The OCSP servers are designated authorized responder. The location of the OCSP server is configured in the profile of the certificate that is being verified. Requests are only sent to the OCSP server location that are manually configured in CA profiles with the ocsp url statement. There are four load balanced OCSP servers behind the URL=http://rootca.allianz.com/ocsp/.

If the OCSP server is not reachable, the access will be denied. There is no other checking method as an option implemented in the certificate's AuthorityInfoAccess extension field. The OCSP is the default checking method. A certificate revocation list (CRL) isn´t configured as an alternative checking method.

The response received is validated using trusted certificates. The response is validated as follows:

1. The CA certificate enrolled for the configured CA profile is used to validate the response.
2. The OCSP response might enclose a certificate to validate the OCSP response. The received certificate **must** be signed and enrolled by the Allianz User CA V. After the received certificate is validated by the CA certificate, it is used to validate the OCSP response.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8 Compliance Audit and Other Assessment

Prior to becoming Sub-CA members of Allianz Root CA the Policy Council proves the compliance of Allianz User CA V to the policies of Allianz Root CA. As SubCA member of Allianz Root Certification Authority Infrastructure, the compliance of Allianz User CA V Policy, CPS and described processes is regularly checked against Allianz RCA Policy/CPS, which in turn is compliant with internal Allianz Security Standards. A control assessment is conducted with support of Allianz User CA V on a regular basis.

The following topics are covered:

- Security policy and planning
- Physical Security
- Technology evaluation
- Personnel examination
- Relevant certificate policies and CPS
- Privacy considerations

8.1 Frequency or circumstances of assessment

Audits are conducted on at least an annual basis. Allianz User CA V will, at its expense, remedy any deficiencies revealed by any audit conducted pursuant to this section within the time period specified in the audit results, or if no such time period is specified within a reasonable time period. Additional audits **may** also take place as part of normal internal reviews. These audits **may** include CA environmental controls, key management operations and Infrastructure/Administrative CA controls and certificate life cycle management.

8.2 Identity/qualifications of assessor

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

8.3 Assessor's relationship to assessed entity

Allianz User CA V **may** initiate third party audits.

8.4 Topics covered by assessment

8.4.1 Initial compliance audit

Allianz User CA V conducted the Allianz RCA initial compliance audit process prior to issuing certificates. The purpose of the Allianz Root CA initial compliance audit process is to determine that the Sub CA complies with the minimum eligibility, operational and technical requirements of the Allianz Root CA.

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 Root CA. After acceptance as participant of Allianz RCA system the participant will be required to conduct the Allianz Root CA 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 Allianz User CA V security infrastructure can be guaranteed continuously in all cases.

8.6 Communication of results

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

9 Other Business and Legal Matters

9.1 Fees

In particular, no fees are charged for the issuance, access, revocation, suspension and validation of issuer certificates and no fees are charged for the usage of the offered directory services. This arrangement is only suitable to the PKI participants named in section 1.4.

9.1.1 Certificate issuance or renewal fees

No fees are taken for issuance or renewal services provided by Allianz User CA V.

9.1.2 Certificate access fees

No fees are taken for access to PKI services provided by Allianz User CA V.

9.1.3 Revocation or status information access fees

No fees are taken for certificate status information services provided by Allianz User CA V.

9.1.4 Fees for other services

No fees are taken for other services provided by Allianz User CA V.

9.2 Financial Responsibility

The scope of this CPS does not include commercial issues such as the financial viability or stability of Allianz User CA V.

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

Confidential Information includes all information disclosed by Allianz User CA V to another PKI participant. Confidential information of Allianz User CA V **shall** include any information concerning the Allianz User CA V Services or the Allianz User CA V System or technology and information belonging to Allianz User CA V, which are marked “confidential” or “proprietary”. “Confidential Information” also includes the results of compliance audits provided to Allianz User CA V, cf. section 8.

9.3.2 Types of Information in particular considered confidential

Personal Information supplied to Allianz User CA V as a result of the practices described in this CPS **may** be covered by national government or other privacy legislation or guidelines. Access to confidential information by operational staff is on a need-to-know basis. Paper based records and other documentation containing confidential information is to be kept in secure and locked containers or filing systems, separate from all other records. Registration Information All registration records are considered to be confidential information, including:

- Certificate applications, whether approved or rejected
- Proof of identification documentation and details
- Certificate information collected as part of the registration records, but this does not act to prevent publication of certificate information in the certificate repository
- Any information requested by Allianz RCA when it receives an application from a third party to operate a CA within the Allianz RCA chain of trust.

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

9.3.3 Information not within the scope of confidential information

Certificates, Certificate revocation and other status information, Allianz User CA V repositories and information included within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 **shall** be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.4 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

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

9.4.3 Information not deemed private

All information not covered by Section 9.4.2.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual Property Rights

All trade marks, service marks, trade names, logos displayed are protected by copyright and other intellectual property laws and **may** not be reproduced or appropriated in any manner without the prior written consent of their respective owners.

9.5.1 Property in Certificates

Allianz Root CA and Allianz User CA V retain all Intellectual Property Rights in and to the Certificates and revocation information issued.

9.5.2 Certificate

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

9.5.3 Distinguished Names

Intellectual property rights in Distinguished Names vest in the assigning subscriber. A Subscriber retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Subscriber.

9.5.4 Copyright

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

9.6 Representations and Warranties

9.6.1 CA representations and warranties

Allianz User CA V makes no representations and gives no warranties regarding the financial efficacy of any transaction completed utilizing a certificate or any services provided by the Allianz User CA V in relation to the certificates.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

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

9.8.1 Safeguards

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

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

These measures include but are not limited to:

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

9.9 Indemnities

Cf. Section 9.8.

9.10 Term and Termination

9.10.1 Term Allianz Root CA certificate

The CPS becomes effective upon publication in the Allianz Root CA website. Amendments to this CPS become effective upon publication in the Allianz Root CA website.

9.10.2 Termination

This CPS as amended from time to time **shall** remain in force until it is replaced by a new version.

9.10.3 Effect of termination and survival

Upon termination of this CPS, Allianz User CA V participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

After termination, Allianz User CA V revokes all certificates issued.

After revocation, Allianz User 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. Upon receipt of a participant, Allianz User CA V **shall** confirm whether the Issuer Certificate of the participant is valid.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, commercially reasonable methods **shall** be used to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

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

9.12.1 Notification mechanism and period

Allianz User CA V reserves the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information.

Allianz User CA V decision to designate amendments as material or non-material **shall** be within Allianz User CA V sole discretion. Proposed amendments to the CPS **shall** appear on the Allianz User CA V.

9.12.2 Circumstances under which OID must be changed

If Allianz User CA V determines significant changes in the certificate practice, the Allianz User CA V can decide to change object identifier corresponding to a Certificate policy. The amendment **shall** enclose new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments **shall** not require a change in Certificate policy object identifier.

9.13 Dispute Resolution Procedures

To the extent permitted by applicable law, the Terms and Conditions or any Relying Party Agreements **shall** include a dispute resolution clause.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees and orders including, but not limited to, restrictions on exporting or importing software, hardware or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

In the event of a conflict between the provisions of this CPS and any related agreement, the terms of this document **shall** take precedence.

9.16.3 Severability

In the event that a clause or provision of this CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CPS **shall** remain valid.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

Allianz User CA V maintains contingency plans in force, including adequate back up and recovery procedures, to ensure that Allianz User 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 primary computer facilities or other operating facilities.

9.16.6 Other Provisions

Not applicable.

10 User CA V Certificate Profile

This certificate is a Root CA signed certificate is used to sign all issued User CA Certificates.

Field	Content	Critical*
1. X.509v1 Field		
1.1. Version	v3	
1.2. Serial Number	08	
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	“11:12:18 29 April 2015”	
1.5.2. Not After	“11:12:18 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 UserCA V”	
1.7. Subject Public Key Info	30 82 01 0a 02 82 01 01 00 e2 5c c1 38 36 b9 91 34 1d c9 37 b0 cd ef e1 ad f4 40 bc 65 ec 49 59 9e ba f1 f9 a5 ad d8 69 01 63 a7 d6 3d 33 ed 75 e8 94 e0 34 33 ef 80 df 09 a1 0b 69 f7 1d 0a 25 58 2b fd fa 33 a9 b1 58 d0 80 71 47 b9 3b 75 c5 91 a5 11 6e b5 7b c3 2c eb b0 e4 9d 43 cd 88 c6 3f 62 5b 08 c5 76 59 50 a1 f2 0f 39 0e 3e 72 66 58 d4 5b 7d 04 04 c6 4d b5 d6 a3 fd 58 e9 45 38 ee 98 0d 68 88 d5 c0 b7 1d f1 6f 84 b5 47 40 e8 5a a7 3b d5 e5 72 7d 09 dd fa 74 f1 0a 00 f8 5e e7 01 ed 7c fa 69 fa 87 cb 69 4c d3 f2 5b e5 71 7d 49 33 5f 11 b6 7f d5 35 d3 7d f7 84 21 43 71 63 56 ec bd c5 8a ec e1 55 63 a2 ee bd 34 13 fa 23 7a eb b0 0d 10 90 43 42 d3 20 10 73 01 77 45 9c 76 72 10 f7 97 d0 ad 48 28 f3 01 78 e7 ed 1e 2c 4f 1f e9 24 b0 76 14 e8 6e 84 c4 ce 1d 7c 20 1b 7f aa 30 54 a1 80 3f 6d 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	
3.2. Subject Key Identifier	7e dc f2 b2 b0 8f 6e bb a8 13 e9 54 d1 49 09 f5 18 78 c8 74	n
3.3. Key Usage		y
3.3.1. Digital Signature	Selected	

Field	Content	Critical*
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	1.3.6.1.4.1.7159.30.33	
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	SSL CA, SMIME-CA, Codesign CA	
3.8. CRL Distribution Point		n
3.8.1. 1st URL	http://rootca.allianz.com/crl/rootca3.crl	
Fingerprint	4c 11 cd 8c 22 df 22 36 7d 57 d1 ac ca 29 14 99 e3 ae e1 af	

*not used for attributes, only extensions

11 Appendix

11.1 Definitions and Acronyms

Authentication	The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.
CA-certificate	A certificate for one CA's public key issued by another CA.
Certificate policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.
Certification path	An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Practice Statement (CPS)	A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.
Computer Emergency Response Team (CERT)	A specialist unit of the technical information security department that is contact for topics related to the technical aspect of information security and takes care of the analysis and defense against hacking attacks and security-related incidents on the Allianz Technology SE.
CPS Abstract	A subset of the provisions of a complete CPS that is made public by a CA.
CPS Summary	Cf. "CPS Abstract".
Identification	The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and (2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification **may** be a certificate applicant,

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

	context of establishing the identity of certificate applicants.

For more definitions refer to **Error! Reference source not found.**.

11.2 Abbreviations

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

11.3 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
[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,"