Certification Practice Statement

For Allianz Infrastructure

Certification Authority V

(Infra-CA V)

Information Owner: Allianz Technology SE

Version: 1.2 / 28.06.2022

Document-ID: AZ-INFRA-CA V CPS

Classification: Public

Change management

Version	Description	Date	Author
0.9	Initial Draft	22.04.2015	Helmut Buss
0.9.1	Initial Review	24.04.2015	Aditya Kumar Yellai
0.9.2	Contact details, Algorithms updated	28.04.2015	Aditya Kumar Yellai
0.9.3	Final Draft	06.05.2015	Helmut Buss
0.9.4	Review	19.11.2015	Vera Kloepper
1.0	Final – With OID Update	10.05.2016	Aditya Kumar Yellai
1.1	• Changed company name to Allianz Technology SE • Updated references to new security policies, practical rules and practices • Updated trusted roles • Added Computer Emergency Response Team	07.04.2022	Thi Hang Nguyen
1.2	Review	28.06.2022	Helmut Buss

CONTENT

1 Introduction

This CPS is a statement of procedures and practices to support the use of certificates for the purpose of securing and authenticating electronic transactions using technical network components within Allianz. Allianz Infrastructure V CA, referred to as INFRA-CA-V hereafter, serves as an intermediate CA of the Allianz Root CA III (RCA III) to issue certificates. This document is organized as suggested by RFC 3647 [RFC3647] in order to ensure comparability.

1.1 Overview

The INFRA-CA-V is the preferred authority for issuing certificates for technical network and Infrastructure components within Allianz. Furthermore, its purpose is to issue and support network certificates on behalf of Allianz. For this purpose, the INFRA-CA-V provides the necessary architecture to support secure client-computer, servers, hosts, router, gateways, VPN, client-server-application (Web-Services) and similar network connections. In order to achieve an overview about the PKI components of INFRA-CA-V please see Figure 1 Overview INFRA-CA-V PKI components.

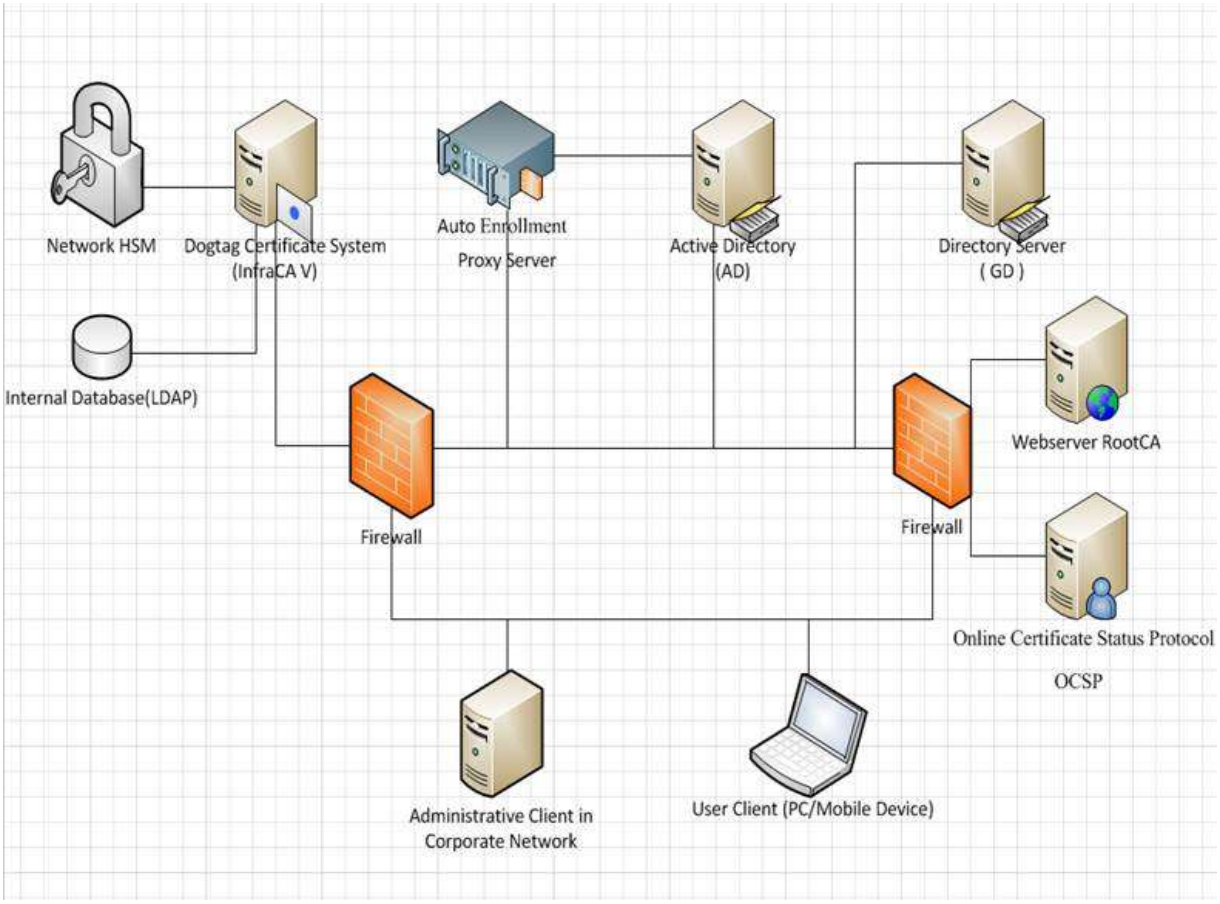

Figure 1 Overview INFRA-CA-V PKI components

1.2 Document name and identification

This CPS is referred to as the “Certification Practice Statement of Allianz Infrastructure V CA”

Object Identifier (OID) for this document is: 1.3.6.1.4.1.7159.30.32

1.3 Conventions

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

1.4 PKI participants

The INFRA-CA-V PKI System uses Dogtag Certificate System software for certificate issuance, management and secure system backup and storage.

1.4.1 Certification authorities

The INFRA-CA-V is designed to act as Sub-CA of Allianz RCA III and therefore interacts with no other subordinate PKI in the Allianz RCA III hierarchy.

1.4.2 Registration authorities

Included in INFRA-CA-Vs PKI is a web-based Registration Authority which allows the devices and applications respectively their administrators to request End-Entity certificates. The RA interface is based on Dogtag Certification Authority System software.

1.4.3 Subscribers

INFRA-CA-V issues End-Entity certificates only. Subscribers are devices and applications throughout Allianz as there are:

- Web Server
- Domain Controller
- Router
- Application / code
- IPSec / VPN
- Web-Services (Client authentication)
- End Entities (PS / Mobile Devices)
- etc.

While the Domain Controllers take care for their certificates automatically, in the other cases the respective administrators are responsible for their devices or applications.

1.4.4 Relying parties

Allianz network infrastructure relies on the certificates issued by INFRA-CA-V. Any application employing secure communication within the Allianz is potentially affected.

1.4.5 Other participants

External contractors **may** act as participants of the INFRA-CA-V PKI.

1.5 Certificate usage

1.5.1 Appropriate certificate usage

INFRA-CA-V Certificates **may** be used to secure network connections by providing means for authentication and encryption.

Additionally certificates issued by INFRA-CA-V **may** be used for code signing.

1.5.2 Prohibited certificate usage

Certificates issued INFRA-CA-V **must** only be used for the purposes and applications enlisted above (Appropriate Certificate Usage). Other usages **must** be approved in advance by written permission of INFRA-CA-V administration.

1.6 Policy administration

1.6.1 Organization administering the document

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

1.6.2 Contact person

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

Allianz Technology SE

Allianz PKI Team

Email: *pki-support@allianz.de*

1.6.3 Person determining CPS suitability for the policy

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

The Allianz CA Owner **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.

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 INFRA-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

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

2.2 Publication of certification information

INFRA-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

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

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

3 Identification and authentication

To ensure the integrity and trustworthiness of operations throughout the PKI hierarchy, INFRA-CA-V complies with the practices for intermediate CAs of Allianz Root CA III.

3.1 Naming

3.1.1 Types of names

A certificate issued by INFRA-CA-V contains in the Subject field a distinguished name,that is in compliance with the X.501 standard and follows ASN.1 syntax structures.

3.1.2 Need for names to be meaningful

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

In case of network devices, the alternative subject name is set to the DNS-Name of the device.

For examples concerning the name conventions used for INFRA-CA-V certificates please consult the Infra CA V Certificate Profile of this document.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation

3.1.4 Rules for interpreting various name forms

In case of network devices or applications the alternative subject name always contains the respective DNS Name.

Code signing certificates contain the email address of the responsible person (who is in charge of the corresponding private key) in the Distinguished Name.

3.1.5 Uniqueness of names

The RA web based registration interface ensures the uniqueness of the certificates Distinguished Names by checking the requested name against the Allianz Global Directory.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

Allianz Technology SE Security delegates responsibility for legitimating applicants for certificates of INFRA-CA-V to a PKI Team within Allianz Technology SE which can be contacted via email: pki-support@allianz.de .

Access to the INFRA-CA-V Registration Authority web-interface is available to authorized persons only. After requesting authorization by filling out the respective forms provided by INFRA-CA-V access to the RA interface is granted based on authentication by the certificate authentication method respectively the corresponding Allianz Global Directory.

Authorized administrators or developers are responsible for the reliable identity of their devices or applications.

INFRA-CA-V is configured not only to support SSL web server certificates but also certificates of technical systems as routers, gateways, hosts or VPN connections or other systems mentioned in section 1.4.3. Therefore, application forms adapted to SSL web servers and IT infrastructure components are supported by INFRA-CA-V.

In case of Domain Controllers the request authentication is handled by the underlying Microsoft infrastructure (AD-Domain membership/Trust relationships).

To obtain an INFRA-CA-V certificate, the applicant **must**:

1. Generate a secure and cryptographically sound key pair,

2. Agree to all terms and conditions of the INFRA-CA-V CPS approved by CA Owner,
3. Complete and submit the certificate application form, providing all information requested by INFRA-CA-V without any errors, misrepresentation, or omissions.

Relevant certificate extensions are default values in the application form and cannot be changed by the applicant. INFRA-CA-V assures the traceable connection from certificate applicant to the network unit applied for. Advanced verifications of application data are not performed by INFRA-CA-V.

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.

3.2.2 Authentication of organization identity

INFRA-CA-V only issues certificates for Allianz internal devices and applications. Organizational identity is validated based on internal directories and network access controls.

3.2.3 Authentication of individual identity

Persons requesting certificates for network devices or applications are authenticated via their network connection based on the NTLM/Certificate authentication method and the Allianz Global Directory.

Domain Controllers employ their native authentication methods.

3.2.4 Non-verified subscriber information

INFRA-CA-V employs policy filters to overwrite any data contained in the certificate request except the DNS name and the public key.

3.2.5 Validation of authority

Authority of requestors is ensured by the use of authorization forms that **must** be filled out by the subscriber and signed by e.g. project manager, line manager etc. before any certificate request is allowed.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authorization for re-key requests

Re-key requests are handled in the same manner as initial certificate request.

3.3.1 Identification and authentication for routine re-key

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

No re-keying after revocation is allowed.

3.4 Identification and authorization for revocation requests

Revocation of certificates is done by the INFRA-CA-V support. Support ensures identity and authorization for revocation by asking the direct line-manager or equivalent for confirmation.

4 Certificate life-cycle operational requirements

The Certificate Management Life Cycle (CMLC) represents the intermediate-level certificate management process within the Allianz RCA System. It consists of 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 INFRA-CA-V life span. The INFRA-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.

4.1 Certificate application

The department or group within Allianz that is responsible for operating the network component, has to authorise the INFRA-CA-V certificates requestor. The authorisation is subject to be approved by PKI Team. Please contact pki-support@allianz.de for inquiries.

4.1.1 Who can submit a certificate application?

Only people holding an authorization issued by Allianz Technology SE CA Administration and approved by LEGBA or head of department of the applicant **may** request certificates at INFRA-CA-V.

Additionally dedicated technical user for internal WebServers, Domain-Controllers and Routers **may** automatically request certificates.

4.1.2 Enrollment process and responsibilities

To obtain a certificate of INFRA-CA-V, an authorized applicant can submit the request by pasting the certificate signing request with format PKCS #10 or DER into the "Certificate Request Input" form on Certificate Manager web service.

The requestor can specify up to 5 DNS names and 2 IP addresses of the network unit in the application form. By pressing the Submit button, the request is sent for signing to INFRA-CA-V and a link for receiving the INFRA-CA-V certificate will be provided.

For router certificate request, a SCEP adapter is installed. In this case an one time password could be obtained via web interface by authorized users to retrieve certificates automatically.

When the internal server certificate is about to expire, the renewal certificate will be sent to an authorized technical user automatically.

MS-Windows client computer, MS-Windows server and other objects that are authenticated in the Active Directory under the Allianz ADS Forest (rootdom.net), can retrieve automatically (auto-enrollment) special designed certificates.To ensure a granular authorization and to accomplish further needs of participants other certificate profiles could be designed.

Participants

- **shall** be aware of all rights and obligations for certificate operating within the INFRA-CA-V.
- **shall** ensure the safety, confidentiality, and integrity of their own private keys, which were generated and stored in a trustworthy environment.

- **shall** not interfere with or damage, or attempt to interfere with or damage, the operational infrastructure of the Allianz RCA III System or any component thereof.

The INFRA-CA-V

- has been structured and is operated in such a manner as to minimise the risk of compromise or wilful damage by a certificate owner
- **shall** define and implement security control measures that monitor the INFRA-CA-V operation. This monitoring system can detect the attempt to damage the infrastructure and collect sufficient evidence for prosecution process. PKI operating surveillance belongs to the operational concept of Allianz RCA and is obligatory for the INFRA-CA-V.

4.2 Certificate application processing

Certificate applications are processed by INFRA-CA-V support personal.

4.2.1 Performing identification and authentication functions

Identification and authentication of subscribers is performed by the INFRA-CA-V support staff.

4.2.2 Approval or rejection of certificate applications

Certificate applications are rejected in case the certificate application and the certificate request do not match, or the requested DNS-name has no valid directory entry. Otherwise authorized certificate applications are approved.

4.2.3 Time to process certificate applications

In general certificates applications are issued within one work day.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

INFRA-CA-V issues solely non personal certificates for network units. The INFRA-CA-V adjusts the relevant policies, signs the request, and publishes in a secure key store.

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

Dependent on the use of the certificate different notification mechanisms are implemented. In general the issued certificate will be sent to the requesting party via Email. In case of certificates for web-services, the certificate will be transmitted as part of a java keystore that is sent via encrypted email to the subscriber. Domain Controllers etc. receive the certificates issued to them automatically via an automated request process.

4.4 Certificate Acceptance

Upon certificate acceptance the subscriber commits to the followings:

- The Subscriber agrees to be bound by the provisions of this CPS. This CPS is presented to the subscriber at the time of registration.
- The Subscriber agrees to exercise all reasonable measures to protect his/her private key and will not allow unauthorised access or use of this private key.
- The proof of the private key possession of the subscriber is given by verifying digital signature.
- All representations made by the subscriber during registration and receipt of the certificate is true and accurate.

4.4.1 Conduct constituting certificate acceptance

The subscriber constitutes his/her certificate acceptance by installing the INFRA-CA-V certificate.

4.4.2 Publication of the certificate by the CA

Certificates for web-services issued by INFRA-CA-V are published in the Group Directory.

4.4.3 Notification of certificate issuance by the CA to other entities

Before implementing the INFRA-CA-V web-services certificates, the target deployment environment **shall** be informed.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

Subscribers of INFRA-CA-V are network devices and applications that use their private key and the corresponding certificate for authentication and encryption as specified in the key usage attributes of the certificate profile.

Certificates can only be used during their lifetimes (given validity period), as long as they are NOT revoked.

The participant's private key **must** only be used for applications according to those utilization methods stated in the certificate.

The following utilization methods are permitted:

- Authentication of user or application data and technical systems (utilization method: digital signature)

- 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 (utilization method: dataEncryption, KeyEncryption)

4.5.2 Relying party public key and certificate usage

The private 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 keys can only be used for certificate based authentication and encryption.

4.6 Certificate Renewal

In general certificate renewal is not supported by INFRA-CA-V. Exceptions (certificate renewal instead of rekey) are only permissible based on well-founded reasons and require a written approval by responsible Information Security Officer.

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

Certificate re-key is currently implemented for Web Server Certificates.

4.7.1 Circumstance for certificate re-key

Re-key is conducted at defined time frame before the expiry of the current certificate.

4.7.2 Who may request certification of a new public key

See initial certificate application (4.1 Certificate application).

4.7.3 Processing certificate re-keying requests

See initial certificate application (4.1 Certificate application).

4.7.4 Notification of new certificate issuance to subscriber

See initial certificate application (4.1 Certificate application).

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See initial certificate application (4.1 Certificate application).

4.7.6 Publication of the re-keyed certificate by the CA

See initial certificate application (4.1 Certificate application).

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

INFRA-CA-V does not support certificate modification. Any desired change to certificate content requires the issuance of a new certificate.

4.8.1 Circumstance for certificate modification

No stipulation.

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

INFRA-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 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.

4.9.2 Who can request revocation

Certificate revocation can be initiated by:

- INFRA-CA-V
- RCA III
- The certificate owner or his/her legal presentative can request revocation of their certificates for any reason or for no reason.

4.9.3 Procedure for revocation request

This section describes the procedures in which revocation is requested by end entity, Allianz RCA III or INFRA-CA-V.

To process revocation the following steps are required:

- Receiving and authenticating the revocation request.
- Revocation of the certificate.
- Publishing certificates in its CRL and replicating them in the certificate repository.
- Issuing a notice containing the certificate details and the date and time of revocation to the participant. The notice **must** not include the reason for revocation.

Revoked certificates are not deleted from the repository of INFRA-CA-V.

4.9.3.1 Certificate Owner Duties

The owner of a revoked certificate has to safeguard the private key associated with the revoked certificate, until the date of certificate revocation.

4.9.4 Revocation request grace period

There is no revocation request grace period foreseen, in specific cases there **may** be further inquiries with the subscriber before revocation.

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

Revocation requests are processed within one business day.

4.9.6 Revocation checking requirement for relying parties

The CRL for verifying the status of certificates issued by INFRA-CA-V is available at:

http://rootca.allianz.com/crl/infra5.crl

Certificate validity checking **must** be performed in accordance with the operating rules published by Allianz RCA III. The relying party **shall** do signature verification and certificate chain verification in standard PKI fashion. This includes the verification of the signature and path validation on the certificate chain associated with the signature.

4.9.7 CRL issuance frequency (if applicable)

The CRLs created by the INFRA-CA-V will be issued to the public repository on at least monthly basis and whenever a change in the CRL occurred.

4.9.8 Maximum latency for CRLs (if applicable)

Four weeks.

4.9.9 On-line revocation/status checking availability

Status information on revoked certificates is available via the online accessible CRL and OCSP.

4.9.10 On-line revocation checking requirements

See 4.9.6

4.9.11 Other forms of revocation advertisements available

The CRL published on rootca.allianz.com is also available in the Active Directory belonging to INFRA-CA-V, which is accessible from internal networks only.

4.9.12 Special requirements re key compromise

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

4.9.13 Circumstances for suspension

A participant certificate will not be suspended.

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

INFRA-CA-V provides a web page hosted CRL and OCSP service for verifying the status of all certificates issued by INFRA-CA-V.

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

INFRA-CA-V CRL-file is distributed via rootca.allianz.com web server. Its availability is under the responsibility of RCA III administration.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

In the event of permanent termination of INFRA-CA-V operation, all subscribers, participants and relying parties are promptly notified. Issued certificates are revoked with the date of the cessation becoming final. In case of termination by the subscriber, the certificate is revoked.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

The INFRA-CA-V private key is stored in a HSM which does not provide any means to extract the private key. Anyway key escrow or recovery is not permitted.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

4.12.3 Facility, Management, and Operational Controls

No stipulation.

4.13 Physical Security Controls

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

The physical infrastructure of INFRA-CA-V houses in one secured data center. This includes the complete productive PKI, including the CA, Registration Authority, key generation, web server, and value added services in the same highly secured facility. All these systems (CA Server and Hardware Security Modules) are located in a highly secured DMZ (Secure Management Area) in the data centre.

4.13.1 Site location and construction

The CA environment is hosted in two geographical redundant secure facilities for HA and disaster recovery. The Certification Authority, Registration Authority and Backup Systems operate within physically secured areas that meet the standards identified in the Allianz Functional Rule for Information Security [AZ-AFRIS] and Guideline for Physical Security [AZ-GPS]

4.13.2 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 implementation guides.

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

4.13.3 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.

4.13.4 Water exposures

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

4.13.5 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.

4.13.6 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.

4.13.7 Waste disposal

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

4.13.8 Off-site backup

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

4.14 Procedural Controls

Access controls and procedures are set in place to ensure that one person acting alone cannot circumvent the entire system.

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

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

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

	• Inspect the management of cryptographic material to ensure security policies, practices, and procedures are followed.
Safe User	• Owns the safe PIN and/or key

4.14.2 Number of persons required per task

The tasks in INFRA-CA-V operation and administration ca be executed by only one specially authorized administrator. An exception applies for the handling of the CAs private key. The HSM is configured to force dual control for private key maintenance.

4.14.3 Identification and authentication for each role

The INFRA-CA-V system is based on Certification Authority system which supports login and authentication based on certificate Users being a member of the CA-Administrator Group are able to perform the tasks of their role.

4.14.4 Roles requiring separation of duties

There are no roles established which require any separation of duties.

4.15 Personnel Controls

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

4.15.1 Qualifications, experience and clearance requirements

The recruitment and selection procedures for INFRA-CA-V personnel take background check, qualifications, experience of potential candidates and the security clearance requirements of each position into account.

4.15.2 Background check procedures

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

Operations personnel **must** notify the Computer Emergency Response Team when a process or action causes a critical security event or discrepancy.

4.15.3 Training requirements

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

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

4.15.4 Retraining frequency and requirements

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

4.15.5 Job rotation frequency and sequence

No stipulation.

4.15.6 Sanctions for unauthorized actions

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

4.15.7 Independent contractor requirements

No stipulation.

4.15.8 Documentation supplied to personnel

All INFRA-CA-V staff has access to all documentation of CA system and training material.

4.16 Audit Logging Procedures

4.16.1 Types of events recorded

The integrity of the INFRA-CA-V is achieved by activating, collecting and monitoring the auditing log for these events:

- Backup and restore certificate Database
- Change CA configuration
- Change CA security settings
- Issue and manage certificate requests
- Revoke certificates and publish CRL
- Store and retrieve archived key (not applicable in our configuration)

4.16.2 Frequency of Processing Log

Audit logs are processed in case of suspected errors, malfunctions or any relevant incident. In general monthly reviews by CA administration staff are set forth.

4.16.3 Retention period for Audit Log

Audit logs **must** be retained for at least ten years.

4.16.4 Protection of Audit Log

Audit logs are accessible for authorized personnel only. CA administrators are entitled to access the logs as part of their CA maintenance work. While available on the CA system, the audit logs are protected by the physical access controls of the secure location on one hand and the network protection provided by the DMZ on other hand. Access to the CA system is granted to CA administrators only.

4.16.5 Audit log backup procedures

A regular backup of the audit logs is executed automatically by the TSM client, which is installed on the CA system.

4.16.6 Audit collection system (internal vs. external)

INFRA-CA-V does not participate in any audit collection system. Audit logs are stored externally in the TSM backup system provided by Allianz Technology SE.

4.16.7 Notification to event-causing subject

Handling of incidents follows the Information Security Practice for Incident Handling [AZ-ISINC][AZ-ISINC][AZ-ISINC].

4.16.8 Vulnerability assessments[AZ-ISINC]

No stipulation.

4.17 Records Archival

INFRA-CA-V maintains an archive of relevant records as defined in the relevant Allianz RCA documents.

4.17.1 Types of records archived

The following types of information are to be recorded and archived automatically by INFRA-CA-V software:

- Audit logs

- Certificate request information
- Certificates, including CRLs generated
- Complete backup records. No backup of private keys
- Copies of e-mail logs
- Formal correspondence
- Customer application records

4.17.2 Retention period for archive

INFRA-CA-V archive will be kept available for 10 years after expiration of the CA certificate.

4.17.3 Protection of archive

While available on the CA system, the archive is only accessible by authorized personnel. Protection is implemented via access control to the system, the physical and network controls provided by the DMZ infrastructure. The backup of the archive is stored within the TSM system of Allianz Technology SE. Protection within the TSM system is implemented only on procedural basis.

4.17.4 Archive backup procedures

The backup of INFRA-CA-Vs archive is performed automatically by the TSM client which is installed on the CA system.

4.17.5 Requirements for time-stamping of records

In order to guarantee the traceability of records, time-stamps are necessary. INFRA-CA-V uses the time-stamps generated by the TSM during backup.

4.17.6 Archive collection system (internal or external)

The INFRA-CA-V archive is produced automatically by the CA system. External storage is implemented via the TSM client that transfers the archive daily to the TSM Servers provided by Allianz Technology SE.

4.17.7 Procedures to obtain and verify archive information

Authorized personal can access the archive in the TSM via the TSM client. It provides methods to restore the complete archive and as well as parts of it. The files can be sorted by date. TSM functionality is used for archive verification.

4.18 Key Changeover

The validity period of the INFRA-CA-V certificate is 15 years. The validation period of end entity certificates are limited to one or two years. Upon expiration of the certificate a new key pair and certificate will be generated.

4.19 Compromise and Disaster Recovery

The INFRA-CA-V and every CA under RCA:

1. Has to establish and maintain detailed documentation covering:
    - Contingency & disaster recovery plan, including key compromise, hardware, software and communications failures, and natural disasters such as fire and flood. See also Allianz Business Continuity Management Recovery Strategy Guide [AZ-BCMG].
    - Configuration baseline, including operating software, and PKI specific application programs.
    - Backup, archiving and offsite storage procedures.
2. Provides the above documentation on the request of persons conducting a security, compliance or CPS practices audit
3. Provides appropriate training to all relevant staff in contingency and disaster recovery procedures
4. Periodically tests the 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.

4.19.1 Incident and compromise handling procedures

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

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

The general disaster recovery plan of Allianz applies.

4.19.3 Entity private key compromise procedures

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

- Inform Root CA Council
- Revoke INFRA-CA-V certificate
- Inform subscribers via intranet and e-mail
- Generate new INFRA-CA-V key pair and certificate
- Publish new certificate

If a subscriber's private key becomes compromised, the responsible person **must** inform the INFRA-CA-V support in order to revoke the certificate.

4.19.4 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 INFRA-CA-V in order to make accessible the logical records kept within the software. Therefore the INFRA-CA-V has:

1. Identified individuals authorised to initiate disaster recovery action
2. Identified major elements at risk, for example
    - Operational hardware
    - Certification authority software application
    - Logical records
    - Registration records
3. Identified criteria that **may** prompt disaster recovery initiation
4. Considered secondary precautionary measures that **may** be required, such as:
    - a backup site
    - trained backup staff

5. Developed recovery actions and timeframes
6. Prioritised recovery actions from most significant to least significant
7. Maintained a record of the hardware and software configuration baseline
8. Maintained records of the necessary equipment and procedures required to recover from an unexpected event such as a hardware failure, including the intended maximum period that the system is down.

4.20 CA or RA termination

When it is necessary to terminate the INFRA-CA-V service, the impact of the termination is to be minimised as much as possible in light of the prevailing circumstances. INFRA-CA-V **shall** at least provide as much prior notice as is practicable and reasonable to participants and relying parties.

5 Technical Security Controls

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

5.1 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 INFRA-CA-V in order to meet the operation requirements explained in chapter 4. The cryptographic procedures and records **must** correspond to the status quo of security measures of cryptographic procedures and to the respectively valid legal stipulations.

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

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

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

5.1.1 Key pair generation

The keys used by INFRA-CA-V CA Server (CA signing and server key) are generated using the HSM key generator. This is integrated in INFRA-CA-V Certification Authority System Software via CSP. End entity keys with a minimum RSA key length of 2048 bits are generated in the requestors systems. Key pairs for web-services are generated using a workflow provided by the RA system.

5.1.2 Private Key delivery to subscriber

Only in case of web-services certificates request, the key pair need to be delivered together with the certificate to the subscriber. The key pair generated by the RA interface is stored together with the issued certificate in a password protected java keystore. This file is sent via encrypted email to the subscriber. The password required to open the keystore is provided in a separate email.

5.1.3 Public key delivery to certificate issuer

INFRA-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. As described above, for web-services the key pair is generated within the RA web-interface, which delivers the public key to the CA.

5.1.4 CA public key delivery to relying parties

The INFRA-CA-V public key respectively CA certificate is published in Allianz Global Directory and it **may** be downloaded from the rootca.allianz.com website.

5.1.5 Key sizes

The INFRA-CA-V requires at least 2048 bit RSA keys for certification. Exceptions are possible in well-founded circumstances.

5.1.6 Public key parameters generation and quality checking

No stipulation.

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

Key usage are configured in certificate templates of the CA system.

5.2 Private Key Protection and Cryptographic Module Engineering Controls

INFRA-CA-V's secret signature key is stored in a FIPS 140-2 Level 3 compliant Hardware Security Modules cluster and is not subject to automated backup procedures.

End-entity private keys are stored in a secure way using key store which locate on their individual network components. The subscriber is responsible for the secure storage of the secret key on the network unit.

5.2.1 Cryptographic module standards and controls

For details and information about the employed HSM please refer to the internally accessible information.

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

In order to export the encrypted private key, e.g. for transfer to a different HSM, multiple person control is implemented.

5.2.3 Private Key escrow

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

5.2.4 Private Key backup

The CAs private key is kept redundant on HSM devices.

5.2.5 Private Key archival

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

5.2.6 Private Key transfer into or from a cryptographic module

Three persons are required to move the private key to a new HSM device (ISO, Operator and Partition owner).

5.2.7 Private Key storage on cryptographic module

INFRA-CA-V stores CA private key in HSMs.

5.2.8 Method of activating private key

The CA private key is activated by using USB-Key with PIN which is accessible for administrators of CA system only.

The private keys intended for use with web-services are protected by java keystores which are activated by entering the valid password.

5.2.9 Method of deactivating private key

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

5.2.10 Method of destroying private key

When conducting the key destruction, multiple control applies. The private key on all redundant devices will be destroyed in succession.

5.2.11 Cryptographic Module Rating

INFRA-CA-V's private key is stored in a FIPS 140-2 Level compliant Hardware Security Modules cluster.

5.3 Other Aspects of Key Pair Management

5.3.1 Public Key Archival

INFRA-CA-V archives all certifies that contain the public keys.

Expired certificates (and CRLs if used) are archived. Archived certificates can only be accessed in authorised circumstances, for example at the participant's request or where a properly constituted subpoena or warrant is produced.

Archived certificates are to be:

- Archived on tamper evident media
- Archived for a minimum period of seven years from the date of expiry
- Securely destroyed at the end of the archive period.

5.3.2 Certificate operational periods and key pair usage periods

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

- CA key and certificate: 15 years
- Subscriber key and certificate: 2 years

5.4 Activation Data

5.4.1 Activation data generation and installation

Activation data for the INFRA-CA-V key is generated at installation in form of USB partition key. Those keys have to be initialized before they are used for private key generation and access in a specific partition of the HSM.

The activation data for java keystore in the web-service certificate request process is generated automatically by the RA web-interface and complies to the password rules as laid out in section User Access Management of Allianz Functional Rule for Information Security [AZ-AFRIS].

5.4.2 Activation data protection

The HSM partition keys are stored securely by the respective partition owners.

5.4.3 Other aspects of activation data

No stipulation.

5.5 Computer security controls

5.5.1 Specific computer security technical requirements

The following computer security controls have been implemented and are enforced by the operating systems and the INFRA-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 INFRA-CA-V systems including data.

5.5.2 Computer security rating

The hardened operating system of INFRA-CA-V and its CA software is approved by Allianz RCA III. Dedicated system audits or (penetration-) tests can be initiated by security department.

5.6 Life Cycle Security Controls

5.6.1 System development controls

The INFRA-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 AG.

5.6.2 Security management controls

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

5.6.3 Life cycle security controls

Any configuration modifications or upgrades of the INFRA-CA-V **must** be tested, documented and approved in advance. A contingency plan is in force, which includes adequate redundancy, back-up and recovery procedures.

5.7 Network Security Controls

The INFRA-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 authorised Allianz Organisation Units are connected to this network by further firewalls. No direct connection to the internet is permitted.

5.8 Timestamping

No stipulation.

6 Certificate, CRL, and OCSP Profiles

6.1 Certificate profile

This section specifies the profile template for INFRA-CA-V certificates and end-entity certificates used within the Allianz RCA III PKI. It is currently recommended that network certificates which are be used within the Allianz RCA framework **should** be issued by this Allianz Infrastructure CA V in Allianz.

There are different certificate profiles in use depending on the intended use of the certificate. You will find the Name and Form of them under 6.1.4 Name forms.

6.1.1 Version numbers

INFRA-CA-V issues X.509 version 3 certificates in accordance with ITU-T Rec. X.509 (1997) [ITU-T]. This standard is identical to ISO/IEC 9594-8 (1997).
The contents of the certificates issued by INFRA-CA-V are shown in the Appendix.

6.1.2 Certificate extensions

The following certificate extensions **must** be critical:

- KeyUsage

For KeyUsage and BasicConstraints (of CA-certificates), the stipulations of the ISIS-MTT-profiling **must** be adhered to (see [ISIS/MTT] ISIS/MTT Version 1.1, Part 1. Table 12: KeyUsage).

6.1.3 Algorithm object identifiers (OIDs)

INFRA-CA-V issues certificates using the following Algorithm object identifiers:

- Signature Algorithm: sha256WithRSAEncryption
- Public Key Algorithm: rsaEncryption

6.1.4 Name forms

Certificates issued by the INFRA-CA-V System enclose the full X.501 distinguished name of the certificate issuer. Certificates **must** contain a Subject DN.

Due to different requirements arising from the certificate use the certificate subjects' DN varies with the certificate usage:

Codesigning:

E = email of the person in charge

CN = organisational unit

OU = organisational unit

O = organisation

C = country

Domain-Controller:

CN = DNS Name

Router:

CN = DNS Name

OU = organisational unit

O = organisation

C = country

Web-Server:

CN = DNS Name

O = Allianz

C = country

Web-Service:

CN = Web-Service Name

OU = Webservice

O = organisation

C = country

6.1.5 Certificate policy object identifier

No stipulation.

6.1.6 Usage of Policy Constraints extension

No stipulation.

6.1.7 Policy qualifiers syntax and semantics

No stipulation.

6.1.8 Processing semantics for the critical Certificate Policies extension

No stipulation.

6.2 CRL profile

6.2.1 Version number(s)

Only X.509 Version 2 CRLs are supported.

6.2.2 CRL and CRL entry extensions

No stipulation.

6.3 OCSP profile

6.3.1 Version number(s)

No stipulation.

6.3.2 OCSP extensions

OCSP Request Extensions	
Nonce	non-critical extension, prevention of replay attacks
AcceptableResponses	non-critical extension, kind of expected response type
Extended revoked extentions	non-critical extension, response contains a "revoked" status for a non-issued certificate.

7 Compliance Audit and other assessment

The following procedures apply to INFRA-CA-V as intermediate CA of RCA. Clients of INFRA-CA-V are not subject to the audit procedures described in this section.

7.1 Frequency or circumstances of assessment

There exist an initial and an ongoing audit procedure. The initial audit of the INFRA-CA-V PKI infrastructure is conducted by RCA III prior to issuing INFRA-CA-V certificates. The purpose of the audit process is to determine that INFRA-CA-V complies with the minimum eligibility, operational and technical requirements of the Allianz RCA Operating Rules.

The ongoing assessments are yearly repeated and are to be carried out by INFRA-CA-V with the results of the reviews reported to Allianz RCA. The audit procedures are conducted according to the internal Allianz audit and revision standards.

7.2 Identity/qualifications of assessor

Any company or person contracted to perform a security audit on INFRA-CA-V **must** have sufficient experience in the application of PKI and cryptographic technologies.

7.3 Assessor's relationship to assessed entity

Allianz RCA III **may** initiate third party audits.

7.4 Topics covered by assessment

The topics covered by a compliance audit will include but not be limited to:

- Security policies and planning
- Physical security
- Technology evaluation
- Certificate authority services administration
- Personnel vetting
- Relevant CPS
- Logical access controls
- Systems management
- Configuration management
- Technology implementation

7.5 Actions taken as a result of deficiency

Allianz RCA decides in each individual case of deficiency what kind of actions **should** be taken in order that the security of the INFRA-CA-V security infrastructure can be guaranteed continuously in all cases.

7.6 Communication of results

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

8 Other Business and Legal Matters

8.1 Fees

No stipulation.

8.1.1 Certificate issuance or renewal fees

No stipulation.

8.1.2 Certificate access fees

No stipulation.

8.1.3 Revocation or status information access fees

No stipulation.

8.1.4 Fees for other services

No stipulation.

8.1.5 Refund policy

No stipulation.

8.2 Financial Responsibility

No Stipulation.

8.2.1 Insurance coverage

No stipulation.

8.2.2 Other assets

No stipulation.

8.2.3 Insurance or warranty coverage for end-entities

No stipulation.

8.3 Confidentiality of business information

8.3.1 Scope of confidential information

All data owned by INFRA-CA-V is classified and marked with the data classification level in compliance with Allianz Information Security Framework. In general INFRA-CA-V operational data is classified as "internal", access is granted on a need-to-know basis only. This also includes the results of compliance audits provided by INFRA-CA-V.

8.3.2 Information not within the scope of confidential information

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

8.3.3 Responsibility to protect confidential information

No stipulation.

8.4 Privacy of Personal Information

INFRA-CA-V does not use any personal information beside the responsible persons email in case of issuing code signing certificates.

8.4.1 Privacy plan

No stipulation.

8.4.2 Information treated as private

No stipulation.

8.4.3 Information not deemed private

No stipulation.

8.4.4 Responsibility to protect private information

No stipulation.

8.4.5 Notice and consent to use private information

No stipulation.

8.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

8.4.7 Other information disclosure circumstances

No stipulation.

8.5 Intellectual property rights

INFRA-CA-V warrants that it is in possession of, or holds licenses for the use of hardware and software required in support of this CPS. All intellectual property rights, including all copyright, in all certificates belong to and will remain the property of INFRA-CA-V. Intellectual property rights in Distinguished Names vest in the assigning subscriber. Copyright in the Object Identifiers (OID) for the INFRA-CA-V System vests solely in INFRA-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 INFRA-CA-V infrastructure, or in accordance with the relevant this CPS.

8.6 Representations and Warranties

No stipulation.

8.6.1 CA representations and warranties

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

8.6.2 RA representations and warranties

No stipulation.

8.6.3 Subscriber representations and warranties

No stipulation.

8.6.4 Relying party representations and warranties

No stipulation.

8.6.5 Representations and warranties of other participants

8.7 Disclaimers of Warranties

8.8 Limitations of Liability

In no event **shall** a member of Allianz be liable for any indirect, special, incidental, or consequential damages, or for any loss of profits, loss of data, or other indirect, consequential, or punitive damages, arising from or in connection with the use, delivery, license, performance, or non-performance of certificates, digital signatures, or any other transactions or services offered or contemplated by this CPS, even if Allianz has been advised of the possibility of such damages.

8.9 Indemnities

By accepting a certificate, the subscriber agrees to indemnify and hold Allianz and its employees, agents and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorney's fees, that Allianz, its employees, agents or contractors **may** incur, that are caused by the user or publication of the certificate, and that arises from (i) falsehood or misrepresentation of fact by the subscriber or a person acting upon instructions from anyone authorised by the subscriber (ii) failure by the subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive Allianz or any person receiving or relying on the certificate or (iii) failure to protect the subscriber's private key, to use a trustworthy system, or to otherwise take precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the subscriber's private key.

8.10 Term and termination

8.10.1 Term

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

8.10.2 Termination

In the event that it becomes necessary to terminate the INFRA-CA-V, all certificates **may** need to be revoked prior to the shutdown. The last duty of the terminated INFRA-CA-V is to publish a finalised CRL.

8.10.3 Effect of termination and survival

After revocation, INFRA-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.

Where practical, key and certificate revocation **should** be timed to coincide with the progressive and planned roll out of new keys and certificates by a successor INFRA-CA-V.

8.11 Individual notices and communications with participants

8.12 Amendments

The CA Owner is the responsible authority for initial publication and acceptance of changes in this CPS.

There are two possible types of policy change:

- The issuance of a new policy
- A change to or alternation of an existing policy.

8.12.1 Procedure for amendment

If an existing CPS requires re-issuance, the change process employed is the same as for initial publication. Note that the new OID issued for a CPS change differs from the previous OID only in the CPS version number.

8.12.2 Notification mechanism and period

New or amended CPSs are published on the internet web site designated for Allianz RCA documentation. CA Owner endorses the INFRA-CA-V CPS and all changes to this CPS. If a new CPS is approved, signed and distributed by Allianz INFRA-CA-V, all earlier versions of the CPS are superseded.

8.12.3 Circumstances under which OID **must** be changed

No stipulation.

8.13 Dispute Resolution Procedures

In the event of any dispute, or disagreement between two or more certificate holders, arising out of or relating to this CPS, Allianz has binding authority to resolve such disputes.

8.14 Governing law

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

8.15 Compliance with applicable law

Cf. section 9.5.

8.16 Miscellaneous Provisions

8.16.1 Entire agreement

No stipulation.

8.16.2 Assignment

In the event of a conflict between the provisions of this CPS and RCA III CPS, INFRA-CA-V provisions **shall** take precedence.

8.16.3 Severability

No stipulation.

8.16.4 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 provided by Allianz INFRA-CA-V **shall** govern.

8.16.5 Force Majeure

INFRA-CA-V maintains contingency plans in force, including adequate backup and recovery procedures, to ensure INFRA-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 INFRA-CA-V primary computer facilities or other operating facilities.

8.17 Other Provisions

8.17.1 Rights of investigation

The INFRA-CA-V reserves the right to:

- Investigate under applicable law all the circumstances behind any compromise or suspected compromise concerning the operation of servers using INFRA-CA-V certificates.
- Any non-compliance or suspected non-compliance with the practices prescribed in this CPS.
- The investigation **may** include all activities described in the Allianz RCA III CPS.

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

8.17.2 Representation of obligations to the INFRA-CA-V

INFRA-CA-V operates under the Allianz RCA III hierarchy and complies with their obligations under this CPS by:

- Making reasonable efforts to ensure the conduct of efficient and trustworthy operations. This includes but does not limit the CA to operate in compliance with:
- Documented operational procedures
- Applicable law
- Operating rules
- Enforcement of the practices within the sphere of its operations as prescribed in the corresponding Allianz RCA III Minimum Operational Requirements guide
- Issuing certificates based upon the receipt of a valid certificate request, in compliance with X.509 standards and meeting all necessary requirements
- Issuing certificates based upon the factual data available at the time of issuance and devoid of any data entry errors
- Investigating any suspected compromise that **may** threaten the integrity of the PKI at any subordinate level within its chain of trust
- Promptly notifying the administrators registered as responsible for INFRA-CA-V certificates in the event the certificate authority initiates revocation of the network certificate
- Maintaining a list of compromised keys:
    - The compromised list is to include relevant information regarding the identity of the individual(s) or organisation(s) concerned, reasons and causes for inclusion on the list and such other information as **may** be required to minimise damage or liability to all Allianz RCA participants.
- Assisting in audits conducted by the Root Certificate Authority III to validate the renewal of their own certificates
- Establishing and maintaining its own CPS within the general context of the Allianz RCA III CPS

8.17.3 Operational compliance

All certificate operations comply with the policy requirements of

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

Audit requirements for certificate operations.

9. Infra CA V Certificate Profile

This certificate is a Root CA III signed certificate which is used to sign all other RCA certificates and all participant CA certificates.

Field	Content	Critical*
1. X.509v1 Field		
1.1. Version	v3	
1.2. Serial Number	09	
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		

Field	Content	Critical*
1.5.1. Not Before	"11:13:02 29 April 2015"	
1.5.2. Not After	"11:13:02 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 Infrastructure CA V"	
1.7. Subject Public Key Info	30 82 01 0a 02 82 01 01 00 cf 44 e8 da f5 d3 df bf 3c d8 57 ba 22 88 24 34 e8 10 b0 6c 4a f4 40 18 58 77 14 03 6b d6 c2 8b c8 7d f1 28 3f fc 04 50 df 4f 1e 27 54 12 f0 75 4d 6b 45 f3 3f 97 aa 0e 6b e3 35 fd 26 26 f8 e9 e0 c5 aa 06 41 f1 ca 58 8b 8c d5 98 8d 7e f3 01 9b 11 1a 0a 8b a5 9a 5e 73 08 85 18 a7 f2 fb 8e 96 ad 50 a9 2f d9 84 21 67 35 23 a0 b5 ec 16 4a 78 8c f3 86 ad 1d 97 82 85 a4 a6 a8 2d c0 c9 73 8b 7d ef fb a5 50 9b c2 ce d1 4a 48 c8 ce 17 65 3b f8 50 8b d9 0b 97 88 07 ce b4 74 f4 6c 7f 9d 1a 97 20 fb 01 6c 21 53 b1 a5 82 19 e7 4a 78 8b f0 8a ba c6 2b 42 aa 3d 06 20 c5 b5 58 d3 dc 9f 2c ba 10 0d f2 2a 82 87 4a 4b 18 4e 8b 08 2f d6 fb 06 60 9d 9b 49 17 b0 5b 3b 0c fb 17 fc 53 36 2b 53 be f6 7a 60 af dc 00 e0 48 dd c1 59 1c 1c cd 05 24 f3 a8 65 b1 e3 e4 99 f5 c3 b5 88 62 01 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	71 bd b2 eb 44 86 21 04 37 b0 6e 0b 74 c0 8c fa 5d 84 ed d0	n
3.3. Key Usage		y
3.3.1. Digital Signature	Selected	
3.3.2. Non Repudiation	Not selected	
3.3.3. Key Encipherment	Not selected	
3.3.4. Data Encipherment	Not selected	
3.3.5. Key Agreement	Not selected	

Field	Content	Critical*
3.3.6. Key Certificate Signature	Selected	
3.3.7. CRL Signature	Selected	
3.4. Certificate Policies		n
3.4.1. Policy Identifier	1.3.6.1.4.1.7159.30.32	
3.4.2. Policy Qualifier ID	1.3.6.1.5.5.7.2.2	
3.4.2.1. User Notice (Organiz.)	Allianz Germany	
3.4.2.2. User Notice (notice No.)	1	
3.4.2.3. User Notice (Display Text)	This Certificate is issued by Allianz Root CA III, by Allianz Germany	
3.4.2.4. URL (ia5String)	http://rootca.allianz.com/cps3/	
3.5. Subject Alternate Names		n
3.5.1. rfc822Name	Not present	
3.6. Basic Constraints		y
3.6.1. Subject Type	CA	
3.6.2. Path Length Constraint	None (empty for maximum)	
3.7. Netscape Extensions		n
3.7.1. CertType	SSLCA, SMIME-CA, Codesign CA	
3.8. CRL Distribution Point		n
3.8.1. 1st URL	http://rootca.allianz.com/crl/rootca3.crl	
Fingerprint	`91 fe c1 ca 37 a5 10 2e 4a aa 4d c4 1e 86 85 50 a2 9a 2a 99`	

*not used for attributes, only extensions

10. Appendix

There are a number of different types of certificates issued by Allianz Infrastructure CA V.

Their profiles are based in the current CPS of InfraCA V. Every effort is made to match these profiles to [RFC-3647].

A. Definitions and Acronyms

Authentication	The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.
CA-certificate	A certificate for one CA's public key issued by another CA.
Certificate policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP 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	A specialist unit of the technical information security department that is contact for topics related to the technical aspect of information security and

Response Team (CERT)	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 [RFC-3647].

B. Abbreviations

ADS	Active Directory Service
BGU	Betriebsgebäude Unterföhring (Data Centre)
CA	Certification Authority
CMLC	Certificate Management Life Cycle
CN	Common Name
CPS	Certification Practise Statement
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DCOM	Distributed Component Object Model
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name Service
FIPS	Federal Information Processing Standard
GISF	Allianz Group Information Security Framework
HSM	Hardware Security Module
ISIS-MTT	Interoperability Standard (ISIS – Mail Trust)
ISO	Information Security Officer
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
RA	Registration Authority
RCA	Root Certification Authority

RFC	Request for Comment
SCEP	Simple Certificate Enrollment Protocol
TSM	Tivoli Storage Management
VPN	Virtual Private Network

C. References

[AZ-BCMG]	Allianz Business Continuity Management Recovery Strategy Guide
[AZ-ITISP]	Allianz Group Information Technology and Information Security Policy Version 2.0 Effective: 22.06.2021
[AZ-AFRIS]	Allianz Functional Rule for Information Security (AFRIS) version 1.0 Effective: 01.07.2020
[AZ-ISPE]	Allianz Information Security Practice 02 – Encryption Version 1.0 Effective: 01.03.2021
[AZ-ISPN]	Allianz Information Security Practice 05 - Network Security Version 1.0 Effective: 01.12.2020
[AZ-ISINC]	Allianz Information Security Practice #09 IS Incident Handling Version 1.0 Effective: 01.09.2021
[AZ-GPS]	Guideline for Physical Security version 1.0 Effective: 08.11.2021
[AZ-ASIDM]	Allianz Standard for Information and Document Management (ASIDM) with regard to de- and encryption (see B. VI. 5. ASIDM)
[RFC-2119]	Key Words for use in RFCs to Indicate Requirement Level, IETF (Bradner), March 1997, http://www.ietf.org/rfc/rfc2119.txt
[RFC-5280]	Internet X.509 PKI Certificate and Certification Revocation List (CRL) Profile, IETF (Cooper, Santesson, Farrell, Boeyen, Housley, and Polk), May 2008, http://www.ietf.org/rfc/rfc5280.txt
[RFC-3647]	Internet X.509 PKI Certificate Policy and Certification Practices Framework, IETF (Chokhani, Ford, Sabett, Merrill, and Wu), November 2003, http://www.ietf.org/rfc/rfc3647.txt
[RFC-2459]	Internet X.509 Public Key Infrastructure Certificate and CRL Profile http://www.ietf.org/rfc/rfc2459.txt
[RFC-2560]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF (Myers, Ankney, Malpani, Galperin, Adams), June 1999, http://www.ietf.org/rfc/rfc2560.txt

[RFC-5019]	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, IETF (Deacon, Hurst), September 2007, http://www.ietf.org/rfc/rfc5019.txt
[RFC-2986]	PKCS #10: Certification Request Syntax Specification , IETF (Nystrom, Kaliski, November 2000, https://tools.ietf.org/html/rfc2986
[BSI TR-02102]	BSI - BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen (bund.de)
[EN319411]	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
[AZ-RCACPS]	Allianz Root CA III CPS http://rootca.allianz.com/download/Allianz_Root_CA_III_CPS.pdf
[ISIS/MTT]	Teletrust: Common industrial Signature Interoperability Specifications. ISIS Mail Trust, Specifications for interoperable PKI applications. July 2002