Certification Practice Statement for Allianz User CA

Information Owner: Allianz Managed Operations & Services SE

Version 1.4 / 13 Mar. 13

Document-Name: Allianz User CA CPS Ver 1.4.doc

Classification: public

Change Management

Version	Description	Date	Author
0.9.0	Final Draft	30.11.2007	Actisis GmbH
0.9.1	Enhancements	10.06.2008	Klaus Heyden
0.9.5	Final	12.06.2008	Klaus Heyden
0.9.8	First User CA Version	12.06.2008	Klaus Heyden
1.1	Review	09.12.2010	Andre Witwer
1.2	Review	28.12.2011	Andre Witwer
1.3	Classification changed to public; NCV04 changed to CCN03	17.02.2012	Andre Witwer
1.4	Review	10.01.2012	Andre Witwer

1 Introduction

1.1 Overview

This CPS is specifically applicable to Allianz User CA and its associated Certificate Infrastructure. The CPS governs the use of Allianz User CA services within Allianz Group and its participation in Allianz Group Root CA II schema. The practices in this CPS focus on the operations of the Allianz User CA. The structure of this CPS is based on Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC3647].

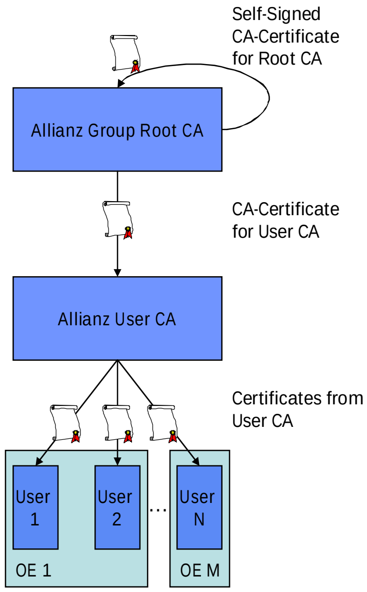

Figure 1: Allianz User CA within Allianz Root CA PKI

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 Certification Practice Statement”, or abbreviated “Allianz User CA 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 1.3.6.1.4.1.7159.30.23

1.3 PKI Participants

1.3.1 Certification Authorities

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

1.3.2 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. The Allianz User CA provides a web-based registration interface that accesses user data from the Allianz Group Global Directory (GD). Users applying for a certificate have to select their user record and receive after proper two factor authentication their certificate via an ActiveX Control automatically.

1.3.3 Subscribers

The Allianz User CA issues End-Entity certificates only. Certificate subscribers are natural persons working for or being in contractual relationship with Allianz.

1.3.4 Relying parties

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

1.3.5 Other participants

Not applicable.

1.4 Certificate Usage

1.4.1 Allowed Certificate Usage

Certificates issued by the Allianz User CA are used to support secure communication and the secure exchange of information between organizational entities operating within the Allianz Group. Two specific Use Cases are implemented:

- Digital Signature
- Key Encipherment, Data Encipherment

1.4.2 Prohibited certificate usage

Certificates issued by Allianz User CA must only be used for the purposes and applications enlisted above (Allowed Certificate Usage). Other usages must be approved in advance by written permission of Allianz User CA administration. Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

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

1.5 Policy Administration

1.5.1 Organization administering the document

Allianz Managed Operations & Services SE (AMOS), A-IT05CES02, Fritz-Schäfferstrasse 9

81737 München, Germany
.

1.5.2 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 Managed Operations & Services SE (ASIC), A-IT05CES02, Allianz User CA Certificate Policy Manager, Dieselstraße 6, 85774 Unterföhring, Germany
E-Mail: PKI-Support@allianz.de.

1.5.3 Entity determining CPS suitability for the policy

This role is carried out by Allianz User CA staff on behalf of the head of Allianz User CA.

1.5.4 CPS approval procedures

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

Allianz Group is the final approval authority of any proposed changes to this CPS. Documentation of the Allianz User CA in particular includes this Certification Practice Statement and a compliance statement in regard to Allianz Group Security Policy [AZ-SP].

1.6 Definitions and Acronyms

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).

Supplemental Definitions and Acronyms are part of the appendix 10.5 to this CPS.

2 Publication and Repository Responsibilities

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

Publication of this CPS is limited to the Allianz Group Intranet for internal use only. A shortened version will be made available at http://rootca.allianz.com/

The access to this information is not limited to participating members only. An Allianz Group RCA representative digitally signs the electronically published copies.

2.1 Repositories

Certificates issued by Allianz User CA are published in the Allianz Group Global Directory. Allianz User CA ensures not to publish private information underlying data protection guidelines.

2.2 Publication of certification information

New or amended policies are published on the intranet web site nominated for Allianz User CA documentation. Subordinate parties are notified by the Allianz User CA of changes to a policy as and when they are approved. Upon revocation of a Subscriber's Certificate, Allianz User CA shall publish an updated Certificate Revocation Lists (CRLs).

2.3 Time or frequency of publication

2.3.1 Certificate publication

A new issued certificate will be published immediately into the Allianz Global Directory. Revoked certificates will be immediately unpublished from the Allianz Global Directory.

Any repository populated with data (certificates, certificate status, certificate revocation etc.) from the Allianz User CA underlies a strict access control as stipulated by the Allianz Group IT-Security Policy (GISP). Equally any Allianz User CA related documentation as this CPS, the CP and similar relevant documents are access controlled and can only be substituted by authorized personnel.

Read only access to such information is unrestricted for business use on a need to know basis. Allianz requires persons to agree to the Terms and Conditions as a condition to accessing Certificates, Certificate status information or CRLs.

Allianz has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting or modifying repository entries.

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 promptly publishes new certificates and changes in certificate status, including revocation and expiry to its repository. Access controls on repositories

3 Identification and Authentication

Allianz User CA / Registration Authority carry out identification and authentication relying on pre-registered user data stored in Allianz Group 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) according to ITU-T

[X.500]. The subscriber certificates issued by the Allianz User CA use the following DN name format:

- Country (C) = DE
- Organization (O) = ALLIANZ
- Organization (OU) = <optional>
- E-Mail (E) = Address according to RFC 822, 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 have to contain 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 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

The subscriber digitally signs the certification request with the private key corresponding to the public key to be certified by Allianz User CA. Allianz User CA 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 eligible for requesting certificates/services are determined by the OE responsible for the Allianz User CA and enforced by control of write privileges to Allianz Group Global Directory.

3.2.2 Authentication of individual identity

Users requesting Allianz User CA Certificates authenticate against the Allianz Group 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 employs policy filters to overwrite any data contained 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 Group Global Directory. Any user listed in the Allianz Group Global Directory is entitled to request an Allianz User CA 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 produced 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 digitally signed request or email produced using a valid private key and certificate that
- shall be revoked, or
- sending a signed document.

4 Certificate Life-Cycle Operational Requirements

The purpose of this chapter is to identify the Allianz User CA Certificate Management Life Cycle. This includes the two different certificate states as part of the certificate life cycle and the certificate types supported by the Allianz User CA System. All certificate operations will comply with the requirements of:

- an applicable certificate policy (CP);
- an applicable CPS
- the minimum operational requirements and operating rules of Allianz Group RCA system and
- legal requirements of domestic and, where applicable, international privacy legislation.

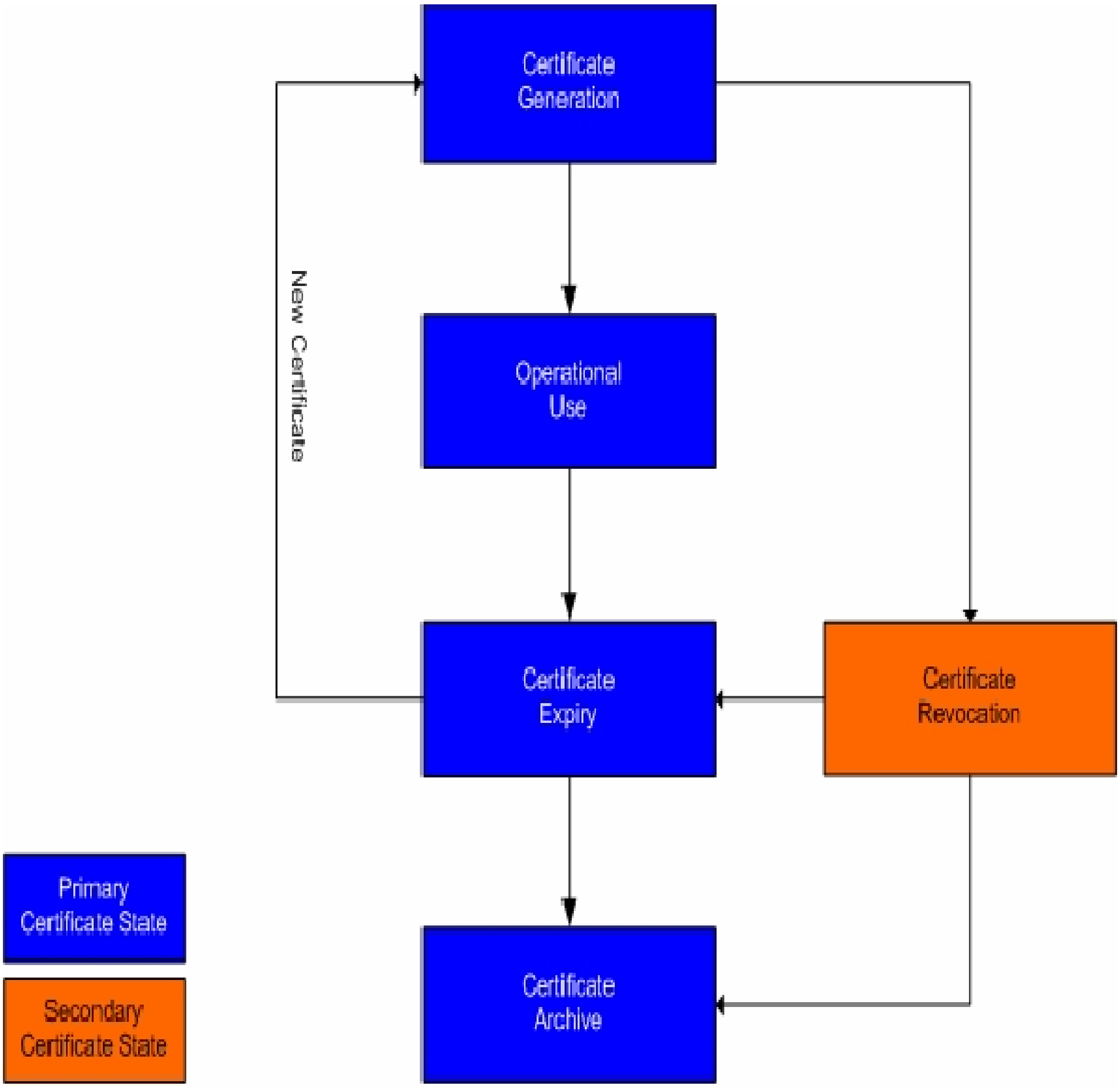

Figure 2: Allianz User CA Certificate Life Cycle

Appropriate operational and audit records will be maintained for all certificate states. The life cycle of an Allianz User CA certificate starts when a certificate is requested and generated, and ends when the certificate expires or is revoked. During this time, a certificate can move through a number of different states. The Allianz User CA Certificate Life Cycle in figure 2 below illustrates the states that may apply to an Allianz User CA certificate during its life cycle. Note that the diagram applies to all types and grades of certificates issued in the Allianz User CA System, although not all certificates will traverse all state changes. These are the states a certificate undergoes as part of its normal lifecycle (primary states):

- Generation;
- Operational Use;
- Expiry; and
- Archive.

Allianz User CA certificates may be revoked before the end of their regular lifetime when the private key related to a certificate is suspected of, or is compromised or for other reasons that may be determined by the issuer (secondary state).

4.1 Certificate Application

Allianz User CA provides the users of the Allianz Group 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?

Certificate applications can be submitted by any user of Allianz Group that is enlisted in Allianz Group Global Directory.

4.1.2 Enrollment process and responsibilities

The enrolment process for certificates issued by Allianz User CA is web-based. Users access the Registration Authority interface with their web-browser. In a 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 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 systems automatically. Certificate request approval is granted by Allianz User CA 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 issues subscriber certificates based on the registration data delivered by the Registration Authorities respectively the Allianz Group 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 then signs the public key of the subscriber as requested. Confirmation of a completed request is returned to the RA respectively to the ActiveX Control that handles the Registration

Procedure. Issued certificates are offered for download to the ActiveX Control performing the Registration Procedure.

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 Group 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 certificate will be revoked by the Registration Authority. 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 documented by the issued certificate can only be used for applications in accordance with the key usages given in the certificate. The subscribers keys can only be used for certificate based 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 does not support certificate renewal as certificate re-key (see below) is required by Allianz User CA. Key pairs must always expire at the same time as the associated certificate. When a subscriber requests certificate renewal, new key pairs have to be generated.

4.6.1 Circumstance for certificate renewal

Key changeover is not automatic. Keys expire at the same time as their associated certificates and the Subscriber must obtain a new key by making an application for a sequent certificate prior to certificate expiry.

4.6.2 Who may request renewal

The Subscriber is notified by the relevant RA prior to the expiration of his certificate and can initiate the Certificate Renewal process using his existing valid certificate and private key pair for authentication. After expiration or revocation of the existing certificate, a new certificate application must be requested.

4.6.3 Processing certificate renewal requests

Renewal requests are processed in the same way as the initial certificate requests. Notification of new certificate issuance to subscriber

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

4.6.4 Notification of new certificate issuance to subscriber

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

4.6.5 Conduct constituting acceptance of a renewal certificate

All valid end-user certificates are published in the Allianz Group Directory (GD) upon creation.

4.6.6 Publication of the renewal certificate by the CA

All valid end-user certificates are published in the Allianz Group Directory (GD) upon creation.

4.6.7 Notification of certificate issuance by the CA to other

No stipulation.

4.7 Certificate Re-key

Certificate re-key is the process by which a new (sequent) certificate is issued to replace an expired (or expiring) certificate. Certificate renewal requires the creation of a new private key and public certificate pair by the Subscriber. The Allianz User CA will not re-key a key pair of an existing certificate. The Allianz User CA only renewal certificates by issuing a new generates key pair.

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate Modification

4.8.1 Circumstance for certificate modification

A Certificate Modification service is not provided. In cases where certificate information changes during the life of a valid certificate, the existing certificate is 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 purpose of revoking a certificate is to permanently prevent the future use of the certificate and its associated private/public key pair, due to a compromise in the private key, the misuse of or errors in the certificate. The circumstances under which a certificate may be revoked are

- the security or confidentiality of the subscribers private key or the Allianz User CA private key or the root key has been compromised or is at material risk of being compromised,
- a security breach,
- the termination of a business relationship between Allianz and the Subscriber,
- etc.

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 should 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.
- The certificate subscriber.

4.9.3 Procedure for revocation request

The Allianz User CA receives a digitally signed certificate revocation request either by the relevant Registration Authority or the Subscriber himself. The Allianz User CA verifies the revocation request and revokes the certificate. The revoked certificate is added to Allianz User CA list of revoked certificates. A new CRL is published at the next scheduled update to the corresponding repository. The Allianz User CA sends a notice containing 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.

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.

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

4.9.7 CRL issuance frequency (if applicable)

CRLs are updated at a minimum as described in 2.3. The CRLs created by the Allianz User CA will be published when the next scheduled time slot is reached. The revoked certificate will be immediately unpublished.

4.9.8 Maximum latency for CRLs (if applicable)

A Certificate Revocation List (CRL) is being kept by the Allianz User CA. The CRL will be published in the Group Directory and web distribution point. Update latency is 15 minutes after change. The CRLs created by the Allianz User CA will be published to the web server when the next update time will be scheduled (described in 2.3.2).

4.9.9 On-line revocation checking requirements

Status information on revoked certificates is available via the online accessible CRL. The CRLs created by the Allianz User CA will be published Allianz Root CA website, using an URL specified in the certificate.

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 provides a web page hosted CRL for verifying the status of all issued certificates.

4.10.1 Operational characteristics

The certificate status service is inter-operational to the CRL service of Allianz Group RCA II. 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 CRLs created by the Allianz User CA will be issued to the web server at a minimum of a time schedule defined in 2.3.2. The IT Service Provider guarantees high availability of service subject to specification of SLA.

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 are backed up. All Certificates (and hence the public keys contained in them) shall be archived. The Backup of the CA key will operate under the same circumstances like the active secret key itself.

The secret key of the subscriber will not be stored for backup. A restore or key escrow of the secret key of the subscriber 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 systems are secured in compliance with GISF 2.5 physical security standard.

5.1.1 Site location and construction

The secured CA environment consists of two separated facilities. The Allianz User CA and Backup Systems operate within physically secured areas that meet the standards identified in the Allianz Group Security Policy.

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.

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

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

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

5.1.3 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 Security Policy.

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 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 Security Policy.

5.1.8 Off-site backup

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

5.2 Procedural Controls

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

5.2.1 Trusted roles

The roles and their obligations described subsequently are grouped by the respective organizational / technical component.

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 GISF Policy/Standard. Every task which requires a multiple control are administered with an m of n person doctrine (with $m \geq 2$ and $n > m$).

5.2.3 Identification and authentication for each role

Allianz User CA systems and processes use the corporate access control infrastructure based on SSO-card, which provides strong authentication and role based access control. Granting and withdrawal of Allianz User CA administrative roles require compliance with user access management standard as laid out in the current GISF Policy/Standard.

5.3 Personnel Controls

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

5.3.1 Qualifications, experience and clearance requirements

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

- are evaluated before employment to assess their suitability;
- enter into non-disclosure agreements to protect against the unauthorized disclosure of confidential information;
- are trained in:
  (a) basic PKI concepts
  (b) the use and operation of Certification authority software
  (c) documented Certification authority procedures
  (d) computer security awareness and procedures
  (e) this CPS.

5.3.2 Recruitment and Qualification of Personnel

The recruitment and selection practices for Allianz User CA 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 their security administrator 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 including 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 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 System staff has access to all training documentation.

5.4 Audit Logging Procedures

Allianz User CA 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 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 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 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 security administrator 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 Group System Operation Standard (GISF 2.4).

5.5.1 Types of records archived

The following operational records are archived by Allianz User CA:

- 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 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.

5.5.5 Archive collection system (internal or external)

The Allianz User CA 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 fresh keys prior to expiration of the current Allianz User CA instance.

5.7 Compromise and Disaster Recovery

Allianz User CA must 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 Group Business Continuity Management Policy and Standards [AZ-BCM].
- Configuration baseline, including operating software, and PKI specific application programs.
- Provides the above documentation on the request of persons conducting a security, compliance or CPS practices audit;
- Provides appropriate training to all relevant staff in contingency and disaster recovery procedures;

Allianz User CA must establish tests to conduct periodically checking the procedures for a 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, only from backup media and in compliance with the configuration baseline;
- the restored service is connected to the communications links and the correct operation of its certificate services tested;
- service operations are resumed using the original operational platform. All files on the hard disk of the test platform are securely deleted.
- Generating a compromise and disaster recovery plan, the following use cases have to be taken into account:

5.7.1 Incident and compromise handling procedures

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data and database records for all Certificates issued. Backups of CA secret key shall be generated and maintained in an appropriate way.

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, Key Compromise Response procedures are enacted by the Computer Incident Response Team (CIRT) as required by the Allianz Group Information Security Policy. If Allianz User CA 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

Therefore the Allianz User CA has prepared a second system providing the certification service currently located in a local separated data centre environment.

- Identified individuals authorized to initiate disaster recovery action;
- Identified major elements at risk, for example;
- Operational hardware;
- Certification authority software application;
- Logical records;
- Registration records;
- Identified criteria that might prompt disaster recovery initiation;
- Considered secondary precautionary measures that may be required, such as:
- a backup site;
- trained backup staff;
- Developed recovery actions and timeframes;
- Prioritized recovery actions from most significant to least significant;
- Maintained a record of the hardware and software configuration baseline;
- Maintained records of the necessary equipment and procedures required to recover from an unexpected event such as a hardware failure, including the intended maximum period that the system is to be down.

5.8 CA or RA Termination

If it is necessary to terminate Allianz User CA services, the impact of the termination will be minimized as much as possible in light of the prevailing circumstances. The Allianz User CA 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 immediately and prior to an emergency shut down. The last act of the terminated Allianz User CA is to issue a CRL with all certificates revoked. The Allianz User CA 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.

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 members in order to meet the requirements explained in chapter 4. 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 System: Allianz User CA Keys - 5 Years - 2048 bit
- Allianz User CA CRL Signing Keys - 5 Years - 2048 bit
- The Allianz User CA keys are exclusively generated by the Hardware Security Module (HSM) as part of the Allianz User CA 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 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 are generated in them and remain there in both encrypted and decrypted forms, and are decrypted only at the time at which they are being used. Allianz User CA has established HSM compliance criteria that ensure the quality and requirements from an HSM are uniform and consistent. The keys used by Allianz User CA Server (CA signing and server key) are generated using the HSM key generator. This is integrated 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 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) secured. Allianz User CA 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 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 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 Root keys are 2048 bit RSA keys. While the currently allowed minimum key size for subscribers are key pairs equivalent in strength to 1024 bit RSA, Allianz User CA on default certifies 2048 bit RSA key pairs for subscribers.

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 Appendix chapter 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 secret signature key is stored in a FIPS 140-2 Level 3 compliant redundant Hardware Security Module Safenet Luna SA 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 key pair generation and CA private key storage, Allianz User CA uses hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-1 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 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 “Shareholders.” 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. For details please refer to the HSM Documentation (see 6.2).

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 140-1 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 move the private key to a new HSM device (ISO, Operator and Partition owner). For details please refer to the HSM Documentation (see 6.2). 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 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 secret signature key is stored in a FIPS 140-2 Level 3 compliant redundant Hardware Security Module Safenet Luna SA.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Allianz User CA, 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 key is generated at installation in form of administrator cards. Those cards have to 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

Cryptographic software in use is Microsoft Enterprise Certification Authority 2003. The operating systems are hardened according to Allianz standard guidelines for server systems.

The following computer security controls have been implemented and are enforced by the hosts' operating systems and the Allianz User CA 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 systems including data.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The Allianz User CA 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

AG6DCI07 establishes a change management system to control and monitor the configurations of the systems and prevent unauthorized modification.

6.6.3 Life cycle security controls

The configuration of the Allianz User CA as well as any modifications and upgrades must be tested, documented and approved in advance. A contingency plan is in force, which includes adequate redundancy, back-up and recovery procedures.

6.7 Network Security Controls

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

The Allianz Group Corporate Network is protected from outside networks by firewalls. Only Allianz Group 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 comply with Allianz Group RCA requirements. For the detailed certificate profile refer to Appendix. The public key in a certificate must be unique. No party, be it 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 appendix.

7.1.2 Certificate Policies

Certificate Profile Extension contains 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 appendix.

7.1.5 Algorithm object identifiers

No stipulation.

7.1.6 Name formats

All certificates must have non-null Issuer DN. All Certificates must contain 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 1.3.6.1.4.1.7159.30.X

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

Certificate validity checking must be performed in accordance to the operating rules of Allianz Group RCA System.

7.2.1 Version number(s)

Only X509 Version 2 CRLs are supported.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP Profile

OCSP Service may be provided in the future.

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 Group Root CA the Policy Council proves the compliance of Allianz User CA to the policies of Allianz Group Root CA. As SubCA member of Allianz Group Root Certification Authority Infrastructure, the compliance of Allianz User CA Policy, CPS and described processes is regularly checked against Allianz Group RCA Policy/CPS, which in turn is compliant with internal Allianz Group Security Standards. A control assessment is conducted with support of Allianz User CA 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 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.

8.3 Assessor's relationship to assessed entity

Allianz User CA may initiate third party audits.

8.4 Topics covered by assessment

8.4.1 Initial compliance audit

Allianz User CA conducted the Allianz Group RCA initial compliance audit process prior to issuing certificates. The purpose of the Allianz Group 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 Group 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 Group Root CA. After acceptance as participant of Allianz Group RCA system the participant will be required to conduct the Allianz Group 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 security infrastructure can be guaranteed continuously in all cases.

8.6 Communication of results

Allianz User CA will provide Allianz Group RCA with copies of all audits and reviews on a timely basis (within 30 days). Allianz Group 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 1.3.

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

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

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

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

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.

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 to another PKI participant. Confidential information of Allianz User CA shall include any information concerning the Allianz User CA Services or the Allianz User CA System or technology and information belonging to Allianz User CA, which are marked “confidential” or “proprietary”. “Confidential

Information" also includes the results of compliance audits provided to Allianz User CA, cf. section 8.

9.3.2 Types of Information in particular considered confidential

Personal Information supplied to Allianz User CA 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 Group RCA when it receives an application from a third party to operate a CA within the Allianz Group 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 repositories and information contained 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 retain all Intellectual Property Rights in and to the Certificates and revocation information issued.

9.5.2 Certificate

Allianz User CA 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 System vests solely in Allianz User CA. 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 infrastructure, or in accordance with the relevant this CPS.

9.6 Representations and Warranties

9.6.1 CA representations and warranties

Allianz User CA 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 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 be liable to any participant, customer or other entity or person for any loss, claim, damage or expense arising from Allianz Group RCA.

9.8.1 Safeguards

Allianz User CA 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 authorized personnel;
- prohibit access to those resources by unauthorized individuals;
- prevent system failures (i.e., other than as a result of abuse).

These measures include but are not limited to:

- Testing of the Allianz User CA Disaster Recovery Plans;
- Performing regular system data backups;
- Performing a backup of the current operating software and certain software configuration files;
- Storing all backups in secure local and offsite storage;

- Maintaining secure offsite storage of other material needed for disaster recovery;
- Periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure;
- Periodically reviewing its Disaster Recovery Plan, including the identification, analysis, evaluation and prioritization of risks.

9.9 Indemnities

Cf. Section 9.8.

9.10 Term and Termination

9.10.1 Term Allianz Group Root certificate

The CPS becomes effective upon publication in the Allianz Group Root CA website. Amendments to this CPS become effective upon publication in the Allianz Group 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 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 revokes all certificates issued.

After revocation, Allianz User CA informs its subscribers and the relevant relying parties as soon as reasonably possible that they shall cease at once to use for any purpose their digital certificates that are digitally identified with the revoked certificate. Upon receipt of a participant, Allianz User CA 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, all earlier versions of the CPS will expire.

9.12.1 Notification mechanism and period

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

9.12.2 Circumstances under which OID must be changed

If Allianz User CA determines significant changes in the certificate practice, the Allianz User CA can decide to change object identifier corresponding to a Certificate policy. The amendment shall contain 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 contain 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 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 maintains contingency plans in force, including adequate back up and recovery procedures, to ensure that Allianz User CA can continue to meet its obligations under the Operating rules without material interruption in the event of the failure or shut down of the primary computer facilities or other operating facilities.

9.16.6 Other Provisions

Not applicable.

10 Appendix

10.1 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.

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.

GISF

Allianz Group Information Security Framework 2.4

PAC

Allianz Group RCA Policy Council.

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 organization 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].

10.2 Relevant referenced documents

GISF: Allianz Group Information Security Framework, Version 2.4

Allianz Group Security Policy:

10.3 References

AZ-BCM

Allianz Group Business Continuity Management Policy and Standards

AZ-SP

Allianz Group Security Policy

RFC 2459

Obsolete RFC Standard - refer to RFC 3280.

RFC 2528

Obsolete RFC Standard – refer to RFC3279.

RFC 2822

P. Resnick, Editor: Internet Message Format April 2001. (Obsoletes: 822)

RFC 3279

W. Polk, R. Housley, L. Bassham: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

RFC 3280

Housley, R., Polk, W. Ford, W. and D. Solo: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002. (Updated in parts by RFC 4325 Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension and RFC 4360 Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)

RFC 3647

S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003

RFC 822

Obsolete RFC Standard – refer to RFC2822.

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,"

10.4 Certificate Profiles

The following certificate profiles are still in draft status and show the profiles of the Allianz Smartcard CA which is used as template for the actual Allianz User CA certificate profile.

10.4.1 User Signing Cert

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 114 (0x72)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz, CN=Allianz User CA
        Validity
            Not Before: Aug 10 15:53:39 2010 GMT
            Not After : Oct 31 22:59:59 2012 GMT
        Subject:           C=DE,           O=Allianz           Group,
emailAddress=some.name@allianz.de, CN=Some name
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
            Modulus (2048 bit):
                00:cb:9d:8b:10:a6:af:7c:7f:ff:86:19:24:7b:1b:
                (…)
                26:a1
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Key Usage: critical
        Digital Signature
        X509v3 CRL Distribution Points:
        URI:http://rootca.allianz.com/uca/uca.crl
        URI:http://rootca.ind.allianz/uca/uca.crl
        Netscape Cert Type:
        SSL Client, S/MIME
        X509v3 Extended Key Usage:
        TLS Web Client Authentication, E-mail Protection,
        X509v3 Authority Key Identifier:
 Keyed:<Hash-Value>
        X509v3 Subject Alternative Name:
        email:some.name@allianz.de
Signature Algorithm: sha1WithRSAEncryption
    5d:02:3c:6e:12:75:51:3f:c9:c1:1b:5a:74:e4:63:0e:0d:a2:
    (…)
    02:1d:b0:0d
```

10.4.2 User Encryption Cert

```
Certificate:
        Data:
            Version:  v3
            Serial Number: 0x61FB9
            Signature Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5
            Issuer: CN=Allianz UserCA,O=Allianz Group,C=DE
            Validity:
                Not Before: Thursday, November 11, 2010 9:03:41 PM CET
Europe/Berlin
                Not  After: Monday, November 12, 2012 9:03:41 PM CET
Europe/Berlin
            Subject: CN=Some Name,E= some.name@allianz.de,O=Allianz,C=DE
            Subject Public Key Info:
                Algorithm: RSA - 1.2.840.113549.1.1.1
                Public Key:
                    Exponent: 65537
                    Public Key Modulus: (2048 bits) :
                        AE:61:67:7E:A1:EF:62:78:E7:89:80:39:37:DF:85:F4:
                        .....
                        3B:6E:7A:63:22:D4:F2:5D:1B:C4:A9:BF:82:98:7D:CB
            Extensions:
                Identifier: Key Usage: - 2.5.29.15
                    Critical: yes
                    Key Usage:
                        Key Encipherment
                        Data Encipherment
                Identifier: Authority Key Identifier - 2.5.29.35
```

```
                    Critical: no
                    Key Identifier:
                        DE:C4:D6:FF:7A:90:48:C0:14:73:BF:FE:6F:1B:B2:F4:
                        F5:88:F8:6C
                Identifier: Extended Key Usage: - 2.5.29.37
                    Critical: no
                    Extended Key Usage:
                        1.3.6.1.5.5.7.3.4
                Identifier: Subject Alternative Name - 2.5.29.17
                    Critical: no
                    Value:
                        RFC822Name: some.name@allianz.de
                        RFC822Name: some.name@allianz.com
                Identifier: Certificate Policies: - 2.5.29.32
                    Critical: no
                    Certificate Policies:
                        Policy Identifier: 1.3.6.1.4.1.7159.30.30.1
                            Policy Qualifier Identifier: CPS Pointer
Qualifier - 1.3.6.1.5.5.7.2.1
                            Policy Qualifier Data:
https://rootca.allianz.com/userca/
        Signature:
            Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5
            Signature:
                A7:6A:CB:3E:D6:7D:EA:66:72:35:B4:0E:DD:C4:08:47:
                …..
                18:7C:E8:26:75:DB:4B:54:35:2C:75:3E:23:9D:38:A9

                FC:13:44:2C:A0:FA:93:14:37:7E:EE:3B:2A:94:A6:AA
```

10.4.3 CA Signing Cert

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8 (0x8)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Root CA II
        Validity
            Not Before: Oct 21 11:44:11 2008 GMT
            Not After : Oct  8 11:44:11 2022 GMT
        Subject: C=DE, O=Allianz Group, CN=Allianz UserCA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:c4:36:2a:12:1e:44:26:e0:9c:e3:ce:c7:51:e4:
                    ...
                    a0:52:12:54:e1:0d:61:6f:d5:07:2a:ed:fc:61:b8:
                    ff:f9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                DE:C4:D6:FF:7A:90:48:C0:14:73:BF:FE:6F:1B:B2:F4:F5:88:F8:6C
            X509v3 Authority Key Identifier:

keyid:C0:7D:0A:37:BC:D9:61:D5:D1:CB:B6:2C:F6:37:3A:09:3C:A2:4B:79

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

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

    Signature Algorithm: sha1WithRSAEncryption
        87:41:e0:fe:e0:24:87:85:24:55:77:d8:22:3f:9f:5a:d5:b8:
        ...
        99:c9:a4:db:67:d5:1f:7d
```

10.4.4 RCA II Signing Cert

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

C0:7D:0A:37:BC:D9:61:D5:D1:CB:B6:2C:F6:37:3A:09:3C:A2:4B:79
```

```
            X509v3 Authority Key Identifier:

keyid:C0:7D:0A:37:BC:D9:61:D5:D1:CB:B6:2C:F6:37:3A:09:3C:A2:4B:79
            X509v3 Basic Constraints: critical
            CA:TRUE
            Netscape Cert Type:
            SSL CA, S/MIME CA, Object Signing CA
            X509v3 CRL Distribution Points:
            URI:http://rootca.allianz.com/rootca2.crl
            X509v3 Certificate Policies:
            Policy: 1.3.6.1.4.1.7159.30.20.1
              CPS: http://rootca.allianz.com/cps2
              User Notice:
                Organization: Allianz Group Germany
                Numbers: 1, 1
                Explicit Text: This Certificate is issued by Allianz
Group
                               Root CA II, by Allianz Group Germany
    Signature Algorithm: sha1WithRSAEncryption
        7b:8e:3f:33:f5:bc:a1:eb:5b:fc:bc:80:5d:f9:74:8b:0d:e0:
        (…)
        12:f4:55:f3:47:0a:8a:d5
```