Certification Practice Statement For Allianz Group Infrastructure Certification Authority (Infra-CA3 / Infra CA4)

Information Owner: A-IT05CES02 INFRA-CA

Version 1.5 A-IT05CES02

Document-ID: AZ-INFRA-CA 3-4 CPS

Classification: public

Change management

Version	Description	Date	Author
0.9	Initial Draft	27.10.2006	Actisis GmbH
0.9a	Second Draft, minor changes based on comments from AGIS	7.11.2006	Actisis GmbH
0.92	Review AGIS	23.11.2006	André Witwer, AG2WMI07
1.1	Review AMOS	15.12.2010	André Witwer, AG6DCI07
1.2	Review AMOS.	27.12.2011	Andre Witwer, A-IT05NCV04
1.3	Classification changed to public. NCV04 changed to CCN03	17.02.2012	Andre Witwer, A-IT05CCN03
1.4	Content changed	23.02.2012	Andre Witwer, A-IT05CCN03
1.5	Review AMOS	14.01.2013	Andre Witwer, A-IT05CES02

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 Group. Allianz Group Infrastructure3 CA and Allianz Group Infrastructure4 CA, referred to as INFRA-CA hereafter, serves as an intermediate CA of the Allianz Group Root CA II (RCA) to issue certificates. This document is organized as suggested by RFC 3647 [RFC3647] in order to ensure comparability.

1.1 Overview

The INFRA-CA is the preferred authority for issuing certificates for technical network and Infrastructure components within Allianz Group. Furthermore, its purpose is to issue and support network certificates on behalf of Allianz Group. For this purpose, the INFRA-CA 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 please see Figure 1 Overview INFRA-CA PKI components.

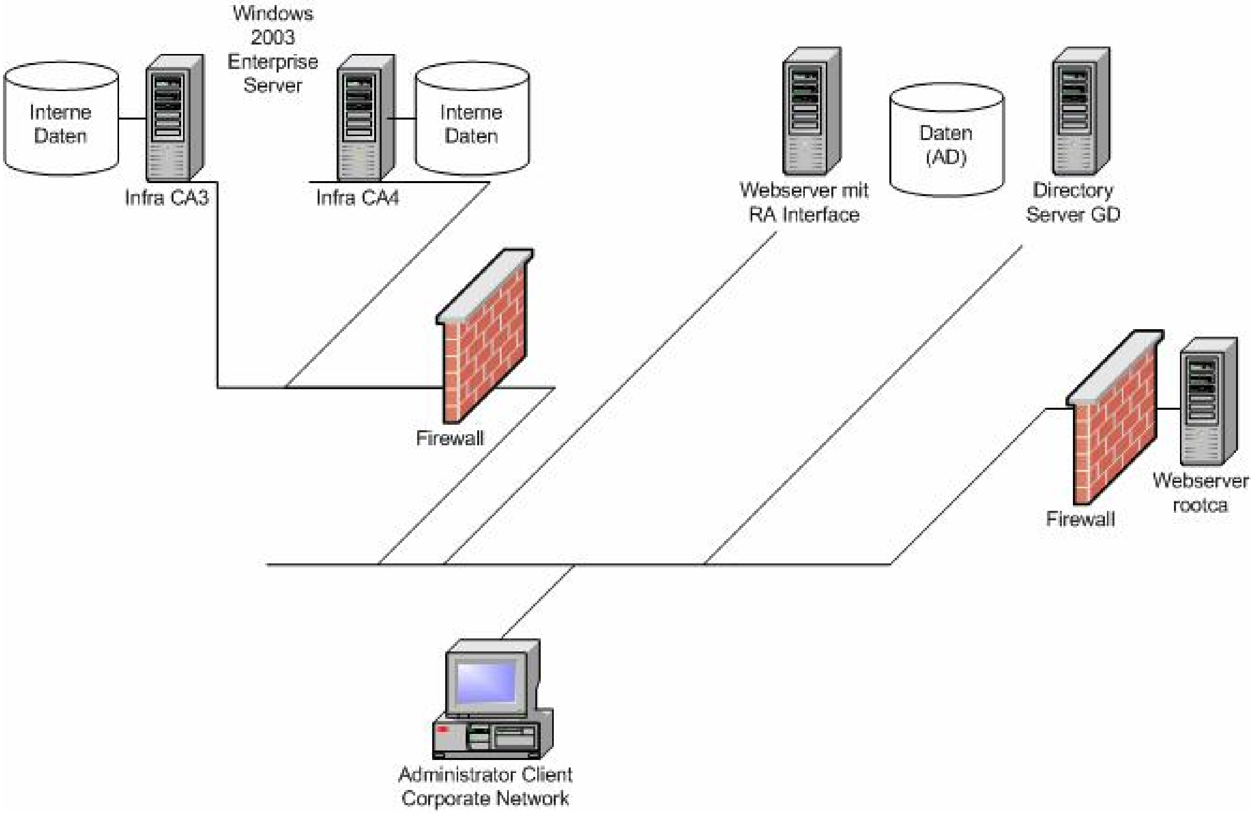


Figure 1 Overview INFRA-CA PKI components

1.2 Document name and identification

This CPS is referred to as the “Certification Practice Statement of Allianz Group Infrastructure 3 / 4 CA”

Object Identifier (OID) for this document is:

CA3/4: 1.3.6.1.4.1.7159.30.22

1.3 PKI participants

The INFRA-CA PKI System uses Microsoft Enterprise Certification Authority 2003 software for certificate issuance, management and secure system backup and storage.

1.3.1 Certification authorities

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

1.3.2 Registration authorities

Included in INFRA-CAs 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 Microsoft Enterprise Certification Authority 2003 software.

1.3.3 Subscribers

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

- Web Server
- Domain Controller
- Router
- Application / code
- IPSec / VPN
- Web-Services (Client authentication)
- 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.

1.3.4 Relying parties

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

1.3.5 Other participants

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

1.4 Certificate usage

1.4.1 Appropriate certificate usage

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

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

1.4.2 Prohibited certificate usage

Certificates issued INFRA-CA 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 administration.

1.5 Policy administration

1.5.1 Organization administering the document

This CPS is published and administered by A-IT05CES02 from Allianz Managed Operations & Services SE.

1.5.2 Contact person

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

Allianz Managed Operations & Services SE
A-IT05CES02 – NZA, Zertifikate und Directory Services
Gutenbergstrasse 8
85774 Unterföhring
Germany
Email: *pki-support@allianz.de*

The contact details of Allianz Group RCA are:

Allianz Managed Operations & Services SE
A-IT05CES02 – NZA, Zertifikate und Directory Services
Gutenbergstrasse 8
85774 Unterföhring
Germany
Email: *pki-support@allianz.de*

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 CPS approval procedures

Allianz Group RCA Approval Council determines the suitability of this CPS and its compliance with other Allianz Group policies. Allianz Group is the final approval authority of any proposed changes to this CPS.

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).

Acronyms and Abbreviations used throughout this document can be found in the Appendix - D Abbreviations.

2 Publication and repository responsibilities

Information relating to INFRA-CA policies, the INFRA-CA and other Allianz Group RCA participants, is available at the Allianz Group RCA Internet Site:

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. The INFRA-CA CPS is actually declared as public.

2.1 Repositories

Certificates issued by INFRA-CA are published only if they are used for web-service authentication. In this case they are published into the Allianz Group Global Directory.

2.2 Publication of certification information

New or amended policies are published on the intranet web site nominated for INFRA-CA documentation.

2.3 Time or frequency of publication

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

2.4 Access controls on repositories

Any repository populated with data (certificates, certificate status, certificate revocation etc.) from INFRA-CA underlies a strict access control as stipulated by the Allianz Group IT-Security Policy.

Equally any INFRA-CA related documentation as this CPS, the CP and similar relevant documents are access controlled and can only be substituted by authorized personnel.

3 Identification and authentication

To ensure the integrity and trustworthiness of operations throughout the PKI hierarchy, INFRA-CA agreed during registration to comply with the practices for intermediate CAs of Allianz Group Root CA II.

3.1 Naming

3.1.1 Types of names

A certificate issued by INFRA-CA contains an X.509-v3 distinguished name in the Subject Name field and is specified as described in Section 7.1 – Certificate Profile.

3.1.2 Need for names to be meaningful

Distinguished Names must be unambiguous and unique due to the rules employed for their creation.

In the 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 certificates please consult the appendix 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.

Codesigning 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 Group Global Directory.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

AMOS Security delegates responsibility for legitimating applicants for certificates of INFRA-CA to a CA Management department within AMOS which can be contacted via email: pki-support@allianz.de .

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

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

INFRA-CA 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 chapter 1.3.3 . Therefore, application forms adapted to SSL web servers and IT infrastructure components are supported by INFRA-CA, see Appendix C.3 Certificate Application Forms (CA / RA Front-end) for screenshots of the application forms.

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

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

1. Generate a secure and cryptographically sound key pair,
2. Agree to all terms and conditions of the INFRA-CA CPS approved by PAC,
3. Complete and submit the certificate application form, providing all information requested by INFRA-CA without any errors, misrepresentation, or omissions.

Relevant certificate extensions as listed in Appendix `Certificate:`

```
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Root CA II
        Validity
            Not Before: Nov 14 11:48:12 2006 GMT
            Not After : Nov 10 11:48:12 2021 GMT
        Subject: C=DE, O=Allianz Group, CN=Allianz Group Infrastructure3 CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ab:36:5f:cb:da:c4:06:5f:02:28:23:95:c7:f0:
                    e8:3c:50:d5:ce:47:05:03:d8:27:cd:f9:3d:89:a3:
                    3c:d6:05:db:d1:34:44:cb:2b:f8:28:74:f5:fa:5c:
                    3b:ff:db:13:7d:83:92:5b:53:2a:fd:48:d0:cc:c1:
                    7c:80:11:56:0a:3f:38:f8:24:e0:df:52:e0:e7:17:
                    11:dc:7f:c6:6f:9a:65:f7:67:24:6a:2e:13:da:52:
                    89:85:ac:90:c8:fe:31:f9:67:b2:a4:ea:0f:6f:05:
                    57:1f:1f:81:84:d4:7c:eb:eb:d7:0b:8b:ec:05:dc:
                    02:d7:aa:a8:f8:ef:62:8f:cf:b6:91:4e:12:2e:5e:
                    5d:16:c9:d5:85:5c:8f:27:e3:85:d6:65:9e:e1:bd:
                    d9:f3:0d:e4:b6:af:20:e2:74:9d:d7:8b:38:0e:9a:
                    4e:cf:dc:30:9e:2b:c0:7f:0e:68:54:e6:2a:e9:0a:
                    ed:90:90:83:83:03:ae:39:cc:0f:be:8b:fb:26:ee:
                    61:4c:3a:da:9f:eb:ed:a0:17:24:50:8c:e6:b4:21:
                    fb:0e:f7:fb:45:b1:c8:fa:ad:6d:48:0e:13:9b:13:
                    14:10:1d:ee:9e:0c:6a:40:40:72:3c:b8:fd:2e:7f:
                    98:0d:c3:c1:78:55:3f:4f:bb:b9:5a:ac:8b:5d:0e:
                    55:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                29:A5:92:C0:D9:D9:B1:AA:EB:74:9C:17:72:78:8A:C1:E0:EA:56:45
            X509v3 Authority Key Identifier:

keyid:C0:7D:0A:37:BC:D9:61:D5:D1:CB:B6:2C:F6:37:3A:09:3C:A2:4B:7
9

            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 R
oot CA II, by Allianz Group Germany

            1.3.6.1.4.1.311.21.1:
                ...
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
    Signature Algorithm: sha1WithRSAEncryption
        05:df:e9:4c:74:a0:15:8e:d0:03:6f:3d:dd:04:f1:d0:23:bf:
        26:5c:d9:a3:cc:36:52:05:8b:3f:41:e3:1a:9d:bf:46:f3:89:
        33:a3:b7:fb:c8:bb:71:5d:ba:9d:a5:e4:eb:05:86:e5:10:49:
```

```
        bf:3b:53:e5:f3:57:28:f4:58:38:3e:4d:1d:22:3f:1a:97:4d:
        1e:78:62:d0:86:30:2b:1f:9f:9a:3d:99:0e:02:2d:2a:32:e8:
        5e:63:4f:25:f9:30:59:cd:13:53:d6:fa:a0:1a:3a:7c:d5:1c:
        5f:e4:84:31:8e:95:1a:dc:fc:c2:6d:8b:ab:96:44:9c:ab:dd:
        87:89:bc:55:33:23:1e:bf:eb:cf:0c:8c:ff:3d:28:e8:43:21:
        25:54:e8:99:d9:0f:f3:44:9d:f1:53:3b:81:79:1e:f3:31:ab:
        dc:be:1c:cb:eb:d9:f7:66:11:8a:af:a7:74:71:01:73:d4:84:
        8f:0c:da:1c:d4:14:d1:1b:9a:ed:dd:25:80:89:51:97:93:f7:
        c5:ae:5e:e0:97:a3:4f:93:bd:0b:0b:93:c9:6a:36:08:cf:11:
        6a:9c:94:bd:d9:39:71:dd:4d:73:34:3b:36:e7:c1:63:1e:85:
        b7:cf:d3:24:b1:0b:f3:6a:a9:c4:fe:5e:2a:3a:9d:f4:38:c3:
        f1:d0:98:a3:4f:0b:f6:9f:79:e5:20:58:54:47:42:60:47:09:
        0f:e3:6a:ea:22:5f:56:98:88:46:78:9e:48:3e:34:51:e6:8a:
        d2:9d:f5:4e:ef:d8:f5:ad:2c:b1:a2:ba:a2:c5:b5:37:e4:ce:
        52:df:99:b6:79:9f:b9:10:f9:75:ac:06:3e:23:a6:9c:88:44:
        35:d6:89:5b:bc:48:ed:a9:47:75:ef:57:de:5e:2b:e0:da:69:
        4a:05:96:b7:77:01:bd:8c:8f:2d:3f:f9:63:19:f2:cc:41:ef:
        41:0e:8b:e0:05:90:27:f3:e6:f7:05:6d:3b:ca:b8:a6:fd:b2:
        f9:2f:c9:54:57:5b:4b:29:80:73:1d:8b:8c:c4:c5:e0:63:48:
        d9:51:85:7e:f5:99:9a:bf:a8:e2:d1:6d:22:c0:cd:82:4a:33:
        8c:70:20:82:d3:91:30:a9:dd:13:f4:58:02:27:63:c7:28:0f:
        40:77:48:3e:1b:37:bf:d0:29:17:91:71:4d:73:ab:2f:c3:1c:
        ad:eb:86:18:bd:0d:3e:d3:13:ec:81:4f:75:3c:02:95:cc:96:
        78:83:c7:2a:b4:9f:7f:c9:97:92:f1:9f:3c:8f:5f:b5:d3:23:
        e5:46:8c:3b:67:fc:03:3e:28:5f:33:4a:52:b1:f4:d1:f2:2f:
        d8:26:2c:65:ca:0e:7f:57
```

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

3.2.1 Method to prove possession of private key

Private Key possession is proved by certification request being signed with the private key corresponding to the public key to be signed.

3.2.2 Authentication of organization identity

INFRA-CA only issues certificates for Allianz Group 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 they are responsible for are authenticated via their network connection based on the NTLM authentication method and the Allianz Group Global Directory.

Domain Controllers employ their native authentication methods.

3.2.4 Non-verified subscriber information

INFRA-CA 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 requests.

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 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 Group 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 Group.

§ 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 Group RCA and the specified INFRA-CA life span. The INFRA-CA certifies technical entities solely after request of trained AMOS 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 subscriber requires authorisation to apply for INFRA-CA certificates. The department or group within Allianz Group responsible for operating the network component has to authorise the requestor. The authorisation is subject to approval by a department of CA Management, delegated by AMOS IT-Security. Please contact pki-support@allianz.de for inquiries.

4.1.1 Who can submit a certificate application?

Only people holding an authorization issued by AMOS CA Administration and approved by LegBA or head of department of the applicant may request certificates at INFRA-CA.

Additionally Domain-Controllers and Routers may automatically request certificates.

4.1.2 Enrollment process and responsibilities

To obtain a certificate of INFRA-CA, an authorized applicant as mentioned in chapter 4.1.1 can follow the web based procedures as described in this section. The web interface for application is depicted in Appendix C.3 Certificate Application Forms (CA / RA Front-end). The applicant pastes the PKCS #10 request into the form and can specify up to 5 DNS names and up to 2 IP addresses of the network unit in the application form. Then, by pressing the Submit button, the request is sent for signing to INFRA-CA and a link is given to receive the INFRA-CA certificate.

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

MS-Windows client computer, MS-Windows server and other objects authenticated in the Active Directory under the ALLIANZ Group ADS Forest (rootdom.net) can retrieve automatically (auto-enrollment) special designed certificates (Chapter 6).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 operating within the PKI of INFRA-CA.
- § ensure the safety, confidentiality, and integrity of their in a trustworthy environment self generated private keys. Not to interfere with or damage, or attempt to interfere with or damage, the operational infrastructure of the Allianz Group RCA System or any component thereof. The INFRA-CA
- § 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 a security policy that provides for the early detection of an attempt to damage the infrastructure and to collect sufficient evidence for prosecution, as it is provided in the operational concept of Allianz Group RCA and is also obligatory for the INFRA-CA.

4.2 Certificate application processing

Certificate applications are processed by INFRA-CA support personal.

4.2.1 Performing identification and authentication functions

Identification and authentication of subscribers is performed by the INFRA-CA 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 issues solely non personal certificates for network units following a valid PKCS #10 request after application via http form or for ADS Systems via DCOM. The INFRA-CA 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 following implied representations:

The Subscriber agrees to be bound by the provisions of this CPS associated with the issued certificates. This CPS presented to the subscriber at the time of registration; and

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; and

The usage of the private key associated with the issued certificate in a digital signature operation, is in effect the digital signature of the subscriber; and

All representations made by the subscriber during registration and receipt of the certificate is true and accurate.

4.4.1 Conduct constituting certificate acceptance

Upon installing the INFRA-CA certificate, the subscriber accepts the terms and provisions of this INFRA-CA CPS.

4.4.2 Publication of the certificate by the CA

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

4.4.3 Notification of certificate issuance by the CA to other entities

In case of INFRA-CA issuing certificates to be used for web-services, the related deployment environment is informed.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

Subscribers of INFRA-CA 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. A single exception is foreseen for OS93 certificates. Exceptions (certificate renewal instead of rekey) are only permissible based on well founded reasons and require a written approval by OE's ISO.

4.6.1 Circumstance for certificate renewal

Expiring certificates for OS93 may be renewed by reusing the same key pair since changing private keys on OS93 requires unacceptable efforts.

4.6.2 Who may request renewal

The responsible OS93 administrator may request the renewal.

4.6.3 Processing certificate renewal requests

The infrequent certificate renewal requests are processed by INFRA-CA staff analogue to initial certificate applications. In particular for certificate renewal the initial certificate requests are reused.

4.6.4 Notification of new certificate issuance to subscriber

See initial certificate application (4.1 Certificate application).

4.6.5 Conduct constituting acceptance of a renewal certificate

See initial certificate application (4.1 Certificate application).

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 actually is implemented as sending a new certificate application.

4.7.1 Circumstance for certificate re-key

Re-key is conducted at 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

No stipulation.

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 revokes certificates after knowledge or well-founded suspicion of non-authorised usage or inconsistent databases. A certificate must be revoked if:

- The corresponding private key has been compromised.
- Material information in the Certificate is no longer valid.
- The issuing CA has ceased operation.
- The Certificate owner has submitted a valid revocation request.

4.9.2 Who can request revocation

Certificate revocation can be initiated by:

- INFRA-CA.
- RCA
- The owner of the certificate, the participant; (participants may request revocation of their certificates for any reason, or for no reason).

4.9.3 Procedure for revocation request

The procedures involved in processing of a revocation request will not depend on the identity of the originator. This section describes the procedures in which revocation is requested by end entity, Allianz Group RCA or INFRA-CA.

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 is not to include the reason for revocation.

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

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 expiry.

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 regular Business day.

4.9.6 Revocation checking requirement for relying parties

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

http://rootca.allianz.com/infraca/InfraCA3.crl

resp.

http://rootca.allianz.com/infraca/InfraCA4.crl

Certificate validity checking must be performed in accordance with the operating rules published by Allianz RCA. 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 will be issued to the web server on at least a 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.

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, 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 provides a web page hosted CRL for verifying the status of all certificates issued by INFRA-CA.

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

SC-CA's Crl-file is distributed via rootca.allianz.com web server. Its availability is under the responsibility of RCA II administration.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

In the event that INFRA-CA terminates its operation permanently all subscribers, participants and relying parties are promptly notified of the termination. Issued certificates are revoked with the date of the termination 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's private key is stored in a HSM which does not provide any mean 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

4.13 Physical Security Controls

Physical security of the Sub-CA is conducted in accordance with the Allianz Group Security Policy. There is one secured data centre housing the physical infrastructure of INFRA-CA. 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 BGU data centre.

4.13.1 Site location and construction

INFRA-CAs production environment consists of components set up in different locations secured in compliance with [AZ-SP].

The secured CA environment consists of three separated facilities where the INFRA-CA servers are hosted: BGU5 Module A and hot standby in Module B. A third Module is located in the Business Continuity Management (BCM) facility in Stuttgart.

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. 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.

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 Security Policy.

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 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 Security Policy.

4.13.8 Off-site backup

The INFRA-CA manages its backup, archive and offsite storage in accordance with the Allianz Group RCA Archiving Policy.

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

Following Roles are established:

§ Hardware and Operation System Administration

§ CA Administration

§ CA Management

§ RA Registration Authority to Issue pending certificates

No person shall have more than one role.

4.14.2 Number of persons required per task

The tasks in INFRA-CA operation and administration need only one specially authorized administrator. An exception applies for the handling of the CAs private key. The used HSM is configured to require multiple control for private key maintenance.

4.14.3 Identification and authentication for each role

The INFRA-CA system is based on the Microsoft Enterprise Certification Authority 2003 software which supports login and authentication based on NTLM. 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 Group INFRA-CA service is being operated in accordance with an approved Allianz Group policy, 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 personnel operating under the Allianz Group RCA system take into account background, qualifications, experience and the security clearance requirements of each position, which are matched against the profiles of potential candidates.

4.15.2 Background check procedures

Background checks can be 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.

4.15.3 Training requirements

Operational personnel must be trained sufficiently to perform their duties in a responsible manner.

4.15.4 Retraining frequency and requirements

Retraining is performed at least annually based on and including 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 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 system staff has access to all CA system documentation.

4.16 Audit Logging Procedures

4.16.1 Types of events recorded

The Integrity of the INFRA-CA is achieved by having activated and monitored 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 the one hand and the network protection provided by the DMZ on the 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 done automatically by the TSM client installed on the CA system.

4.16.6 Audit collection system (internal vs. external)

INFRA-CA is does not participate in any audit collection system. Audit logs are back upped externally in the TSM backup system provided by AMOS.

4.16.7 Notification to event-causing subject

Handling of incidents follows the Allianz Group IT-Security Standard for Incident Handling, GISF 2.2 [AZ-SP].

4.16.8 Vulnerability assessments

No stipulation.

4.17 Records Archival

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

4.17.1 Types of records archived

The following types of information are to be recorded and archived automatically by INFRA-CA 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-CAs 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 Login to the system and the physical and network controls provided by the DMZ infrastructure. The backup of the archive is stored within the TSM system of AMOS. Protection within the TSM system is implemented only on procedural basis.

4.17.4 Archive backup procedures

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

4.17.5 Requirements for time-stamping of records

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

4.17.6 Archive collection system (internal or external)

The INFRA-CA 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 AMOS.

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 files selected by date the complete archive as well as parts (files) of it. TSM functionality is used for archive verification.

4.18 Key Changeover

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

4.19 Compromise and Disaster Recovery

INFRA-CA will establish and maintains detailed documentation covering its:

- Contingency & disaster recovery plan, including key compromise, hardware, software and communications failures, and natural disasters such as fire and flood.
- Configuration baseline, including operating software and PKI specific application programmes
- Backup, archiving and offsite storage procedures.
- 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.

Periodically (yearly) tests the INFRA-CA 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 are handled according to the Allianz Group Incident Handling Standard. In addition the INFRA-CA 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 Group applies.

4.19.3 Entity private key compromise procedures

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

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

If a subscriber’s private key becomes compromised, the responsible person must inform the INFRA-CA 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 in order to make accessible the logical records kept within the software. Therefore the INFRA-CA has:

- Identified individuals authorised to initiate disaster recovery action
- Identified major elements at risk, for example
- Operational hardware;
- Certificate Authority software;
- 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;
- Well-trained backup staff
- Developed recovery actions and timeframes;
- Prioritised 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 recovering from an unexpected event such as a hardware failure, including the intended maximum period that the system is to be down.

4.20 CA or RA termination

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

5 Technical Security Controls

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

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 group INFRA-CA in order to meet the requirements explained in chapter 4. The cryptographic procedures and records used 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 INFRA-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 must be generated in them and remain there in both encrypted and decrypted forms, 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, 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-1CA 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 in the requestors systems with a minimum RSA key length of 1024 bit. 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 the case of certificates requested for web-services, there is a need to deliver the key pair 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 file. 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 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 public key respectively CA certificate is published in Allianz Group Global Directory and it may be downloaded from the rootca.allianz.com website.

5.1.5 Key sizes

The INFRA-CA requires at least 1024 or preferred 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)

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.

5.2 Private Key Protection and Cryptographic Module Engineering Controls

INFRA-CA’s 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 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 at [LUNA_DOKU]

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

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)

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 redundantly on three 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). For details please refer to the HSM Documentation (see 6.2)

5.2.7 Private Key storage on cryptographic module

5.2.8 Method of activating private key

The CA private key is activated using operator cards 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

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 control applies. The private key on all redundant devices will be destroyed in succession.

5.2.11 Cryptographic Module Rating

INFRA-CA's secret signature key is stored in a FIPS 140-2 Level 3 compliant redundant Hardware Security Module Safenet Luna SA.

5.3 Other Aspects of Key Pair Management

5.3.1 Public Key Archival

INFRA-CA archives all public keys it certifies.

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; and
- 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

There is one exception for OS/390 keys, which are subject to certificate renewal resulting in an extended key usage.

5.4 Activation Data

5.4.1 Activation data generation and installation

Activation data for the INFRA-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).

The activation data for java keystores used 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 Allianz Group User Access Management Standard (GISF2.2).

5.4.2 Activation data protection

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

5.4.3 Other aspects of activation data

No stipulation.

5.5 Computer security controls

5.5.1 Specific computer security technical requirements

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 INFRA-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 INFRA-CA systems including data.

5.5.2 Computer security rating

The hardened operating system of INFRA-CA and its CA software is approved by Allianz Group RCA II. 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 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

A-IT05CES02 establishes a change management system to control and monitor the configurations of the systems and prevent unauthorized modification.

5.6.3 Life cycle security controls

The configuration of the INFRA-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.

5.7 Network Security Controls

The INFRA-CA is an online system. Access to the CA servers is protected by a firewall. The Allianz Group LAN is protected from outside networks by firewalls. Only Allianz Group 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 baseline profile for INFRA-CA certificates and end-entity certificates used within the Allianz Group RCA PKI. It is currently recommended that network certificates to be used within the Allianz Group RCA framework should be issued by this Allianz Infrastructure CA in Allianz Group.

There are different certificate profiles in use depending on the intended use of the certificate. For details of the issued certificates please refer to Appendix Certificate:

```
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Root CA II
        Validity
            Not Before: Nov 14 11:48:12 2006 GMT
            Not After : Nov 10 11:48:12 2021 GMT
        Subject: C=DE, O=Allianz Group, CN=Allianz Group Infrastructure3 CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ab:36:5f:cb:da:c4:06:5f:02:28:23:95:c7:f0:
                    e8:3c:50:d5:ce:47:05:03:d8:27:cd:f9:3d:89:a3:
                    3c:d6:05:db:d1:34:44:cb:2b:f8:28:74:f5:fa:5c:
```

```
                    3b:ff:db:13:7d:83:92:5b:53:2a:fd:48:d0:cc:c1:
                    7c:80:11:56:0a:3f:38:f8:24:e0:df:52:e0:e7:17:
                    11:dc:7f:c6:6f:9a:65:f7:67:24:6a:2e:13:da:52:
                    89:85:ac:90:c8:fe:31:f9:67:b2:a4:ea:0f:6f:05:
                    57:1f:1f:81:84:d4:7c:eb:eb:d7:0b:8b:ec:05:dc:
                    02:d7:aa:a8:f8:ef:62:8f:cf:b6:91:4e:12:2e:5e:
                    5d:16:c9:d5:85:5c:8f:27:e3:85:d6:65:9e:e1:bd:
                    d9:f3:0d:e4:b6:af:20:e2:74:9d:d7:8b:38:0e:9a:
                    4e:cf:dc:30:9e:2b:c0:7f:0e:68:54:e6:2a:e9:0a:
                    ed:90:90:83:83:03:ae:39:cc:0f:be:8b:fb:26:ee:
                    61:4c:3a:da:9f:eb:ed:a0:17:24:50:8c:e6:b4:21:
                    fb:0e:f7:fb:45:b1:c8:fa:ad:6d:48:0e:13:9b:13:
                    14:10:1d:ee:9e:0c:6a:40:40:72:3c:b8:fd:2e:7f:
                    98:0d:c3:c1:78:55:3f:4f:bb:b9:5a:ac:8b:5d:0e:
                    55:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                29:A5:92:C0:D9:D9:B1:AA:EB:74:9C:17:72:78:8A:C1:E0:EA:56:45
            X509v3 Authority Key Identifier:

keyid:C0:7D:0A:37:BC:D9:61:D5:D1:CB:B6:2C:F6:37:3A:09:3C:A2:4B:7
9

            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 R
oot CA II, by Allianz Group Germany

            1.3.6.1.4.1.311.21.1:
                ...
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
    Signature Algorithm: sha1WithRSAEncryption
        05:df:e9:4c:74:a0:15:8e:d0:03:6f:3d:dd:04:f1:d0:23:bf:
        26:5c:d9:a3:cc:36:52:05:8b:3f:41:e3:1a:9d:bf:46:f3:89:
        33:a3:b7:fb:c8:bb:71:5d:ba:9d:a5:e4:eb:05:86:e5:10:49:
        bf:3b:53:e5:f3:57:28:f4:58:38:3e:4d:1d:22:3f:1a:97:4d:
        1e:78:62:d0:86:30:2b:1f:9f:9a:3d:99:0e:02:2d:2a:32:e8:
        5e:63:4f:25:f9:30:59:cd:13:53:d6:fa:a0:1a:3a:7c:d5:1c:
        5f:e4:84:31:8e:95:1a:dc:fc:c2:6d:8b:ab:96:44:9c:ab:dd:
        87:89:bc:55:33:23:1e:bf:eb:cf:0c:8c:ff:3d:28:e8:43:21:
        25:54:e8:99:d9:0f:f3:44:9d:f1:53:3b:81:79:1e:f3:31:ab:
        dc:be:1c:cb:eb:d9:f7:66:11:8a:af:a7:74:71:01:73:d4:84:
        8f:0c:da:1c:d4:14:d1:1b:9a:ed:dd:25:80:89:51:97:93:f7:
        c5:ae:5e:e0:97:a3:4f:93:bd:0b:0b:93:c9:6a:36:08:cf:11:
```

```
        6a:9c:94:bd:d9:39:71:dd:4d:73:34:3b:36:e7:c1:63:1e:85:
        b7:cf:d3:24:b1:0b:f3:6a:a9:c4:fe:5e:2a:3a:9d:f4:38:c3:
        f1:d0:98:a3:4f:0b:f6:9f:79:e5:20:58:54:47:42:60:47:09:
        0f:e3:6a:ea:22:5f:56:98:88:46:78:9e:48:3e:34:51:e6:8a:
        d2:9d:f5:4e:ef:d8:f5:ad:2c:b1:a2:ba:a2:c5:b5:37:e4:ce:
        52:df:99:b6:79:9f:b9:10:f9:75:ac:06:3e:23:a6:9c:88:44:
        35:d6:89:5b:bc:48:ed:a9:47:75:ef:57:de:5e:2b:e0:da:69:
        4a:05:96:b7:77:01:bd:8c:8f:2d:3f:f9:63:19:f2:cc:41:ef:
        41:0e:8b:e0:05:90:27:f3:e6:f7:05:6d:3b:ca:b8:a6:fd:b2:
        f9:2f:c9:54:57:5b:4b:29:80:73:1d:8b:8c:c4:c5:e0:63:48:
        d9:51:85:7e:f5:99:9a:bf:a8:e2:d1:6d:22:c0:cd:82:4a:33:
        8c:70:20:82:d3:91:30:a9:dd:13:f4:58:02:27:63:c7:28:0f:
        40:77:48:3e:1b:37:bf:d0:29:17:91:71:4d:73:ab:2f:c3:1c:
        ad:eb:86:18:bd:0d:3e:d3:13:ec:81:4f:75:3c:02:95:cc:96:
        78:83:c7:2a:b4:9f:7f:c9:97:92:f1:9f:3c:8f:5f:b5:d3:23:
        e5:46:8c:3b:67:fc:03:3e:28:5f:33:4a:52:b1:f4:d1:f2:2f:
        d8:26:2c:65:ca:0e:7f:57
```

B Sample Certificates.

6.1.1 Version numbers

INFRA-CA 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 are shown in the Appendix `Certificate:`

```
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Root CA II
        Validity
            Not Before: Nov 14 11:48:12 2006 GMT
            Not After : Nov 10 11:48:12 2021 GMT
        Subject: C=DE, O=Allianz Group, CN=Allianz Group Infrastructure3 CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ab:36:5f:cb:da:c4:06:5f:02:28:23:95:c7:f0:
                    e8:3c:50:d5:ce:47:05:03:d8:27:cd:f9:3d:89:a3:
                    3c:d6:05:db:d1:34:44:cb:2b:f8:28:74:f5:fa:5c:
                    3b:ff:db:13:7d:83:92:5b:53:2a:fd:48:d0:cc:c1:
                    7c:80:11:56:0a:3f:38:f8:24:e0:df:52:e0:e7:17:
                    11:dc:7f:c6:6f:9a:65:f7:67:24:6a:2e:13:da:52:
                    89:85:ac:90:c8:fe:31:f9:67:b2:a4:ea:0f:6f:05:
                    57:1f:1f:81:84:d4:7c:eb:eb:d7:0b:8b:ec:05:dc:
                    02:d7:aa:a8:f8:ef:62:8f:cf:b6:91:4e:12:2e:5e:
                    5d:16:c9:d5:85:5c:8f:27:e3:85:d6:65:9e:e1:bd:
                    d9:f3:0d:e4:b6:af:20:e2:74:9d:d7:8b:38:0e:9a:
                    4e:cf:dc:30:9e:2b:c0:7f:0e:68:54:e6:2a:e9:0a:
                    ed:90:90:83:83:03:ae:39:cc:0f:be:8b:fb:26:ee:
                    61:4c:3a:da:9f:eb:ed:a0:17:24:50:8c:e6:b4:21:
                    fb:0e:f7:fb:45:b1:c8:fa:ad:6d:48:0e:13:9b:13:
                    14:10:1d:ee:9e:0c:6a:40:40:72:3c:b8:fd:2e:7f:
                    98:0d:c3:c1:78:55:3f:4f:bb:b9:5a:ac:8b:5d:0e:
                    55:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                29:A5:92:C0:D9:D9:B1:AA:EB:74:9C:17:72:78:8A:C1:E0:EA:56:45
            X509v3 Authority Key Identifier:

keyid:C0:7D:0A:37:BC:D9:61:D5:D1:CB:B6:2C:F6:37:3A:09:3C:A2:4B:7
9

            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 R
oot CA II, by Allianz Group Germany

            1.3.6.1.4.1.311.21.1:
                ...
            1.3.6.1.4.1.311.20.2:
                .
.S.u.b.C.A
    Signature Algorithm: sha1WithRSAEncryption
        05:df:e9:4c:74:a0:15:8e:d0:03:6f:3d:dd:04:f1:d0:23:bf:
        26:5c:d9:a3:cc:36:52:05:8b:3f:41:e3:1a:9d:bf:46:f3:89:
        33:a3:b7:fb:c8:bb:71:5d:ba:9d:a5:e4:eb:05:86:e5:10:49:
        bf:3b:53:e5:f3:57:28:f4:58:38:3e:4d:1d:22:3f:1a:97:4d:
        1e:78:62:d0:86:30:2b:1f:9f:9a:3d:99:0e:02:2d:2a:32:e8:
        5e:63:4f:25:f9:30:59:cd:13:53:d6:fa:a0:1a:3a:7c:d5:1c:
        5f:e4:84:31:8e:95:1a:dc:fc:c2:6d:8b:ab:96:44:9c:ab:dd:
        87:89:bc:55:33:23:1e:bf:eb:cf:0c:8c:ff:3d:28:e8:43:21:
        25:54:e8:99:d9:0f:f3:44:9d:f1:53:3b:81:79:1e:f3:31:ab:
        dc:be:1c:cb:eb:d9:f7:66:11:8a:af:a7:74:71:01:73:d4:84:
        8f:0c:da:1c:d4:14:d1:1b:9a:ed:dd:25:80:89:51:97:93:f7:
        c5:ae:5e:e0:97:a3:4f:93:bd:0b:0b:93:c9:6a:36:08:cf:11:
        6a:9c:94:bd:d9:39:71:dd:4d:73:34:3b:36:e7:c1:63:1e:85:
        b7:cf:d3:24:b1:0b:f3:6a:a9:c4:fe:5e:2a:3a:9d:f4:38:c3:
        f1:d0:98:a3:4f:0b:f6:9f:79:e5:20:58:54:47:42:60:47:09:
        0f:e3:6a:ea:22:5f:56:98:88:46:78:9e:48:3e:34:51:e6:8a:
        d2:9d:f5:4e:ef:d8:f5:ad:2c:b1:a2:ba:a2:c5:b5:37:e4:ce:
        52:df:99:b6:79:9f:b9:10:f9:75:ac:06:3e:23:a6:9c:88:44:
        35:d6:89:5b:bc:48:ed:a9:47:75:ef:57:de:5e:2b:e0:da:69:
        4a:05:96:b7:77:01:bd:8c:8f:2d:3f:f9:63:19:f2:cc:41:ef:
        41:0e:8b:e0:05:90:27:f3:e6:f7:05:6d:3b:ca:b8:a6:fd:b2:
        f9:2f:c9:54:57:5b:4b:29:80:73:1d:8b:8c:c4:c5:e0:63:48:
        d9:51:85:7e:f5:99:9a:bf:a8:e2:d1:6d:22:c0:cd:82:4a:33:
        8c:70:20:82:d3:91:30:a9:dd:13:f4:58:02:27:63:c7:28:0f:
        40:77:48:3e:1b:37:bf:d0:29:17:91:71:4d:73:ab:2f:c3:1c:
        ad:eb:86:18:bd:0d:3e:d3:13:ec:81:4f:75:3c:02:95:cc:96:
        78:83:c7:2a:b4:9f:7f:c9:97:92:f1:9f:3c:8f:5f:b5:d3:23:
        e5:46:8c:3b:67:fc:03:3e:28:5f:33:4a:52:b1:f4:d1:f2:2f:
        d8:26:2c:65:ca:0e:7f:57
```

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 issues certificates using the following Algorithm object identifiers:

§ Signature Algorithm: sha1WithRSAEncryption

§ Public Key Algorithm: rsaEncryption

6.1.4 Name forms

Certificates issued by the INFRA-CA System contain the full X.500 distinguished name of the certificate issuer. Certificates must contain a Subject DN.

Due to the varying 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 Group

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

No stipulation.

7 Compliance Audit and other assessment

The following procedures apply to INFRA-CA as intermediate CA of RCA. Clients of INFRA-CA 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 PKI infrastructure is conducted by RCA prior to issuing INFRA-CA certificates. The purpose of the audit process is to determine that INFRA-CA complies with the minimum eligibility, operational and technical requirements of the Allianz Group RCA Operating Rules.

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

7.2 Identity/qualifications of assessor

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

7.3 Assessor's relationship to assessed entity

Allianz Group RCA II 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 Group PAC decides in each individual case of deficiency what kind of actions should be taken in order that the security of the INFRA-CA 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 Group RCA II. Allianz Group RCA II 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 is classified and marked with the data classification level in compliance with Allianz Group Information Security Framework. In general INFRA-CA 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, cf. section 8.

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 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 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. Intellectual property rights in Distinguished Names vest in the assigning subscriber. Copyright in the Object Identifiers (OID) for the INFRA-CA System vests solely in INFRA-CA. 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 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 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 Group 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 Group has been advised of the possibility of such damages.

8.9 Indemnities

By accepting a certificate, the subscriber agrees to indemnify and hold Allianz Group 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 Group, 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 Group 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 operational period is currently not limited.

8.10.2 Termination

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

8.10.3 Effect of termination and survival

After revocation, INFRA-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.

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.

8.11 Individual notices and communications with participants

8.12 Amendments

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

8.12.2 Notification mechanism and period

New or amended policies are published on the internet web site designated for Allianz Group RCA documentation. PAC endorses the INFRA-CA CPS and all changes to this CPS. If a new CPS is approved, signed and distributed by A-IT05CES02 INFRA-CA, 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 Group 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 A-IT05CES02 INFRA-CA 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 II CPS, INFRA-CA 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 A-IT05CES02 INFRA-CA shall govern.

8.16.5 Force Majeure

INFRA-CA maintains contingency plans in force, including adequate back up and recovery procedures, to ensure INFRA-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 INFRA-CA's primary computer facilities or other operating facilities.

8.17 Other Provisions

8.17.1 Rights of investigation

The INFRA-CA 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 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 Group RCA CPS.

INFRA-CA 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

INFRA-CA operates under the Allianz Group RCA 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 Group RCA 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 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 might be required to minimise damage or liability to all Allianz Group RCA participants;
- Assisting in audits conducted by the Root Certificate Authority to validate the renewal of their own certificates.
- Establishing and maintaining its own CPS within the general context of the Allianz Group RCA CPS.

8.17.3 Operational compliance

All certificate operations comply with the policy requirements of

- this CPS; and
- the Allianz Group 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.

Appendix

A CA Signing Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Root CA II
        Validity
            Not Before: Nov 14 11:48:12 2006 GMT
            Not After : Nov 10 11:48:12 2021 GMT
        Subject: C=DE, O=Allianz Group, CN=Allianz Group Infrastructure3 CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ab:36:5f:cb:da:c4:06:5f:02:28:23:95:c7:f0:
                    e8:3c:50:d5:ce:47:05:03:d8:27:cd:f9:3d:89:a3:
                    3c:d6:05:db:d1:34:44:cb:2b:f8:28:74:f5:fa:5c:
                    3b:ff:db:13:7d:83:92:5b:53:2a:fd:48:d0:cc:c1:
                    7c:80:11:56:0a:3f:38:f8:24:e0:df:52:e0:e7:17:
                    11:dc:7f:c6:6f:9a:65:f7:67:24:6a:2e:13:da:52:
                    89:85:ac:90:c8:fe:31:f9:67:b2:a4:ea:0f:6f:05:
                    57:1f:1f:81:84:d4:7c:eb:eb:d7:0b:8b:ec:05:dc:
                    02:d7:aa:a8:f8:ef:62:8f:cf:b6:91:4e:12:2e:5e:
                    5d:16:c9:d5:85:5c:8f:27:e3:85:d6:65:9e:e1:bd:
                    d9:f3:0d:e4:b6:af:20:e2:74:9d:d7:8b:38:0e:9a:
                    4e:cf:dc:30:9e:2b:c0:7f:0e:68:54:e6:2a:e9:0a:
                    ed:90:90:83:83:03:ae:39:cc:0f:be:8b:fb:26:ee:
                    61:4c:3a:da:9f:eb:ed:a0:17:24:50:8c:e6:b4:21:
                    fb:0e:f7:fb:45:b1:c8:fa:ad:6d:48:0e:13:9b:13:
                    14:10:1d:ee:9e:0c:6a:40:40:72:3c:b8:fd:2e:7f:
                    98:0d:c3:c1:78:55:3f:4f:bb:b9:5a:ac:8b:5d:0e:
                    55:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                29:A5:92:C0:D9:D9:B1:AA:EB:74:9C:17:72:78:8A:C1:E0:EA:56:45
            X509v3 Authority Key Identifier:

keyid:C0:7D:0A:37:BC:D9:61:D5:D1:CB:B6:2C:F6:37:3A:09:3C:A2:4B:7
9

            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 R
oot CA II, by Allianz Group Germany

            1.3.6.1.4.1.311.21.1: 
                ...
            1.3.6.1.4.1.311.20.2: 
                .
.S.u.b.C.A
    Signature Algorithm: sha1WithRSAEncryption
        05:df:e9:4c:74:a0:15:8e:d0:03:6f:3d:dd:04:f1:d0:23:bf:
        26:5c:d9:a3:cc:36:52:05:8b:3f:41:e3:1a:9d:bf:46:f3:89:
        33:a3:b7:fb:c8:bb:71:5d:ba:9d:a5:e4:eb:05:86:e5:10:49:
        bf:3b:53:e5:f3:57:28:f4:58:38:3e:4d:1d:22:3f:1a:97:4d:
        1e:78:62:d0:86:30:2b:1f:9f:9a:3d:99:0e:02:2d:2a:32:e8:
        5e:63:4f:25:f9:30:59:cd:13:53:d6:fa:a0:1a:3a:7c:d5:1c:
        5f:e4:84:31:8e:95:1a:dc:fc:c2:6d:8b:ab:96:44:9c:ab:dd:
        87:89:bc:55:33:23:1e:bf:eb:cf:0c:8c:ff:3d:28:e8:43:21:
        25:54:e8:99:d9:0f:f3:44:9d:f1:53:3b:81:79:1e:f3:31:ab:
        dc:be:1c:cb:eb:d9:f7:66:11:8a:af:a7:74:71:01:73:d4:84:
        8f:0c:da:1c:d4:14:d1:1b:9a:ed:dd:25:80:89:51:97:93:f7:
        c5:ae:5e:e0:97:a3:4f:93:bd:0b:0b:93:c9:6a:36:08:cf:11:
        6a:9c:94:bd:d9:39:71:dd:4d:73:34:3b:36:e7:c1:63:1e:85:
        b7:cf:d3:24:b1:0b:f3:6a:a9:c4:fe:5e:2a:3a:9d:f4:38:c3:
        f1:d0:98:a3:4f:0b:f6:9f:79:e5:20:58:54:47:42:60:47:09:
        0f:e3:6a:ea:22:5f:56:98:88:46:78:9e:48:3e:34:51:e6:8a:
        d2:9d:f5:4e:ef:d8:f5:ad:2c:b1:a2:ba:a2:c5:b5:37:e4:ce:
        52:df:99:b6:79:9f:b9:10:f9:75:ac:06:3e:23:a6:9c:88:44:
        35:d6:89:5b:bc:48:ed:a9:47:75:ef:57:de:5e:2b:e0:da:69:
        4a:05:96:b7:77:01:bd:8c:8f:2d:3f:f9:63:19:f2:cc:41:ef:
        41:0e:8b:e0:05:90:27:f3:e6:f7:05:6d:3b:ca:b8:a6:fd:b2:
        f9:2f:c9:54:57:5b:4b:29:80:73:1d:8b:8c:c4:c5:e0:63:48:
        d9:51:85:7e:f5:99:9a:bf:a8:e2:d1:6d:22:c0:cd:82:4a:33:
        8c:70:20:82:d3:91:30:a9:dd:13:f4:58:02:27:63:c7:28:0f:
        40:77:48:3e:1b:37:bf:d0:29:17:91:71:4d:73:ab:2f:c3:1c:
        ad:eb:86:18:bd:0d:3e:d3:13:ec:81:4f:75:3c:02:95:cc:96:
        78:83:c7:2a:b4:9f:7f:c9:97:92:f1:9f:3c:8f:5f:b5:d3:23:
        e5:46:8c:3b:67:fc:03:3e:28:5f:33:4a:52:b1:f4:d1:f2:2f:
        d8:26:2c:65:ca:0e:7f:57
```

B Sample Certificates

B.1 Code-Signing

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            38:5d:1f:61:00:00:00:00:02:ac
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Infrastructure3 CA
        Validity
            Not Before: Mar 19 14:26:46 2010 GMT
            Not After : Mar 18 14:26:46 2012 GMT
        Subject: C=DE, O=Allianz, CN=Allianz CodeSigning Certificate
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:e2:48:30:90:f7:88:d5:71:a1:35:d1:9b:a9:3e:
```

```
                    ...
                    ca:73
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Subject Key Identifier:
                34:19:2B:BF:D5:25:C5:FA:AD:42:03:66:37:5A:9F:9B:30:1D:AA:A3
            1.3.6.1.4.1.311.21.7:
                0-.%+.....7.....7...............3...Z...z..e...
            X509v3 CRL Distribution Points:

URI:ldap:///CN=Allianz%20Group%20Infrastructure3%20CA,CN=nsvmucc
j,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=rootdom,D
C=n
et?certificateRevocationList?base?objectClass=cRLDistributionPoint

URI:http://nsvmuccj.rootdom.net/CertEnroll/Allianz%20Group%20Inf
rastructure3%20CA.crl
                URI:http://rootca.allianz.com/infraca/InfraCA3.crl
                URI:http://rootca.ind.allianz/infraca/InfraCA3.crl

            Authority Information Access:
                CA Issuers -
URI:ldap:///CN=Allianz%20Group%20Infrastructure3%20
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=rootdom,
DC=
net?cACertificate?base?objectClass=certificationAuthority
                CA Issuers -
URI:http://nsvmuccj.rootdom.net/CertEnroll/nsvmuccj
.rootdom.net_Allianz%20Group%20Infrastructure3%20CA.crt
                CA Issuers -
URI:http://rootca.allianz.com/infraca/InfraCA3.crt
                CA Issuers -
URI:http://rootca.ind.allianz/infraca/InfraCA3.crt

            X509v3 Extended Key Usage:
                Code Signing
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......
            X509v3 Subject Alternative Name:
                email:pki-support@allianz.de
    Signature Algorithm: sha1WithRSAEncryption
        a1:2e:b0:e0:04:59:17:a0:b4:5d:87:92:92:05:bb:ba:43:2a:
        ...
        44:3d:d7:40
```

B.2 Domain Controller

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            19:1d:bc:c1:00:00:00:00:1a:73
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Infrastructure3 CA
        Validity
            Not Before: Feb 25 11:17:51 2011 GMT
            Not After : Feb 25 11:17:51 2012 GMT
        Subject: CN=ndcmucup.wwg00m.rootdom.net
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c2:4a:e3:b5:ed:b2:4c:bb:4a:4d:ee:55:d8:12:
                    ...
                    4a:50:49:c7:d0:6a:8f:f8:f1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            1.3.6.1.4.1.311.21.7:
                0..&+.....7.....7..............3...._...4..f...
            X509v3 Extended Key Usage:
                Microsoft Smartcardlogin, TLS Web Server Authentication, TLS
Web
 Client Authentication
            1.3.6.1.4.1.311.21.10:
                0&0..
+.....7...0
..+.......0
..+.......
            X509v3 Subject Alternative Name:
                DNS:ndcmucup.wwg00m.rootdom.net
            X509v3 Subject Key Identifier:
                AB:98:D1:40:B5:86:09:8E:9A:03:66:7B:67:C0:7E:7A:D2:47:1B:84
            X509v3 CRL Distribution Points:

URI:ldap:///CN=Allianz%20Group%20Infrastructure3%20CA,CN=nsvmucc
j,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=rootdom,D
C=n
et?certificateRevocationList?base?objectClass=cRLDistributionPoint

URI:http://nsvmuccj.rootdom.net/CertEnroll/Allianz%20Group%20Inf
rastructure3%20CA.crl
                URI:http://rootca.allianz.com/infraca/InfraCA3.crl
                URI:http://rootca.ind.allianz/infraca/InfraCA3.crl

            Authority Information Access:
                CA Issuers -
URI:ldap:///CN=Allianz%20Group%20Infrastructure3%20
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=rootdom,
DC=
net?cACertificate?base?objectClass=certificationAuthority
                CA Issuers -
URI:http://nsvmuccj.rootdom.net/CertEnroll/nsvmuccj
.rootdom.net_Allianz%20Group%20Infrastructure3%20CA.crt
                CA Issuers -
URI:http://rootca.allianz.com/infraca/InfraCA3.crt
                CA Issuers -
URI:http://rootca.ind.allianz/infraca/InfraCA3.crt

    Signature Algorithm: sha1WithRSAEncryption
        a2:6c:23:04:db:85:4f:65:84:69:09:d2:cc:d8:f5:2c:8c:a5:
        ...
        71:08:de:d9
```

B.3 Router

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            17:1a:a2:6f:00:00:00:00:00:04
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Infrastructure3 CA
        Validity
            Not Before: Nov 14 15:21:48 2006 GMT
            Not After : Nov 13 15:21:48 2008 GMT
        Subject: C=DE, O=Allianz Group, CN=advpn-si-ad.allianz.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d7:07:e4:48:09:f6:de:15:71:39:91:08:e6:a8:
                    ...
                    a3:10:93:96:a4:15:c2:ca:c1
                Exponent: 3 (0x3)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                1.3.6.1.5.5.8.2.2
            X509v3 Subject Key Identifier:
                52:D9:82:04:AF:D0:65:73:31:73:4E:C7:09:E9:30:24:E3:AE:8A:E1
            X509v3 Authority Key Identifier:

keyid:29:A5:92:C0:D9:D9:B1:AA:EB:74:9C:17:72:78:8A:C1:E0:EA:56:4
5

            X509v3 CRL Distribution Points:

URI:ldap:///CN=Allianz%20Group%20Infrastructure3%20CA,CN=nsvmucc
j,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=rootdom,D
C=n
et?certificateRevocationList?base?objectClass=cRLDistributionPoint

URI:http://nsvmuccj.rootdom.net/CertEnroll/Allianz%20Group%20Inf
rastructure3%20CA.crl
                URI:http://rootca.allianz.com/infraca/InfraCA3.crl
                URI:http://rootca.ind.allianz/infraca/InfraCA3.crl

            Authority Information Access:
                CA Issuers -
URI:ldap:///CN=Allianz%20Group%20Infrastructure3%20
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=rootdom,
DC=
net?cACertificate?base?objectClass=certificationAuthority
                CA Issuers -
URI:http://nsvmuccj.rootdom.net/CertEnroll/nsvmuccj
.rootdom.net_Allianz%20Group%20Infrastructure3%20CA.crt
                CA Issuers -
URI:http://rootca.allianz.com/infraca/InfraCA3.crt
                CA Issuers -
URI:http://rootca.ind.allianz/infraca/InfraCA3.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
    Signature Algorithm: sha1WithRSAEncryption
        40:80:c5:42:2b:dc:b9:a1:d7:2e:11:e9:e4:b9:80:f0:37:93:
```

```
        ...
        21:c2:f4:2e
```

B.4 Webserver

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            12:49:78:d9:00:00:00:00:02:41
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Infrastructure3 CA
        Validity
            Not Before: Feb 15 08:28:53 2010 GMT
            Not After : Feb 15 08:28:53 2012 GMT
        Subject: C=DE, ST=Hessen, L=Frankfurt, O=Allianz ASIC SE,
OU=AG6DCI01, C
N=mail.ip.allianz/emailAddress=christof.chen@allianz.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d5:11:fd:96:9e:93:45:37:c6:ef:60:69:81:92:
                    ...
                    61:24:e0:bb:4e:7b:86:2c:b5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                59:3A:AF:61:B3:37:39:93:C3:9C:91:81:07:E2:70:43:07:CF:11:B1
            X509v3 CRL Distribution Points:

URI:ldap:///CN=Allianz%20Group%20Infrastructure3%20CA,CN=nsvmucc
j,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=rootdom,D
C=n
et?certificateRevocationList?base?objectClass=cRLDistributionPoint

URI:http://nsvmuccj.rootdom.net/CertEnroll/Allianz%20Group%20Inf
rastructure3%20CA.crl
                URI:http://rootca.allianz.com/infraca/InfraCA3.crl
                URI:http://rootca.ind.allianz/infraca/InfraCA3.crl

            Authority Information Access:
                CA Issuers -
URI:ldap:///CN=Allianz%20Group%20Infrastructure3%20
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=rootdom,
DC=
net?cACertificate?base?objectClass=certificationAuthority
                CA Issuers -
URI:http://nsvmuccj.rootdom.net/CertEnroll/nsvmuccj
.rootdom.net_Allianz%20Group%20Infrastructure3%20CA.crt
                CA Issuers -
URI:http://rootca.allianz.com/infraca/InfraCA3.crt
                CA Issuers -
URI:http://rootca.ind.allianz/infraca/InfraCA3.crt

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            1.3.6.1.4.1.311.21.7:
                0-.%+.....7.....7..............3...G...)..d...
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......0
..+.......
            X509v3 Subject Alternative Name:
                DNS:mail.ip.allianz
    Signature Algorithm: sha1WithRSAEncryption
        0b:b4:05:94:8e:aa:fe:9c:83:5d:51:83:51:3a:a0:40:72:e3:
        ...
        3f:64:20:6a
```

B.5 Webservice

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            51:85:61:66:00:00:00:00:02:75
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Allianz Group, CN=Allianz Group Infrastructure3 CA
        Validity
            Not Before: Feb 27 15:10:09 2010 GMT
            Not After : Feb 27 15:10:09 2012 GMT
        Subject: C=DE, ST=Bayern, L=Muenchen, O=Allianz Shared Infrastructure
Se
rvices SE, OU=Allianz Group, CN=banking.allianz.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:c9:50:c0:16:fc:3a:3f:9a:4c:3b:a8:a9:b0:ae:
                    ...
                    d9:79
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Subject Key Identifier:
                A8:69:B3:77:D7:BD:AF:20:DC:DB:BC:C0:D9:0B:02:9B:B3:2C:DD:95
            1.3.6.1.4.1.311.21.7:
                0..&+.....7.....7..............3....*......d...
            X509v3 CRL Distribution Points:

URI:ldap:///CN=Allianz%20Group%20Infrastructure3%20CA,CN=nsvmucc
j,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=rootdom,D
C=n
et?certificateRevocationList?base?objectClass=cRLDistributionPoint

URI:http://nsvmuccj.rootdom.net/CertEnroll/Allianz%20Group%20Inf
rastructure3%20CA.crl
                URI:http://rootca.allianz.com/infraca/InfraCA3.crl
                URI:http://rootca.ind.allianz/infraca/InfraCA3.crl

            Authority Information Access:
                CA Issuers -
URI:ldap:///CN=Allianz%20Group%20Infrastructure3%20
```

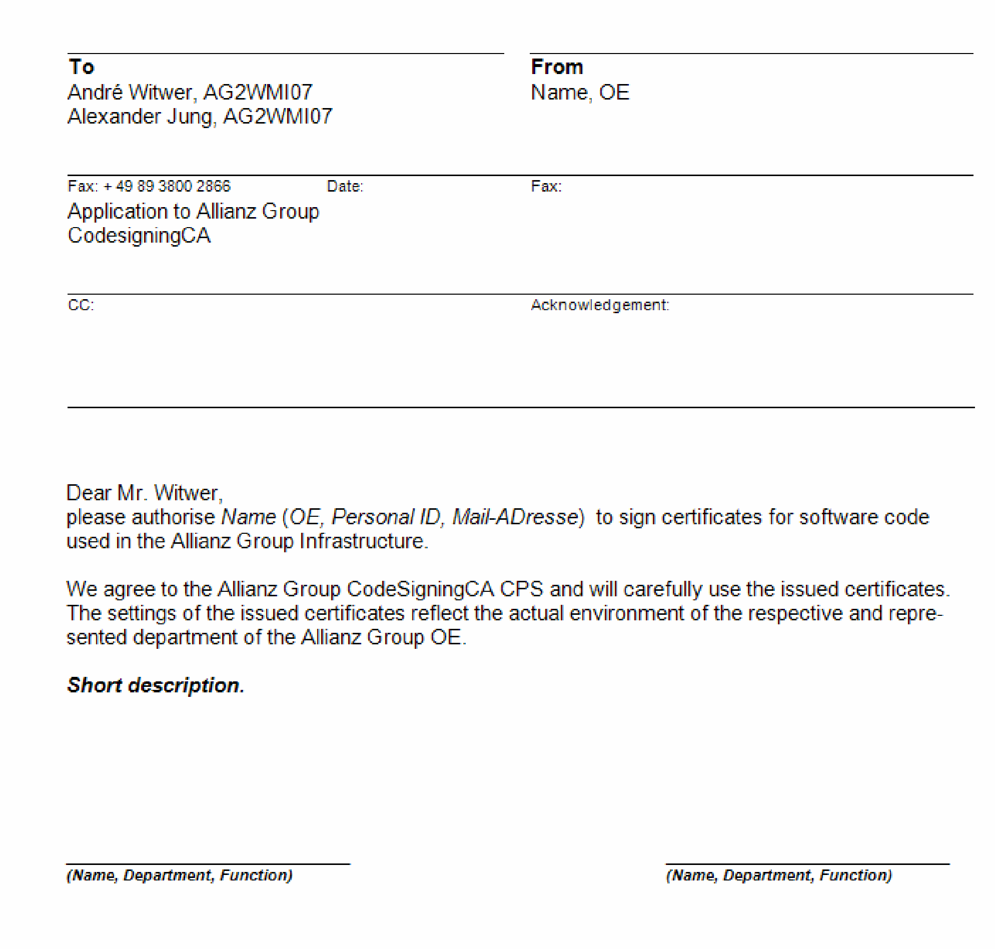
```
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=rootdom,
DC=
net?cACertificate?base?objectClass=certificationAuthority
                CA Issuers -
URI:http://nsvmuccj.rootdom.net/CertEnroll/nsvmuccj
.rootdom.net_Allianz%20Group%20Infrastructure3%20CA.crt
                CA Issuers -
URI:http://rootca.allianz.com/infraca/InfraCA3.crt
                CA Issuers -
URI:http://rootca.ind.allianz/infraca/InfraCA3.crt

            X509v3 Extended Key Usage:
                TLS Web Client Authentication
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......
            X509v3 Subject Alternative Name:
                email:martin.grassl@allianz.de
    Signature Algorithm: sha1WithRSAEncryption
        80:13:27:3a:70:0c:ea:07:19:3b:66:27:32:f8:5d:13:07:70:
        ...
        b6:75:c5:77
```

C Workflow Screenshots

C.1 Certificate Request Authorization Forms (Codesigning)

Certificate Requests to be processed by INFRA-CA must be authorized. The following screenshots document the authorization forms to be filled out in order to achieve the required authorization.



To
André Witwer, AG2WMI07
Alexander Jung, AG2WMI07

From
Name, OE

Fax: + 49 89 3800 2866 Date:
Application to Allianz Group
CodesigningCA

Fax:

CC:

Acknowledgement:

Dear Mr. Witwer,
please authorise *Name* (*OE, Personal ID, Mail-ADresse*) to sign certificates for software code used in the Allianz Group Infrastructure.

We agree to the Allianz Group CodeSigningCA CPS and will carefully use the issued certificates. The settings of the issued certificates reflect the actual environment of the respective and represented department of the Allianz Group OE.

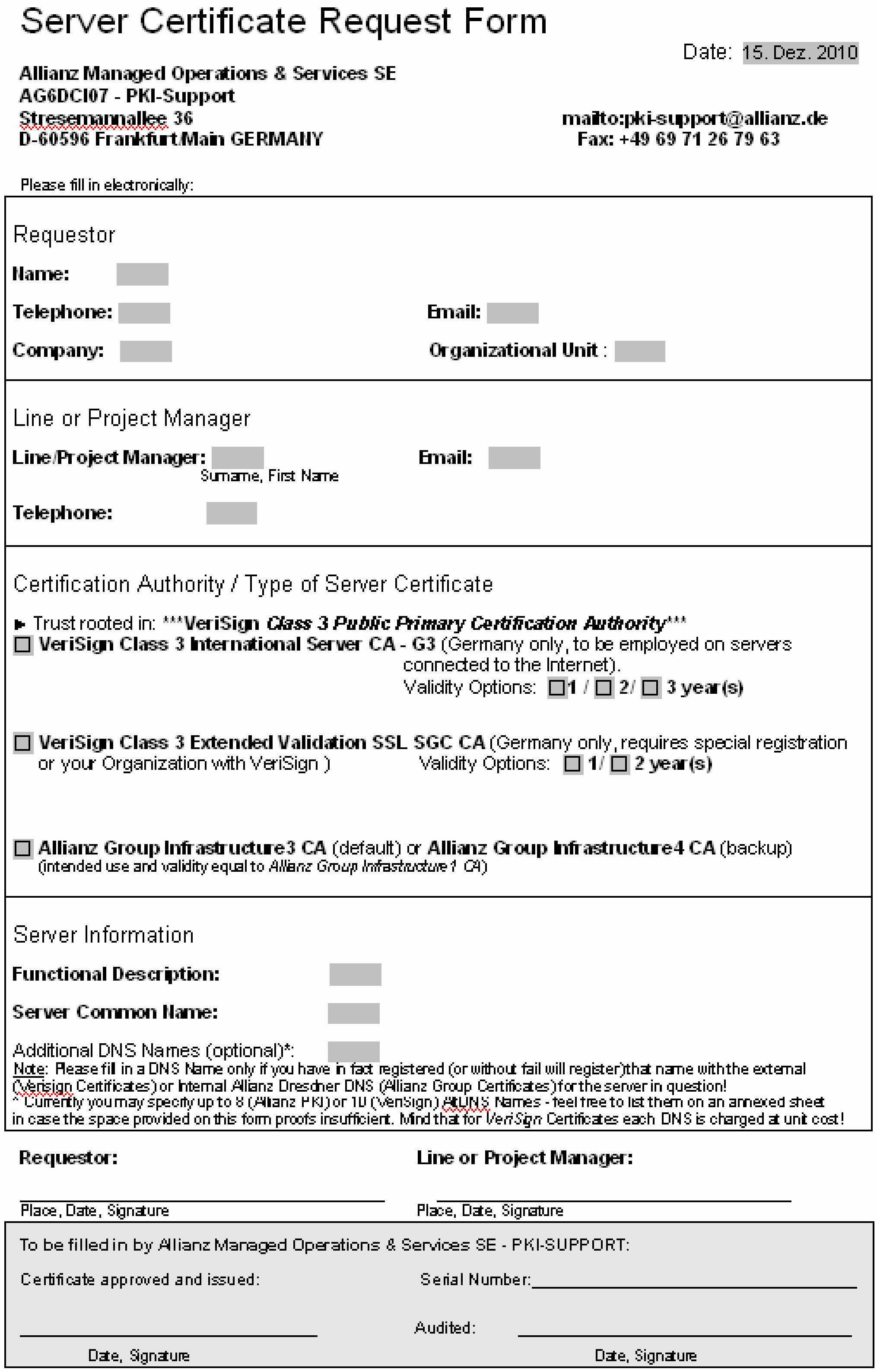
Short description.

(Name, Department, Function)

(Name, Department, Function)

Figure 2 Certificate Request Authorization Form (Codesigning)

C.2 Certificate Request Authorization Forms (Webserver)



Server Certificate Request Form

Date: 15. Dez. 2010

Allianz Managed Operations & Services SE
AG6DCI07 - PKI-Support
Stresemannallee 36
D-60596 Frankfurt/Main GERMANY

mailto:pki-support@allianz.de
Fax: +49 69 71 26 79 63

Please fill in electronically:

Requestor

Name:

Telephone: **Email:**

Company: **Organizational Unit :**

Line or Project Manager

Line/Project Manager: **Email:**
Surname, First Name

Telephone:

Certification Authority / Type of Server Certificate

► Trust rooted in: *****VeriSign *Class 3 Public Primary Certification Authority******

□ **VeriSign Class 3 International Server CA - G3** (Germany only, to be employed on servers connected to the Internet).
Validity Options: □**1** / □ **2**/ □ **3 year(s)**

□ **VeriSign Class 3 Extended Validation SSL SGC CA** (Germany only, requires special registration or your Organization with VeriSign)
Validity Options: □ **1**/ □ **2 year(s)**

□ **Allianz Group Infrastructure3 CA** (default) or **Allianz Group Infrastructure4 CA** (backup)
(intended use and validity equal to *Allianz Group Infastructure1 CA*)

Server Information

Functional Description:

Server Common Name:

Additional DNS Names (optional)*:

Note: Please fill in a DNS Name only if you have in fact registered (or without fail will register)that name with the external (Verisign Certificates) or Internal Allianz Dresdner DNS (Allianz Group Certificates) for the server in question!
* Currently you may specify up to 8 (Allianz PKI) or 10 (VeriSign) AltDNS Names - feel free to list them on an annexed sheet in case the space provided on this form proofs insufficient. Mind that for *VeriSign* Certificates each DNS is charged at unit cost!

Requestor: **Line or Project Manager:**

Place, Date, Signature Place, Date, Signature

To be filled in by Allianz Managed Operations & Services SE - PKI-SUPPORT:

Certificate approved and issued: Serial Number:__________________________

Audited:

Date, Signature Date, Signature

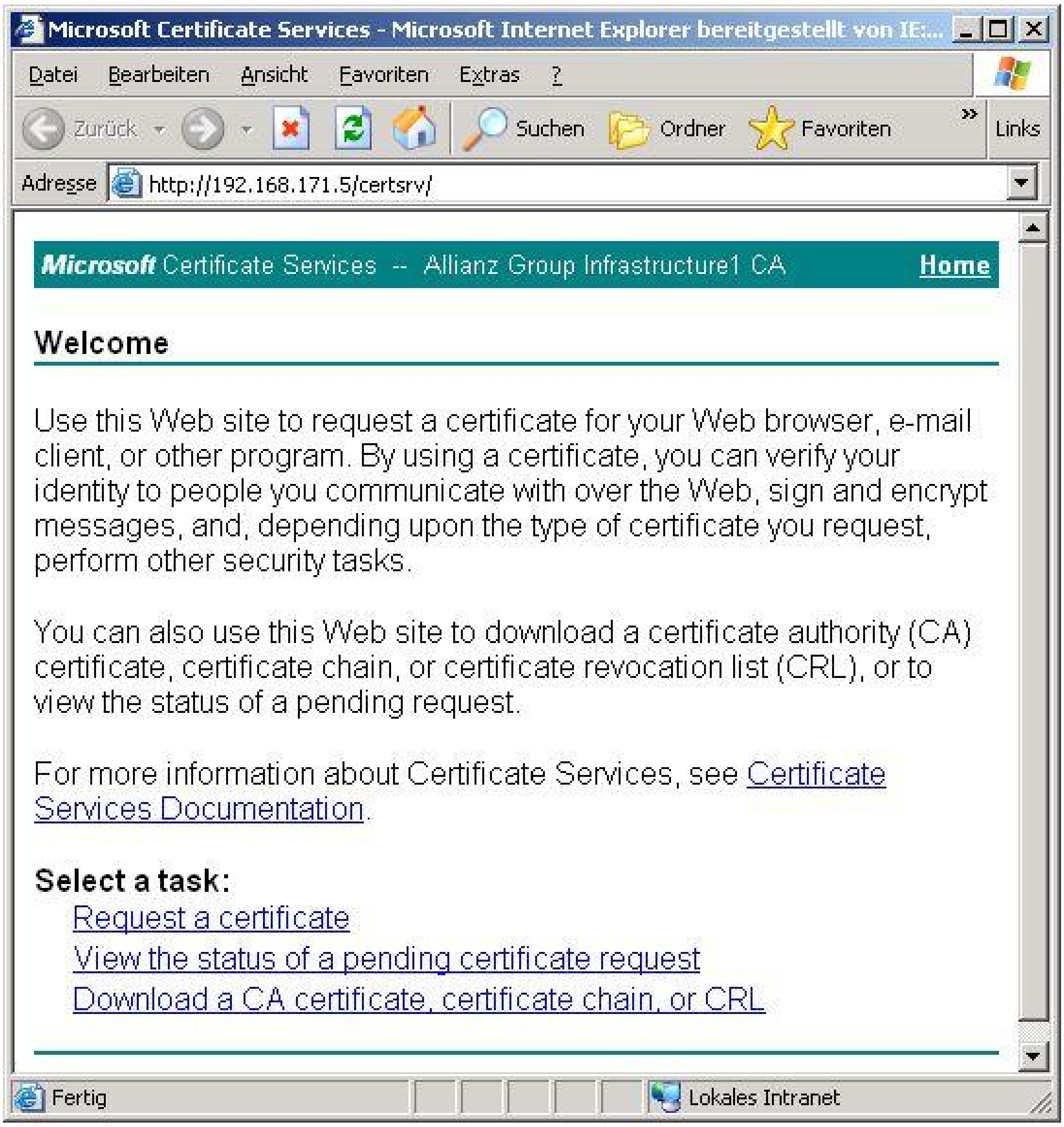
Figure 3 Certificate Request Authorization Form (Server certificate)

C.3 Certificate Application Forms (CA / RA Front-end)

On the next pages there are several screenshots documenting the web-interface presented to certificate subscribers. While Codesigning, Webserver and VPN certificates are handled via template selection (see Figure 6 Certificate Application Form – step 3, Submission of Certificate Request. Formfields for PCKS#10/7 Requestdata, Selectionbox for certificate template selection

) for requesting web service certificates there is an separate interface implemented (see Figure 8 Certificate Application Form for web service clients – step 2. Form fields for client name and choice of deployment area

).


Microsoft Certificate Services - Microsoft Internet Explorer bereitgestellt von IE:...
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Ordner
Favoriten
Links
Adresse
Fertig
Lokales Intranet

http://192.168.171.5/certsrv/

Microsoft Certificate Services -- Allianz Group Infrastructure1 CA Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

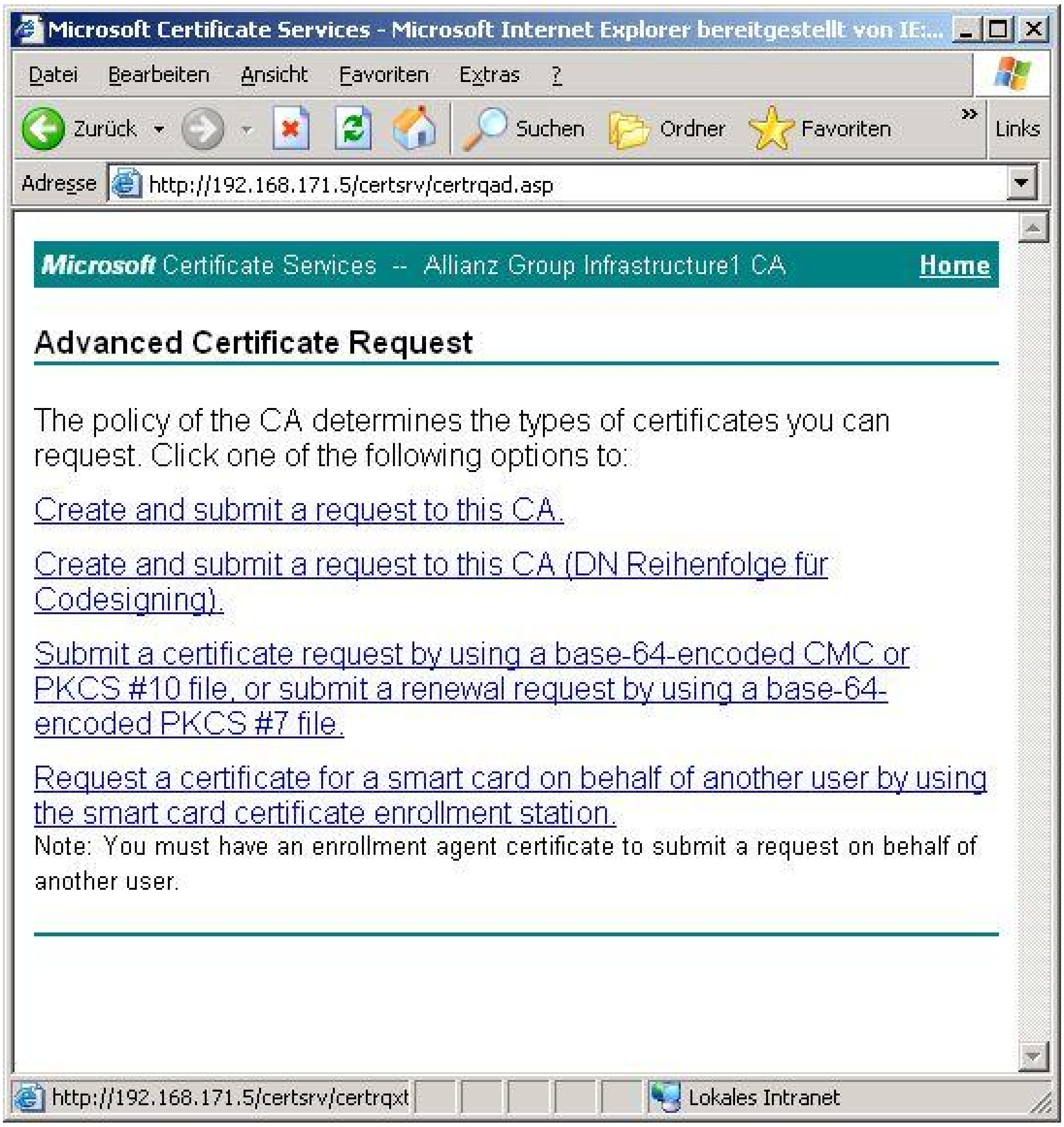
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:

- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

Figure 4 Certificate Application Form – step 1



Microsoft Certificate Services - Microsoft Internet Explorer bereitgestellt von IE:...
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück
Suchen
Ordner
Favoriten
Links
Adresse http://192.168.171.5/certsrv/certrqad.asp

Microsoft Certificate Services -- Allianz Group Infrastructure1 CA **Home**

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

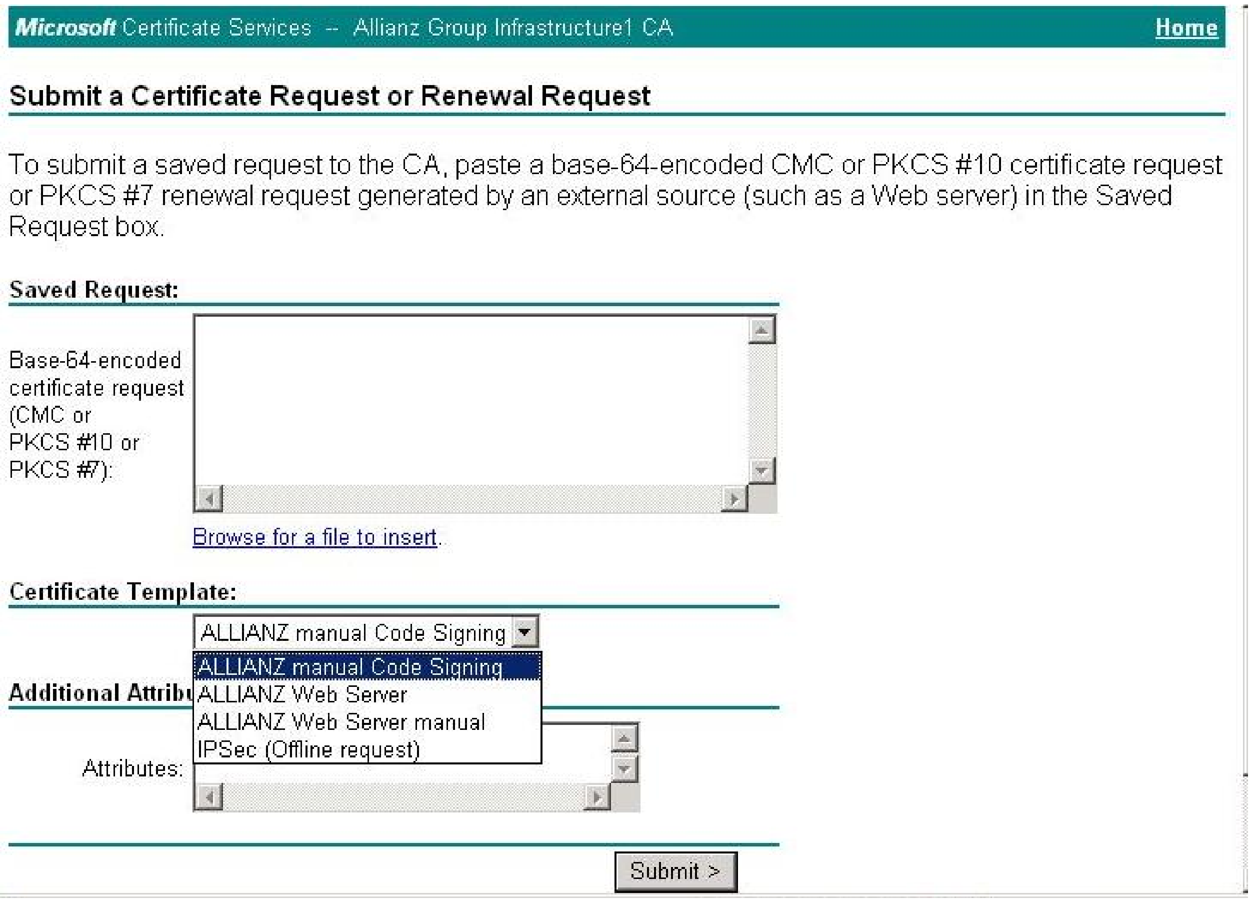
Create and submit a request to this CA (DN Reihenfolge für Codesigning).

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.

Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Figure 5 Certificate Application Form – step 2, Advanced Certificate Request



Microsoft Certificate Services -- Allianz Group Infrastructure1 CA
Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Browse for a file to insert.

Certificate Template:

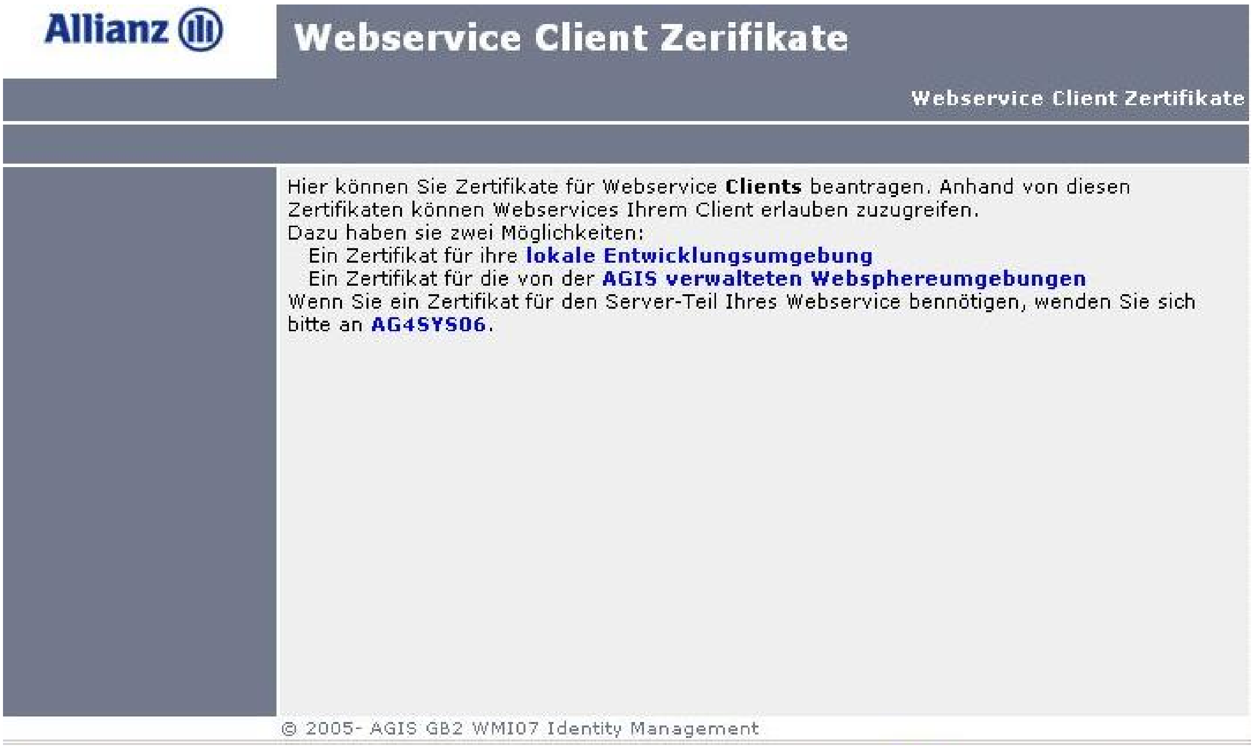
ALLIANZ manual Code Signing

Additional Attribu

Attributes:

Figure 6 Certificate Application Form – step 3, Submission of Certificate Request. Formfields for PCKS#10/7 Requestdata, Selectionbox for certificate template selection

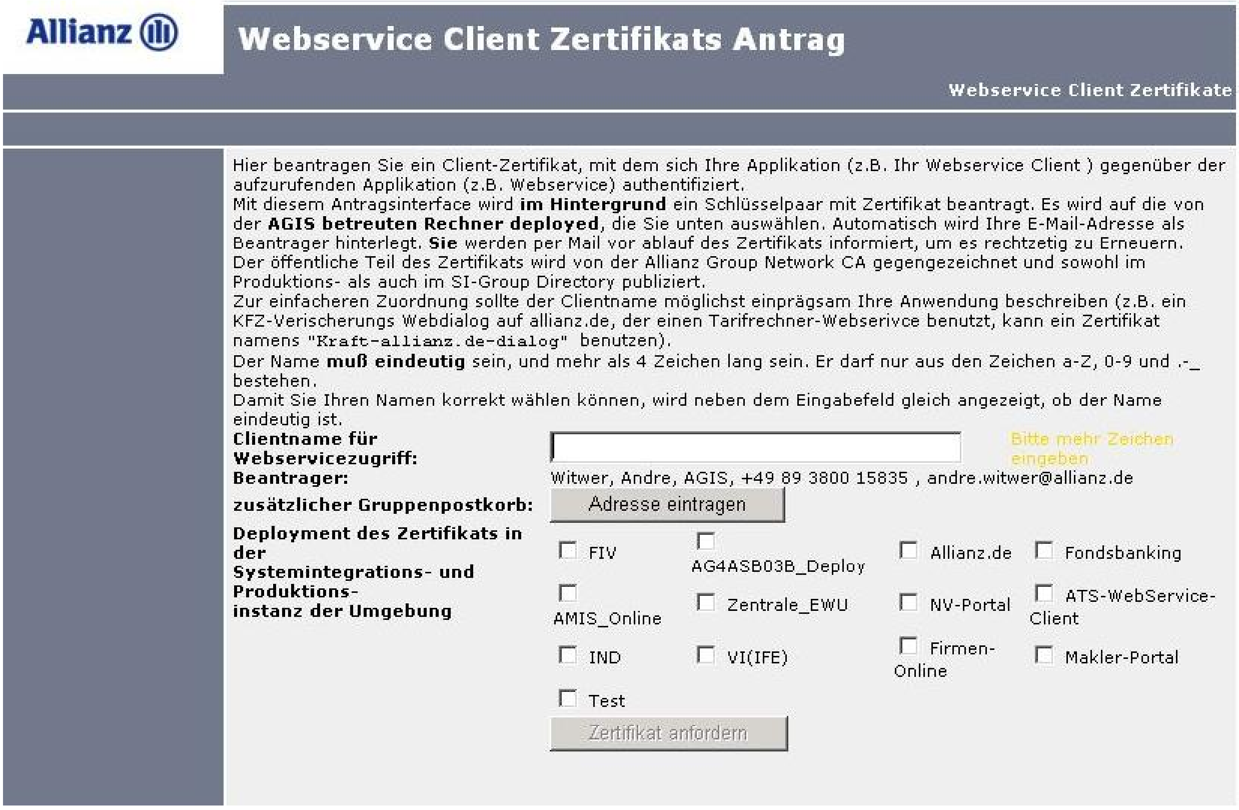
.



Hier können Sie Zertifikate für Webservice **Clients** beantragen. Anhand von diesen Zertifikaten können Webservices Ihrem Client erlauben zuzugreifen.
Dazu haben sie zwei Möglichkeiten:
Ein Zertifikat für ihre **lokale Entwicklungsumgebung**
Ein Zertifikat für die von der **AGIS verwalteten Websphereumgebungen**
Wenn Sie ein Zertifikat für den Server-Teil Ihres Webservice bennötigen, wenden Sie sich bitte an **AG4SYS06**.

© 2005- AGIS GB2 WMI07 Identity Management

Figure 7 Certificate Application Form for web service clients – step 1



Allianz
Webservice Client Zertifikats Antrag
Webservice Client Zertifikate

Hier beantragen Sie ein Client-Zertifikat, mit dem sich Ihre Applikation (z.B. Ihr Webservice Client) gegenüber der aufzurufenden Applikation (z.B. Webservice) authentifiziert.
Mit diesem Antragsinterface wird **im Hintergrund** ein Schlüsselpaar mit Zertifikat beantragt. Es wird auf die von der **AGIS betreuten Rechner deployed**, die Sie unten auswählen. Automatisch wird Ihre E-Mail-Adresse als Beantrager hinterlegt. **Sie** werden per Mail vor ablauf des Zertifikats informiert, um es rechtzetig zu Erneuern.
Der öffentliche Teil des Zertifikats wird von der Allianz Group Network CA gegengezeichnet und sowohl im Produktions- als auch im SI-Group Directory publiziert.
Zur einfacheren Zuordnung sollte der Clientname möglichst einprägsam Ihre Anwendung beschreiben (z.B. ein KFZ-Verischerungs Webdialog auf allianz.de, der einen Tarifrechner-Webserivce benutzt, kann ein Zertifikat namens "Kraft-allianz.de-dialog" benutzen).
Der Name **muß eindeutig** sein, und mehr als 4 Zeichen lang sein. Er darf nur aus den Zeichen a-Z, 0-9 und .-_ bestehen.
Damit Sie Ihren Namen korrekt wählen können, wird neben dem Eingabefeld gleich angezeigt, ob der Name eindeutig ist.

Clientname für Webservicezugriff: Bitte mehr Zeichen eingeben

Beantrager: Witwer, Andre, AGIS, +49 89 3800 15835 , andre.witwer@allianz.de

zusätzlicher Gruppenpostkorb: Adresse eintragen

Deployment des Zertifikats in der Systemintegrations- und Produktions-instanz der Umgebung

☐ FIV ☐ AG4ASB03B_Deploy ☐ Allianz.de ☐ Fondsbanking
☐ AMIS_Online ☐ Zentrale_EWU ☐ NV-Portal ☐ ATS-WebService-Client
☐ IND ☐ VI(IFE) ☐ Firmen-Online ☐ Makler-Portal
☐ Test

Zertifikat anfordern

Figure 8 Certificate Application Form for web service clients – step 2. Form fields for client name and choice of deployment area

D 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
HSM	Hardware Security Module
ISIS-MTT	Interoperability Standard (ISIS – Mail Trust)
ISO	Information Security Officer
NTLM	NT LAN Manager (Network Authentication based on Challenge / Response)
OCSP	Online Certificate Status Protocol
OE	Organisational Entity
OID	Object Identifier
OS/390	Operating System 390
OU	Organisational Unit
PAC	Policy Approval Council
RA	Registration Authority
RCA	Root Certification Authority
RFC	Request for Comment
SCEP	Simple Certificate Enrollment Protocol
TSM	Tivoli Storage Management
VPN	Virtual Private Network

E References

[RFC3647] Available at http://www.ietf.org/rfc/rfc3647.txt?number=3647

[AZ-SP] Allianz Group Security Policy – GISF 2.5

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

[AZ-RCACPS] Allianz Group Root CA II CPS

[ISIS/MTT] Teletrust: Common industrial Signature Interoperability Specifications. ISIS Mail Trust, Specifications for interoperable PKI applications. July 2002