Certification Practice Statement for EH CICA

Information Owner: Euler Hermes
Version 1.0 / 2012
Document-Name: EH CICA CPS.doc
Classification: internal

Change Management

Version	Description	Date	Author
1.0	Final version	14.12.2012	Stephane Tailland

1 Introduction

1.1 Overview

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

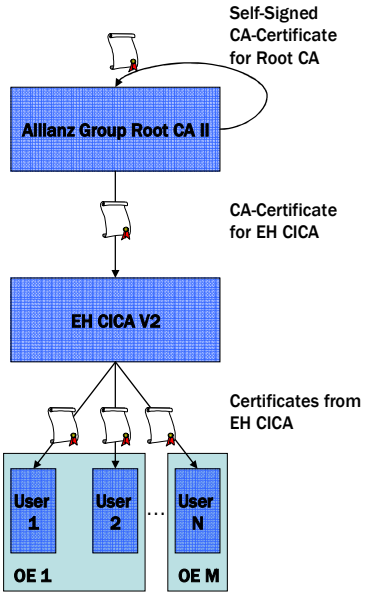

Figure 1: EH CICA within Allianz Root CA II PKI

All certificate operations comply with: The policy requirements of:

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

The technology requirements of:

- Relevant internal guidelines for the physical protection of technology assets;
- X.500 directory services;
- X.509 certificate format;
- X.509 CRL format;
- X.500 Distinguished name standards;

- Public Key Cryptographic Standards (PKCS)
- 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.

1.2 Document Name and Identification

The CPS at hand is referred to as the “Euler Hermes Customer Issuance Certification Authority V2 Certification Practice Statement”, or abbreviated “EH CICA CPS”.

The structure of this CPS is based on Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC3647].

The OID of the CPS at hand is 1.3.6.1.4.1.7159.30.36.1.

1.3 PKI Participants

1.3.1 Certification Authorities

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

1.3.2 Registration Authorities

A Registration Authority (RA) is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewing certificates on behalf of EH CICA. EH CICA provides a web-based registration interface that accesses user data from Euler Hermes Internal Customers Directory. Users applying for a certificate have to authenticate using the user identifier and password provided by Euler Hermes.

1.3.3 Subscribers

EH CICA issues End-Entity certificates only. Certificate subscribers are persons being in contractual relationship with Euler Hermes.

1.3.4 Relying parties

Relying parties are Euler Hermes entities (operating or being in charge of processes / IT-systems that authenticate subscribers using certificates of EH CICA) and recipients or senders of secured E-Mail.

1.3.5 Other participants

Not applicable.

1.4 Certificate Usage

1.4.1 Allowed Certificate Usage

Certificates issued by EH CICA are used to support secure communication and the secure exchange of information between Euler Hermes customers/partners and organisational entities operating within Euler Hermes. Two specific Use Cases are implemented:

- authentication to applications
- Email encryption

1.4.2 Prohibited certificate usage

Certificates issued by EH CICA must only be used for the purposes and applications enlisted above (Allowed Certificate Usage). Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

EH CICA Certificates are not designed, intended, or authorised for resale.

1.5 Policy Administration

1.5.1 Organization administering the document

Euler Hermes SA
1 Place des Saisons
92048 La Defense
France

1.5.2 Contact person

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

The EH CICA Certificate Policy Manager
c/o Euler Hermes SA
1 Place des Saisons
92048 La Defense
France

E-Mail: EHCICAV2CERTIFICATEPM@EULERHERMES.COM

1.5.3 Entity determining CPS suitability for the policy

This role is carried out by EH CICA staff on behalf of the head of EH CICA.

1.5.4 CPS approval procedures

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

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

1.6 Definitions and Acronyms

This CPS assumes that the reader is familiar with basic PKI concepts, including:
The use of digital signatures for authentication, integrity and non-repudiation;
The use of encryption for confidentiality;
The principles of asymmetric encryption, public key certificates and key pairs; and
The role and function of Certificate Authorities (CAs).
Accessorily Definitions and Acronyms are part of the appendix 10.5 to this CPS.

2 Publication and Repository Responsibilities

This CPS is published in the public repository section of the EH CICA registration authority, at the following address: http://ca.eulerhermes.com

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

2.1 Repositories

Certificates issued by EH CICA are published in the Euler Hermes Customers Directory. This directory is for internal usage only. EH CICA ensures not to publish private information underlying data protection guidelines.

2.2 Publication of certification information

New or amended policies are published on the Euler Hermes web site nominated for EH CICA documentation.

Subordinate parties are notified by EH CICA of changes to a policy as and when they are approved.

Upon revocation of a Subscriber's Certificate, EH CICA shall publish an updated Certificate Revocation Lists (CRLs) in the EH Customers Directory.

2.3 Time or frequency of publication

2.3.1 Certificate publication

A new issued certificate will be published immediately into the EH Customers Directory.

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

Read only access to such information is unrestricted for business use on a need to know basis. Euler Hermes requires persons to agree to the Terms and Conditions as a condition to accessing Certificates Information.

Euler Hermes has implemented logical and physical security measures to prevent unauthorised persons from adding, deleting or modifying repository entries.

2.3.2 Certificate-Revocation-List publication

Newly revoked certificates are enlisted on the CRL regularly within 60 minutes. The CRL update is dependent on availability of underlying infrastructure services (network etc). The validity of a CRL is 48 hours.

2.3.3 Access controls on repositories

Information published in the repository portion of the EH CICA registration authority web site is publicly accessible. Read-only access to such information is unrestricted.

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

3 Identification and Authentication

EH CICA / Registration Authority carry out identification and authentication relying on pre-registered user data stored in Euler Hermes Customers Directory.

3.1 Naming

3.1.1 Types of names

All certificate holders require a Distinguished Name that is in compliance with the X.501 ITU-T recommendation for Distinguished Names. The attribute Common Name (CN) is part of Subject DN and Issuer DN.

The names of the subscribers are entered as a Distinguished Name (DN) according to ITU-T [X.500].

The subscriber certificates issued by EH CICA use the following DN name for email encryption certificates

Country (C) = Country stored in Customers Directory account of certificate subscriber

Organization (O) = Organization stored in Customers Directory account of certificate subscriber

E-Mail (MAIL) = Address to which encrypted mail will be sent using the issued certificate

Common Name (CN) = first name and surname stored in Customers Directory account of certificate subscriber

User identifier (UID) = identifier of the Customers Directory account of the certificate subscriber

The subscriber certificates issued by EH CICA use the following DN name for authentication certificates

Country (C) = Country stored in Customers Directory account of certificate subscriber

Organization (O) = Organization stored in Customers Directory account of certificate subscriber

Common Name (CN) = first name and surname stored in Customers Directory account of certificate subscriber

User identifier (UID) = identifier of the Customers Directory account of the certificate subscriber

3.1.2 Need for names to be meaningful

Distinguished Names which are allowed by EH CICA have to contain the subscribers name and Customers Directory user identifier as a meaningful part.

3.1.3 Anonymity or pseudonym of subscribers

Subscribers must not be anonymous or pseudonymous.

3.1.4 Rules for interpreting various name forms

Certificates issued for email encryption purpose contain the email address that is secured with the certificate in question, in addition to the full name and user identifier of the subscriber.

Certificates issued for authentication purpose contain the full name and user identifier of the subscriber.

3.1.5 Uniqueness of names

EH CICA ensures that:

Only one usable email encryption certificate (i.e. not expired, not revoked) exists for a given email address

Only one usable authentication certificate (i.e. not expired, not revoked) exists for a given EH Customers Directory user identifier

The only exception to these rules is when a new certificate is issued to replace an expiring one. In these circumstances two valid certificates may exist for the same entity during a short period of time.

3.1.6 Recognition, authentication, and role of trademarks

No Stipulation.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

No stipulation.

3.2.2 Authentication of individual identity

Users requesting EH CICA Certificates authenticate against the EH Customers Directory by means of their user identifier and password.

Users requesting email encryption certificates must also prove they have access to the email address in question by clicking on a one time link sent by the registration authority.

3.2.3 Non-verified subscriber information

No stipulation

3.2.4 Validation of authority

Authority of requestors is ensured by authentication against the EH Customers Directory. Any user listed in the EH Customers Directory is entitled to request an EH CICA Certificate on his own.

3.2.5 Criteria for interoperation

No stipulation.

3.3 Identification and Authorization for Re-key Requests

3.3.1 Identification and authentication for routine re-key

A new certificate must be issued upon expiration of the existing one.

Key-pair generation, certification and private key activation are performed analogous to the initial issuing process.

3.3.2 Identification and authentication for re-key after revocation

A new certificate must be issued after revocation.

Key-pair generation, certification and private key activation are performed analogous to the initial issuing process.

3.4 Identification and Authorization for Revocation Requests

- A request to revoke keys and certificates may be submitted by the Subscriber using the RA web application. As a pre-requisite the subscriber must be identified and authenticated by the RA.
- Revocation can also be performed by a RA operator authenticated using a PIN code and OTP token.

4 Certificate Life-Cycle Operational Requirements

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

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

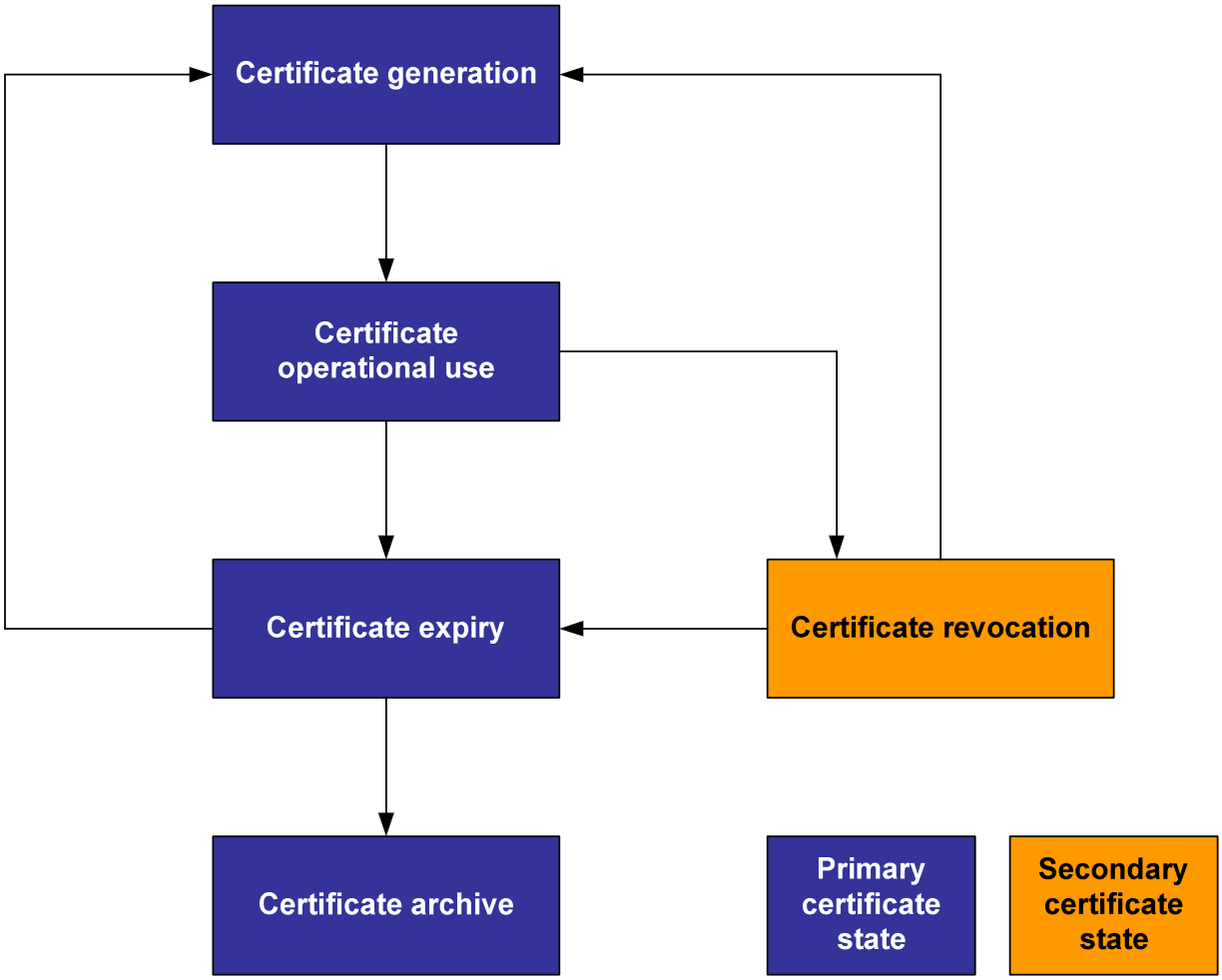

Figure 2: EH CICA Certificate Life Cycle

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

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

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

4.1 Certificate Application

EH CICA provides the Euler Hermes customers with Authentication and Encryption certificates. Group encryption certificates for shared email accounts are supported but they are necessarily bound to a single person named "email address manager".

4.1.1 Who can submit a certificate application?

Certificate applications can be submitted by any person having a business need to securely communicate with Euler Hermes or one of Euler Hermes's affiliated companies.

This specifically applies to customers and commercial partners or Euler Hermes.

Certificate subscribers must necessarily own an EH Customers Directory account.

4.1.2 Enrolment process and responsibilities

The certificate enrolment is always initiated by the RA using one time link emails sent to subscribers. These links are valid for a limited period of time (usually a few hours) and can only be used in the registration authority web application by the certificate subscriber to which they are destined.

When clicking on the one time link the subscriber is requested to authenticate in the RA web application, check the details of the new certificate and provide a password to secure the PKCS#12 file that will later be generated by the CA.

The RA forwards the certificate application to the CA which in turn generates the new key pair and certificate. A PKCS#12 file containing this certificate and the key pair is created. This PKCS#12 file is protected using the password previously entered by the subscriber and returned to the RA where it can be downloaded by the subscriber.

4.1.3 Authentication certificate applications

After appropriate checks on the identity and authority of the subscriber registration authority operator sends a one time link email to the subscriber.

This is only allowed by the system if the subscriber does not already own a valid authentication certificate (i.e. not revoked, not expired), or if the authentication certificate owned by the subscribers nears expiration.

4.1.4 Email encryption certificates:

The subscriber enters the email address that is to be secured in the registration authority web application and receives a similar one time link email, this time to the address previously entered.

4.2 Certificate Application Processing

Certificate applications are processed by EH CICA systems automatically with no human approval.

4.2.1 Performing identification and authentication functions

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

4.2.2 Approval or rejection of certificate applications

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

- The RA is authenticated to the CA and authorized to request certificate issuances
- The integrity of the request message sent by the RA has not been compromised.
- The content of the request message is correct (all fields and extensions are complete and conforming to naming conventions).

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate Issuance

4.3.1 Certificate Requests

EH CICA issues subscriber certificates based on the registration data delivered by the Registration Authority.

4.3.2 Verification and Rejection of Certificate Requests

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

4.3.3 CA actions during certificate issuance

The CA generates a key pair, issues a certificate and creates a PKCS#12 file protected with the password received in the request message from the RA.

In the event of an encryption certificate being generated, the key pair is stored in escrow to allow future recovery.

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

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

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

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

4.4.2 Publication of the certificate by the CA

All valid end-user certificates are published in the Euler Hermes Customers Directory upon creation.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

The Subscriber is responsible for taking sufficient measures to protect their own private key against any access by third parties.

EH CICA must be notified immediately if the Subscriber has any reasons to suspect that an unauthorised third party has access or has come into possession of their private key. In this case the certificate will be revoked by the Registration Authority.

Euler Hermes provides certificates solely for the usage in communication between the Subscriber and Euler Hermes or one of Euler Hermes' affiliated companies. Any usage of the certificate in communication between the Subscriber and a third party is prohibited. Euler Hermes will accept no liabilities for loss or damage caused to the Subscriber or any third party as a result of such use of the certificate.

The Subscriber must discontinue the use of their private key after expiration or revocation of the certificate, except for the decryption of archived email that had been encrypted with the expired or revoked certificate.

4.5.2 Relying party public key and certificate usage

The private key of the participant documented by the issued certificate can only be used for applications in accordance with the key usages given in the certificate. The subscribers keys can only be used for certificate based authentication and encryption.

4.6 Certificate Renewal

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

EH CICA does not support certificate renewal. Only certificate re-issuance is supported.

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other

No stipulation.

4.7 Certificate Re-key

Certificate re-key is the process by which a new (sequent) certificate is issued to replace an expired (or expiring) certificate. Certificate renewal requires the creation of a new private key and public certificate pair.

EH CICA does not support certificate renewal. Only certificate re-issuance is supported.

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate Modification

4.8.1 Circumstance for certificate modification

A Certificate Modification service is not provided. In cases where certificate information changes during the life of a valid certificate, the existing certificate is revoked and a new certificate application is made using the modified information.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

The purpose of revoking a certificate is to permanently prevent the future use of the certificate and its associated private/public key pair, due to a compromise in the private key, the misuse of or errors in the certificate. The circumstances under which a certificate may be revoked are

- the security or confidentiality of the subscribers private key or the EH CICA private key or the root key has been compromised or is at material risk of being compromised,
- a security breach,
- the termination of a business relationship between Euler Hermes and the Subscriber,

- etc.

A Subscriber can revoke his certificate at any time without warning. Certificate revocation can also be performed by RA operators.

After revocation of a certificate the RA sends the subscriber an email informing of the revocation and its cause.

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

4.9.2 Who can request revocation

Certificate revocation can be initiated by:

- A Registration Authority operator (who can revoke a certificate following a request made in due form by the subscriber or by a person of the subscriber's organization)
- The certificate subscriber

4.9.3 Procedure for revocation request

Revocation requests are recorded either by the certificate subscriber or by a RA operator in the RA web application, which forwards a revocation request message to the CA.

The CA verifies the request message and revokes the certificate. The revoked certificate is added to the EH CICA list of revoked certificates. A new CRL is published at the next scheduled update to the corresponding repository.

Following the acknowledgement of the revocation request by the CA, the RA sends a notice to the subscriber containing the certificate details, the date, time and reason of the revocation.

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

4.9.4 Revocation request grace period

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

Once a certificate has been revoked, it cannot revert back to operational use (valid status). If a replacement certificate is required, the respective subscriber has to apply for a new certificate.

4.9.5 Time within which CA must process the revocation request

The revocation of a certificate must take place immediately.

4.9.6 Revocation checking requirement for relying parties

Euler Hermes Entities that rely on certificates issued by EH CICA are bound to check status of subscribers' certificates and CA certificates prior to every use.

4.9.7 CRL issuance frequency (if applicable)

CRLs are updated at a minimum as described in 2.3. The CRLs created by EH CICA will be published when the next scheduled time slot is reached.

4.9.8 Maximum latency for CRLs (if applicable)

A Certificate Revocation List (CRL) is being kept by EH CICA. The CRL will be published in the EH Customers Directory. Update latency is 60 minutes after change.

4.9.9 On-line revocation checking requirements

Status information on revoked certificates is available to relying parties in the EH Customers Directory.

4.9.10 Other forms of revocation advertisements available

No stipulation.

4.9.11 Special requirements re key compromise

No stipulation.

4.9.12 Circumstances for suspension

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

4.9.13 Who can request suspension

No stipulation.

4.9.14 Procedure for suspension request

No stipulation.

4.9.15 Limits on suspension period

No stipulation.

4.10 Certificate Status Services

EH CICA publishes its CRL in the EH Customers Directory for verifying the status of all issued certificates.

4.10.1 Operational characteristics

It is required, that the Relying Parties check the validity of the issuer certificate (including the validity of the issuing CA certificate) with respect to every action signed with that issuer certificate.

4.10.2 Service availability

The CRLs created by EH CICA will be published to the EH Customers Directory at a minimum of a time schedule defined in 2.3.2. The IT Service Provider guarantees high availability of service subject to specification of SLA.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

All secret keys of the CA-System used within the EH CICA are backed up. All Certificates (and hence the public keys contained in them) shall be archived. The private keys of email encryption certificates are escrowed by EH CICA and protected by a certificate stored in hardware security module.

The recovery of an escrowed private key is only authorized if the certificate is no more in operational use (either in status expired or revoked).

Only the manager of a given email address can recover private keys of certificates linked to this address. The manager of an email address is the subscriber of the latest encryption certificate registered for this address.

The email address manager must connect to the RA web application, choose the certificate whose private key is to be recovered and provide a password to protect the PKCS#12 file that will later be generated by the CA.

The RA forwards the recovery request to the CA which in turn extracts the private key from escrow. A PKCS#12 file containing the certificate and its key pair is created. This file is protected using the password previously entered by the requestor and returned to the RA where it can be downloaded.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

EH CICA is placed in a secured data centre.

Data centres have security controls in place to restrict access to their computer systems, software and files to prevent them against theft, tampering or unauthorised access.

Data Centres also have physical controls in place as required by the Allianz Group Information Security Policy, and implement backup and recovery plans as required by the Allianz Group Business Continuity Management Policy.

5.2 Procedural Controls

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

5.2.1 Trusted roles

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

5.2.2 Number of persons required per task

All certification, administration and user administration tasks require compliance with multiple control requirements as laid out in the current GISF Policy/Standard. Every task which requires a multiple control are administrated with a m of n person doctrine (with $m \geq 2$ and $n > m$).

5.2.3 Identification and authentication for each role

EH CICA systems and processes use the corporate access control infrastructure based on login and PIN code/OTP, which provides strong authentication and role based access control. Granting and withdrawal of EH CICA administrative roles require compliance with user access management standard as laid out in the current GISF Policy/Standard.

5.3 Personnel Controls

EH CICA has adopted and employs personnel and management practices to ensure the trustworthiness, integrity and professional conduct of its staff. The personnel standards described below are applied.

5.3.1 Qualifications, experience and clearance requirements

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

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

- are trained in: (a) basic PKI concepts, (b) the use and operation of Certification authority software, (c) documented Certification authority procedures, (d) computer security awareness and procedures, (e) this CPS.

5.3.2 Recruitment and Qualification of Personnel

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

5.3.3 Background check procedures

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

5.3.4 Training requirements

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

5.3.5 Retraining frequency and requirements

Retraining will occur based on the necessary measurements.

5.3.6 Job rotation frequency and sequence

No stipulation.

5.3.7 Sanctions for unauthorized actions

Unauthorised actions by EH CICA System staff are submitted to appropriate authorities including, but not limited to, the Corporate Security Officer.

5.3.8 Independent contractor requirements

No stipulation.

5.3.9 Documentation supplied to personnel

EH CICA System staff has access to all training documentation.

5.4 Audit Logging Procedures

EH CICA is obliged to maintain adequate records and archives of information pertaining to the operation of the PKI. The CA software automatically preserves an audit trail for the primary states in the EH CICA certificate life cycle, i.e., generation, operational use, expiry and archive.

5.4.1 Types of events recorded

The minimum audit records to be kept include all:

1. Types of registration records, including records relating to rejected applications;
2. Certificate generation requests, whether or not certificate generation was successful;
3. Certificate issuance records, including CRLs;
4. Audit records, including security related events.

5.4.2 Frequency of Processing Log

Audit logs may be reviewed by Security Officers if needed..

5.4.3 Retention period for Audit Log

Audit Log retention period is 3 years.

5.4.4 Protection of Audit Log

Access control is configured to prevent unauthorized access and modification or deletion of audit logs.

5.4.5 Audit log backup procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

Operations personnel must notify their security administrator when a process or action causes a critical security event or discrepancy.

5.4.8 Vulnerability assessments

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

5.5 Records Archival

All relevant data (see 4.4.1) is archived according to Allianz Group System Operation Standard (GISF 2.5).

5.5.1 Types of records archived

The following operational records are archived by EH CICA:

- All audit data collected in terms of Section 5.4
- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information e.g., revocation and renewal application information

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

Euler Hermes protects the archive so that only authorised Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorised viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive backup procedures

Euler Hermes incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Archive collection system (internal or external)

Euler Hermes archive collection systems are internal.

Only authorised Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

Key changeover does not apply to end entity certificates since EH CICA certificate will not be rolledover but replaced by new key CA instance.

5.7 Compromise and Disaster Recovery

EH CICA must establish and maintain detailed documentation covering:

- Contingency & disaster recovery plan, including key compromise, hardware, software and communications failures, and natural disasters such as fire and flood. See also Allianz Group Business Continuity Management Policy and Standards [AZ-BCM].
- Configuration baseline, including operating software, and PKI specific application programs.
- Provides the above documentation on the request of persons conducting a security, compliance or CPS practices audit;
- Provides appropriate training to all relevant staff in contingency and disaster recovery procedures;

EH CICA must establish tests to conduct periodically checking the procedures for a full restoration of operational services as follows:

- the current operational platforms are shut down and disconnected from the communications links;
- system operating software, application programs and operational data is restored onto new hardware platforms, only from backup media and in compliance with the configuration baseline;
- the restored service is connected to the communications links and the correct operation of its certificate services tested;

- service operations are resumed using the original operational platform. All files on the hard disk of the test platform are securely deleted.
- Generating a compromise and disaster recovery plan, the following use cases have to be taken into account:

5.7.1 Incident and compromise handling procedures

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

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

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

5.7.3 Entity private key compromise procedures

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

5.7.4 Business continuity capabilities after a disaster

Therefore the EH CICA has prepared a second system providing the certification service currently located in a local separated data centre environment.

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

5.8 CA or RA Termination

If it is necessary to terminate EH CICA services, the impact of the termination will be minimised as much as possible in light of the prevailing circumstances. The EH CICA will at least provide as much prior notice as is practicable and reasonable to participants and relying parties.

5.8.1 Keys and Certificates

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

6 Technical Security Controls

6.1 Key Pair Generation and Installation

- Technical security controls are carried out on the basis of documented processes and stipulations following the status quo of technology. These security controls are duly fulfilled by EH CICA members in order to meet the requirements explained in chapter 4. The cryptographic procedures and records used correspond to the status quo of security measures of cryptographic procedures and to the respectively valid legal stipulations. The following RSA key pairs are used in the EH CICA System: EH CICA Keys - 12 Years - 2048 bit
- EH CICA CRL Signing Keys: CA signing key is used
- The EH CICA keys are exclusively generated and stored by the Hardware Security Module (HSM) as part of the EH CICA systems.
- The Key Generation is described in the key ceremony document, part of the operation manual.

6.1.1 Key pair generation

It is a fundamental principle of EH CICA 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. EH CICA key pairs will exclusively be generated by the CA. Where cryptographic modules are used, the private keys are generated in them and remain there in both encrypted and decrypted forms, and are decrypted only at the time at which they are being used. EH CICA has established HSM compliance criteria that ensure the quality and requirements from an HSM are uniform and consistent. The keys used by EH CICA Server (CA signing key) are generated using the HSM key generator. This is integrated in Primekey EJBCA using PKCS#11. End entity keys are generated on the requestors systems with a minimum RSA key length of 2048 bit.

6.1.2 Private key delivery to subscriber

All private keys are generated by the CA and delivered to the end-user in the form of a password protected PKCS#12 file.

6.1.3 Public key delivery to certificate issuer

No stipulation. Public keys are generated by the CA and delivered to the end-user in the form of a password protected PKCS#12 file.

6.1.4 CA public key delivery to relying parties

EH CICA makes its CA Certificates available to Subscribers at the EH CICA registration authority web site.

Allianz Root CA Certificates are available to subscribers at the Allianz Root CA web site.

EH CICA generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance.

6.1.5 Key sizes

Generally the EH CICA Root keys are 2048 bit RSA keys. While the currently allowed minimum key size for subscribers are key pairs equivalent in strength to 1024 bit RSA, EH CICA on default certifies 2048 bit RSA key pairs for subscribers.

6.1.6 Public key parameters generation and quality checking

No stipulation.

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

EH CICA secret signature key is stored in a FIPS 140-2 Level 3 compliant redundant Hardware Security Module: Safenet LUNA SA1700.

End-entity private keys need to be stored in a secure way at the local key store on their individual computer. The subscriber is responsible for the secure storage of the secret key.

6.2.1 Cryptographic module standards and controls

For EH CICA CA key pair generation and storage, EH CICA uses hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-1 Level 3.

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

Euler Hermes has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. EH CICA uses “Secret Sharing” to split the activation data needed to make use of a CA private key into separate parts called “Secret Shares” which are held by trained and trusted individuals called “Shareholders.” A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module. In order to export the private key encrypted, e.g. for transfer to a different HSM, multiple person control is implemented via the administrator cards required by the HSM. For details please refer to the HSM Documentation (see 6.2).

The chosen values for m is 8, and n is 3, however only 5 secrets will be kept by human shareholders. 3 secrets will be store in different secure places in the case of lost key or password.

6.2.3 Private key escrow

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

6.2.4 Private key backup

The CAs private key is kept redundantly on three HSM devices and an additional backup module.

6.2.5 Private key archival

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

6.2.6 Private key transfer into or from a cryptographic module

FIPS 140-1 Level 3 permits private key import to HSM modules. Export is only possible from one HSM to the backup HSM. Private key generation is only performed on hardware security modules. Three persons are required to move the private key to a new HSM device (ISO, Operator and Partition owner). For details please refer to the HSM Documentation (see 6.2). The exported key can only operate under the same circumstances as the active key in the HSM.

6.2.7 Private key storage on cryptographic module

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

6.2.8 Method of activating private key

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

6.2.9 Method of deactivating private key

The CAs private key is deactivated manually to prevent requirement of shareholders each time the application is restarted. However, in the case of an electric shutdown of an HSM, partition need to be reactived.

6.2.10 Method of destroying private key

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

6.2.11 Cryptographic Module Rating

EH CICA secret signature key is stored in a FIPS 140-2 Level 3 compliant redundant Hardware Security Module LUNA SA1700.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

EH CICA CA and Subscriber Certificates are backed up and archived as part of routine backup procedures. Expired certificates are kept in the system because digitally signed or encrypted documents often outlast the validity period of the certificate used to sign or encrypt the

document. Certificates whose validity period has expired must continue to be accessible to allow the certificate to be used to prove the authenticity of, a document.

6.3.2 Usage Periods for the Public and Private Keys

The usage periods for public and private keys are:

- CA key and certificate: 12 years
- Subscriber key and certificate: max. 3 years

6.4 Activation Data

6.4.1 Activation data generation and installation

Activation data for the EH CICA key is generated at installation in form of administrator cards. Those cards have to be initialized before they are used for private key generation and access in a specific HSM/partition (see 6.2.2).

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

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

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

Applications are developed by Euler Hermes in accordance with Allianz Software Development Security standard, and implemented or maintained are following the requirements of the Allianz System Operation Security standard.

6.6.2 Security Management Controls

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

6.6.3 Life cycle security controls

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

6.7 Network Security Controls

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

6.8 Timestamping

No stipulation.

7 Certificate, CRL, and OCSP Profiles

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

7.1 Certificate Profile

Certificates issued by EH CICA comply with Allianz Group RCA requirements. For the detailed certificate profile refer to Appendix. The public key in a certificate must be unique. No party, be it an end-entity or a Sub CA, may have its public key signed by more than one Certification Authority.

7.1.1 Key Usage

Key usage is present in all issued certificates as defined in the appendix.

7.1.2 Certificate Policies

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

7.1.3 Version number(s)

Certificates comply to X.509 v3 standard.

7.1.4 Certificate extensions

Certificate extensions are used as described in the appendix.

7.1.5 Algorithm object identifiers

No stipulation.

7.1.6 Name formats

All certificates must have non-null Issuer DN. All Certificates must contain a Subject DN.

7.1.7 Name constraints

Name constraints shall not be used.

7.1.8 Certificate policy object identifier

The Certificate policy object identifier is 1.3.6.1.4.1.7159.30.X

7.1.9 Usage of Policy Constraints extension

No stipulation.

7.1.10 Policy qualifiers syntax and semantics

No stipulation.

7.1.11 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL Profile

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

7.2.1 Version number(s)

Only X509 Version 2 CRLs are supported.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP Profile

OCSP Service may be provided in the future.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8 Compliance Audit and Other Assessment

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

The following topics are covered:

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

8.1 Frequency or circumstances of assessment

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

8.2 Identity/qualifications of assessor

The assessment is to be conducted by qualified internal or external audit personnel, with the results of such reviews reported to EH CICA.

8.3 Assessor's relationship to assessed entity

EH CICA may initiate third party audits.

8.4 Topics covered by assessment

8.4.1 Initial compliance audit

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

8.4.2 Ongoing compliance audit

The assessment is to be conducted by qualified internal or external audit personnel, with the results of such reviews reported to Allianz Group Root CA. After acceptance as participant of Allianz Group RCA system the participant will be required to conduct the Allianz Group Root CA

review process in conjunction with any significant changes to the deployment of their system, but in no event less than at least annually.

8.5 Actions taken as a result of deficiency

Allianz Group PAC decides in each individual case of deficiency what kind of actions should be taken in order that the security of the EH CICA security infrastructure can be guaranteed continuously in all cases.

8.6 Communication of results

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

9 Other Business and Legal Matters

9.1 Fees

In particular, no fees are charged for the issuance, access, revocation, suspension and validation of issuer certificates. This arrangement is only suitable to the PKI participants named in section 1.3.

9.1.1 Certificate issuance or renewal fees

No fees are taken for issuance or renewal services provided by EH CICA.

9.1.2 Certificate access fees

No fees are taken for access to PKI services provided by EH CICA.

9.1.3 Revocation or status information access fees

No fees are taken for certificate status information services provided by EH CICA.

9.1.4 Fees for other services

No fees are taken for other services provided by EH CICA.

9.2 Financial Responsibility

EH CICA Subscribers shall maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

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

9.3.2 Types of Information in particular considered confidential

Personal Information supplied to EH CICA as a result of the practices described in this CPS may be covered by national government or other privacy legislation or guidelines. Access to confidential information by operational staff is on a need-to-know basis. Paper based records and other documentation containing confidential information is to be kept in secure and locked containers or filing systems, separate from all other records.

All registration records are considered to be confidential information, including:

- Certificate applications, whether approved or rejected;

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

9.3.3 Information not within the scope of confidential information

EH CICA repositories and information contained within them are not considered Confidential/Private Information.

Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.4 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

The collection, processing and use of personal data SHALL be admissible only if permitted or prescribed by any legal provision or if the subscriber has consented.

9.4.3 Information not deemed private

All information not covered by Section 9.4.2.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual Property Rights

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

9.5.1 Property in Certificates

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

9.5.2 Certificate

EH CICA reserves the right to revoke any certificate in accordance with the procedures and policies set out in this CPS at any time.

9.5.3 Distinguished Names

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

9.5.4 Copyright

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

9.6 Representations and Warranties

9.6.1 CA representations and warranties

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

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

In no event shall EH CICA be liable to any participant, customer or other entity or person for any loss, claim, damage or expense arising from Allianz Group RCA.

9.8.1 Safeguards

EH CICA has introduced a number of measures to reduce or limit its liabilities in the event that the safeguards in place to protect its resources fail to:

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

These measures include but are not limited to:

- Testing of the EH CICA Disaster Recovery Plans;
- Performing regular system data backups;
- Performing a backup of the current operating software and certain software configuration files;
- Storing all backups in secure local and offsite storage;
- Maintaining secure offsite storage of other material needed for disaster recovery;
- Periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure;
- Periodically reviewing its Disaster Recovery Plan, including the identification, analysis, evaluation and prioritisation of risks.

9.9 Indemnities

Cf. Section 9.8.

9.10 Term and Termination

9.10.1 Term Allianz Group Root certificate

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

Upon termination of this CPS, EH CICA participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

After termination, EH CICA revokes all certificates issued.

After revocation, EH CICA informs its subscribers and the relevant relying parties as soon as reasonably possible that they shall cease at once to use for any purpose their digital certificates that are digitally identified with the revoked certificate. Upon receipt of a participant, EH CICA shall confirm whether the Issuer Certificate of the participant is valid.

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

If a new CPS is approved, signed and distributed by EH CICA, all earlier versions of the CPS will expire.

9.12.1 Notification mechanism and period

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

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

9.12.2 Circumstances under which OID must be changed

If EH CICA determines significant changes in the certificate practice, the EH CICA can decide to change object identifier corresponding to a Certificate policy. The amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 Dispute Resolution Procedures

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

9.14 Governing Law

Place of performance and of jurisdiction shall be the domicile of the Euler Hermes Business Unit which has issued the Contract to the Subscriber.

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

EH CICA maintains contingency plans in force, including adequate back up and recovery procedures, to ensure that EH CICA can continue to meet its obligations under the Operating rules without material interruption in the event of the failure or shut down of the primary computer facilities or other operating facilities.

9.16.6 Other Provisions

Not applicable.

10 Appendix

10.1 Definitions and Acronyms

Authentication

The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below.

Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.

CA-certificate

A certificate for one CA's public key issued by another CA.

Certificate policy (CP)

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Certification path

An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS)

A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

CPS Abstract

A subset of the provisions of a complete CPS that is made public by a CA.

CPS Summary

Cf. "CPS Abstract".

Customers Directory

Directory containing identity and authentication information for EH customers and partners.

Identification

The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization.

In the context of a PKI, identification refers to two processes:

(1) establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and

(2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing certification authority (issuing CA)

In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

GISF

Allianz Group Information Security Framework 2.5

PAC

Allianz Group RCA Policy Council.

PKI Participant

An organization (or individual) that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

PKI Disclosure Statement (PDS)

An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.

Policy qualifier

Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information.

Registration authority (RA)

An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Related Participants of a Sub CA

The term includes all relying parties as well as all subscribers of the respective Sub CA; in particular subscribing employees and customers of the participating organisation operating the respective Sub CA.

Relying party

A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate.

Relying party agreement (RPA)

An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.

Set of provisions

A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework.

Subscriber

A subject of a certificate who is issued a certificate

Subscriber Agreement (SA)

An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

Validation

The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants.

For more definitions refer to [RFC 3647].

10.2 Relevant documents

GISF: Allianz Group Information Security Framework, Version 2.5

Allianz Group Security Policy:

10.3 References

AZ-BCM

Allianz Group Business Continuity Management Policy and Standards

AZ-SP

Allianz Group Security Policy (current version was GISP 2.4)

RFC 2459

Obsolete RFC Standard - refer to RFC 3280.

RFC 2528

Obsolete RFC Standard – refer to RFC3279.

RFC 2822

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

RFC 3279

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

RFC 3280

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

RFC 3647

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

RFC 822

Obsolete RFC Standard – refer to RFC2822.

X.500

X.500 Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services

X.501

Information technology - Open Systems Interconnection - The Directory: Models ITU-T Recommendation X.501 was revised by ITU-T Study Group 7 (2001-2004) and approved on 2 February 2001. An identical text is also published as ISO/IEC 9594-2.)

X.509

ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology - Open Systems Interconnection: The Directory: Authentication Framework,"

10.4 Certificate Profiles

The following certificate profiles are showing the profiles of the Allianz Smartcard CA which is used as template for the actual Allianz Group User CA certificate profile.

10.4.1 CICA Secure Email

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
01:40:53:05:82:05:be:5a
Signature Algorithm: sha1WithRSAEncryption
Issuer: CN=EH CICA CA, OU=EH Tech, O=Euler Hermes, L=Paris, ST=IDF, C=FR
Validity
Not Before: Dec 14 14:07:00 2012 GMT
Not After : Dec 14 14:07:00 2015 GMT
Subject: emailAddress=some.name@domain.com/UID=Customer UID, CN=Some Email, O=Euler Hermes TECH, C=FR
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:82:44:9b:31:51:d1:d6:2c:63:c6:07:04:60:bb:
0a:86:e1:3f:ed:89:63:83:94:b0:74:c8:ff:8b:0b:
f2:58:ab:d6:b2:5f:a5:d1:b7:5a:ca:f0:13:28:55:
10:4f:e2:17:69:ef:d5:e8:d5:58:b9:7a:33:34:5d:

61:b1:8b:f8:b5:29:f6:74:f0:c1:f1:a6:cd:f2:b1:
ea:bf:b7:41:9c:dd:4f:9a:6c:a1:2d:75:ea:31:7a:
a7:d0:64:8f:14:1d:82:15:aa:8e:64:b3:25:61:6d:
c0:af:e0:bd:d0:e7:50:b2:65:b1:d9:80:cf:3c:99:
66:48:32:ea:b2:1e:c3:be:de:e5:b3:7f:1d:2a:c1:
53:a3:24:d9:95:fa:5f:4f:d1:f3:ce:85:4e:fc:7d:
83:db:d9:e8:45:3d:87:a3:8c:d1:17:06:fa:b5:ad:
8d:36:54:63:47:f6:6e:67:a1:bf:29:b3:36:f1:93:
e2:16:bc:34:05:9e:c9:b8:42:f1:be:44:e4:fc:a5:
90:f6:09:00:0b:80:fc:98:bf:76:19:55:5c:8d:d8:
06:4b:0d:4e:f9:bf:11:8a:45:ae:af:81:c0:f9:f2:
b1:24:1c:35:d2:f8:84:a2:0c:59:bd:6b:97:92:49:
7a:1d:2e:2f:a0:96:52:5f:73:5b:67:87:9b:10:1d:
ef:57
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
14:7E:6A:99:EE:7E:62:58:1A:87:97:55:8A:45:E0:35:4F:E1:1B:6A
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Authority Key Identifier:
keyid:68:71:28:65:E8:5D:A9:8B:E8:D8:FD:77:C4:D8:A8:27:3B:4E:36:6
D

X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.7159.30.36.1
CPS: http://rootca.allianz.com/cps2

X509v3 CRL Distribution Points:
URI:https://cica.eulerhermes.com/crl

X509v3 Key Usage: critical
Key Encipherment
X509v3 Extended Key Usage:
E-mail Protection
Signature Algorithm: sha1WithRSAEncryption
7d:fc:23:74:36:15:f0:b7:ab:c6:f6:17:33:ad:95:b8:82:54:
9f:97:46:6c:0c:e7:7e:6b:fc:0f:00:18:9d:f9:15:53:64:7d:
3e:d9:78:9d:b4:92:2e:b0:92:c4:44:ac:fa:9f:70:70:1b:79:
f4:c1:a1:81:92:49:bc:e3:69:1b:ce:31:d9:8b:93:bb:4b:24:
ee:7a:32:cc:b5:a9:75:27:f5:e7:a6:78:99:0d:86:bb:81:79:

c2:88:b0:1d:be:b3:22:19:bf:ca:ec:08:0b:d4:08:f5:d8:5f:
be:84:3c:5d:d5:5e:47:c4:9e:fd:4b:49:9b:82:b3:96:02:66:
46:71:76:ba:03:3b:fa:f4:2d:d8:19:d2:01:86:f6:4c:e2:03:
21:8d:97:f0:26:18:23:d9:7d:66:33:3d:33:a6:74:9a:1c:1f:
c2:ce:dc:31:90:8c:15:fb:88:3b:2c:97:9f:29:62:0f:d8:1a:
c6:1c:e3:d3:e6:41:28:6b:1f:77:5e:16:31:e2:c5:96:28:05:
91:80:f9:15:02:7b:8b:ae:0c:d2:c8:c4:39:c2:2b:cc:7e:95:
83:4f:f9:30:15:05:82:c1:b2:cd:48:01:d0:2b:8c:49:39:d9:
18:db:4c:fd:9a:11:6f:9d:34:de:b6:da:eb:8f:9c:0b:a3:33:
15:35:77:e6:9e:6f:17:9e:9e:ba:18:54:eb:67:5d:62:c1:36:
cc:37:78:d4:94:c5:c4:e6:13:72:56:fb:74:26:55:76:30:e7:
03:97:1e:57:98:92:6e:f2:23:51:05:a6:21:26:27:0b:ce:02:
b9:38:75:d8:ce:43:23:50:3f:33:26:f6:ea:87:47:9f:43:93:
a7:d6:93:85:e9:07:b4:83:94:32:48:c1:10:c4:cd:27:08:53:
db:b9:2c:db:f1:3c:4a:5e:79:5f:bd:fd:20:fc:5b:4b:f3:bb:
6f:f1:f9:4c:df:4c:41:94:1f:85:17:30:27:65:a7:95:5e:2e:
7b:b7:70:6d:00:d1:86:37:ce:c2:4c:2c:9b:ff:e0:4c:2f:6f:
ec:52:9f:11:4a:f5:0a:48:2d:c9:d2:35:ec:55:9a:1c:60:ed:
23:75:fa:cb:f0:13:bd:24:2d:d3:a1:21:57:9a:54:41:64:e4:
de:00:67:f7:d1:fa:8b:63:64:0c:15:cb:bc:76:c4:8d:66:97:
63:8b:25:3a:b3:a3:1b:fa:5e:a7:5f:7b:28:12:c9:c4:51:c2:
35:26:ff:5c:bc:ee:9e:10:e8:54:93:5f:4b:38:c6:61:04:16:
11:ff:ed:31:86:68:5b:4e:22:35:11:f6:aa:ab:0e:e6:e3:b3:
90:ec:ba:19:ea:9b:2b:ad

10.4.2 CICA SmartLink

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            72:89:e3:74:9d:09:5f:f6
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=EH CICA CA, OU=EH Tech, O=Euler Hermes, L=Paris,
ST=IDF, C=FR
        Validity
            Not Before: Dec 14 14:17:00 2012 GMT
            Not After : Dec 14 14:17:00 2015 GMT
        Subject: UID=Customer UID, CN=Some Name, O=Euler Hermes TECH,
C=FR
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
```

```
                Modulus (2048 bit):
                    00:87:3d:b7:91:75:13:a5:ca:61:39:43:85:9c:47:
                    a0:a1:af:d4:56:ac:fe:7f:47:1b:67:fe:b9:b5:18:
                    71:f0:cd:29:b2:2e:0a:cd:c8:d0:ae:d0:58:9c:af:
                    e6:f2:1d:a8:a9:6e:22:30:7e:12:72:f9:f4:41:6e:
                    3e:01:4a:93:dd:21:5f:6c:8a:e3:73:a8:e4:67:08:
                    47:ae:a6:9a:68:19:d0:f9:84:96:01:f8:32:eb:5c:
                    7b:32:5a:69:0e:ab:2d:28:62:89:53:5b:b4:13:29:
                    67:5a:86:8a:fd:41:1b:de:a2:09:6b:b5:c4:a3:f4:
                    0b:b2:2f:c7:f5:cc:24:f1:18:af:b1:af:be:a2:99:
                    46:da:c3:0c:59:bd:dc:d7:d4:06:78:d8:c4:56:0d:
                    ea:22:eb:f6:9a:93:0d:a9:87:ea:7b:ff:50:f0:1d:
                    1d:26:1a:1a:61:0d:62:32:69:f4:f2:7a:d4:9c:41:
                    c6:5c:a0:26:4d:79:05:1b:da:d9:c4:21:c6:7d:55:
                    af:02:06:fc:82:d0:6d:1b:2c:fc:cb:fe:34:09:e4:
                    f4:4a:16:2f:81:16:b1:1b:bc:01:06:cf:9d:22:bd:
                    cf:7c:8a:cb:80:dc:17:6e:1c:ca:9d:25:2a:a4:67:
                    3e:0b:58:b4:e5:c2:83:80:16:9b:43:4a:76:b8:70:
                    30:97
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:

FA:B4:3F:C5:C9:23:74:6F:59:CC:28:D3:5C:08:09:F0:AE:E3:F1:F7
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:

keyid:68:71:28:65:E8:5D:A9:8B:E8:D8:FD:77:C4:D8:A8:27:3B:4E:36:6D

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.7159.30.36.1
                  CPS: http://rootca.allianz.com/cps2

            X509v3 CRL Distribution Points:
                URI:https://cica.eulerhermes.com/crl

            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Client Authentication
    Signature Algorithm: sha1WithRSAEncryption
        16:86:7e:22:ca:8b:6f:db:65:47:82:cf:90:b2:73:99:82:b5:
        13:4c:5e:8a:05:cc:b2:52:7b:bf:d1:98:b3:6a:10:a0:6e:87:
        f2:52:96:3f:6c:a0:53:be:81:bd:88:08:72:ef:4b:21:39:a6:
        51:97:6c:d8:30:dd:ba:06:dd:ce:1e:6e:65:eb:b7:bc:ec:46:
        02:0c:52:18:47:b3:72:10:7c:01:f6:41:01:a2:dd:24:1e:73:
```

```
66:a4:28:52:98:ac:9f:2c:db:28:b6:94:3c:9b:f3:9f:14:0c:
e4:d8:81:4e:9f:ea:32:05:b4:eb:a7:c8:02:e7:a3:c8:56:a2:
4e:7a:20:e0:aa:23:bd:c6:47:24:75:7c:18:6e:35:82:d0:03:
5a:a2:03:08:14:cc:e6:37:7f:f6:c2:73:af:fc:1a:6d:6c:46:
eb:3b:64:ea:1c:dd:27:1d:97:6c:30:09:3d:35:30:54:aa:b2:
d0:2d:bf:2e:85:07:c1:3c:65:27:a1:39:4f:38:dd:3d:64:ef:
15:8b:13:62:aa:9b:d4:53:44:3d:ef:f7:76:e7:0c:86:2c:9c:
8c:a5:c2:6f:49:2e:b9:81:f8:5a:e4:5e:5a:03:27:dd:4d:70:
3e:2f:6b:6c:68:03:2d:79:8e:15:1c:09:01:81:fa:6c:08:52:
20:2c:8b:fd:b7:60:cf:e3:22:5b:49:1d:fb:b2:a1:e7:04:25:
47:10:20:02:f3:33:fc:8a:50:6e:c3:a2:16:98:99:68:66:8c:
a4:e6:c3:63:e7:65:98:5d:1c:c7:b3:8c:04:30:98:01:ba:5d:
f6:33:b8:28:f8:fd:b1:08:18:20:2a:e3:85:54:e1:15:70:93:
8a:e0:81:8b:9b:b7:3d:d0:85:7f:73:d9:82:1f:af:fd:1e:a0:
9e:53:fb:27:b9:6f:d8:54:a5:49:33:de:89:7a:39:3a:35:50:
fc:a1:0e:53:de:65:b2:05:a1:71:e6:35:d7:c2:56:76:42:49:
8a:3f:79:b9:b8:57:a8:f0:ce:7c:be:2a:b4:08:49:3a:73:1d:
30:0a:c7:f0:16:40:b0:53:fe:bd:11:b6:58:fe:07:a7:69:85:
e1:7b:07:b6:6b:e0:af:b7:a8:d4:84:9b:2b:90:45:f4:7b:e4:
e0:91:54:e6:bd:7f:83:eb:48:ff:aa:93:99:2b:83:8e:ee:25:
9b:48:49:4f:3d:1d:83:75:b8:29:8d:1d:b7:23:d5:12:61:9e:
ac:14:3f:48:b4:f2:4b:b8:de:26:de:d2:f7:19:17:44:d1:5e:
f2:47:7d:03:53:c0:b0:1e:c2:17:56:da:94:0e:47:c9:c6:dc:
```