IT Security Association Germany

TeleTrusT
Pioneers in IT security.

TeleTrusT EBCA
European Bridge Certificate Authority

Certificate Policy

for members of the
TeleTrusT European Bridge CA

Document information

Version 2.4

26/02/2019

IT Security Association Germany (TeleTrusT)
Chausseestrasse 17
D-10115 Berlin
Germany

Tel. +49 30 4005 4310
Fax +49 30 4005 4311

info@ebca.de
http://www.ebca.de

History

Version	Date	Modification	Author
1.08	11/01/2012	Association name revised	Dr Holger Mühlbauer
1.09	08/02/2012	Appearance and terminology revised	Marieke Petersohn
1.10	21/01/2014	Preparation for revision on 27/01/2014	Dr. Willi Kafitz
1.11	27/01/2014	Revision	Wolfgang Siegert/ Michael Thiel/ Dr. Frank Losemann/ Dr. Willi Kafitz/ Marieke Petersohn/ Martin Fuhrmann
1.12	14/02/2014	Revision	Dr. Willi Kafitz/ Martin Fuhrmann
1.13	21/03/2014	Glossary revised	Wolfgang Siegert/ Willi Kafitz/ Martin Fuhrmann
1.14	03/04/2014	Revision	Martin Fuhrmann
1.15	16/04/2014	Revision	Martin Fuhrmann
2.0	22/04/2014	Final Version, adaptation of the date and version number	Martin Fuhrmann
2.1	12/06/2014	Elimination of errors in Glossary	Martin Fuhrmann
2.2	17/07/2014	New EBCA logo inserted	Martin Fuhrmann
2.3	28/06/2016	Changes of regulations on the venue of the PKI	Marieke Petersohn
2.3	21/09/2016	Changes in Translation	Ida Köhler
2.4	26/02/2019	Association name revised	Morad Abou Nasser

Contents

1 Introduction

1.1 Overview

This Certificate Policy (CP) is intended for participants of the TeleTrusT European Bridge CA (EBCA). It contains stipulations and requirements regarding the participating public key infrastructures (PKIs) and the certificates to be used.

This CP sets out the technical and organizational compliance requirements that are used to create relationships of trust among the member organizations of the EBCA. This CP follows the structure of RFC 3647.

The EBCA participant (hereinafter referred to as 'the participant') declares that:

- Their CA complies with the stipulations and requirements of this CP
- They have created their own CP (participant's CP) which implements the requirements of this CP
- They have passed the interoperability test [1]

The participant's CA certificates are to be published in the EBCA's certificate list following application (see 1.5.4) and submission of the above declaration of conformity.

This certificate policy describes the security requirements governing the operation of CAs for the issue and use of X.509-compliant certificates. The policy also defines the basic protection for the use of certificates for third parties. It describes a transparent level of security for the confidentiality and authentication of messages, such as the exchange of emails using the S/MIME format. The requirements are also binding within the EBCA for other purposes such as certificate authentication in connection with SSL/TLS. Existing members are granted a transition period of one year starting from the adoption of the new CP for implementation and documentation.

Should stricter security requirements apply, the framework of this policy makes it easier to individually verify the security level of the PKI concerned.

1.1.1 Aim of this CP

This CP is intended to support the objectives of the EBCA. Its aim is to establish secure inter-organizational electronic business processes with the help of public key infrastructures.

The following requirements must be met:

- Technical interoperability
- Comparability of security levels
- Adequate minimum standards

The EBCA provides a platform for both technical conformity by profiling technical standards and for testing to ascertain mutual interoperability.

This policy lays down the EBCA's stipulations regarding the minimum standards of security required for the operation of an EBCA-compliant PKI. Use of the structure adopted in RFC 3647 enables the externally transparent, comparative account of the security standards of the PKIs in the EBCA.

By submitting the declaration of conformity, each member of the EBCA confirms that they comply with this CP. To enable comparability, each member has its own CP (or its implementation as a CPS) which confirms the minimum standards of this CP in an appropriate manner.

This document and its member-specific version may also serve as a reference document for contractual arrangements (i.e. it is suitable as a reference for bilateral contracts).

1.1.2 RFC 3647 structure

This document is structured according to RFC 3647 and follows the sub s contained in it.

[1] The technical conformity needed to achieve interoperability using the example of secure email is described in the document “Test specification for interoperability test and functionality for exchanging secure emails with certificates under European Bridge CA” (cf. EBCA S/MIME, 1.6.4 reference).

The structure based on this internationally recognized framework improves transparency and comparability. This structure is intended to enhance the comparability of policies and thus the level of security.

1.1.3 Conventions

The words "must", "may", "should" and "can" are used in this CP and should be understood as follows:

- **must, may not, may only**
  Binding stipulation by the EBCA
- **should**
  Used for requirements which must be followed except in justified exceptional circumstances
- **can**
  Optional

State-of-the-art operation
Operation depends on the participant's internal security policies and standards. They can be based on the state of the art of IT security as described in the BSI Federal Office for Information Technology Security's protection manual[2] and in ISO/IEC 27001 et seq.[3]

Proper execution of service
Proper execution of service means that the service can be based on the state of the art regarding both technology and organizational processes.

1.1.4 Validity

This policy is binding on members of the EBCA.

1.2 Document name and identification

This certificate policy is entitled:

Certificate Policy for members of the TeleTrusT European Bridge CA,
Version: 2.2 – Date: 17th July 2014
The Object Identifier (OID) for this document is 1.3.6.1.4.1.20351.1.2.1.

1.3 PKI participants

Participants are organizations which run their own Public Key Infrastructure or have appointed a Trust Service Provider (TSP).

1.3.1 Certification authorities

Certification authorities (CAs) are entities which issue certificates to participants and carry out the contractual obligations of participants of the European Bridge CA. Participant´s CAs may exist inside or outside the participant's organization.

1.3.2 Registration authorities

Registration authorities (RAs) are entities which carry out registration for subscribers. Participant´s RAs may exist inside or outside the participant's organization.

1.3.3 Subscribers

Subscribers are natural persons or technical entities which have sole control over the private key. If subscribers are natural persons the assignment of certificates to subscribers must be unambiguously carried out since a signature or authentication certificate uniquely refers to a natural identity. If a certificate is issued for a function or a group of persons, then this should be clearly recognizable in the certificate subject as such (for example by adding the attribute "Team Certificate," if a confusion of a person certificate is not otherwise excluded). The responsible natural persons or legal entities have a contractual relationship with the participant's CA concerning the issue of certificates.

1.3.4 Relying parties

The term 'relying parties' refers to all people and organizations using certificates of subscribers and with access to the EBCA's services.

[2] Bundesamt für Sicherheit der Informationstechnik (BSI), IT-Grundschutzhandbuch, see http://www.bsi.de/gshb

[3] ISO/EC 27001 and family of standards, http://www.iso.org

1.3.5 Other participants

This policy does not apply to participants who have not entered into any obligations with the EBCA.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

EBCA participants must disclose the permitted use of certificates in their CPs.

The permitted use of certificates is governed by the "KeyUsage" attributes contained in the certificate as well as the provisions in the participant's associated CP.

1.4.2 Prohibited certificate uses

No stipulation

1.5 Policy administration

1.5.1 Organization administering the document

The EBCA Board

IT Security Association Germany (TeleTrusT)
Chausseestrasse 17
D-10115 Berlin
Germany

1.5.2 Contact persons/Secretariat

TeleTrusT European Bridge CA
[Responsible for service]
Chausseestrasse 17
D-10115 Berlin

info@ebca.de
http://www.ebca.de

Tel.: +49 30 4005 4310
Fax: +49 30 4005 4311

1.5.3 Maintenance of this policy

The content of this policy is maintained by the members of the TeleTrusT-Technik team of the EBCA. Its content undergoes a review as warranted or every three years which is then approved by the Board of the EBCA.

The adoption of non-essential changes can be accelerated as follows. The management distributes a document among the members of the Board in which the proposed changes are highlighted and can set a deadline by which any objections must be submitted. If no objections have been received by the time the deadline expires, the new version is deemed to have been approved.

1.5.4 CP approval procedures[4]

Participants apply for their issuing CA to be adopted by the EBCA. The search for certificates issued by external Trust Service Providers will be limited to the relevant email-domains. Application includes participation in the EBCA's interoperability test and a declaration of conformity. Specifically, the participant must declare:

- That their issuing CA meets the requirements of this CP
- That the implementation of these requirements is described in the participant's CP specified

If the participant's CA does not comply in all respects, the EBCA participant must submit a statement specifying the aspects of the CA which do not comply.

The EBCA Board will then review the declaration of conformity and decide whether to accept the CA (and hence the corresponding CPS).

Participants agree to notify the EBCA in advance of any amendments which do not conform with the existing CP/CPS as well as of any decision to cease their certification services.

[4] Divergence from RFC-3647: Whereas RFC specifies the requirements on an organizational CPS, this document describes a bridge infrastructure. Therefore, demands are made on the CP of a participant.

If participants do not meet the requirements of this CP, the EBCA is entitled to refuse or revoke participation in the EBCA.

If a participant makes considerable changes to their PKI or CP, the Board may demand that another declaration of conformity be submitted. The same shall apply if the EBCA's CP is substantially altered.

1.5.5 Responsibility for the recognition of a CP with respect to this CP

The Board of the EBCA is responsible for recognizing a participant's CP.

1.6 Definitions and acronyms

Definitions and acronyms are listed in the annex.

1.6.1 German definitions

See Glossary

1.6.2 English definitions

See Glossary

1.6.3 Abbreviations and acronyms

See Glossary

1.6.4 References

- [RFC 3647], S. Chokhani et. Al., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", http://www.faqs.org/rfcs/rfc3647.html.
- [EBCA S/MIME], European Bridge CA, "Testspezifikation für den Interoperabilitätstest und Funktionalität für den Austausch sicherer E-Mails mit Zertifikaten unter der European Bridge CA".
- [ECRYPT], European Network of Excellence in Cryptology (ECRYPT), D.SPA.10 – ECRYPT Yearly Report on Algorithms and Keysizes, http://www.ecrypt.eu.org/.
- [ISO 27001], ISO/IEC 27001 - Information security management, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.
- [SigAlg], Bundesnetzagentur, 'Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Section I Nr. 2 SigV vom 22. November 2001', published annually in the Federal Gazette.
- [Common PKI] ISIS/MTT Version 1.1, Part 1. Table 12: KeyUsage.
- [ITWissen], ITWissen Das große Online-Lexikon für Informationstechnologie, http://www.itwissen.info/.
- [T7], T7 e.V. Berufsverband der Trustcenterbetreiber, http://www.t7ev.org/ws/T7-de/Common-PKI.

2 Publication and repository responsibilities

2.1 Repositories

Participants must provide the EBCA and its participants with access to revocation data. A repository service for accessing certificates can also be made available.

Participants are to ensure the proper provision of state-of-the-art repository services under their security policies.

Participants must ensure that personal data which is subject to data protection is not published on the EBCA's channels without the consent of those concerned.

2.2 Publication of certification information

Participants agree to make their CP or those sections of its policy relating to the operation of the PKI available to both the operator of the EBCA and the other participants.

Participants agree to the publication of their participation in the EBCA as well as the disclosure of their Root certificate and Sub CA certificates within the EBCA network. As far as possible, the participants declare in their CP, that they indicate the participation in the EBCA and the performing of the interoperability tests.

2.3 Time and frequency of publication

Participants must indicate the time and frequency of the publication of repository information (revocation information, directory services). Revocation information must be published without delay following the revocation of the certificate concerned.

The CP of a participant or the part of their policy concerning the operation of the PKI as well as changes thereto or to its architecture must be disclosed to the EBCA four weeks beforehand.

2.4 Access controls on repositories

Operators of repository services for certificates and revocation information must ensure proper access control in order to prevent unauthorized changes to such information.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The naming rules for the SubjectDistinguishedName (Subject DN) and IssuerDistinguishedName (Issuer DN) must be defined in accordance with standard X.501. The SubjectDN and IssuerDN must contain the attribute CommonName (CN).

Writing the email address separately in the field SubjectAltName is recommended. The naming rules contained in RFC 822 should be observed. Email addresses can be part of the DN.

3.1.2 Need for names to be meaningful

Certificates can refer to natural or legal persons or technical entities. They must always be clearly recognizable as such. They must clearly identify the subscriber within the validity of the CP. Certificates for organization- or function-related groups of persons as well as for organization-related email authorities must clearly differ from certificates for natural persons. A 1: n relationship between certificates and subscribers is inadmissible for end entity certificates. Clearly identified group certificates are an exception. It can then be used as additional method (for example electronic seal) if the unambiguous identification of the subscriber is not affected.

3.1.3 Anonymity or pseudonymity of subscribers

A certificate issued as a pseudonym must be recognizable as such to people. If certificates are created using pseudonyms, the participant's RA and the participant's CA must keep a record of the real identity of the subscriber on file.

3.1.4 Rules for interpreting various name forms

The email address of the subscriber must be entered on certificates that are used for secure email (especially encryption and authentication certificates).

3.1.5 Uniqueness of names

When names are decided, it must be ensured that the selected DN is unique within the issuing CA. The name of the CA certificate must be unique within the EBCA.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation

3.2 Initial identity validation

3.2.1 Methods to prove possession of private key

No stipulation

3.2.2 Authentication of organization identity

No stipulation

3.2.3 Authentication of individual identity

The RA shall ensure the reliable and, as far as one can judge, unambiguous identification and verification of application data in connection with the integrity, authenticity and confidentiality requirements of its state-of-the-art security policy.

3.2.4 Non-verified subscriber information

No stipulation

3.2.5 Validation of authority

The process for verifying eligibility to apply must be documented.

3.2.6 Criteria for interoperation (interaction)

No stipulation

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

No stipulation

3.3.2 Identification and authentication for re-key after revocation

The RA shall ensure the reliable identification and verification of previous application data under its security policy.

3.4 Identification and authentication for revocation request

Under its security policy, the RA shall ensure the reliable identification and authentication of the applicant.

4 Certificate life-cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application?

Only the responsible natural person or legal entity may apply for personal or organizational certificates or certificates for technical processes. A suitable method for the verification of responsibility must be documented.

4.1.2 Enrollment process and responsibilities

Registration must be a documented process that meets the identification requirements specified in Section 3.2.3.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Before registration, subscribers are to be reliably identified using a documented process.

4.2.2 Approval or rejection of certificate applications

The requirements for the acceptance of a certification application must be documented. Acceptance may only be granted to identified applicants.

4.2.3 Time to process certificate applications

No stipulation

4.3 Certificate issuance

4.3.1 Trust Service Provider actions during certificate issuance

Certificates may only be issued in response to valid certificate applications. The activities involved in the issue of certificates must be based on documented processes. It must be ensured that there is a clear link between a subscriber and the associated key-pair. Verification is to be carried out using documented processes.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The subscriber is to be notified using the related documented processes.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The process for the safe transfer of certificates and the circumstances leading to the acceptance of a certificate by the subscriber must be documented.

4.4.2 Publication of the certificate by the CA

Participants' CA certificates must be disclosed to the EBCA.

Newly issued end-user certificates can be published in a repository service.

4.4.3 Notification of certificate issuance by the CA to other PKI participants

When a CA certificate is issued whose CA is participating in the EBCA, the EBCA must be notified without delay.

If the CA of a participant registered in the EBCA issues a Sub CA certificate, the EBCA must be informed of this and publish this information.

There are no stipulations concerning user certificates.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscriber's responsibilities must be documented by the trust service provider and the subscriber must be informed.

The subscriber's private key documented in the certificate may only be used for applications that are consistent with the uses specified in the certificate.

The following uses are permitted:

- Authenticating user or application data and technical systems (usage type: "digital signature")

- Decrypting user or application data or symmetric keys which are used for the encryption of such data in the 'hybrid method' (usage types: "dataEncryption", "KeyEncryption")
- Indicating the validity (usage type: "non-repudiation/content-commitment") of an electronic signature by the subscriber

4.5.2 Relying party public key and certificate usage

No stipulation

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Certificate renewal while retaining the asymmetric key pair is only allowed if the unique link between subscriber and private key continues to be ensured.

The circumstances for certificate renewal must be documented.

4.6.2 Who may request renewal?

The CA documents how authorization is to be verified.

4.6.3 Processing certificate renewal requests

The processing of an application for certificate renewal must be a documented process that meets the identification requirements in Section 3.2.3.

4.6.4 Notification of new certificate issuance to subscriber

The subscriber is to be notified in accordance with the documented processes.

4.6.5 Conduct constituting acceptance of a renewal certificate

The process for secure certificate delivery and circumstances leading to the acceptance of the certificate by the subscriber must be documented.

4.6.6 Publication of the renewal certificate by the CA

A renewed CA certificate must be disclosed to the EBCA without delay.

Renewed end-user certificates can be published in a repository service.

4.6.7 Notification of certificate issuance by the CA to PKI participants

The renewal of a CA certificate must be disclosed to the EBCA without delay.

There are no stipulations governing user certificates.

4.7 Certificate re-key

4.7.1 Circumstances for certificate re-key

The CA must describe the circumstances under which a newly produced key pair can be certified together with the previous certificate data. Such circumstances include, e.g.:

- Revocation of the previous certificate owing to key compromise
- The expiry of the existing certificate

4.7.2 Who may request certification of a new public key?

The CA shall document how authorization is to be verified.

4.7.3 Processing certificate re-keying requests

No stipulation

4.7.4 Notification of new certificate issuance to subscriber

The subscriber shall be notified in accordance with the documented processes.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The process for secure certificate delivery and circumstances leading to the acceptance of the certificate by the subscriber must be documented.

4.7.6 Publication of the re-keyed certificate by the CA

Renewed CA certificates must be disclosed to the EBCA without delay.
Newly issued end-user certificates can be published in a repository service.

4.7.7 Notification of certificate issuance by the CA to PKI participants

Renewals of CA certificates must be disclosed to the EBCA without delay.
There are no stipulations regarding user certificates.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

The CA must describe the circumstances under which a certificate is to be altered, e.g.:

- If the name in the certificate cannot be uniquely tied to the subscriber
- If the email address contained in the certificate can no longer be tied to the subscriber

In technical terms, this means recertification.

4.8.2 Who may request certificate modification?

The CA shall document how authorization is to be verified.

4.8.3 Processing certificate modification requests

No stipulation

4.8.4 Notification of new certificate issuance to subscriber

The subscriber shall be notified in accordance with the documented processes.

4.8.5 Conduct constituting acceptance of modified certificate

The process for secure certificate delivery and circumstances leading to the acceptance of the certificate by the subscriber must be documented.

4.8.6 Publication of the modified certificate by the CA

An amended CA certificate must be disclosed to the EBCA without delay. Reissued end-user certificates can be published in a repository service.

4.8.7 Notification of certificate issuance by the CA to other entities

The amendment of a CA certificate must be disclosed to the EBCA without delay. There are no stipulations governing user certificates.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

The CA must describe the circumstances under which a certificate is to be revoked, e.g.

- A key has been compromised
- A key pair can no longer be uniquely tied to its subscriber
- There is no longer a unique link between the certificate and the key

If the private signature key of the CA is compromised, the EBCA must be notified without delay.

4.9.2 Who can request revocation?

The CA shall document how authorization is to be verified.

4.9.3 Procedure for revocation request

Both the RA and the CA must document the certificate revocation procedure.

4.9.4 Revocation request grace period

The CA should document deadlines for a revocation request against a subscriber.

4.9.5 Time within which Trust Service Provider must process the revocation request

The revocation of a certificate must take place without delay.

4.9.6 Revocation checking requirement for relying parties

The methods available for verifying revocation information must comply with the EBCA's conformity criteria.

4.9.7 CRL issuance frequency

The frequency of the publication of CRLs must be documented by the CA. Up-to-date revocation information must be made available quickly.

4.9.8 Maximum latency for CRLs

The maximum latency for CRLs must be documented by the CA.

4.9.9 Online revocation/status checking availability

Revocation information must be posted online.

4.9.10 Online revocation checking requirements

At least one publicly accessible http or LDAP address **must** be included in the CRL distribution points (CDPs) specified in the certificate to enable the certificate to be verified online. Both an http and an LDAP query **should** be possible. An OCSP request may also be added.

4.9.11 Other forms of revocation advertisements available

Revocation information must be posted online. The availability of this online service must be documented.

4.9.12 Special requirements regarding key compromise

No stipulation

4.9.13 Circumstances for suspension

This status must be posted online.

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

4.10.1 Operational characteristics

If an online status monitoring service is operated, how it works must be described.

4.10.2 Service availability

The availability of the status monitoring service must be documented. Current status information should be made available quickly.

4.10.3 Optional features

No stipulation

4.11 End of subscription

In the event of termination by the subscriber, the certificate must be revoked.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

In the case of key escrow, the trust service provider must document the key escrow processes. These processes must be state-of-the-art and must comply with its own security policy. Key escrow should not be used for signature keys.

4.12.2 Session key escrow and recovery policy and practices

No stipulation

5 Facility, management and operational controls

Facility, management and operational controls are to be carried out based on state-of-the-art documented processes and stipulations being part of the participant's safety policy. These controls are to be properly performed by participants in order to meet the operational requirements described in Section 4.

To reflect the structure of RFC 3647, the headings contained in this document are used.

The CP of the participant should at least contain the requirements for the following sections:

- Section 5.6 Key changeover of trust service provider
- Section 5.7 Compromise of the private key of trust service provider
- Section 5.8 Trust service provider or RA termination

5.1 Physical security controls

5.1.1 Site location and construction

The PKI must be operated in Europe (EU + EFTA). Deviations among participants having the PKI operated by a professional trust center, are possible and require an approval of the EBCA Board. Point of reference for a decision is the operational site for the EBCA relevant Root or Sub CA.

5.1.2 Physical access

No stipulation

5.1.3 Power, heating and air conditioning

No stipulation

5.1.4 Water exposure

No stipulation

5.1.5 Fire prevention and protection

No stipulation

5.1.6 Media storage

No stipulation

5.1.7 Waste disposal

No stipulation

5.1.8 Off-site backup

No stipulation

5.2 Procedural controls

5.2.1 Trusted roles

No stipulation

5.2.2 Number of persons required per task

No stipulation

5.2.3 Identification and authentication for each role

No stipulation

5.2.4 Roles requiring separation of duties

No stipulation

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

No stipulation

5.3.2 Background check procedures

No stipulation

5.3.3 Training requirements

No stipulation

5.3.4 Retraining frequency and requirements

No stipulation

5.3.5 Job rotation frequency and sequence

No stipulation

5.3.6 Sanctions for unauthorized actions

No stipulation

5.3.7 Contracting personnel requirements

No stipulation

5.3.8 Documentation supplied to personnel

No stipulation

5.4 Audit logging procedures

5.4.1 Types of events recorded

No stipulation

5.4.2 Frequency of processing log

No stipulation

5.4.3 Retention period for audit log

No stipulation

5.4.4 Protection of audit log

No stipulation

5.4.5 Audit log backup procedures

No stipulation

5.4.6 Audit collection system (internal vs. external)

No stipulation

5.4.7 Notification to event-causing subject

No stipulation

5.4.8 Vulnerability assessments

No stipulation

5.5 Records archival

5.5.1 Types of records archives

No stipulation

5.5.2 Retention period for archive

No stipulation

5.5.3 Protection of archive

No stipulation

5.5.4 Archive backup procedures

No stipulation

5.5.5 Requirements for time-stamping of records

No stipulation

5.5.6 Archive collection system (internal/external)

No stipulation

5.5.7 Procedures to obtain and verify archive information

No stipulation

5.6 Trust service provider´s key changeover

Specific information in this chapter is expected in the policy of the EBCA participant.

5.7 Trust service provider´s compromise and business continuation

Specific information in this chapter is expected in the policy of the EBCA participant.

5.7.1 Incident and compromise handling procedure

See 5.7

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

See 5.7

5.7.3 Trust service provider´s private key compromise procedures

See 5.7

5.7.4 Business continuity capabilities after a disaster

See 5.7

5.8 Trust service provider or RA termination

Specific information in this chapter is expected in the policy of the EBCA participant.

6 Technical security controls

Technical controls are to be carried out based on state-of-the-art documented processes and stipulations. These controls are to be properly performed by participants in order to meet the requirements described in Section 4.

The cryptographic algorithms and protocols used must reflect current security aspects of cryptographic methods and the applicable legal requirements.

To reflect the structure of RFC 3647, the headings contained in this document are used.

The CP of the participant should at least contain the requirements for the following sections:

- Section 6.1 Key pair generation and installation
- Section 6.2.4 Private key backup
- Section 6.3.2 Certificate operational periods and key pair usage periods

6.1 Key pair generation and installation

Specific information in this chapter is expected in the policy of the EBCA participant.

6.1.1 Key pair generation

See 6.1

6.1.2 Private key delivery to entity

See 6.1

6.1.3 Public key delivery to certificate issuer

See 6.1

6.1.4 Trust service provider´s public key delivery to users

See 6.1

6.1.5 Key sizes

State-of-the-art key lengths should be used [ECRYPT]. Algorithm catalogue of the “Bundesnetzagentur (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway)", published annually in the “Federal Network Agency's Official Gazette".

6.1.6 Public key parameters generation and quality control

No stipulation

6.1.7 Key usage purposes

No stipulation

6.2 Private key protection and cryptographic module engineering controls

No stipulation, see 6.2.4.

6.2.1 Standards and security controls for cryptographic modules

No stipulation

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

No stipulation

6.2.3 Private key escrow

No stipulation

6.2.4 Private key backup

Specific information in this chapter is expected in the policy of the EBCA participant.

6.2.5 Private key archival

See 6.2.4

6.2.6 Private key entry into or out of cryptographic modules

See 6.2.4

6.2.7 Private key storage in cryptographic modules

See 6.2.4

6.2.8 Method of activating private key

See 6.2.4

6.2.9 Method of deactivating private key

See 6.2.4

6.2.10 Method of destroying private key

See 6.2.4

6.2.11 Cryptographic module rating

See 6.2.4

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulation

6.3.2 Certificate operational periods and key pair usage periods

Specific information in this chapter is expected in the policy of the EBCA participant.

6.4 Activation data

6.4.1 Activation data generation and installation

No stipulation

6.4.2 Activation data protection

No stipulation

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

No stipulation

6.5.2 Computer security rating

No stipulation

6.6 Life cycle security controls

6.6.1 System development controls

No stipulation

6.6.2 Security management controls

No stipulation

6.6.3 Life cycle security ratings

No stipulation

6.7 Network security controls

No stipulation

6.8 Timestamping

No stipulation

7 Certificate, CRL and OCSP profiles

7.1 Certificate profile

7.1.1 Version numbers

Certificates must comply with standard X.509 v3 (Type 0x2).

7.1.2 Certificate extensions

The CA must define the certificate extensions. The EBCA conformity criteria are to be observed. Setting as few certificate extensions to critical as possible is recommended.

The following certificate extensions must be critical:

- "KeyUsage"
- "BasicConstraints" (mandatory only if a CA certificate is concerned)

For the "KeyUsage" and "BasicConstraints" (of CA certificates), the stipulations of Common PKI must be complied with (see [Common PKI], reference 1.6.4).

Certificates that are used for secure email must contain the email address of the subscriber either:

- In the "SubjectAltName" (RFC 822Name, preferred), or
- In the "DistinguishedName" (DN)
- In technical certificates, the primary system name should be included in the "DistinguishedName" (DN).

7.1.3 Algorithm object identifiers

No stipulation

7.1.4 Name forms

The CA must document name forms. The EBCA conformity criteria should always be observed. In addition, the following requirements apply.

The "CommonName" (CN) must be given in the "DistinguishedName" (DN).

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifiers

Entering the OID of this CP as a non-critical extension in the attribute "certificatePolicies" is recommended.

7.1.7 Usage of policy constraints extension

No stipulation

7.1.8 Policy qualifiers syntax and semantics

No stipulation

7.1.9 Processing semantics for the critical certificate policy extension

No stipulation

7.2 CRL profile

7.2.1 Version numbers

Version 1 CRLs (Type 0x0) or higher must be used. However, to ensure interoperability, Version 2 (Typ 0x1) CRLs must be used.

7.2.2 CRL and CRL entry extensions

No stipulation

7.3 OCSP profile

7.3.1 Version numbers

Current: OCSPv1 used; in future: SCVP to be used

7.3.2 OCSP extensions

If the CA issues an OCSP status check, this extension must be documented. The EBCA's conformity criteria are to be observed when defining these extensions.

8 Compliance audit and other assessment

Audits and other assessments of participants' PKIs are to be carried out based on state-of-the-art documented processes and stipulations that are part of the participant's security policy. Audits are to be properly performed by participants.

To reflect the structure of RFC 3647, the headings contained in this document are used without setting binding requirements for content design.

8.1 Frequency and circumstances of assessment

No stipulation

8.2 Identity/qualifications of assessor

No stipulation

8.3 Assessor's relationship to assessed entity

No stipulation

8.4 Topics covered by assessment

No stipulation

8.5 Actions taken as a result of deficiency

No stipulation

8.6 Communication of results

No stipulation

9 Other business and legal matters

Part of the participant's CP comprises financial and legal matters that have to be legally compliant.

To reflect the structure of RFC 3647, the headings contained in this document are used without setting binding requirements for content design.

The CP of the participant should at least contain the requirements for the following sections:

- Section 9.4 Privacy of personal information
- Section 9.10 Term and termination
- Section 9.11 Individual notices and communications with participants
- Section 9.14 Governing law

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation

9.1.2 Certificate access fees

No stipulation

9.1.3 Revocation or status information access fees

No stipulation

9.1.4 Fees for other services

No stipulation

9.1.5 Refund policy

No stipulation

9.2 Financial responsibility

No stipulation

9.2.1 Insurance coverage

No stipulation

9.2.2 Other assets

No stipulation

9.2.3 Insurance or warranty coverage for end-entities

No stipulation

9.3 Confidentiality of business information

No stipulation

9.3.1 Scope of confidential information

No stipulation

9.3.2 Information not within the scope of confidential information

No stipulation

9.3.3 Responsibility to protect confidential information

No stipulation

9.4 Privacy of personal information

The German privacy laws, where possible, should be applied as orientation.

9.4.1 Privacy plan

No stipulation

9.4.2 Information treated as private

No stipulation

9.4.3 Information not deemed private

No stipulation

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

No stipulation

9.6 Representations and warranties

No stipulation

9.6.1 CA representations and warranties

No stipulation

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 PKI participants

No stipulation

9.7 Disclaimers of warranties

No stipulation

9.8 Limitations of liability

No stipulation

9.9 Indemnities

No stipulation

9.10 Term and termination

No stipulation

9.10.1 Term

No stipulation

9.10.2 Termination

No stipulation

9.10.3 Effect of termination and survival

No stipulation

9.11 Individual notices and communications with participants

No stipulation

9.12 Amendments

No stipulation

9.12.1 Procedure for amendment

No stipulation

9.12.2 Notification mechanism and periods

No stipulation

9.12.3 Circumstances under which OID must be changed

No stipulation

9.13 Dispute resolution provisions

No stipulation

9.14 Governing law

No stipulation

9.15 Compliance with applicable law

No stipulation

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation

9.16.2 Assignment

No stipulation

9.16.3 Severability

No stipulation

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation

9.16.5 Force majeure

No stipulation

9.17 Other provisions

10 Glossary

Certification Authority

Certification Authority (CA) is responsible "for the creation, issuance, management and revocation of digital certificates" (cf. ITWissen, see 1.6.4. reference). Within the context of the European Bridge CA participating CAs must fulfill the contractual obligations of the European Bridge CA. Participating CAs may exist inside or outside the participant´s company/organization.

Certificate Policy of EBCA

The document describes the requirements for EBCA participants. The participant confirms the compliance of the EBCA CP´s stipulations in his CP or in the Certification Practice Statement (CPS). The EBCA CP complies with RFC 3647. This is also to be expected in the CPs of EBCA participants. If trust service providers with individual CP are needed for the certificate procurement (registration, certification, issue etc.) the EBCA participant, however, must comment on the regulatory obligations within his area of responsibility (relating to the handling with key material when revoking certificates etc.).

Certification Practice Statement

Certification Practice Statement (CPS) is a document describing the mode of operation of a PKI, generally more elaborately as in the CP. A CPS specifies the security standards of the PKI published in the Certificate Policy and regulates the operation. Whereas each member of the EBCA must have a CP of his own to enable the comparability, the publication of a CPS is not necessary if the minimum standards in the CP are confirmed in appropriate manner.

Certificate Revocation List

Certificate Revocation List (CRL) is a revocation list which contains information about revoked certificates in order to prevent abuse. The revocation list comprises the current serial numbers of invalid certificates. They are issued and signed by Certification Authority (CA) and are available for download. LDAP directory services or a status request to an OCSP server can be used to verify the validity of certificates.

Certificate Revocation

Certificates can or must in certain cases be revoked in order to prevent abuse of digital certificates before their validity expires. Since revocation can never be rescinded, it permanently prevents the use of certificates and the associated PSE. A certificate must be revoked when the private key has been compromised, a key pair can no longer be uniquely tied to its subscriber or when there is no longer a unique link between the certificate and the key. If the private signature key of the Certification Authority (CA) is compromised, the EBCA must be notified without due delay. EBCA members must provide at least one publicly accessible http or LDAP address for the verification of revocation information, which is included in the CRL distribution point (CDP) of certificates.

Common PKI

"The Common PKI specification describes a profile of internationally widespread and acknowledged standards for electronic signatures, encryption and public key infrastructures" (cf. T7, see 1.6.4. reference). The Common PKI Specification describes standards on the basis of these the EBCA participants have agreed in the interoperability test.

Certificate Distribution Point

A Certificate Distribution Point (CDP or also CRLDP) is a distribution point of the revocation list displayed in the certificate, to which the revocation list (CRL) is linked.

DistinguishedName

"DistinguishedName" (DN) is a technical name comprising of numerous name parts, which clearly describes the issuing CA and/or the subscriber in the certificate path. "The DN ensures that a digital certificate is never issued for different persons with the similar name" (cf. ITWissen, see 1.6.4. reference). The CA and the serial number as well as the name are stored to ensure the unambiguousness of a digital certificate. The "DistinguishedName" is defined in standard X.501. The EBCA stipulates that in certificates the email address of the subscriber must be included in the DistinguishedName" (DN). Furthermore, the "CommonName" (CN) muss be given in the "DistinguishedName" (DN).

End Entity Certificate

End Entity Certificates are certificates which are directly issued for a natural person or technical (end) entity. If subscribers are natural persons the certificate should be clearly linked to the subscriber in the EBCA since a signature or authentication certificate clearly refers to a natural identity. If a certificate is issued for a function or group of persons this should be clearly recognizable in the certificate subject as such ("Subject") (for example by adding the attribute "Team Certificate", if a confusion with a personal certificate is not otherwise excluded.)

European Bridge CA

The TeleTrusT European Bridge CA (EBCA) is a consolidation of individual, equal Public-Key-Infrastructures (PKI) in a PKI network of trust. It enables secure and authentic communication between businesses, institutions and public authorities.

ISO/IEC 27001

ISO/IEC 27001 is the standard for Information Security Management (ISM) of the International Organization for Standardization (ISO), which aims at ensuring the security of information in organizations (cf. ISO 27001, see 1.6.4. reference). The internal security guidelines and standards of participants, which can be oriented toward ISO/IEC 27001, are decisive for the operation of the EBCA (see term Security Policy).

KeyUsage

(referred to CA certificates)

In the certificate extension "KeyUsage" the operational properties of the public key are specified. CAs must take into account the conformity criteria of the EBCA when determining the certificate extension. The "KeyUsage" should be designated as critical.

LDAP

"Lightweight Directory Access Protocol (LDAP) is a TCP/IP-based directory access protocol, which has caught on as a standard solution for accessing network repository services for databases, emails, storage areas and other resources on the Internet and intranets" (cf. ITWissen, see 1.6.4. reference). The EBCA provides a central LDAP directory service to ensure the distribution of certificates. If the LDAP directory is integrated, subscribers can send a request for encryption certificates of EBCA participants out of their applications and exchange encrypted data with these persons.

Object Identifier

The Object Identifier (OID) is a sequence of characters and numbers which is used for the description and globally unique identification of abstract objects in the computer science. The EBCA highly recommends that OIDs of the related CPs in X.509 Certificates are to be entered into the non-critical extension of the attribute "certificatePolicies". The OID of this document is:
1.3.6.1.4.1.20351.1.2.1.

OCSP

The Online Certificate Status Protocol (OCSP) is a protocol using to verify the current status of a certificate online. The status request via OCSP helps to identify whether a certificate is still valid or revoked. In this procedure an OCSP client sends a status request to the OCSP server and receives the answer "good, revoked or unknown" from the server. Each EBCA participant must provide a method (for example CRL, LDAP, OCSP) for the verification of the certificate´s validity.

Public Key Infrastructure

A Public Key Infrastructure (PKI) is defined as an environment "in which services for the encryption and the digital signature on the basis of public key procedure are available. In this security structure the public key of a subscriber (…) with relevant identification features is authorized by CA (…) by means of a digital signature" (cf. ITWissen, see 1.6.4. reference).

Security Policy

The Security Policy is a binding document describing the security policy of a company/organization. This policy contains "guidelines and rules which are to be followed by persons having access to database, systems and resources. In this policy rules and practices are defined for transmitting, processing and storing data. The security policy includes personal, technical, organizational as well as legal influencing factors" (cf. ITWissen, see 1.6.4. reference). The secure handling with cryptographic key material for the PKI can be bindingly regulated in a security policy in regard of labour law even beyond the CP. In the revised version of standard ISO 27001:2013 the handling with cryptography has become such an independent Control so that the security policy is more important than ever.

Registration Authority

The "Registration Authority (RA) is an optional entity within a security infrastructure (PKI). It closely cooperates with the Certification Authority (CA) and is responsible for the secure identification and registration of subscribers. It verifies the identity of the subscriber (…), sends the application to the CA and hands over the Personal Identification Number (PIN) issued by the CA to the subscriber" (cf. ITWissen, see 1.6.4. reference). RA´s participants of the EBCA can be based in or outside the company/organization of EBCA participants. They guarantee a reliable identification and authentication of applicants within the framework of their guidelines.

Registration Process

The registration is the ascertainment of identity in the personalization process at a registration authority (RA) and the signed transmission of data over a secure channel to the trust center. This must be preceded for an application. The participant in the process for digital signatures is assigned a suitable, unique name. Before registration subscribers are to be reliably identify using a documented process. The registration must also be a documented process.

Relying Parties

Relying Parties are subscribers, i.e. all people and organizations using certificates of subscribers and with access to EBCA´s services. Subscribers of EBCA participants can use the EBCA directory service to search for the public keys of EBCA participants and download them via the EBCA directory service. This can also be integrated into the email client as LDAP directory.

RFC 822

In RFC 822 standard the syntax and format of email messages are described. An email comprises of a body which contains the message to be transmitted and a header, which contains information about i.a. the sender, recipient, date and subject. In order to guarantee an EBCA-compliant identification and authentication of certificates naming rules should be applied in accordance with RFC 822 standard.

RFC 3647

The internet standard RFC 3647 is an internationally recognized framework which describes the certification of a PKI and its CP in accordance with X.509 standard (issuance of digital certificates) of the International Telecommunication Union (ITU). The EBCA CPs, as well as its members, are oriented towards RFC 3647 and they enables an outwardly transparent and comparable representation of security standards of PKIs operated within the EBCA.

Subject DistinguishedName

The entry "SubjectDistinguishedName" (Subject DN) is the name of an issued certificate and clearly identifies the subscriber. The unambiguity of "Subject DNs" is guaranteed if the same "Subject DN" is never assigned to two or more different entities. In the EBCA the naming rules must be defined for the "SubjectDistinguishedName" in accordance with X.501 Standard.

S/MIME

The Secure/Multipurpose Internet Mail Extensions (S/MIME) enable emails or other MIME-based messages (for example AS2) to be sent and received securely. S/MIME "is a secured option of MIME protocol which guarantees the confidentiality, authenticity and integrity of email clients" (cf. ITWissen, see 1.6.4. reference).

Technical Interoperability

Technical interoperability, besides the comparability of the security level and minimum adequate standards, is a criterion which new EBCA participants must fulfil. The EBCA´s interoperability tests will be carried out and they must be successfully completed.

Technical Conformity

The EBCA provides a platform for the technical conformity by profiling technical standard Common PKI as well as for the execution of tests to determine the mutual interoperability. The technical conformity is proved within the context of the EBCA´s interoperability tests.

Subscriber Certificate Policy

In the Subscriber Certificate Policy (Subscriber CP) the EBCA subscriber (Subscriber) declares that his CA is compliant with the guidelines and requirements of the EBCA CP, that he has issued his own subscriber CP, which implements the guidelines of the EBCA CP and that the subscriber has successfully passed the required interoperability test.

Trust Service Provider

A Trust Service Provider (TSP) / Certification Service Provider (CSP), provides services for issuing and using electronic certificates. TSP represents an umbrella term in the context with digital certificates and covers all service providers who render services in the field of electronic certification.

X.509 conformed Certificates

X.509 conformed certificates are, according to X.509 standard of the International Telecommunication Union (ITU), issued digital certificates on which "the names and the digital signature of the issuers are visible (…) The X.509 standardized certificates can also be email certificates using for the secure transmission of emails and files and for the identification toward websites as well" (cf. ITWissen, see 1.6.4. reference). Subscriber certificates of the EBCA must be compliant with standard X.509 v3 (Type 0x2).