IT Security Association Germany

TeleTrusT
Pioneers in IT security.

TeleTrusT EBCA
European Bridge Certificate Authority

Declaration of conformity

for participation in the
TeleTrusT European Bridge CA

Information on this document

Version 2.7

26/02/2019

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

Tel: +49 (0)30 4005 4310
Fax: +49 (0)30 4005 4311

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

Contents

1 Aim 3
2 Interoperability 3
3 Publications..... 3
4 Identification..... 3
5 Proper operation 3
6 Information following cessation of business 3
7 Deregistration 3
8 Payments..... 4

History

Version	Date	Modification	Author
2.2	01/12/2010	Terminology revised	Dr Holger Mühlbauer
2.3	11/01/2012	Association name revised	Dr Holger Mühlbauer
2.4	08/02/2012	Appearance and terminology revised	Marieke Petersohn
2.5	18/07/2014	New EBCA logo inserted	Martin Fuhrmann
2.6	28/06/2016	Content adjustments “venue of the PKI”	Marieke Petersohn
2.6	21/09/2016	Changes in Translation	Ida Köhler
2.7	26/02/2019	Association name revised	Morad Abou Nasser

1 Aim

The TeleTrusT European Bridge CA (EBCA) has been set up by TeleTrusT to provide participating businesses, public authorities and institutions with an inexpensive and reliable method for the mutual validation of certificates. The EBCA acts as a bridge between participants by verifying the Root certificates of participating organizations, supporting the exchange of employee certificates, and hence enabling for example the cross-organizational, secure exchange of emails (signed and encrypted). The participating organizations recognize the European Bridge CA as a trusted mediator and therefore do not have to make separate agreements with each other.

2 Interoperability

To ensure the necessary interoperability of all public key infrastructures (PKIs), each new participating organization must complete an interoperability test before joining the EBCA. TeleTrusT may refuse registration if conformity is not confirmed by the test. Should the test results indicate that technical or organizational adjustments are still needed to enable interoperability, the new participant must be willing to make the necessary adjustments. Moreover, new participants must be willing to subsequently adapt components should this be necessary for the EBCA community to maintain interoperability, e.g. in response to technical development or other changing requirements. TeleTrusT may update and revise the requirements specified in the annex. The most recently amended version of the annex must be implemented. TeleTrusT shall notify participants of such changes in good time and provide a reasonable period for migration.

3 Publications

The Participating Organization agrees to the publication of its participation in the EBCA and to the publication of its Root and Sub CA certificates under their control as trust anchor. Adjustments to the Root and Sub CA certificates (expiration/renewal) must be reported immediately to the EBCA. The Participating Organization also declares its consent to providing access to the operation of PKI related parts of its Certificate Policy (CP) or its Certificate Practice Statement (CPS) accessible to both TeleTrusT as the operator of the EBCA as well as the other participating organizations.

4 Identification

It must be possible to reliably identify the users of the PKI. The character of other certificates (server, role, organizational certificates) must be clearly visible to the recipient. A certificate issued as a pseudonym certificate must also be identifiable as such.

5 Proper operation

The Participating Organization shall perform the certification services under its CP in a proper, state-of-the-art manner. The EBCA's minimum requirements (see annex) for the Participating Organization's PKI must be met. Justified deviations are possible.

6 Information following cessation of business

The Participating Organization must announce the discontinuation of its certification services to the EBCA in good time.

7 Deregistration

The EBCA Community is entitled to deregister a participating organization that fails to comply with these minimum obligations.

8 Payments

TeleTrusT is entitled to receive sums of money for running the EBCA. Such payments are to be agreed separately.

............................., ...	............................., ...
Date, place	Date, place
....	....
IT Security Association Germany (TeleTrusT)	Participating Organization

Annex

Organizational and technical requirements for participation in the European Bridge CA (EBCA):

A) Requirements for a participating PKI and its architecture

- Personal identification and registration of the certificate holder
- Access to recall data from the EBCA and its participants (Certificate Revocation Lists (CRLs) which are retrievable in internal or via replicated directories or available from a web server or by using an OCSP server)
- When names are assigned (to users and PKI certificates), it must be ensured that the chosen domain names (DNs) are unique across all participating infrastructures.
- 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.

B) Requirements for the certificates used

- The Certificates are X.509v3-compliant.
- The private key is a key with a length based on the current state of the art in accordance with the algorithm-catalog of the “Bundesnetzagentur (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway)", as published annually in the "Federal Network Agency's Official Gazette".
- The attribute ‘key usage’ is set to signature and/or encryption.
- Certificates must be in the .crt, .der or .p7b file format.

In addition, it is also helpful if

- As few attributes of the certificate as possible are regarded as ‘critical’.

C) Requirements for CA products

- There are no mandatory requirements for CA products since they are not involved in the distribution process.

D) Requirements for the PKI client

- Import of Root certificates in a standard format (e.g. PKCS#7)
- Support for the S/MIMEv2 format
- Signed emails must always be replaced in opaque signed mode. This means that the email is signed and sent as a whole as a signed file. The text body is therefore part of the .p7 file.