



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

Particularly, the following laws apply to certification:

1. Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC), currently published on http://data.europa.eu/eli/reg_impl/2024/482/oj
2. Ordinance on the Procedure for the Issuance of Security Certificates and Recognitions by the Federal Office for Information Security (BSIZertV) of 17 December 2014, Federal Law Gazette 2014, Part I, No. 61, p. 2231, currently published on http://www.gesetze-im-internet.de/bsizertv_2014/index.html
3. Act on the Federal Office for Information Security (BSIG) of 14 August 2009, Federal Law Gazette I p. 2821 in the current version, currently published on http://www.gesetze-im-internet.de/bsig_2009/index.html
4. Administrative Procedure Act (VwVfG) in the version published on 23 January 2003 (Federal Law Gazette I p. 102), currently published on <http://www.gesetze-im-internet.de/vwvfg/BJNR012530976.html>
5. special fee regulation of the BMI for individually attributable public services in its area of responsibility (BMIBGebV), Section 7 (BSI Act) of 2. September 2019, Federal Law Gazette I p. 1365., currently published on <https://www.bsi.bund.de/Gebuehrenverordnung>

§§ 2, 8 BSIZertV specify which information an application for certification must contain and which additional information must be documented, e.g. in annexes. The additional information requested in the application form and the annexes are required for planning, preparing and implementing the certification activities.

BSI's certification body issues new certificates only in accordance with the programme 'Product certification: European Common Criteria (EUCC)' in the European Common Criteria-based cybersecurity certification scheme (EUCC). BSI's certification body may still accept applications for the review of already issued German IT security certificates under its former national programme "Product certification: CC-Products". Such application is permitted only for the following certification review activity if the issued German IT security certificate will remain unaltered:

- Maintenance,
- Partial Re-evaluation,
- Partial ALC Re-evaluation,
- Re-assessment.

Per point 1. Applicant for the certification of an ICT product

In accordance with Articles 8 (5), 9 and chapters V to VII of EUCC Regulation (Regulation (EU) 2024/482), and § 6 (2) BSIZertV, the applicant bears the responsibility for ensuring its cooperation in the course of certification including the cooperation of any third party who



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

controls or owns parts of the ICT product, its documentation or its production or development environment. According to Article 8 of the EUCC Regulation and § 8 (1) BSIZertV, the applicant has to submit a declaration from each third party expressing its consent with the application, its willingness to cooperate and to support the applicant in order to meet requirements and provisions in the course of certification and after the certificate has been issued. § 13 (2) of the Administrative Procedure Act (VwVfG) shall remain unaffected.

A declaration shall therefore contain:

- name and address of the third party,
- identification and explanation which parts of the ICT product to be certified referred to in point 3 of the application are covered by the declaration,
- a confirmation that the rights of the aforementioned parts are held by the party,
- the party's consent to provide documents or evidence related to the aforementioned parts as required in the evaluation criteria,
- the party's consent to grant access and information to production or development sites involved with the aforementioned parts in the course of carrying out evaluation and certification activities,
- the party's consent to assist the applicant in meeting the requirements and provisions of the EUCC certification scheme over the course of certification and after the certificate has been issued.

Article 8 (6) in the Implementing Regulation (EU) 2024/482 requires a link to website containing supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881 and a description of the applicant's vulnerability management and vulnerability disclosure procedures. See point 5 regarding further information.

Per point 3: ICT product to be certified

The description including version details shall uniquely identify the target of evaluation submitted to certification, commonly an ICT product, as it is placed and promoted on the market and supplied to customers. The certificate issued later identifies the target of evaluation based on the provided details..

The description shall be consistent with the Security Target that is submitted by the applicant. Any given version number shall match and be consistent with the product details at the time of application. Those details may change and shall be notified in the course of certification, e.g. if the ICT product is modified or revised. The notification shall be submitted by email to the certification body with reference to this application and adopted in the security target. The certificate, the final evaluation and certification report refer to the final details at the time the certificate is issued.

The product type chosen in the application shall match the classification published on BSI's certification website and, where necessary, further specified by the applicant.

The development and production status of the ICT product may be described by the following two options:

- (i) ICT product in design or development,



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

(ii) Final ICT product

If the application targets a composite evaluation in the technical domain „Smartcard and Similar Devices“, the applicant shall provide the evaluation details of the underlying hardware component and the respective ETR for Composition. The information is mandatory.

Per point 4: Evaluation Criteria

The most recent release of Common Criteria and, where requested, protection profile (PP) or technical guideline valid at the time the application applies to the certification application. The applicant may choose to apply the modified release of the criteria or specification if it has been amended over the course of certification. If, however, the criteria or specification becomes formally void, its last valid release has to be applied.

In principle, BSI's certification body uses the latest release of the Common Criteria, published as ISO/IEC 15408 and 18045, or the contents of the corresponding publication of the CCRA. The transitional provisions of Article 2 of Commission Implementing Regulation (EU) 2024/482 apply to the use of CC version 3.1 (see also https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202403144). BSI's certification body recommends using the most recent release of Common Criteria.

When applying for higher assurance requirements than set out in a PP, such choice shall be justified by the applicant since higher requirements may contradict the rationale stated in the PP. Such justification has to be comprehensible and plausible. Higher requirements often increase certification efforts that need to be carefully planned and coordinated with the certification body's schedule. When a PP is used to meet specific legal requirements, the exact assessment level stated in the PP should be considered, i.e. the assurance requirements should not be levelled up.

The applicant is responsible for selecting the commensurate scope of requirements stated in a technical guideline. The certification body reserves the right to define the scope of requirements. Including a technical guideline into an ICT product's certification however cannot substitute a regular certification in accordance with the technical guideline.

Further voluntary information on the product's relation to government projects or regulations help the certification body to understand the classification of the application and the planning. In these cases, special conditions may apply for the validity and maintenance of the certificates. The applicant's consent to forward the planning data for the certification activities to the project owner helps to better coordinate the certification activities with the project schedule.

Per point 5: Type of certification

Certain documents must be submitted together with the application about its planning and preliminary evaluation. Along these documents, further product information may be required while carrying out the evaluation and certification activities in accordance with the Common Criteria, where necessary.



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

Enclosure Document security target:

The content and concept of a security target is defined in the Common Criteria, Part 1.

Enclosure link to their website containing supplementary cybersecurity information:

Article 55 of Regulation (EU) 2019/881 requires publishing further information like guidance for secure usage, support period, etc. on a publicly available website.

Enclosure s vulnerability management and vulnerability disclosure procedures:

The Implementing Regulation (EU) 2024/482 requires a description of the vulnerability management and disclosure procedures in any case. If the application contains the assurance component ALC_FLR.2, the developer documentation for this assurance component is sufficient to fulfill the requirements.

Enclosure Overview of development and production sites:

A list of the development and production sites relevant to the product is required and should include:

1. name of the organisation operating the site and, if different, the name of the organisation responsible for the site and the test evidence available at the site;
2. exact address of the site; and
3. type of the site (e.g. product development, testing, delivery, chip production, device assembly) and a brief description of the site's role in the life cycle of the product.

Please note that complete descriptions of the processes, procedures and rules that apply at the respective location or site are not yet required at this stage of the application.

Example of a location or site list:

1a). Name of organization operating the site	1b). Name of organization responsible for evaluation evidence	2. Exact address of the site	3. Type of site and role in life cycle

Enclosure List of the cryptographic mechanisms (algorithms and communication protocols) offered via the product's external interfaces:

If cryptographic services or a set of their security functionalities are offered through the product's external interfaces and identified in the security target, their evaluation and certification demands special attention due to legal requirements. Cryptographic services encompass for instance encryption functions, hash value generation, signature generation, random number generation, key generation, protocols with cryptographic components. Therefore, the applicant should provide an overview of relevant cryptographic mechanisms in order to identify possible requirement conflicts at this early stage and to optimise the certification schedule. The following information should be provided per mechanism:

1. Purpose:



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

- Authenticity as often modelled using FCS_COP.1
 - Authentication as often modelled using FIA_UAU.{4,5,6}, FCS_COP.1, FPT_TDC.1 and/or FIA_API.1
 - Key Agreement as often modelled using FCS_CKM.{1,2} and/or FCS_COP.1
 - Confidentiality as often modelled using FDP_UCT.1, FPT_ITC.1 and/or FCS_COP.1
 - Integrity as often modelled using FDP UIT.1, FPT_ITI.{1,2}, FDP_SDI.{1,2} and/or FCS_COP.1
 - Trusted Channel, which offers secure communication to meet the security objective of integrity and/or confidentiality together with authenticity and is often modelled using FTP_ITC.1 or FTP_TRP.1.
 - Random Number Generation) as often modelled using FCS_RND.1 or used by one of the above-mentioned services
 - Cryptographic primitive), , which is available to the product user as a cryptographic function without a specific intended use
2. Cryptographic mechanism
 3. Standard for the mechanism'S implementation
 4. Key Size(s) in Bits
 5. Applied Standard, where relevant, that requires the cryptographic mechanism for the product's use case. Example of standards
 - BSI TR-03116
 - Catalog of algorithms (SigG/SigV)
 - Requirement list for the tachograph



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

Example of a crypto table:

1. Purpose	2. Cryptographic Mechanism	3. Standard of Implementation	4. Key Size in Bits	5. Standard of Application
Authenticity	RSA-signature generation and verification (RSASSA-PSS) using SHA-256	[PKCS#1 v2.2] (RSA), [FIPS 180-4] (SHA)	Modulus length=2048	[AlgoKat]
Authentication	ECDSA-signature generation and verification using SHA-256	ANSI X9.62 (ECDSA), FIPS 180-4 (SHA)	Key sizes corresponding to the used elliptic curve brainpoolP256r1 (RFC 5639) and secp256r1 (SEC2)	–
Key Agreement	DH	[HaC] ¹	Plength = 2048	–
Confidentiality	AES in CBC mode	[FIPS 197] (AES), [SP 800-38A] (CBC)	k =128	–
Integrity	AES in CMAC mode	[FIPS 197] (AES), [SP 800-38B] (CMAC)	k =128	–
	HMAC with SHA-256	FIPS 180-4] (SHA), [RFC 2104] (HMAC)	k ≥ 256	–
Trusted Channel	TLS v1.2	[RFC 5246]	–	–
Cryptographic Primitive	AES	[FIPS 197] (AES)	k =128, 192, 256	–
	SHA-512	[FIPS 180-4] (SHA)	none	–
	RSA-encryption	According to section 5.1.1 RSAEP and	modulus length=2048	–

¹ see „Handbook of Applied Cryptography“

Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

	and - decryption	section 5.1.2 RSADP in [PKCS v2.1]		
	Deterministic RNG DRG.3	[AIS 20]	n. a.	n. a.

Ideally, the list should be enclosed with the security target.

Re-certification:

Re-certification are certification activities in order to uphold the product's trustworthiness after a change affecting product's security properties and functions, a so-called 'major change'.

Enclosure Impact analysis report on the changes (IAR):

Certification activities related to the maintenance of issued certificates such as re-certification, partial re-evaluation or maintenance depend on a description and analysis of changes and their impact on the product security properties and functions. Specification AIS 38 describes the necessary contents and is available on BSI's certification web site (www.bsi.bund.de/zertifizierung). Based on the document the certification body examines if a re-certification or partial re-evaluation should be carried out. The applicant should be prepared to provide more information or evidence in order to support the body's decision.

Enclosure updated configuraton list:

Certification activities related to the maintenance of issued certificates such as re-certification, partial re-evaluation or maintenance requires the update of the existing configuration list in accordance to the requirements of the assurance level stated in the certificate. The current changes and their state in relation to the product's prior configuration list as referred in the issued certificate have to be discernable and identifiable.

Enclosure updated user guidance:

Certification activities related to the maintenance of issued certificates such as re-certification, partial re-evaluation or maintenance require, where relevant, the presentation of the product's user guidance. The current changes and their state in relation to the product's prior user guidance as referred in the issued certificate have to be discernable and identifiable.

Retention of certification ID:

In specific cases such as the application of only a few security-related product changes the ID of the prior certificate can be retained on the applicant's request, even in a recertification. In such case, the certification ID will be extended by an extension identifying the change. For example, the ID ,AVA_VAN.[No]-EUCC-BSI-DAkKS[No]-[YYYY-MM]-[No]' is modified into , AVA_VAN.[No]-EUCC-BSI-DAkKS[No]-[YYYY-MM]-[No]-MA'.

Maintenance:

The certification type maintenance aims at upholdig a product certificate after a so-called "minor change" to the product whose impact on the product's security properties and functions is negligible. Whether the change is minor or major decides the certifiacton body on the grounds of the documents submitted with this application. In that regard, the



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

certification body may also request the vote of the evaluation facility. The applicant may however obtain the evaluation facility's vote itself and submit the vote together with the application.

If the prior issued certificate covers the assurance family ALC_PAM in accordance with specification ISO/IEC TS 9569, security patches or other changes to the TOE can be applied to certified product without terminating the certificate. Such security patches may therefore also be subject of maintenance activities. Specification "ISO/IEC TS 9569, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045" can be obtained from ISO/IEC.

Enclosure vote of the prior involved evaluation facility:

For the reason of its product knowledge drawn from prior certification, the evaluation facility analyses the IAR and votes on whether a product change qualifies as minor or major. The vote supports the later decision of the certification body.

Partial Re-evaluation:

This certification type is limited to repeating a few and specific assessments of the product changes after certificate issuance, i.e. product changes are only re-evaluated in the application of a few specific assurance components of the CC. The applicant may choose an accredited and, if necessary, authorised evaluation facility, whereas choosing the previously involved facility is recommended.

Insofar the changes do not require the alteration of the certificate, their description is added as a maintenance report to the certificate. If throughout the proceedings a certificate may become invalid, e.g. a new vulnerability, the prior certificate will be withdrawn and a new one carrying the same validity date of the prior one issued. Should security requirements or functionalities change after certificate issuance, such as modified or new SFRs, a re-certification is strongly commended.

Partial ALC Re-evaluation:

Changes related to assurance class ALC are covered by this type of certification. This type does not repeat the vulnerability analysis as present at certificate issuance. This type also does not include the reassessment of the product's attack resistance in review of its changed lifecycle (ALC), e.g. to what specific changes to a production process alter the product's attack resistance. Such review of attack resistance demands for a re-certification.

The applicant may discuss available options with the certification body at any time.

Re-Assessment of prior AVA- assessments:

The applicant may apply for a review of the product's resistance against a specific attack potential or the changed threat scenario that has changed since certificate issuance. This type is carried out by the very evaluation facility that was involved in the prior certification activity. This type of certification is limited to evaluation activities concerning assurance family AVA_VAN and, where required, the evidence to be renewed for class ALC.



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

Per point 6: Evaluation facility

Involvement of a evaluation facility:

The certification types (first) certification, re-certification, partial re-evaluation, and reassessment mandate for the involvement of an accredited and, where necessary, authorised evaluation facility. The applicant may choose a facility for (first) certification from the list of notified bodies (NANDO) at its discretion. The certification types re-certification, partial re-evaluation, and reassessment require that the facility involved in prior certification has to become engaged again. A maintenance of the certificate incurred by minor product changes may require the involvement of the evaluation facility only under exceptional circumstances. The facilities involvement will be determined by the applicant and certification body.

Evaluation plan:

The contracted evaluation facility provides for the schedule of evaluation activities and coordinates the plan with the certification body. The plan encompasses the type, scope, and estimated dates of evaluation activities. The evaluation plan becomes part of the applicant's evaluation contract with the evaluation facility. The applicant bears responsibility for the timely submission of the plan to the certification body or the lack thereof.

Indended starting and ending date:

The feasibility of the proposed dates should be agreed with the certification body, commonly during the kick-off meeting.

Per point 7: Details on prior evaluations

In accordance to § 8, para. 2, no. 6 BSIZertV and if available, an application shall contain information on audits and assessments already carried out by other evaluation facilities. This could be, for example,; a completed or aborted certification under the EUCC or a comparable certification scheme and regardless of the result achieved or evaluated security properties of the product. Evaluations of single security characteristics of the ICT product would be of interest as well. The certification body may in preparation of its activities determine whether results or evidence from prior evaluation activities can be reused.

Per point 8: Details on conflict of interest

In case an applicant is or becomes informed that the evaluation facility involved in the certification proceedings will participate or has participated in the development of the product submitted to certification or in the preparation of product documentation, in particular the security target or test protocols or evidence, such information has to be provided in the application or during the certification proceedings without undue delay.

In order to meet certification requirements conflicts of interest related to the certification proceedings have to be declared at all times. If the applicant becomes aware of any financial, commercial or legal circumstances that may exert influence or control over parties involved in the certification proceedings or impede the impartiality or independence of the certification activities, the applicant has to inform of any such matters without undue delay. Parties can



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

be organisations or individuals other than the applicant itself such as other manufacturers, developers, sponsor or the evaluation facility.

Per point 9: Public notification prior to certificate issuance

As no information on the proceedings of a maintenance or reassessment are published, the applicant for maintenance or reassessment procedures does not need to make a statement here.

Per point 10: Public notification of certificate issuance

In accordance to article 42 of Commission Implementing Regulation (EU) 2024/482 (EUCC), the issued certificate and its necessary enclosures including their current status are to be published in pertinent sources which is primarily ENISA's certification web site.

In accordance to § 7, para. 1 BSIZertV, the certification body may publish certificates and its enclosures also on other media. Relevant media are BSI's certification website, the KES journal and, if necessary for international recognition, the CCRA portal.

In accordance to § 7, para. 5 BSIZertV, the applicant may revoke its consent to certificate publication at any time until certificate issuance. After revocation, the applicant is no longer asked for permission again and shall announce such change by its own discretion in time and writing.

In addition, the certification body may waive certificate publication in accordance to § 7, para. 5 BSIZertV when public security interests are affected or when public or private interests are concerned by the publication. The certification body will bring such circumstances to the attention of the applicant.

Should the certificate not be published it is not being recognised in the EUCC certification scheme or other international certificate recognition agreements such as the CCRA.

Per point 12: Costs

The fees charged by the certification body for the proceedings of the application are set out in the schedule of fees valid at the time of application. If the certification activities cannot be completed until certificate issuance, the certification body will charge costs on a pro rata basis. To ensure smooth processing, the applicant shall complete and submit form sheet 'Additional information for BSI cost accounting in accordance with BMIGebV2' together with the application. In the event of billing relevant changes over the course of certification activities, the applicant has to update the respective form accordingly. At the closure of certification proceedings the applicant may want to review the form for changes on request of the certification body. Correct and up-to-date information is essential for expeditious settlement of charged fee.

The certification body reserves the right to involve an external party into certification activities while the body retains full responsibility and control over the proceedings and its results. Travel expenses of that external party's personnel incurred by carrying out certification activities have to be passed on by the certification to the applicant as charges of the certification personnel and in accordance to the schedule of fee.



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

If the applicant has a legally binding declaration of cost coverage by and with another party in conformance to the Special Fee Ordinance BMI, the certification body can settle its charges and fees directly with this other party only after the applicant has submitted this declaration.

For instance and through declaration, the evaluation facility may cover the cost of site assessments in non-EU countries or a certificate consumer may cover certain testing activities.

In such cases, the applicant is commended to assign in the form a reference number to the organisation assuming the costs in order to help the certification body with subsequent allocation of the costs.

Per point 14: Final declaration of consent

In accordance to Article 56 (6) of the Cybersecurity Act (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019) and to § 3, para. 1, point 6, BSIG, BSI's certification body is eligible and responsible for certification activities at assurance level 'high' and in justified cases at assurance level 'substantial'.

In conjunction with Commission Implementing Regulation (EU) 2024/482 on the adoption of the European certification scheme EUCC and § 4, para. 2 of the BSI Certification Regulation, BSI's certification body determines the procedure for issuing certificates listed in the Regulation and publishes procedural decisions and information for this purpose. These procedural decisions and information are set out in the following documents:

- „Procedure description for the certification of products“ (VB-Produkte)
- „Product certification: European Security Certification Common Criteria programme“ (EUCC)
- „Product certification: Common Criteria (CC) IT security certification programme“ (CC-Produkte)
- Various notes on application and interpretations of the scheme (AIS).

The documents are published on the BSI's website (www.bsi.bund.de/zertifizierung, section „Certification of Products“ and www.bsi.bund.de/AIS).

In order to meet current obligation, the following metadata and process data must be deleted from product or site security targets in PDF form before publication: 'Title', 'Author', "Topic" and 'Keywords'. The same obligation applies to XMP metadata or metadata of the document generator. By submitting the application, the applicant consents that such metadata is going to be removed by the certification body using a suitable tool. Metadata removal will not change the technical content, date or version of the to be published document.

The applicant furthermore agrees to the rules and provisions of data protection as further described in annex 'CC-222b: Data protection notes on the certification procedure'. In particular, the applicant acknowledges that the certification body will not remove personal data from the security target and that the applicant bears the responsibility for permissions to publish such data.

The applicant also acknowledges the following notes related to BSI Certification Ordinance (BSIZertV):



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

- a. On submission of the certification application, the certification activities are carried out as an administrative procedure in accordance with the requirements of the Administrative Procedure Act (VwVfG), the Ordinance on the Procedure for the Issuance of Security Certificates and Recognitions by the Federal Office for Security in Information Technology (BSI-ZertV) and the requirements of the above-mentioned procedural descriptions.
By submitting an application, the applicant commits to fulfil and comply with the aforementioned requirements.
- b. The applicant is obliged to submit all required information, documents, evidence related to the target of evaluation free of charge and without undue delay. That includes parts of and rights to the product that are necessary for its deployment and operation as well as access to sites involved in the design, development or production of the product (see VB-Produkte, chap. 3.1.1, EUCC, chap.5 and BSIZertV, § 6, para. 1 and § 11, para. 1). Unless the applicant presented the aforementioned points to the certification body, its obligation also covers the right of the evaluation facility to pass on such points in order to meet the requirements for the certification decision.
Furthermore, the applicant warrants the participation of a certifier (personnel of the certification body its involved external party) in relevant evaluation activities.
- c. The proceeding of certification activities can be terminated by the applicant at its discretion or by the certification body by means of a negative certification decision. The applicant will receive the body's decision with a justification that includes reasons, for example the absence or infeasibility of documents or evidence to meet the certification requirements. The applicant may appeal to the decision in accordance to VwVfG.
- d. In accordance to § 3, para. 2 of the BSIZertV, the applicant is obliged to retain and archive the evaluated IT product referred to in point 3 in its certified configurations and that evidence, which is referenced in the product's configuration list valid at the time the certificate is issued. The retention period should begin with the day of certificate issuance and ends at least 5 years after the expiry or withdrawal of the certificate. Retention periods for special cases are explained in the Implementing Regulation (EU) 2024/482. The aforementioned items shall be made available to the certificate body free of charge at at any time upon request.
- e. In accordance to § 3, para. 1 of BSI Certification Ordinance, the certification body archives the application including its enclosed documents and the documents being created or presented over the course of certification activities in electronic or paper form.
- f. Inspection of documents by the DAkkS in course of the BSI accreditation according to DIN/ISO 17065 is based on § 3, German law on accreditation. Regulation of confidentiality between DAkkS and BSI result from the BSI application for accreditation (cf. R-17011 and explanations in ISO/IEC 17011).



Explanatory notes on completing the application form CC-Zert-002a_Zertan_e, the required annexes and information on the certification procedure

The applicant also acknowledges the following notes related to Act on the Federal Office for Information Security (BSIG):

The certificate will be issued if the assessment criteria are met (see Section 9 (4) No. 1 of the BSI Act and the Federal Ministry of the Interior (BMI)), and if the issuance of the certificate has not been refused on the grounds that overriding public interests, in particular the security policy concerns of the Federal Republic of Germany, preclude the issuance (see Section 9 (4) No. 2 in conjunction with Section 9 (4a) of the BSI Act). In preparation for the assessment of this matter, information will be obtained from security authorities based on the application.