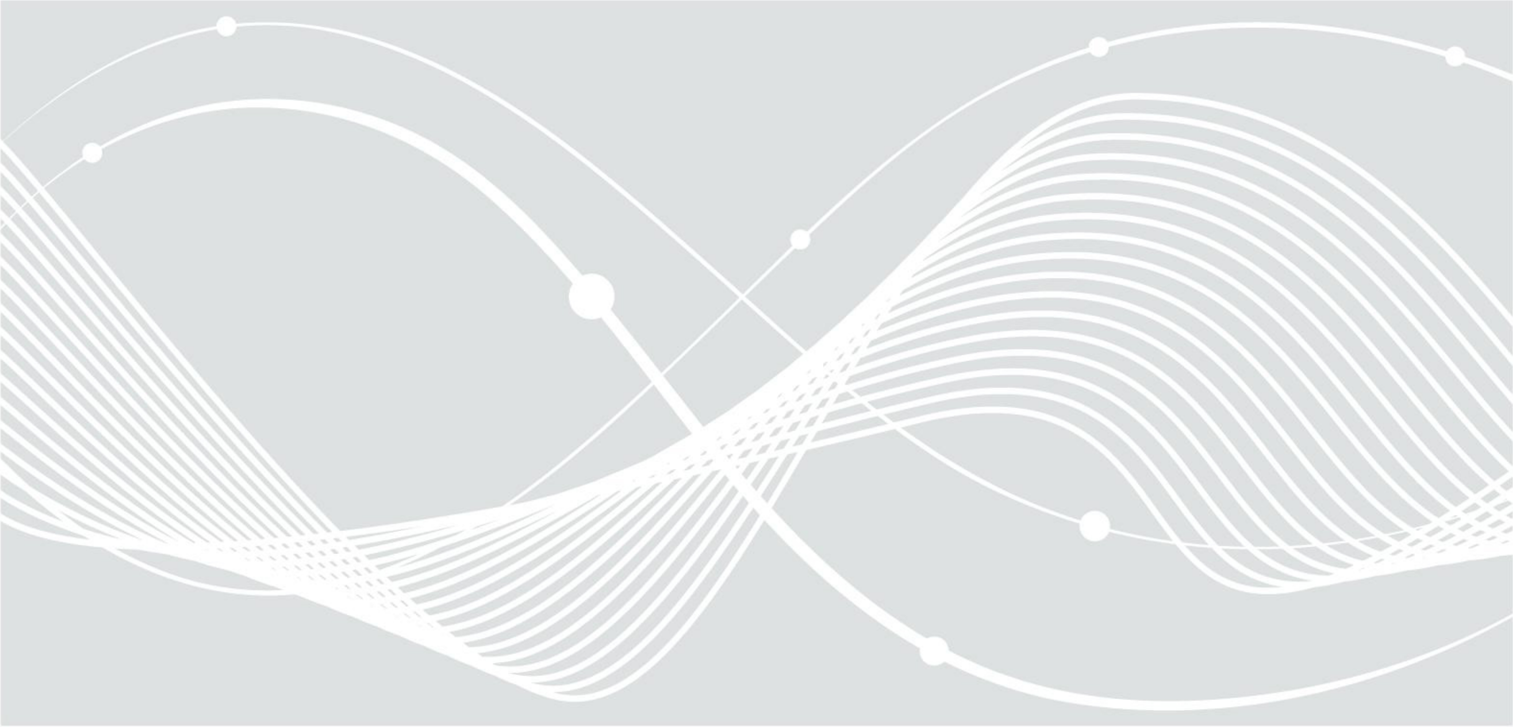
Federal Office
for Information Security

Technical information on the IT security certification of products, protection profiles and sites

(including confirmations in accordance with SigG)

BSI 7138

Version 2.1, as per 5 November 2012



Document history

Version	**Date**	**Reason for the change**	**Status**	**Distribution list**
1.0	February 2005		Approved	Public
2.0	October 2010	Fundamental updating and supplementation	Approved	Public
2.1	November 2012	Correction following int./ext. comments, updating	Approved	Public

Disclaimer: This document is an English translation of the German document "Hinweise für Antragsteller für die IT-Sicherheitszertifizierung von Produkten, Schutzprofilen und Standorten; Einschließlich Bestätigungen nach SigG, BSI 7138". In cases of doubt the German version shall prevail.

Foreword

In our information society, great importance is attached to information technology (IT) systems. Given the increasing dependency on the smooth functioning of such systems and the importance of information security in technical infrastructures, demands regarding security must also increase - in particular against the background of informational self-determination of each individual citizen, the sensitivity of information of the state and the economy, the fact that the health and lives of people may depend on IT systems in some areas and in order to protect critical infrastructures.

In this respect, the Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security] offers several IT certification services based on the BSI Act [BSIG] as part of a number of activities for increasing IT security.

Therefore, this publication, which is intended to be a technical guideline for the certification procedure, is directed in particular at manufacturers, distributors and developers of IT products who seek a German IT Security Certificate for an IT product or for a confirmation of technical components under the German Signaturgesetz [SigG [Signature Act]] in order to obtain proof of the trustworthiness of the security features of products from an independent body.

Likewise, this publication is directed at authors of protection profiles who wish to have their conformity with the Common Criteria [CC] certified and also to operators of development and production sites who wish to have them CC-certified.

The certification of information security management systems (ISMS) under ISO 27001 based on the IT-Grundschutz is described in other BSI publications.

It may also be necessary to furnish proof that other requirements are met, such as regarding functionality and interoperability in the operation of an IT product or IT system. For this purpose, BSI makes available technical guidelines (Technische Richtlinien (TR)), each of which describe requirements and test regulations for a certain class of products. The conformity of an IT product or IT system with such a technical guideline of BSI can also be confirmed with a certificate by BSI. The procedure in this respect is also described in another publication.

Further information is available from BSI, on the BSI website (www.bsi.bund.de/zertifizierung) and the evaluation facilities recognized by BSI for these evaluations. Interested persons can contact BSI via:

Bundesamt für Sicherheit in der Informationstechnik
Referat S22
Postfach 20 03 63
53133 Bonn
Phone (infoline): +49 22899 9582-111
E-mail: zertifizierung@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 Overview of the certification and confirmation procedures

1.1 Basic information on the certification procedure

The awarding of security certificates of IT products, protection profiles and sites is governed in the BSI Act [BSIG]. Execution regulations are included in the *BSI-Zertifizierungsverordnung* [BSIZertV [BSI Certification Ordinance]], in the *BSI-Kostenverordnung* [BSIKostV [BSI Regulations on Ex-Parte Costs]] and in decrees of the Federal Ministry of the Interior regarding questions of detail.

The procedure is carried out at BSI

- in accordance with the quality management manual and the procedural instructions of the certification body and in accordance with the standard DIN EN 45011,
- in accordance with the requirements of the international recognition arrangements [CCRA] and [SOGIS-MRA],
- in consideration of the relevant evaluation criteria CC/CEM[1] as well as additional Notes on Application and Interpretations regarding the scheme (AIS).

Certification is carried out as an application procedure. Following the preliminary assessment, the technical evaluation takes place based on the relevant evaluation criteria. The evaluation is performed by an evaluation facility approved by BSI (see chapter 3.2) and is technically monitored by the certification body. The evaluation ends with a positive (pass) or negative (fail) evaluation result. The applicant is notified based on this vote. If the evaluation result is positive, the certificate and the certification report will be enclosed with the notice. The applicant may give notice of appeal against the notice. In the case of a positive completion of the certification, the certification report will also be published on the BSI website, unless publication has been explicitly objected to.

Certification can be refused in accordance with [BSIG] if overriding public interests are opposed to the certification.

All parties involved (BSI and the evaluation facilities recognized by BSI) are obliged to keep business secrets in confidence and guarantee compliance with this important prerequisite through numerous measures. In special individual cases, the parties can conclude a non-disclosure agreement (NDA). Certification procedures can be carried out in each case as an initial certification, re-certification, maintenance or re-assessment.

Confirmation procedures under the Signature Act (SigG) are also carried out as an initial confirmation, re-confirmation or addendum confirmation following the same basic rules.

The particularities regarding the different forms stated above are explained in chapter 5.

Below, the types of procedures and their respective particularities compared to the above-mentioned basic aspects are described.

1.2 Certification of the security of IT products

In order to sufficiently minimize the risks involved in using information technology (IT), it is necessary that security functions are an integral component of modern IT. Therefore, the goal should be to design, manufacture and use information-processing systems in such a way that there is appropriate protection, such as against errors in operation and attempted manipulation and against directed attacks on assets to be protected. Manufacturers and developers of IT products[2] have dealt with this problem in numerous ways and today offer products which are much closer to the goal of "IT security".

In particular in the field of IT security, the interests and needs of the users are assisted by the fact that an independent, neutral instance examines and assesses the products. Thus, users can have trust in the evaluation results achieved as they are confirmed and published by a neutral authority with a certificate.

A certificate may be used by the manufacturer or distributor of the certified product within the framework of their marketing, as proof of qualification during tenders or in order to meet the requirements of their customers. The BSI IT security certificate for IT products, also referred to as

[1] In particular exceptional cases, other criteria like ITSEC/ITSEM may also be relevant.

[2] Regarding the product term, see chapter 2

"German IT Security Certificate" is recognized by numerous countries in certain evaluation levels within the framework of international recognition arrangements (see chapter 2.2).

So-called protection profiles (PP) under the Common Criteria offer the opportunity to define security requirements for product classes and security services as an effective standard (see chapter 5.4). The inclusion of protection profiles during the product development phase facilitates their evaluation, and the resulting products effectively meet the specific demands of the users. A protection profile is used in order to prepare uniform and comparable security targets for IT products. Certified protection profiles are available on the BSI website www.bsi.bund.de/zertifizierung, the CC website www.commoncriteriaportal.org, the SOGIS website www.sogisportal.eu or additionally on the websites of other national certification bodies.

The user requirements are in particular connected with the traditional threats of loss of

- the availability of data and services,
- confidentiality of information,
- integrity of data and
- authenticity of data.

In order to evaluate the security functionalities, the Common Criteria [CC], which also constitute an ISO standard (ISO/IEC 15408), are available as main criteria. Certification based on the older European security criteria ITSEC [ITSEC] is possible only in justified exceptional cases.

The certification report made available upon positive completion of a certification procedure includes the following in addition to a description of the product in terms of security:

- Confirmation that the evaluation was carried out in accordance with the recognized procedures and criteria,
- Confirmation that the product meets the security requirements specified in the security target regarding the functionality and scope of the evaluation,
- Information for the user as to how the product in question is to be used in practice with respect to the certification results.

If the applicant objects to the publication of the certification report, the certificate will not be governed by the international recognition arrangements and will not be included in the corresponding public lists by BSI.

1.3 Certification of protection profiles

Protection profiles (PP) under the Common Criteria [CC] offer the opportunity to define security requirements for product classes and security services as an effective standard. The inclusion of protection profiles during the product and system development phase facilitates their evaluation, and the resulting products and systems effectively meet the specific demands of the users.

The author of a protection profile is usually an authority or user organization, as a protection profile is a standard for security requirements with regard to subsequent product certifications. Therefore, an authority or user organization can file an application for the certification of a protection profile with BSI.

BSI develops protection profiles in order to define national security requirements in provisions for evaluation. Protection profiles are evaluated and certified in order to confirm their conformity with the concepts of the respective evaluation criteria (e. g. the CC). Certification of a protection profile which is contrary to the public interest in defining an evaluation standard can be refused in accordance with BSIG.

At present, protection profiles are certified by the certification bodies participating in the recognition arrangement (see chapter 2.1) and registered nationally. The previously certified or registered protection profiles are available on the BSI website www.bsi.bund.de/zertifizierung, the CC website www.commoncriteriaportal.org, the SOGIS website www.sogisportal.eu or additionally on the websites of other national certification bodies.

1.4 Certification of sites (site certification)

Development and production sites for IT products can be evaluated and certified separately under the Common Criteria. The operator of such a site can file an application for certification of a site with BSI. The goal of such a site certification is usually evaluating the site security, configuration management and acceptance and supply processes. This will be defined in each case in a site security target. The results then are to be suitable for re-use in subsequent certification procedures for IT products which are developed or produced at that site. With a site certification, it is possible to achieve synergy effects of product certifications, e. g. if different products of the same type and of different developing companies, if applicable, are produced at the same site.

During the evaluation, in particular also supporting documents for the site certification under the CC are used (Supporting Document Site - Certification [SupDoc-SC], see also in this respect the respective Notes on Application and Interpretations (AIS 47)).

A site certificate is taken into account for a product certificate within the framework of the product evaluation for the assurance class Life-Cycle - ALC of the Common Criteria. Particular codes of practice for the integration are defined in specific AIS documents.

Site certificates are not automatically covered by the international recognition arrangements. However, the re-use of results of a site evaluation in a product evaluation is supported within the framework of the arrangements. The certification body dealing with the integration will make the decision in individual cases.

1.5 Confirmation of technical components under the Signature Act (SigG)

The Federal Office for Information Security is recognized by the Bundesnetzagentur [Federal Network Agency], which is the competent regulator in accordance with § 18 (1) SigG for telecommunication and mail as confirmation body[3].

On 22 May 2001, the *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften* [Act on Framework Conditions for Electronic Signatures and for Modifying other Regulations] (of 16 May 2001] (Signature Act - SigG), which is adjusted to EU Directive 1999/93/EC took effect. The related *Verordnung zur elektronischen Signatur* [Regulation on Electronic Signatures] (Signaturverordnung [Signature Regulation] -SigV) took effect on 22 November 2011 and defines the framework conditions and requirements for the use of qualified electronic signatures. The Signature Act was amended most recently on 17 July 2009, the Signature Regulation on 15 November 2010.

In accordance with § 2 no. 13 SigG, products for qualified electronic signatures are secure signature generation units, signature application components and technical components for certification services. They must comply with the requirements under § 17 (1) - (3) SigG and the Signature Regulation § 24 SigV. In accordance with the information under § 17 (4) and § 18 (1) SigG, products are to be tested sufficiently according to the state of the art of science and technology and to be confirmed by a confirmation body under § 18 SigG. An exception applies to signature application components and to a part of the technical components for certification services in accordance with § 17 para. 2 and 3 no. 2 and 3 SigG. In these cases, the developer declarations in accordance with §15 (5) SigV are sufficient.

The policies for the evaluation of products for qualified electronic signatures are included in appendix 1 to the Signature Regulation.

Evaluation level requirements:

The evaluation of the products for qualified electronic signatures in accordance with § 15 para. 7 and § 17 para. 4 of the Signature Act has to take place in accordance with the Common Criteria [CC][4] as amended.

The evaluation must meet the following requirements:

a) In the case of technical components under § 2 no. 12 letter a)[5] SigG it must at least comprise the evaluation assurance level EAL 4 (CC) or E 3 (ITSEC),

[3] Publication in the Federal Gazette no. 31 of 14 February 1998, page 1787, on issuance of confirmations for products in accordance with § 15 para. 7 sentence 1 (or §17 para. 4) SigG.

[4] The evaulation in accordance with ITSEC [ITSEC] is still admissible in principle but BSI does no longer support the use of ITSEC for these evaluations as ITSEC and the related evaluation method no longer comply with the state of the art.

[5] "Technical components for certification services" are software and hardware products designed to create signature keys and to transfer them to a secure signature generation unit.

b) In the case of secure signature generation units under § 2 no. 10[6] of the Signature Act it must at least comprise EAL 4 (CC) or E 3 (ITSEC),

c) i) In the case of technical components for certification services for digital signatures under § 2 no. 12 letter b) and c)[7] of the Signature Act which are used outside of a particularly secured area ("trust centre"), it must at least comprise EAL 4 (CC) or E 3 (ITSEC);
ii) In the case of technical components for certification services for digital signatures under § 2 no. 12 b) and c) of the Signature Act which are used within a particularly secured area it must comprise at least EAL 3 (CC) or E 2 (ITSEC),

d) in the case of signature application components under § 2 no. 11[8] of the Signature Act, it must comprise at least EAL 3 (CC) or E 2 (ITSEC).

In the case of EAL 4 and EAL 3 under the CC, tests for a high potential for attack and a complete misuse analysis must be carried out in addition to the measures prescribed for this evaluation level, unless evaluations under c) ii) are concerned[9]. If the evaluation levels ITSEC E 3 and E 2 are used, the strengths of the security mechanisms must be assessed as "high" for all products. The mechanisms for signature and hash value calculation must correspond to the catalog published by the Federal Network Agency [Sig-AlgoKat].

The confirmation of technical components under the Signature Act is a special form of an evaluation and certification procedure. It is based on an evaluation of the respective IT product under the CC and / or ITSEC but takes into account the special requirements of the Act and the associated Regulation regarding functionality, scope and level of the evaluation (see above). The special requirements must be enshrined in the respective product-specific document "Security Target" and then must be taken into account during the product evaluation by the evaluation facility. BSI recommends using suitable protection profiles. In practice, an evaluation process usually takes place based on which a certificate is issued and compliance with the laws is confirmed.

In order to achieve synergy effects when carrying out the certification and confirmation, the applications for certification and confirmation should be filed simultaneously. Otherwise, increased efforts and expenses are to be expected.

Within the framework of the technical evaluation, requirements and policies, in particular special requirements and / or interpretations of laws, of the Federal Network Agency BNetzA must also be taken into account in addition to the application of the relevant evaluation criteria under the CC. If the evaluation result is positive, the applicant will receive the confirmation certificate and the confirmation report in addition to the notice.

As the procedure for the confirmation of products is mainly similar to the course of a certification procedure, the confirmation procedure will only be mentioned in the further description of the procedure where the procedure differs.

[6] "Secure signature generation units" are software or hardware units for storing and applying the respective signature key.

[7] "Technical components for certification services" are software or hardware products designed for b) keeping qualified certificates publicly verifiable and retrievable, if need be, or c) creating qualified time stamps.

[8] "Signature application components" are software and hardware products which are designed for a) allocating data to the process of generating or verifying qualified electronic signatures or b) verifying qualified electronic signatures or verifying qualified certificates and showing the results.

[9] This means for the current version of CC version 3.1, revision 4 and higher that the level EAL 4 defined in this criteria version in addition to the component AVA_VAN.5 must be used in the case of evaluations required under EAL 4; in the case of evaluations under EAL 3, the level EAL 3 defined in this criteria version in addition to the component AVA_Van.5 and ADV_FSP.4, ADV_TDS.3, ADV_IMP.1 must be used.

2 National and international aspects of certification

2.1 National certification policy for the certification of the security of IT products by BSI

The IT security certification services under the Common Criteria by BSI are carried out as an application procedure. Certification can take place if it is determined that the respective evaluation regulations are met and that the issuance of the certification is not opposed to overriding public interests, in particular security concerns of the Federal Republic of Germany (BSIG § 9, para. 4 (2))[10].

In principle, certification procedures for IT products at BSI must be carried out using evaluation regulations, e. g. protection profiles which were certified or recognized by BSI as being suitable (see chapter 5.4). If no protection profile is available for a product type which has been recognized as being suitable by BSI, BSI will decide in individual cases based on an individual product-specific security target on the basic certifiability prior to start of the procedure.

The evaluation levels and the selection of the assurance components in accordance with the evaluation criteria which are admitted for a certification procedure basically depend on the valid international agreements, i. e. at present assurance components of the Common Criteria up to and including the assurance components of the level EAL 4 as well as the assurance family Flaw Remediation (family ALC_FLR). However, BSI may also limit the accepted evaluation level below the regulations of the arrangements, e. g. to EAL 2.

The use of components from higher evaluation levels calls for the availability of a specific evaluation methodology and an extended monitoring by the certification body. However, the resources necessary for extended monitoring are not always available; this may result in delayed processing. Higher evaluation levels can generally be accepted if required by regulations for national IT security projects, national or EU laws or regulations or protection profiles recognized by BSI. This also applies in specifically defined technical areas of the European recognition arrangements, such as the smart card technical domain. The certification body will decide in individual cases whether the applicant can claim a special interest in the use of a higher assurance level, for example due to a special need for trustworthiness in the typical application environment of a product.

The certification procedure takes place after acceptance of the complete application based on a schedule jointly agreed between applicant, evaluation facility and certification body, but generally after receipt of the application. The handling of the procedure can be given a higher priority within the certification body if a particular public interest has been determined or in the case of products which are used in national IT infrastructures (for example electronic passport and ID card, public health sector, critical federal infrastructures).

2.2. International recognition arrangements

2.2.1 Basic regulation for the certification of the security of IT products by BSI

International arrangements have been negotiated and signed by the respective countries for the mutual recognition of IT security certificates. To a large extent, these arrangements prevent multiple certifications of the same product in different countries where IT security certificates are based on the CC or ITSEC, if applicable. Generally, these recognition arrangements stipulate:

- How the respective arrangement is coordinated and implemented. This is the responsibility of a Management Committee in each case (such as SOGIS-MC or CCRA-MC); the preliminary work in this respect is carried out by several work groups;
- How the recognition and mutual monitoring of national certification bodies takes place;
- At which evaluation assurance levels (depth and scope of the assessment) and technical domains the recognition is applicable; and

[10] In this respect, it is to be noted that the final decision on whether the issuance is not opposed to overriding public interests, in particular security concerns of the Federal Republic of Germany, is taken only upon certification, i.e. at the time of signing the certification notice and the certificate. An attempt will be made to make sure that no negative decision regarding public interests is taken in the end by means of an examination upon accepting the application.

- Which restrictions apply to the recognition of certificates if such certificates are opposed to national, international or EU laws or regulations. This applies in particular in the areas of application of national security.

BSI signed an arrangement on the recognition of IT security certificates in Europe for CC and ITSEC certificates [SOGIS-MRA] and a worldwide arrangement [CCRA] on the recognition of CC certificates.

Certificates which are issued by other bodies in accordance with these arrangements will be recognized as being equivalent to a BSI certificate up to the evaluation levels stated in the arrangements if the target of evaluation (TOE) originates from countries which participate in CCRA or SOGIS-MRA or if the product originates from the EU or EFTA[11] countries (unless they are already members of CCRA or SOGIS-MRA). Otherwise, recognition by BSI will generally be limited up to EAL 2 (CC) respectively E 1 (ITSEC). Exceptions to the latter limitation of recognition regarding the assurance level shall be given if the certificate refers to an EU Regulation which requests a certain evaluation level or if a licensing office or authority endorses the certification and if critical production steps take place in the EU or an EFTA country.

Recognition of a certificate in accordance with the international agreements stated does generally not include recognition of the suitability of selected cryptographic algorithms and functions or recognition of test results regarding the implementation and strength of cryptographic algorithms and functions. In this respect, national rules and regulations take precedence. Decisions on exceptions are taken in individual cases.

Recognition of a certificate by BSI may be refused if recognition is opposed by overriding public interests - in particular security concerns of the Federal Republic of Germany (BSIG § 9, para. 4, 2).

Site certificates issued by other certification bodies are generally not subject to recognition by BSI; however, evaluation results can be re-used in BSI certification procedures in individual cases.

Certificates issued by other certification bodies and which have not been published or do not bear the respective logo are generally not recognized by BSI.

The recognition of confirmations under the German Signature Act or the corresponding EU Directive are not covered by the international recognition arrangements CCRA and SOGIS-MRA.

BSI generally does not recognize IT security certificates issued by certification bodies outside the CCRA or SOGIS-MRA.

The incorporation of the results of an existing product certificate issued by another national certification body of CCRA or SOGIS-MRA nations into a BSI certification procedure based on it, e.g. for a follow-up version of the product or in the case of an enhancement of functionality, is generally possible but specific ancillary conditions and particularities are applicable to the furnishing of the evidence, the requirements to the evaluation facility and executing the evaluation. This is determined in individual cases by the certification body of BSI.

2.2.2 The European arrangement (SOGIS-MRA V3)

The currently valid European arrangement was signed in April 2010 by the national bodies of the following countries: Germany, Finland, France, UK, the Netherlands, Norway, Sweden and Spain. In this arrangement, recognition of certificates for IT products based on the Common Criteria and / or ITSEC regarding certain evaluation assurance levels (EAL) is determined. In this respect, recognised certification bodies at the effective date are the national bodies from Germany, France, UK, the Netherlands and Spain.

In addition, a higher-ranking recognition for certain technical areas (“technical domains”) is provided for under certain framework conditions.

In this respect, the technical domain “smart Cards And Similar Devices” Was Defined In The Arrangement. Accredited certification bodies in this respect at the effective date are the national bodies from Germany, France, UK and the Netherlands. The recognition of a certificate from this product sector requires proof of the use of the respective supporting documents (“JIWG Supporting Documents”).

Another technical domain was defined for “hardware devices with security boxes”. The recognition of a certification from this product sector requires proof of conformity of the product with a

[11] EFTA: European Free Trade Association (Iceland, Liechtenstein, Norway, Switzerland)

recommended protection profile allocated to this category ("SOGIS Recommended PP") and the use of the respective supporting documents ("JIWG Supporting Documents").

In addition, the certificates for protection profiles based on the Common Criteria are recognized.

In December 2010, the national certification body of Italy was included in the arrangement as a recognizing body and also recognized as a certification body for Common Criteria up to and including the evaluation assurance level EAL 4.

The national body of Austria was included in the arrangement as a recognizing body in May 2011. A current list of the signatory states and / or the recognized certification bodies as well as the SOGIS Recommended PPs is available on the website www.sogisportal.eu.

Within the framework of this European recognition, BSI recognizes the following certificates, taking into account the above-mentioned ancillary conditions, if the above-mentioned superordinate restrictions (see chapter 2.2.1) are not applicable:

- Certificates for IT products based on ITSEC which were issued prior to April 2010 by the national certification bodies of France, the UK and, from January 2009 onwards, the Netherlands or certificates with high evaluation levels which were issued under the previous arrangement and which were re-certified under the new arrangement before the end of April 2012.
- Certificates for IT products based on the Common Criteria up to EAL 7 which were issued prior to April 2010 by the national certification bodies of France, the UK and, from January 2009 onwards, the Netherlands or certificates with high assurance levels which were issued under the previous arrangement and which were re-certified under the new arrangement before the end of April 2012.
- Certificates for IT products based on ITSEC up to E 3, low strength of mechanism (basic), of the national certification bodies of France, the UK, the Netherlands and Spain which were issued from April 2010 onwards.
- Certificates for IT products based on the Common Criteria when using assurance components up to EAL 4 of the national certification bodies of France, the UK, the Netherlands and Spain issued from April 2010 onwards and of Italy from December 2010 onwards.
- Certificates for IT products based on the Common Criteria when using assurance components up to EAL 7 in the technical domain "Smart cards and similar devices" of the national certification bodies of France, the UK and the Netherlands issued from April 2010 onwards.
- Certificates for protection profiles based on the Common Criteria of the national certification bodies of France, the UK, the Netherlands and Spain issued from April 2010 onwards and of Italy from December 2010 onwards.

A current list of the signatory states and the recognized certification bodies is available at www.sogisportal.eu.

The cooperation in different working groups ensures a continuous exchange of information between the signatory states.

The SOGIS logo with the corresponding additional text on a BSI certificate indicates whether and how it is covered by this recognition arrangement. If a certificate which is not covered by a certain technical domain includes assurance components above level EAL 4 (CC) or E 3 basic (ITSEC), only the evaluation results of this assurance component associated with level EAL 4 and / or E 3 basic will be recognized.

2.2.3 The international CC arrangement (CCRA)

In May 2000, an arrangement (Common Criteria Arrangement) on the mutual recognition of IT security certificates and protection profiles based on the CC up to and including the evaluation assurance level EAL 4, supplemented by the assurance category Flaw Remediation (ALC_FLR family) was adopted (CC-MRA). The national bodies of the following countries joined the arrangement by July 2011: Australia, Denmark, Germany, Finland, France, Greece, the UK, India, Israel, Italy, Japan, Canada, Malaysia, New Zealand, the Netherlands, Norway, Austria, Pakistan, Republic of Korea, Republic of Singapore, Sweden, Spain, Czech Republic, Turkey, Hungary, USA.

Within the framework of this arrangement, BSI recognizes the following certificates, taking into account the above-mentioned ancillary conditions, if the above-mentioned superordinate restrictions (see chapter 2.2.1) are not applicable (version as per August 2012):

- Certificates for IT products based on the Common Criteria using assurance components up to EAL 4 or the assurance family Flaw Remediation (family ALC_FLR) and certificates for protection profiles based on the Common Criteria of the national certification bodies of Australia/New Zealand, France, the UK, Italy (from September 2009 onwards), Japan (from October 2003 onwards), Canada, Malaysia (from Sept. 2011 onwards), the Netherlands (from January 2006 onwards), Norway (from February 2006 onwards), Republic of Korea (from May 2006 onwards), Sweden (from February 2008 onwards), Spain (from August 2006 onwards), Turkey (from November 2010 onwards), USA.

A current list of the signatory states and the recognized certification bodies is available on the website www.commoncriteriaportal.org.

The Common Criteria are continuously developed further by several working groups, ensuring a continuous exchange between the different nations.

The CCRA logo with the corresponding additional text on a BSI certificate indicates whether and how a certificate is covered by this recognition arrangement. If a certificate includes evaluation assurance components above level EAL 4, only the components of this component family which are allocated to level EAL 4 will be recognized.

At present, the countries of the CCRA are discussing a redesign of the arrangement which in future may mean a stronger linking of recognition to the use of jointly agreed protection profiles (so-called collaborative Protection Profiles, cPP), as well as associated technology-specific evaluation methodology (Supporting Documents). Further details regarding this development are available under www.commoncriteriaportal.org (Vision Statement).

3 Parties involved in the certification process

Three parties are involved in the entire certification process:

- The applicant: (Developer, sponsor or distributor of an IT product / authority or user organization as author of a protection profile[12] / responsible operator of a development or production site),
- The evaluation facility chosen by the applicant,
- The certification (and confirmation) body of BSI.

3.1 Applicant with tasks and duties

The applicant files an application with BSI for

- certification and / or confirmation under SigG of their product,
- certification of a protection profile or
- certification of a development or production site.

The applicant concludes an evaluation contract with an evaluation facility recognized by BSI (except for the following forms: maintenance process and addendum confirmation). If the application is filed by a sponsor or distributor of the product, the application must be accompanied by a written declaration of the developer in order to ensure cooperation in the procedure and provision of the required evidence on the product.

With the application, the applicant obliges to cooperate, i. e.

- to make available any information (evidence) required for certification or confirmation under SigG regarding the target of evaluation to the evaluation facility and the certification body including necessary improvements if any security-relevant defects are detected during the evaluation and the certification body or the evaluation facility requests additions to the evidence provided,
- during a product certification or confirmation under SigG: to make available the product itself and required test tools, if any, and product training for the evaluator and certifier, if applicable,
- to grant the evaluation facility and the certification body access to all development and production sites for performing the test activities which are included in the evaluation process.
- to refund the costs of the procedure (fees and and expenses) settled by BSI with the applicant based on the BSI Regulations on Ex-Parte Costs [BSIKostV].

The applicant guarantees the correctness of the information provided. In the case of missing or insufficient proof, a certification procedure may be canceled or ended with a negative result by the certification body.

The corporate policy of the applicant and the practice regarding the confidential handling and forwarding to third parties of the documents regarding the evaluated product influences the assessment of the exploitability of potential vulnerabilities within the framework of the evaluation, for example any information regarding the product which is published by the developer is deemed to be available to an attacker and thus eases attacking the product.

As many certification procedures are processed simultaneously in the certification body and as the evaluation facility usually carries out several evaluations at the same time, the applicant is obliged to keep to the schedule agreed to at the beginning of the procedure to the greatest extent possible. If delays become apparent, the evaluation facility and the certification body are to be informed in order to re-agree on an updated plan for the procedure.

With the application for certification, the applicant agrees

- that any evaluation-relevant evidence and (in the case of a product evaluation) the evaluated product will be archived for a period of at least 5 years (in special cases 10 years) by the applicant and will be made available to BSI on request free of charge, if applicable, if subsequent evaluations regarding the certification result become necessary.

[12] The applicant for a protection profile certification is generally an authority, a regulatory public instance or an organization involved with the standardization. Application for certification of a protection profile always takes place in coordination with the certification body of BSI.

- that the documents made available to BSI and the BSI-internal files regarding the procedure by BSI are archived by BSI in accordance with the registry guidelines of the certification scheme at BSI.
- that after positive completion of the procedure, the result of the certification and possibly the confirmation under SigG as well as the certification report and possibly the confirmation report including the public version of the security target - completely or in parts and also in digital form - will be published by BSI.[13]
- that personal data resulting from the application may be electronically stored at BSI for the purpose of carrying out the procedure applied for.

Upon the positive completion of a product related certification procedure, the applicant has the possibility to receive a certification button (as an electronic print template), which may be used for purposes such as marketing.

With the consent of the applicant, it is possible to state the fact that the procedure is ongoing after start of the evaluation in BSI publications in the section "...Products in Certification...", stating the name of the applicant (name of the organization) and the name of the target of evaluation.

During the preparation and documentation of the evidence required for the certification / confirmation, the applicant may commission, among other things, recognized evaluation facilities with consultation services irrespective of the evaluation. In many cases, this is expressly recommended by BSI.

The result of the procedure (e. g. certification notice, certificate, certification report and the cost notice) is sent to the applicant by mail.

The applicant may file an objection against the decision of BSI to issue or refuse a certificate or confirmation under SigG within 4 weeks after receipt. The objection is to be filed in writing with the certification body. In order to reduce the 4-week period and thus in order to achieve a publication of the certification result more quickly, the applicant may renounce the objection in writing.

3.2 Accredited evaluation facilities with tasks and duties

Evaluations with the goal of certifying a product, a protection profile or a development or production site or with the goal of confirmation under the Signature Act are carried out by evaluation facilities approved by BSI.

Approval of an evaluation facility always relates to a specific criteria manual, i. e. ITSEC or CC and specific technical areas of expertise or assurance levels, if applicable. For example, special requirements are to be met for evaluations in the product sector of smart cards and similar products such as hardware security modules or integrated circuits. A prerequisite for the approval of an evaluation facility is an accreditation under DIN EN ISO /IEC 17025. BSI monitors recognition in accordance with the respective requirements, such as by means of annual audits.

The evaluation facilities recognized by BSI and BSI have entered into a contract governing their mutual rights and duties. Detailed requirements regarding the approval of evaluation facilities are described in the document "*Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern*" [Process Description on the Approval of Evaluation Facilities and Certification of IT Security Service Providers] [VB-Stellen].

Based on the accreditation under DIN EN ISO/IEC 17025 and the contractual regulation with BSI, the evaluation facility is obliged in each evaluation procedure to ensure the confidentiality of the documents made available and the confidentiality of the evaluation results internally in the evaluation facility as well as in the communication with the applicant and the certification body in accordance with the need-to-know principle.

Process-related requirements which the evaluation facility has to observe when carrying out the evaluations are described in the document "*Anforderungen an die Prüfstelle für die Evaluierung von Produkten, Schutzprofilen und Standorten nach CC und ITSEC*" [Evaluation Facility Requirements for the Evaluation of Products, Protection Profiles and Sites under the CC and ITSEC] [BSI 7125]. Notes on Application and Interpretations regarding the Scheme (AIS) supplement these specifications.

[13] In special cases, the applicant may withdraw this consent during the ongoing procedure. However, the certificate will not be recognized within the framework of the international recognition arrangements in this case.

The evaluation facility is obliged to comply with these instructions of the certification scheme as well as the requirements of the evaluation criteria and the evaluation method and is responsible for the technical correctness of its evaluation results. The evaluation results are documented in evaluation reports and reasons for the decision of the evaluator are provided in these evaluation reports. Additional requests of the certification body for carrying out the evaluation and regarding evaluation reports must be complied with by the evaluation facility.

The applicant receives the evaluation reports from the evaluation facility after approval or annotation by the certification body. In case of additional claims to the developer and / or the applicant on the part of the evaluation facility or the certification body, additions to the required evidence can be provided by the applicant on this basis.

As numerous certification procedures are processed simultaneously, the evaluation facility is obliged to abide by the schedule agreed upon at the start of the procedure to the furthest extent possible. If delays become apparent, the certification body and the applicant are to be informed in order to re-agree on an updated plan for the procedure.

An overview of the approved evaluation facilities is published by BSI in the publication [BSI 7148] and on the BSI website under “Certification and Recognition”.

3.3 Certification body and confirmation body of BSI with tasks and duties

It is the task of the certification and confirmation body to ensure the equivalence of all evaluation results and the complete and correct course of the procedure. In order to achieve this, the certification body monitors each procedure with regard to a uniform approach and methodology and thus comparable assessments.

Specific tasks of the certification and confirmation body include acceptance of the security target for product and site evaluations, the evaluation, annotation and approval of the evaluation reports, participation in evaluation meetings, monitoring of audits of the development and production sites and of test and penetration activities by the evaluation facility (in the case of product evaluations) as well as the preparation and coordination of possibly required interpretations of the criteria manuals.

In the case of confirmation procedures under SigG, the acceptance of the final evaluation report (Evaluation Technical Report, ETR) includes the final evaluation for conformity with the Signature Act as a special step.

For completing the certification procedure, the certification body prepares the certification notice, the certificate and the certification report as well as the confirmation notice and the confirmation, if applicable, (document and report in one file in this respect). Certification reports and confirmation reports are published by the certification body[14]. The confirmation as well as the associated evaluation report of a confirmation procedure is made available to the Federal Network Agency.

The certification body of BSI is obliged in every certification procedure, due to its character as national IT security authority and because of the necessary fulfillment of the content requirements under DIN EN 45011 and international recognition arrangements, to ensure the confidentiality of the documents made available and the evaluation results internally within the certification body as well as in the communication with the applicant and evaluation facility in accordance with the need-to-know principle. Under certain conditions, it is possible in exceptional cases that an additional non-disclosure agreement (NDA) is concluded between applicant and BSI.

In the case of certification of a protection profile, the tasks of the certification body include commenting on the protection profile itself and the evaluation, annotation and approval of the evaluation reports as well as the preparation and coordination of possibly necessary interpretations of the criteria manuals.

As several certification and confirmation procedures are processed simultaneously within the certification body and the scope of the necessary commenting on the evaluation reports is not foreseeable in detail, delays in the processing of the procedures may occur occasionally. Likewise, a necessary processing of national certification projects with a higher priority may result in delays in other procedures (see chapter 2.1). The certification body communicates any delays which become

[14] The applicant may object to the publication of a certification report before the procedure is completed. However, in this case the certificate is not covered by the international recognition arrangements CCRA / SOGIS-MRA.

apparent to the applicant and the evaluation facility promptly in order to agree on an updated procedure planning, if need be.

The requirements under the criteria manuals were phrased in a generic manner so that they can be applied to a product sector which is as broad as possible. As a result, the criteria requirements must be interpreted again and again for specific individual cases. In order to ensure the comparability of the evaluation results of different evaluation facilities, the certification body in such cases prepares binding interpretations in coordination with the evaluation facility. Based on these individual decisions from specific certification procedures, the certification body with the involvement of all evaluation facilities can then prepare generalized interpretations. These interpretations are published as AIS documents. There are a few exceptions in which certain AIS documents are not published. Where necessary, the certification body brings in national interpretations in the international coordination regarding a recognition by the members of the recognition arrangements.

3.4 External support during monitoring

BSI entered into a contractually agreed cooperation for monitoring during product certification procedures with Fraunhofer Institute for Open Communication Systems, FOKUS, Berlin. The “CertLab” established there can be commissioned by BSI to carry out a certain monitoring within the framework of a certification procedure. The regulations and processes of the certification body and CertLab ensure that confidentiality is maintained and that monitoring at CertLab can be carried out in a manner comparable to the one at BSI. The monitoring staff at CertLab has the same function and thus the same tasks and duties as the monitoring staff at BSI. The authorization for the CertLab employees only relates to certain technologies and product groups and only to the respective certification procedure. The approval of the final evaluation report and the certification of the product thus takes place exclusively by BSI.

4 The certification process as a phase model

The initial and re-certification of products and sites[15] and / or initial and re-certification[16] of products is divided into the following phases:

4.1 Phase 1 (Preparatory phase and logistics):

Certification is usually preceded by a consultation of the applicant by BSI and / or an approved evaluation facility (occasionally referred to as pre-evaluation): In this phase, the draft of the security target is prepared and an analysis is conducted as to which evidence is already available to the developer and / or still has to be prepared or supplemented. If lists of developers or evaluation results from previous procedures are re-used, the applicant will prepare a so-called impact analysis report (IAR) and attach it to the certification application.

Applicant and evaluation facility conclude an evaluation contract.

The evaluation facility provides an evaluation plan based on this information. The evaluation plan includes information regarding the execution of the evaluation in terms of content, the applicable criteria and interpretations and the time planning (milestone plan) as well as a declaration to be independent. Afterwards, the certification application will be filed with BSI. The security target and the evaluation planning is then agreed in a joint kick-off meeting together with BSI and the evaluation facility.

After completion of these preparations, the procedure is then included in the certification scheme and the applicant receives a formal confirmation of receipt, stating the certification ID[17] and the monitoring staff of the certification body of BSI or CertLab. If requested by the applicant in the certification application, the product will be included in the list of products in certification, which is published on the BSI website. If required, the applicant will train evaluators and monitoring staff.

Priorities can be given to the processing in accordance with the above-mentioned national certification policy.

4.1.1 Certification application / confirmation application form

The application form includes information which is needed for the start of the procedure and its handling. There are special application forms for product certification, certification of protection profiles, confirmation under SigG and site certification under the CC.

Application forms are available on the BSI website under "Certification and Accreditation".

[15] The phase model is identical with only correspondingly adjusted terms relating to the certification of site (for example “site security target” instead of “security target” or “site” instead of “product”).

[16] In the case of confirmation procedures accordingly: Confirmation application, confirmation ID, confirmation report, confirmation notice,...

[17] The certification ID is the identifier of the procedure at BSI; it is stated in each correspondence for identifying documents and the certification report;
Product certificates: BSI-DSZ-CC-nnnn-jjjj (DSZ= German IT security certificate, CC= naming the criteria manual, nnnn = sequential application number, jjjj = year of issuance of the certificate (is added only when the certificate is issued))
Site certificates: BSI-DSZ-CC-S-nnnn-jjjj (DSZ= German IT security certificate, CC= naming the criteria manual, S= site, nnnn = sequential application number, jjjj = year of issuance of the certificate (is added only when the certificate is issued))
Certificates for protection profiles: BSI-CC-PP-nnnn-jjjj (CC= naming the criteria manual, PP= protection profile, nnnn = sequential application number, jjjj = year of issuance of the certificate (is added only when the certificate is issued))
Supplementation by maintenance procedures: Supplementation of the respective ID by: -MA-kk-llll (MA=Maintenance, kk=sequential number, llll=year of maintenance supplementation.
Confirmation under SigG: BSI.nnnnn.TE.mm.jjjj (nnnnn = sequential application number, TE=technical component under SigG/SigV, mm=month, jjjj=year of issuance of the confirmation (is only added upon issuance of the confirmation))

The following possible applications need to be distinguished:

1. a) The certification application relates to the certification of a product.
   b) The certification application relates to the re-certification or maintenance of a product already certified because the product was changed.
   c) The certification application relates to the re-assessment of a product already certified according to the state of the art.
2. a) The application relates to the confirmation of a product under SigG.
   b) The application relates to the re-confirmation or addendum confirmation of a product already confirmed, as the product was changed.
3. a) The certification application relates to the certification of a protection profile.
   b) The application relates to the re-certification or maintenance of a protection profile already certified because it was changed.
4. a) The certification application relates to the certification of a development or production site.
   b) The application relates to the re-certification or maintenance of a site already certified because it was changed.

Within the framework of the application (pre-printed form), the following data are collected amongst others:

- The exact name of the target of evaluation
- The applicable security criteria / evaluation bases
- The assurance level aimed for by the applicant (in the case of a confirmation application, only certain levels are possible in accordance with SigG)
- The protection profile to be used for the product evaluation
- Type of the certification (initial certification, re-certification/maintenance, re-assessment) and / or type of confirmation (initial confirmation, re-confirmation/addendum confirmation)
- The evaluation facility commissioned by the applicant (not required in the case of maintenance or addendum confirmation)
- A declaration regarding the archiving
- A declaration regarding the announcement of the pending procedure
- A declaration of consent of the applicant to the publication of the certification and / or confirmation result
- In the case of a confirmation application: Declaration of consent of the applicant that the evaluation report as well as a copy of the confirmation may be provided to the Federal Network Agency in the case of a positive completion of the procedure.
- If applicable, information on the need for a certification button (in the case of products)
- Consent regarding data protection during the storage of relevant procedural data

In the case of product certification or confirmation under SigG, several appendices form part of the applications, such as

- the declaration of the manufacturer regarding his cooperation: The declaration of the manufacturer regarding his cooperation shall be required if the applicant is not the manufacturer of all components of the product or does not hold the rights in the required complete documents regarding the subject of certification himself. An example may be a case where a part of the product was purchased from a supplier and the applicant does not hold the rights themselves in the development documents which are required for the assurance level aimed for. The letter of declaration must state: the name of the organization declaring its cooperation and the components of the subject of certification to which this declaration relates.
- the Security Target document: The design of the Security Target document is defined in the evaluation criteria (Common Criteria Part 1). In the case of a confirmation under SigG, an appendix to the Security Target is necessary which states how the relevant requirements under SigG and SigV are implemented by the product.

- the evaluation planning of the evaluation facility suggested for coordination: The evaluation planning comprises information regarding the type, scope and planned implementation of the evaluation according to the specifications for the evaluation facilities.
  - a list of the development and production sites relevant for the product. This list should comprise:

    (i) Name of the organization operating the site and, if different, the name of the organization which is responsible for the site and any evidence of evaluation available at the site;
    (ii) Exact address of the site;
    (iii) Type of the site (e. g. product development / test / delivery / chip production / device assembly / ...) in addition to a short description of the site's role in the life-cycle of the product[18].

In the case of site certifications, different appendices form part of the application, such as

- the document Site Security Target: The design of the Site Security Target document is defined in the regulations stated in the application (see document Notes on Application and Interpretations AIS 47 [AIS 47]),
- The evaluation planning suggested for coordination of the evaluation facility (the evaluation planning comprises information regarding the type, scope and planned implementation of the evaluation according to the specifications for the evaluation facilities).

In the case of follow-up procedures such as re-certification / maintenance and / or re-confirmation / addendum confirmation, the following appendices are required additionally:

- A description of the changes with an impact analysis (IAR). The required contents are stated in the Notes on Application and Interpretations AIS 38 [AIS 38] document, which is available on the website of BSI,
- An updated configuration list in accordance with the requirements of the relevant assurance level. The current version of the changes compared to the configuration list of the certified / confirmed version of the product must be recognizably identified,
- If applicable, changed application manuals regarding the target of evaluation. The current version of the changes compared to the manuals of the certified / confirmed previous version of the product must be declared in evidence,

With the application, the applicant accepts the BSI Regulations on Ex-Parte Costs. The applicant also accepts the approach in the processes of the certification body and the possible outsourcing of the monitoring to CertLab (see above) including the settlement of external travel costs of CertLab.

The application must be signed manually and bear a company stamp.

The certification or confirmation application is to be sent in writing to:

Bundesamt für Sicherheit in der Informationstechnik
Referate S22/S23- Zertifizierungsstelle
Postfach 20 03 63
53133 Bonn

The application can be sent in advance by e-mail to: zertdokus@bsi.bund.de

4.1.2 Exchange of documents in the pending procedure

The exchange of documents between applicant, evaluation facility and certification body usually takes place electronically by encrypted e-mail. For this purpose, the BSI provides the encryption program Chiasmus. In communications between BSI and the evaluation facility, the use of this program is mandatory. The applicant can purchase a license for this program from BSI. However, the program is not mandatory for the applicant. If the applicant does not have this program, the developer documentation will be sent to BSI via the evaluation facility.

If other encryption programs are used by the applicant in communications with the BSI, it cannot be ensured that the documents can be decrypted or filed in a timely fashion in the electronic filing system of the respective certification procedure due to the BSI-internal security policy and the IT used.

Electronic documents regarding a certification procedure must be sent to the following e-mail address:

[18] Note: The complete documents regarding the description of the processes, procedures and rules applicable at the site are not yet needed here.

zertdokus@bsi.bund.de
as the decryption and registration of incoming documents is usually not carried out by the certifiers themselves but by the administration of the certification body. The delivery to personal BSI e-mail addresses of certifiers is usually done additionally as a carbon copy for their attention.

Documents which are sent to BSI as a hard copy or which are delivered by courier directly to the gate of BSI, Godesberger Allee 185-189 must be wrapped in a suitable and sealed inner envelope and must read "*ungeöffnet an die Zertifizerungsstelle*" [english: "sent to certification body unopened"] so that the confidentiality of the documents is also given while they are being transported in the internal BSI mail system. The outer envelope is addressed to BSI:

Bundesamt für Sicherheit in der Informationstechnik
Referate S22/S23- Zertifizierungsstelle
Postfach 20 03 63
53133 Bonn

Documents which are sent to BSI on a CD must be stored on the CD in encrypted form. Evaluation facility and certification body mark their respective documents regarding the procedure (evaluation documents, comments) as "firmenvertraulich" and / or "company confidential".

4.2 Phase 2 (Evaluation):

The applicant makes available the evidence in each case and, in the case of product-related procedures, the product in question.

The evaluation facility carries out the technical test, called evaluation. The evaluation is divided into different partial steps according to the assurance aspects of the criteria manual used. The evaluation facility documents and provides reasons for the evaluation results in partial evaluation reports in accordance with the respective targets of the certification scheme of BSI. These partial evaluation reports are a component of the final evaluation technical report (ETR).

The certification body monitors the evaluation (monitoring) in order to ensure a uniform approach and methodology and comparable assessments. For this purpose, the evaluation reports are reviewed and commented on, if applicable, by the monitoring staff. Comments and additional requests are to be processed by the evaluation facility and the applicant, if applicable. The monitoring staff can monitor certain activities of the evaluation facility, such as the execution of tests/penetration tests or the execution of site audits at the developer in each case on site.

Subsequent improvements of the product and the manufacturer's documentation by the applicant are always possible during the procedure.

The certification body can schedule evaluation meetings with the evaluation facility and / or the developer in order to have the detailed planning and the evaluation result explained or to clarify controversial matters. In order to coordinate the activities for the vulnerability analysis and the penetration tests, a so-called AVA kick-off meeting is usually held with the evaluation facility. The developer may also attend this meeting. Among other things, questions regarding the analysis and the assessment of cryptographic procedures are discussed in this meeting.

All parties involved in the project are obliged to notify the other parties involved of deviations from the agreed schedule and then to agree again on the milestone plan.

After all partial evaluation reports have been accepted, the evaluation facility prepares the summarizing part of the evaluation report in order to finalize the evaluation. It will be prepared in the language (German or English) in which the security target was prepared. The certification body then carries out a formal acceptance of the ETR. Applicant and evaluation facility are informed about this acceptance. By doing so, all content-related prerequisites for the issuance of the certificate are given. In order to publish the security target in the course of the certification, a reduced public version of the security target can be agreed between applicant and BSI following certain rules (see AIS 35).

4.2.1 Subject of the assessment, target of evaluation (TOE)

The assessment and rating under the Common Criteria or ITSEC is called evaluation. The subject of the assessment is therefore called target of evaluation (TOE) within the framework of a certification under the CC or ITSEC.

In the case of product certifications, the TOE is an IT product including the user guidance manuals. CC version 3.1 defines target of evaluation as: "*set of software, firmware and / or hardware possibly* *accompanied by guidance*". The TOE to be evaluated is defined at the outset of a certification procedure by the applicant in the Security Target (ST) document.

It is possible to evaluate products of different kinds:

- software products (e. g. operating systems, database systems, application programs, VPN software, firewalls)
- hardware products (e. g. smart card integrated circuits)
- combinations from software and hardware (e. g. hardware on a smart card together with an operating system and an application included in it, hardware security modules, card terminals)
- combinations of individual SW products

One main prerequisite is that the security properties confirmed in the certificate at the end of the procedure are in keeping with the observance of confidentiality, availability, integrity and authenticity of assets to be protected (assets).

In the case of a protection profile certification, the TOE is the respective Protection Profile document and its conformity with the concepts of CC will be compared and confirmed.

In the case of site certifications, the TOE is a development or production site or a corresponding organizational unit which offers certain services within the framework of the development of production, within its determined physical, logical and organizational limits. The logical delimitation describes the role which the site plays in the life-cycle of a product development or production. The physical delimitation is given due to the relevant rooms and the place. Within these delimitations, procedures, processes and rules are examined. The site to be assessed is defined at the outset of a certification procedure by the applicant in the document Site Security Target (SST).

In the case of a confirmation under SigG, the TOE is an IT product including the guidance manuals as it is also applicable for product certifications. However, the product must be a secure signature generation device, a signature application component or a technical component for certification services within the meaning of the Signature Act or the Signature Regulation.

4.2.2 Development phase of a product

Depending on the development status of the product, different types of evaluation and certification of a product can be differentiated: The overview below shows examples of the different development phases of a product:

Development phase	**Type of evaluation and certification**
Planning / design	Evaluation and certification and / or confirmation under SigG accompanying the development
Draft	Evaluation and certification and / or confirmation under SigG accompanying the development
Implementation	Evaluation and certification and / or confirmation under SigG accompanying the development
Prototype	Evaluation and certification and / or confirmation under SigG accompanying the development
Existing product	Evaluation and certification and / or confirmation under SigG of a finished product; Renewal of an existing certificate by re-assessment process, i. e. re-evaluation of the resistance against attacks of the certified version of a product in the context of the respective security target according to the state of the art as well as updating of the site security of relevant development and production sites, in special events
Enhancements / update	assurance continuity process, i.e.: Re-evaluation / re-certification resp.re-confirmation under SigG, or maintenance resp. addendum confirmation under SigG, depending on the security relevancy of the changes

Experience has shown that the earlier in the development phase of a product the evaluation and certification is started, the more cost-efficient and time-saving the manner is in which the procedure can be carried out for the developer. The planning of the evaluation and certification can be determined between the parties involved depending on the respective development phase of the product in order to integrate the parties into the development process.

The evaluation and certification accompanying the development take place simultaneously to the product development. In doing so, the necessary evaluation steps are carried out incrementally so that the certificate can be available at nearly the same time as the product is launched.

Procedural particularities of these types of evaluation and certification are stated in chapter 5.

4.2.3 Condition of a site during certification

At the time of evaluation and certification of a site under the CC (as part of a product certification or as independent site certification), the physical, logical and organizational limits must be defined and the procedures, processes and rules must be implemented on site and their application must be verifiable.

4.2.4 Manufacturers' evidence for the fulfillment of the evaluation requirements

Due to the specifications of the security criteria, certain evidence is requested from the applicant for the evaluation of an IT product or a site, depending on the assurance level chosen.

During the evaluation of an <u>IT product</u>, certain evidence regarding the product (e. g. design information, manuals and evaluation results) is requested in documented form in addition to the provision of the product. The scope and depth of description of this information depends on the respective assurance components under the CC and / or ITSEC used, which are determined in the Security Target document. The corresponding information must be provided by the applicant. This may take different forms:

1. A recognized evaluation facility may check the condition of the available documentation regarding the target of evaluation in advance within the framework of a pre-evaluation. On this basis, the achievable evaluation level based on the documented evidence can be determined and the costs for necessary updates can be estimated as realistically as possible and a sensible project planning is facilitated. A first analysis of the security properties of the product may also take place within the framework of the pre-evaluation in order to prevent basic problems of the evaluation.
2. The product developers or process owners themselves prepare the required evidence within the framework of the normal development process as design or process documentation. Any errors in the documentation which are detected, such as inconsistencies or non-documented properties, are corrected by the developers during the evaluation. However, this requires that the developer already has experience with certifications under the CC.
3. An external body prepares any missing evidence on behalf of the applicant in direct cooperation with developers and process owners at the developer. These tasks can be carried out by one of the approved evaluation facilities, amongst others. If this evaluation facility is also to be commissioned with the evaluation of the product, it must be warranted that the evaluators were not involved in the preparation of the evidence in any way whatsoever in order to ensure objectivity during the subsequent evaluation.
4. In certain cases, the evaluator can compile additionally required evidence of the product from different sources under certain framework conditions and in coordination with the certification body, e. g. determine such information from interviews with the developers. This accelerates the evaluation process in certain cases (see [AIS 23]).
5. If the source code of products or other highly sensitive design information, which is classified under a documented security policy of the developer must not leave the development environment, it also can be examined by the evaluator in the development environment itself in coordination with the certification body.

BSI makes available to the applicant the AIS 42 “*Hinweise zur Erstellung von Herstellerdokumenten für eine CC-Evaluierung*” [Notices for the Preparation of Developer Documentation for a CC Evaluation] [AIS 42] and AIS 42 “*Anleitungen zur Erstellung von Protection Profiles and Security Targets*” [Instructions for Preparing Protection Profiles and Security Targets] [AIS 42] brochures on the BSI website.

During the evaluation of a <u>development or production site</u>, the descriptions of processes, procedures and rules applicable at the respective site are needed in documented form. The scope and depth of description of this information also depend on the respective assurance components under the CC used, which are determined in the document Site Security Target. The provision of documents is governed accordingly by the same rules stated for the evaluation of IT products.

4.3 Phase 3 (Certification):

The certification body prepares the certificate document, the certificate report and issues a certification notice (in the case of confirmation procedures: confirmation notice and confirmation (includes confirmation certificate and report). Applicant and evaluation facility have the opportunity to comment on the draft of the certification report and / or the confirmation.

If the applicant does not revoke their consent to publication, the results of the procedure will be publicly announced. The international recognition arrangements call for publication of the certification report; a certificate will only be recognized internationally if the certification report is published.

A cost notice will be sent to the applicant separately.

4.3.1 Publication of certification and confirmation results

Publication by BSI

Information regarding the certified products, protection profiles and sites are published by BSI in the regularly updated publications.

- BSI Forum (BSI's organ in the magazine KES): Summary of the content of the new certificate or confirmation issued since the last edition of this magazine.
- Certification and Recognition section on the BSI website (www.bsi.bund.de/zertifizierung): Here, certificates are structured in the form of overview lists by product types / sites / protection profiles; for confirmations under SigG, the respective certificate and / or the confirmation is listed and the certification report, the confirmation if applicable and the security targets are offered for download.

  Products in certification / confirmation will also be listed in separate lists if the applicant consents.
- Publication "German IT Security Certificates" [BSI 7148]: Here, certificates are structured in the form of overview lists by product types / sites / protection profiles; for confirmations under SigG, the respective certificate and / or the confirmation is listed.

If the applicant revokes the consent on publication of the certification result which was provided to BSI in writing, no listing in the publications stated will take place. In this case, the certificate is also not covered by the international recognition arrangements SOGIS-MRA and CCRA.

Confirmations granted under SigG must be published in accordance with the regulation of the Federal Network Agency.

Publication by other bodies

Websites of the recognition arrangements:

Within the framework of the international recognition arrangement CCRA, an overview of the products and protection profiles certified under the CC is listed on the website www.commoncriteriaportal.org for certificates covered by the arrangement.

Product certificates covered by the European recognition arrangement SOGIS-MRA are published on the websites of the respective certification bodies. Protection profiles recommended by the members of SOGIS-MRA are published on the website www.sogisportal.eu.

Website of the Federal Network Agency:

The Federal Network Agency publishes the confirmations issued under SigG of all confirmation bodies recognized by the Federal Network Agency on its website www.bundesnetzagentur.de in the section “Qualified electronic signature”.

Publication by the applicant

If reference is made to the certification or confirmation under SigG in publications of the applicant, the application must use the certification identifier e. g. BSI-DSZ-CC-nnnn-yyyy and a reference to the source of the certification / confirmation report on the BSI website or use the so-called certification button (see below).

Support of the applicant

Language for the certification report / for a confirmation under SigG

The certificate and the certification report can be prepared in German or English language. Usually, the language chosen by the applicant for the Security Target document is authoritative. A confirmation under SigG is prepared in German language.

Public version of the security target:

The Security Target document forms part of the publication of the certification results as appendix to the certification report. The applicant can make available a reduced public version of the complete security target in accordance with the rules of [AIS 35]. For this purpose, the public version must be available to the evaluation facility prior to completion of the evaluation activities and forms part of the acceptance by the certification body.

Handover of the certificate / press release:

If the applicant publishes a press release after completion of the procedure, BSI asks that the wording be previously agreed with the certification body.

BSI offers the opportunity to have the certificate / the confirmation handed over to a representative of the company at certain public events, for example conferences and trade shows which BSI attends. This means in particular the following events: Cebit, ITSA, Common Criteria Conference, Moderner Staat, RSA Conference.

A handover to a representative of the company at the premises of BSI can also be organized after agreement.

Certification button:

Upon request of the applicant (see certification application), BSI makes available a print template for a certification button in certain graphic formats (rgb, cmyk) for issued product certificates. This template will be prepared after completion of the procedure and sent to the applicant. In particular the conditions for use are applicable; for example, the button may only be used as long as the certification is valid and as long as the promise to archive has been made (usually 5 years).

4.3.2 Costs of certification and confirmation

BSI charges fees and expenses for a certification or confirmation procedure to the applicant in a cost notice based on the Regulations on Ex-Parte Costs [BSIKostV]. In the case of initial procedures, these fees and expenses are lump-sums depending on the complexity of the procedure plus further additional expenditures and expenses in the case of business trips. In the case of follow-up procedures (e. g. re-certification, maintenance, re-assessment), the service will be charged at actual costs in addition to a basic lump-sum. The counselling preliminary discussions with BSI prior to filing the application are free of charge.

With the application, the applicant recognizes the BSI Regulations on Ex-Parte Costs. The applicant also agrees that BSI may settle external travel costs of CertLab with the applicant if the monitoring is outsourced to CertLab (see above).

The evaluation facility and the applicant usually agree on a regulation as to costs for a pre-evaluation. The settlement of the evaluation costs incurred by the evaluation facility is contractually agreed between the applicant and the evaluation facility. The costs for the evaluation depend on the complexity of the product, the product type and the commissioned assurance level and cannot be generally quantified. Upon request, the evaluation facilities can make estimates or prepare corresponding offers.

Additional optional services of BSI, such as the verifying of subsequent translations of the certification report, are charged at actual costs.

4.3.3 Cancellation / discontinuation of certification or confirmation procedures

The applicant can withdraw the application for certification or confirmation at any time in the procedure. This must also be notified to BSI in writing. In this case, the procedure will be terminated by BSI with costs.

The procedure can also be discontinued by BSI at any time during the procedure due to special circumstances. This includes the following cases:

- The applicant or the evaluation facility does not provide evidences over a period of more than 3 months, contrary to the agreed planning. The discontinuation is notified in writing with a period of notice of 4 weeks and will be implemented when the procedure is not re-activated by making available the evidences requested and agreeing on a new schedule;
- It becomes apparent that the procedure cannot be successfully terminated, for example due to technical defects in the product. In this case, it is also possible to issue a formal notice of rejection;
- The evaluation facility has lost the necessary recognitions of BSI;
- An incomplete application filed is not completed within 6 months.

The applicant and the evaluation facility are informed about the discontinuation of a procedure and the costs are settled.

5 Types of certification and confirmation

This chapter focuses on the possible types of evaluation, certification and confirmation and the resulting particularities in the course of the process. The information regarding technical, legal and organizational framework conditions apply as described in the chapters above.

5.1 Initial certification of a product

For the initial certification of a product, the applicant makes available technical information regarding the product prior to application and / or together with the application, if possible. Scope and depth of the certification planned is stated by the applicant in the Security Target document in accordance with the requirements of the evaluation criteria.

BSI decides on the basic certifiability of the product from a technical point of view subject to the positive completion of the evaluation taking into account the security target and the legal framework conditions.

The applicant chooses the evaluation facility. The evaluation facility must have recognition by BSI, which is necessary for the evaluation, and knowledge of the product technology and must be able to prove this to the certification body.

The positive completion of certification requires that the applicant makes available any and all evidence that is necessary under the evaluation criteria and the special requirements of BSI, if applicable, to the evaluation facility and BSI. It is recommended to have any evidence which is available to the applicant prior to start of the procedure be inspected by a recognized evaluation facility with regard to the usability for the procedure in order to be able to determine a possible need for supplementation at an early stage and by doing so to allow for more exact planning.

The inclusion of mechanisms and protocols in the certification can include additional assessment by BSI. BSI may also refuse the inclusion of cryptographic mechanisms and protocols in the certification, in particular if there is a public interest or if matters of national security are affected.

After receipt of the application, the applicant receives a confirmation of receipt. The content of the application and the related appendices is examined. Afterwards, BSI decides whether the application is accepted, whether the monitoring is outsourced to CertLab and whether the evaluation process at the evaluation facility can be started. A joint kick-off meeting serves the coordination of questions as to the content and the approach, such as the coordination of a joint schedule for the processing of the respective different evaluation aspects. Upon acceptance of the application, a unique certification identifier is allocated.

The evaluation facility makes available to the certification body the results regarding the individual evaluation aspects in accordance with the planning agreed in evaluation reports. The certification body examines the evaluation reports and carries out spot checks; the list of developers is also included in this respect. If applicable, subsequent requests or open questions are communicated to the evaluation facility. If there are major problems, evaluation meetings will usually be held.

Prior to the start of execution of the tests and vulnerability analysis (test class AVA under the CC), detailed evaluation requirements and concepts regarding this evaluation complex are agreed in a meeting (AVA kick-off meeting).

Any audits of the development and production environment at the manufacturer's premises required in the procedure are usually monitored on site by the certification body. These audits are required in cases such as the assurance class ALC under the CC version 3.1 from a certain assurance level/evaluation level onwards. If a site certificate is already available, it may be integrated in the procedure and it will result in significant savings of evaluation costs for this aspect of the evaluation.

However, traveling to the developer's premises may also be required within the framework of tests if some of the test activities need to be carried out directly at the developer.

Following the processing of the different evaluation aspects by the evaluation facility and inspection by the certification body or CertLab, if applicable, the final report of the evaluation facility (evaluation technical report, ETR) is prepared and accepted. The acceptance is notified in writing by BSI.

The certification report is then prepared and BSI completes the procedure by issuing the certificate.

After expiry of the period for objection in accordance with the Administration Act, the certification notice is final and conclusive and publication, settlement and archiving are carried out.

5.2 Initial confirmation of a product under SigG

The process is the same as for the product certification. In addition, an inspection is carried out prior to accepting the confirmation application checking whether the product basically meets the requirements of the Signature Act and whether the security target and / or the required appendix includes the relevant requirements regarding the Signature Act. The evaluation facility must incorporate these requirements in the evaluation and document the results in the evaluation reports.

Upon acceptance of the ETR, an additional final examination is performed checking whether the evaluation is able to prove that the legal requirements stated in the security target are met. Instead of the certification report, a confirmation report is prepared in accordance with the requirements of the Federal Network Agency. The confirmation is issued and the procedure is completed as in the case of a certification. The BSI notifies the Federal Network Agency about the confirmation issued.

5.3 Maintenance of the trustworthiness of a product

As a certificate and a confirmation under SigG are applicable for a specific evaluated version of a product, it is necessary to renew the certificate and / or the confirmation in the case of changes to the product or the development process and / or production process, if applicable, taking into account the current attack techniques.

- In the case of security-relevant changes to the product or the development processes and / or production processes or in the case of comprehensive changes, re-certification and / or re-assessment is required (so-called “major change”).
- In the case of security-relevant changes and manageable scope of the changes to the product or the development processes and / or production processes, if applicable, an existing certificate and / or a confirmation can be extended to the new product version or the changed process conditions (maintenance / addendum confirmation) (so-called “minor change”).

The applicant describes the changes in an impact analysis report (IAR), which is to be attached to the certification/confirmation application. The decision on the required selection of the process is the responsibility of the certification body after examining the IAR. The basic approach and the differentiating criteria are described in the document “Assurance Continuity, CCRA Requirements” [CC-AC] and in [AIS 38].

An existing certificate “ages” or may even cease to be valid due to the further development of attack techniques, when new vulnerabilities of a form of product technology become known or when the validity of cryptographic algorithms and parameters expires. In order to verify the validity of a certificate, a re-assessment of the resistance against attacks can be applied for and carried out according to the state of the art (re-assessment). This examination can also be carried out by means of a re-assessment in the case of a certificate for which a re-assessment is explicitly required after a certain period of time.

A certificate which is valid only for a limited period of time can be renewed within the framework of re-certification / re-confirmation.

5.3.1 Re-certification / re-confirmation

The above-mentioned aspects for an initial certification with regard to the basic course of the procedure, the evaluation by the evaluation facility and the monitoring by the certification body shall also apply to a re-certification/re-confirmation. However, the examination can be focused on the changes made to the product. In the case of a re-certification/re-confirmation, the following is determined based on the changes to the product and the list of developers (IAR) between the certification body and the evaluation facility within the framework of the plan for the procedure: the scope which the re-evaluation is to have, the evaluation steps which have to be carried out again and / or the earlier evaluation results which can be re-used and thus for what evaluation steps updated evaluation reports are to be presented.

However, resistance against attacks is completely re-assessed in each case according to the current state of the art (e. g. CC assurance aspect AVA) and the current validity of cryptographic algorithms and parameters is taken into account.

New audits of the development and production environment will also be carried out if the audits are older than two years.

After positive completion of the re-evaluation, the technical events are documented by the certification body in an updated certification report and / or confirmation report and a new certificate and / or a new confirmation is issued.

5.3.2 Maintenance / addendum confirmation

In the case of a maintenance process and / or an addendum confirmation, the maintenance of the trustworthiness of the product is examined based on the description of the changes to the product (IAR) and the updated list of developers directly by the certification body unless the previous certification was carried out more than two years ago.

However, the resistance against attacks is not re-assessed according to the current state of the art but the resistance against attacks at the time of the initial or re-certification or the last re-assessment carried out most recently shall apply. Additions regarding the validity of cryptographic algorithms and parameters can be made.

In the case of an addendum confirmation, the fulfillment of the requirements under SigG relating to the changes to the product are examined.

In the case of a positive decision, the result is documented by the certification body in a maintenance report as an addition to the existing certification report, in the case of an addendum confirmation accordingly in an addendum to the confirmation report.

A maintenance process or an addendum confirmation is possible up to 2 years after issuing of a certificate. Afterwards, a re-certification/re-confirmation or re-assessment is required.

5.3.3 Re-assessment

In the case of a re-assessment, the certified version of a product including the version carried out subsequently by maintenance is subjected again to a current vulnerability analysis and, if required, to penetration tests according to the state of the art by the evaluation facility that carried out the last evaluation. The starting point is the certification or re-certification carried out most recently or the last re-assessment.

The scope of the work is agreed between the evaluation facility and the certification body. The work focuses on the assurance aspect of the vulnerability analysis (AVA). If applicable, an update of the document in support of composition procedures (ETR for Composite Evaluation) is also to be prepared. New or improved attack techniques must be considered. The current validity of cryptographic algorithms and parameters is taken into account. If new or supplemented conditions for using the product result, the updated manuals or the updated security targets will also be incorporated into the evaluation (AGD and ASE). In the case of a composition procedure, current documents from the platform certification must be available; if applicable, a re-assessment of the platform certificate may be required in this respect (for more details please refer to AIS 36).

In addition, the validity of the audits of the development and production sites will be examined if this evaluation aspect was a part of the certification. If the relevant audits are more than two years old or if changes occur, these evaluation aspects will also be updated (ALC).

In order to coordinate the necessary work, an AVA kick-off meeting will be held if applicable.

The evaluation facility carries out the necessary evaluation work and makes available the relevant evaluation reports to the certification body. After acceptance of the reports and the positive result, the existing certificate is confirmed by the certification body with the current date, otherwise the current (possibly lower) resistance against attacks is reported to the applicant. In the latter case, the certification body reserves the right to withdraw a certificate.

5.4 Use of a protection profile during the product certification

When preparing the Security Target document (ST), a protection profile that is certified or recognised as being suitable by BSI must generally be used (see chapter 1.3). By doing so, the comparability of different product certificates for a product type, e. g. within the framework of tenders, is improved and simultaneously the product certification process is designed in a more efficient way. If no protection profile that is recognized as being suitable is available for a product type, the preparatory phase will be more complex as BSI will have to decide on the basic certifiability of the product prior to start of the procedure based on individual product-specific security targets.

Protection profiles are available for different product types. The protection profiles certified by BSI are published on the BSI website. Further protection profiles are available on the website of the CC recognition arrangement CCRA. The conformity of a certified protection profile with CC is recognized within the framework of CCRA. The suitability of the contents of a protection profile which was not certified by BSI and which is to be used for carrying out a product certification with BSI is examined in individual cases.

In accordance with the concepts of CC, a protection profile differentiates whether a security target has to "strictly" or "demonstrably" conform with the protection profile. "Strict" conformance requires that all security requirements of the protection profile be incorporated into the security target, possibly supplemented by additional requirements. "Demonstrable" conformance grants the author of the security target more discretion as to how the requirements from the protection profile are to be incorporated.

Details regarding the preparation of security targets are explained in the document AIS 41 "Guidelines for PPs and STs" [AIS 41], available on the BSI website.

5.5 Support of additional follow-up procedures (composition)

In the case of products of the "smart card and similar devices" class, there is the concept to support a certification of a composite product based on a certification of a product (platform product) already carried out in a certain form. Doing so ensures on the one hand that the product and evaluation facilities' know-how from the evaluation of the platform is protected, but that the evaluator and certifier of the composite product on the other hand receive sufficient information for the overall examination.

In this case, the evaluation facility carrying out the evaluation of the platform prepares a document, "ETR for composite evaluation", in accordance with the concept as described in [AIS 36] within the framework of the evaluation which is considered by the certification body for the acceptance of the evaluation.

The concept is applicable to all evaluation facilities and internationally between the certification bodies of the SOGIS-MRA recognition arrangement.

Other forms of composition evaluations are generally possible under the CC using the assurance class ACO for certain evaluation levels and must be agreed in individual cases.

5.6 Re-use of evaluation results during product evaluations

a) The re-use of evaluation results of the evaluation from a product certification procedure (basic procedure) for another product certification procedure (follow-up procedure) of the same applicant is generally possible. However, it is necessary to have the evaluation reports of the basic procedure be available to the evaluation facility wishing to re-use certain results. This is the only way to determine and assess which parts can be re-used in which form. In order to protect the know-how of the evaluation facility of the basic procedure, this procedure is usually not applied in the case of a change of the evaluation facility but only in the case that the basic procedure and the follow-up procedure are carried out by the same evaluation facility. A typical application is the re-evaluation/certification of an updated version of a product or the evaluation/certification of similar products of a manufacturer.

b) For the re-use of evaluation results of a development or production site of a manufacturer across evaluation facilities, extended regulations under [AIS 38] are to be applied under special framework conditions within the national certification scheme of BSI. This procedure may be applied if a site is used for the development or production of several products of the same type of one manufacturer, for example.

In the case of sites which are used by several manufacturers, the process of the site certification is authoritative.

Further explanations can be found in [AIS 38].

c) In the case of a re-assessment of the resistance against attacks of a certified product, an assessment is conducted in individual cases to see which evaluation steps can be re-used for the vulnerability analysis and penetration tests. This depends on the further development of specific opportunities for attack on part of the previous assessment of the product within the framework of the initial certification or re-certification or a previous re-assessment.

d) In the case of composition certifications in the smart card domain, the platform with additional product parts (e. g. operating system and application) is certified, based on a platform certification (e. g. for a chip hardware). In this respect, the certification results of the platform can only be used for a certain period of time during the composition certification. If this period is exceeded or if relevant attack scenarios regarding the platform have become known in the meantime, a re-assessment of the resistance against attacks of the platform will be required first. More details are governed by the notes for application and interpretation AIS 36.

5.7 Site certification under the Common Criteria

For the issuance of a site certificate under the Common Criteria for a development or production site for IT products, it is necessary to make available a site security target when applying for the certificate. This document states scope and depth of the certification planned in accordance with the evaluation criteria [CC] and [SupDoc-SC] as well as the related AIS 47.

BSI decides on the basic certifiability of the site from a technical point of view subject to the positive completion of the evaluation taking into account the security target and the legal framework conditions.

The applicant chooses the evaluation facility. The evaluation facility must have the recognition by BSI that is necessary for the evaluation.

The positive completion of a certification requires that the applicant makes available any and all evidence that is necessary under the evaluation criteria and the special requirements of BSI, if applicable, to the evaluation facility and BSI.

If technical reasons stand in the way of certification, BSI can stop or reject the certification process.

After the positive completion of the evaluation, the technical results are documented by the certification body in a certification report.

In the case of changes at the site, a re-certification or a maintenance process can be carried out analogously to the one in product procedures (see chapter 5.3).

6 Security criteria and interpretations

Several criteria manuals were developed as a evaluation and assessment basis. The current criteria manual, which is applied here, is the "Common Criteria for Information Technology Security Evaluation (CC)" [CC]. The CC have evolved from further developments and harmonizations of previous national or European criteria (ITSEC [ITSEC], Orange Book, Federal Criteria of the USA, former Canadian criteria). For consistent application of the CC, the "Common Evaluation Methodology (CEM)" [CEM] evaluation manual was prepared and agreed upon internationally. As an introduction and overview regarding the Common Criteria, part 1 of the CC [CC] is recommended, which explains the concept of security criteria. Additional information can be found on the BSI website.

Current information regarding the CC can be found on the website of the CC recognition arrangement (www.commoncriteriaportal.org). There, the currently valid version and previous versions of the criteria are available for download.

The European criteria ITSEC [ITSEC] may only be applied in special exceptional cases, e. g. if former contracts exist between a requester and a manufacturer or if this is exclusively required by laws and ordinances.

The requirements regarding the criteria manuals are designed to be applicable to a product spectrum which is as wide as possible and have therefore been formulated in a generic manner which in parts is open to interpretation. For this reason, notes on application and interpretations regarding the scheme (AIS) are published as separate documents by the certification body of BSI.

For example, the AIS documents deal with challenges of the evaluation of hardware and smart cards, requirements regarding random number generators, evaluation methodology for higher assurance levels, development and evaluation for formal security models, guideline documents for supporting the applicant in providing evidence and different process-related regulations.

The AIS documents include internationally agreed documents on the application of criteria manuals, such as the documents of the Joint Interpretation Working Group (JIWG Supporting Documents under the SOGIS recognition arrangement)[19] and the so-called CC Supporting Documents under the international recognition arrangement CCRA[20].

In document [AIS 32], the BSI certification scheme governs which version of the evaluation criteria can be applied as well as possible transition regulations and periods. In addition, AIS 32 lists coordinated and valid changes to the criteria which have not yet been incorporated into a new release or a new version of the criteria.

The documents named can be found on the BSI website under www.bsi.bund.de/zertifizierung in the "Certification and Recognition" section. They are to be applied in accordance with their classification (e. g. as guideline or binding) in the evaluation and certification procedures.

As a result of the certification proviso in the case of a public interest under BSIG § 9 para. 4 (2), special requirements are made regarding the selection of cryptographic algorithms and functions and regarding the respective evaluation methodology. The applicable framework conditions are discussed in specific procedure specifications or technical guidelines of BSI and are discussed at the beginning of a certification/confirmation procedure.

The selection of cryptographic algorithms applies to certain applications of the catalog of the Federal Network Agency, the technical guidelines BSI TR-03116, "*Technische Richtlinie für eCard-Projekte der Bundesregierung*" [Technical Guideline for eCard Projects of the Federal Government], or the technical guideline BSI TR-02102, "*Kryptographische Verfahren: Empfehlungen und Schlüssellängen*" [Cryptographic Procedures: Recommendations and Key Lengths]. If weaker or proprietary algorithms are used, BSI will decide in individual cases, if applicable subject to conditions, as to whether the respective algorithm can be accepted within the framework of the

[19] The JIWG Supporting Documents and / or documents of the Joint Interpretation Library (JIL) are prepared by the certification bodies recognized in the European recognition arrangement (SOGIS-MRA) and are published by the national certification bodies as well as the website www.sogisportal.eu.

[20] The CC Supporting Documents of the CCRA are prepared by the work groups of the arrangements and published via the national certification bodies and the website www.commoncriteriaportal.org.

certification. If proprietary algorithms are used, increased expenditure of time is to be expected for the evaluation and acceptance by BSI.

For confirmation procedures under SigG, the above-mentioned requirements of the Signature Act and the Signature Regulation as well as additional implementation guidelines of the Federal Network Agency, if applicable, are to be taken into account (see www.bundesnetzagentur.de, section “Qualified electronic signature”).

Upon official acceptance of a certification application, the relevant versions of the evaluation criteria and interpretations (AIS) are usually determined within the framework of a kick-off meeting. These versions are then authoritative for the pending procedure and are referred to upon completion of the procedure in the certification report. A transition to newer versions is possible during a pending procedure after mutual agreement. This may involve additional expenditure for the applicant or the evaluator. This procedure does not apply to AIS relating to attack techniques. The most current test specifications are to be taken into account in this area and the certification body decides in individual cases on the application of the relevant interpretations.

7 Validity of the certificate and the confirmation

A product certificate and a confirmation under SigG relate only to the version of the product stated and if all conditions regarding the generation, configuration and the use of the product are observed and the product is operated in the environment which is described in the certification / confirmation report and in the security targets.

A certificate / confirmation under SigG confirms the trustworthiness of the product in accordance with the security targets as of the time of issue. As attacks with new methods or refined methods are possible after issuance of the certificate / confirmation, the resistance of the product may regularly be reviewed within the framework of the Assurance Continuity program of BSI (e. g. by re-certification or re-assessment). The certification body recommends that an assessment of the resistance be carried out at regular intervals (for example annually). There are certificates which include an obligation for re-assessment after a certain period of time.

In the case of changes to the product, the validity of a certificate / confirmation under SigG can be expanded to new versions. In this respect, it is a prerequisite that the applicant apply for maintaining the trustworthiness (i. e. a re-certification / maintenance procedure and / or a re-confirmation / addendum confirmation) in compliance with the corresponding rules and that the evaluation does not discover any vulnerabilities.

Conditions for the user result from the certification report / confirmation report and the evaluated manuals.

Information regarding the application environment results from the certification report / confirmation report and the security target.

Conditions for the holder of the certificate result from the certification notice / confirmation notice. If the conditions specified in the notice are not complied with, BSI may withdraw the notice and thus the certificate.

The user of a certified or confirmed product has to take into account the results, ancillary conditions and conditions expressed in the certificate / the confirmation in their risk management process. In order to take into account the further development of attack methods and techniques, the user should define a time interval in which a re-assessment of the product is required and request re-assessment from the holder of the certificate / confirmation through the Assurance Continuity program of BSI.

The obligation to archive the manufacturer's evidences, the certified / confirmed product and the evidence of evaluation are usually limited to a period of five years after such certificate / confirmation is issued. After expiry of this period, a certificate can no longer be reviewed.

The certification body can limit the time of the formal validity of a certificate. The validity of a certificate can also be limited by the time frame cryptographic algorithms or parameters used are accepted depending on the field of application of the product. This is stated in the certification report.

The validity of a site certificate is limited to a period of two years.

The validity of a confirmation under SigG is limited to a certain period of time. Additional or specific ancillary conditions of the Federal Network Agency, such as special time frames cryptographic algorithms or parameters are accepted in the context of SigG are to be taken into account.

Certificates or confirmations under SigG can be revoked in certain cases, taking into account the regulations of the Administrative Procedures Act, such as if it turns out that the basis for the issuance was not given.

8 Glossary and definition of terms

Important terms used in this document are listed and explained below. The explanations apply in the context of the BSI certification and confirmation under SigG and do not claim to be generally valid or complete. Sources ([...]) are listed in the chapter "Sources".

AIS	Notes on Application and Interpretation of the Scheme
Recognition of evaluation facilities	General: Confirmation that an evaluation facility meets the requirements for carrying out certifications within the framework of quality management procedures, conformity assessments etc. Specific: A recognition at BSI as an evaluation facility can take place if the requirements under DIN EN ISO/IEC 17025 and proof of qualification on carrying out evaluations are met for a certain area of expertise (e.g. Common Criteria). A recognition can also relate to certain special areas, such as “smart card and similar devices”.
Applicant	The (natural or legal) person applying for a certification with BSI
Impact analysis report (IAR)	In the case of an intended re-use of evaluation reports from previous procedures, the impact analysis report explains which changes to the product have been made, which security relevance these changes have and which evaluation results are to be re-used
BSIG	Act governing the tasks of BSI [BSIG]
CC	Abbreviation for Common Criteria for Information Technology Security Evaluation [CC]; ISO/IEC 15408
CEM	Abbreviation for Common Methodology for Information Technology Security Evaluation [CEM];
DIN EN 45011	Standard for certification bodies
EAL	CC: abbreviation for Evaluation Assurance Level (Evaluation Level)
Individual evaluation reports	Report of an evaluation facility regarding parts of the assurance aspects of a target of evaluation (TOE) determined in the criteria manuals corresponding to the rules in the certification scheme
Evaluation accompanying development	Evaluation carried out parallel to the development of a TOE (and interwoven with the development)
Certification accompanying development	Certification procedure with evaluation accompanying development
Initial certification	Initial execution of a certification, e. g. for an IT product (see re-certification)
Evaluation	Test and assessment of a TOE in accordance with the requirements of a criteria manual
Evaluation report Evaluation technical report	Final report presented by an evaluation facility on the course and the results of the evaluation of a TOE. The evaluation report (ETR) includes the individual evaluation reports regarding all evaluation aspects which are relevant in a procedure.
Evaluation plan	Project plan and schedule for carrying out the evaluation. Among other things, the plan contains information regarding the planning of contents, the persons involved and the schedule.
Evaluation contract	Contract between the applicant for a certification and a recognized evaluation facility regarding the evaluation to be carried out
TOE	Target of Evaluation
Company confidential (German: firmenvertraulich)	Confidential process documents are labeled as company confidential, such as developer's documents, evaluation reports and review protocols. The bodies involved in the certification procedure have to ensure by suitable measures that company confidential documents are protected

	against unauthorized disclosure.
ISO/IEC 17025	General requirements regarding the competence of testing and calibration laboratories
IT Component	Term from BSIG: The terms IT components and IT product are used as synonyms.
IT product	Summarizing term for objects for which a certification in accordance with BSIG can be carried out (characteristic can be limited by technical rules, usually any combination of hardware and / or software)
IT security certificate	see Certificate
IT system	A specific IT installation with a certain purpose and a specific application environment
ITSEC	Abbreviation for the European “Information Technology Security Evaluation Criteria” [ITSEC]
ITSEM	Abbreviation for the European “Information Technology Security Evaluation Manual” [ITSEM]: ITSEC evaluation manual
Cost notice	In accordance with [BSIKostV], the applicant is invoiced for the costs incurred by BSI in a cost notice.
Criteria manual	Collective name for security criteria, evaluation criteria, security standards and the like: Rules and standards with (technical) requirements regarding a TOE and / or specifications for carrying out the evaluation of the TOE and assessment of the results (here: those published by BSI or generally recognized)
Maintenance	Simplified procedure for extending the validity of a certificate to new product versions in the case of changes without relevance to security (also referred to as “assurance continuity with minor change”)
Need-to-know	Principle for protecting the confidentiality of information: Only those persons who are authorized and absolutely need to know the respective information obtain knowledge about it
Re-assessment	Updating of the assessment of the resistance against attacks of the certified version of a product in the context of the respective security target according to the state of the art as well as updating of the site security of relevant development and production sites
Site visit	Audit of the development environment of the manufacturer. An evaluation is carried out within the framework of site visits checking whether the documented procedures for configuration control and the security in the development environment are used.
Protection profile (PP)	An amount of security requirements which does not depend on the implementation and covers an identifiable partial amount of security goals.
Monitoring staff	Employees of the certification body of BSI or CertLab who carry out the monitoring in a certification procedure and usually also write the certification report.
Monitoring	The certification body or CertLab monitors each evaluation carried out with the goal of a BSI certification in order to ensure a uniform approach and methodology and comparable assessment.
Evaluation facility	(Public or private) body that carries out the evaluation and whose results are recognized for issuing certification notices (here: an evaluation facility recognized by BSI or an evaluation facility working on the basis of legal authority)
Assurance level	Requirements package regarding the documentation and evaluation (in case of CC: evaluation assurance level and / or package)
Re-certification	Re-certification based on a certification already carried out, such as after changes to the product, change of the delivery procedure etc.

Schutzprofil	German translation of the term protection profile
Security target	English term for the German “Sicherheitsvorgaben”
Security criteria	see Criteria manual
Security target (ST)	Part of the documentation of a TOE. Security targets under the CC or ITSEC contain a specification of the security performances required from a TOE which are to be verified during an evaluation. Among other things, they specify the security-specific functions and / or functional requirements, the security goals, the threats to these goals and the intended application environment.
Assurance level	A pre-defined amount of assurance level components from part 3 of the CC that represents a certain point on the scale defined in CC for measuring the assurance level
Pre-evaluation	Optional procedure carried out after agreement between the applicant, the certification body and the evaluation facility in order to determine whether and to what extent the certification goal can be achieved and / or which preliminary work has yet to be performed.
Certificate	In the certificate, the certification result is confirmed in the form of a short summary. The certificate is one of the appendices of the certification notice.
Certification	Name of the entire procedure, consisting of the following phases: Application filed with BSI, evaluation of the TOE by an evaluation facility with monitoring by BSI, final certification, issuance and publication of the certificate.
Certification ID	Synonym of the term certification identifier
Application for a certificate	Formal application which forms the basis for the start of a certification procedure.
Certification notice	Administrative notice communicating the certification result to the applicant. The appendices to the certification notice consist of the certification, the certification report and the cost notice, which is served separately.
Certification identifier	Descriptor of the certification procedures, consisting of information about the technical rules and a sequential number. After issuing the certificate, the year of issuance of the certificate is added. Synonym of the term certification ID
Certification report	Report prepared by the certification body about subject matter, course and results of the certification procedure. The certification report is published (usually by the applicant).

9 Sources

AIS Notes on Application and Information regarding the scheme; website of BSI www.bsi.bund.de/zertifizierung

AIS 1 Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers [Carrying out the Site Visit in the Development Environment of the Manufacturer]

AIS 14 Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) [Requirements regarding the Structure and Content of ETR (Evaluation Technical Report) Parts for Evaluations under the CC (Common Criteria)]

AIS 19 Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC [Requirements regarding Structure and Content of the Summary of ETR (Evaluation Technical Report) for Evaluations under the CC (Common Criteria) and ITSEC]

AIS 23 Zusammentragen von Nachweisen der Entwickler [Compilation of evidence of the Developers]

AIS 27 Transition from ITSEC to CC

AIS 32 CC-Interpretationen im deutschen Zertifizierungsschema [CC Interpretations in the German Certification Scheme]

AIS 35 Öffentliche Fassung eines Security Target (ST-lite) [Public Version of a Target (ST-lite)]

AIS 36 ETR-lite für zusammengesetzte EVGs (ETR-lite) [ETR-lite for Composite TOEs (ETR-lite)]

AIS 41 Guidelines for PPs and STs

AIS 42 Hinweise zur Erstellung von Herstellerdokumenten für eine CC-Evaluierung mit Anlage [Notes for the Preparation of Developer Documents for a CC Evaluation with Appendix]: Guidelines for Developer Documentation according to Common Criteria Version 3.1

AIS 45 Erstellung und Pflege von Meilensteinplänen [Preparation and Maintenance of Milestone Plans]

AIS 47 Regelungen zu Site Certification [Regulations regarding Site Certification]

BSI 7148 “Deutsche IT-Sicherheitszertifikate” publication [German IT Security Certificates] as amended

BSI 7125 Anforderungen an die Prüfstelle für die Evaluierung von Produkten, Schutzprofilen und Standorten nach CC und ITSEC [Requirements regarding the Evaluation Facility for the Evaluation of Products, Protection Profiles and Sites under the CC and ITSEC]

BSIG Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, (BSI-Gesetz – BSIG) [Act on the Federal Office for Information Security (BSI Act - BSIG)], Source: Bundesgesetzblatt [Federal Law Gazette] Jahrgang [volume] 2009 part I no. 54, 19 August 2009, www.bsi.bund.de/zertifizierung

BSIKostV BSI-Kostenverordnung - Kostenverordnung für Amtshandlungen des Bundesamtes für Sicherheit in der Informationstechnik [BSI Regulations on Ex-Parte Cost - Cost Regulations for Ex Parte Costs of Official Acts of the Federal Office for Information Security in the Information Technology], for the current version refer to the BSI website www.bsi.bund.de/zertifizierung

BSIZertV Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung-BSIZertV) [Ordinance on the Procedure for Issuance of a Security Certificate by the Federal Office for Information Security (BSI Certification Regulations -BSIZertV)] of 7 July 1992, Federal Law Gazette I page 1230

CC Common Criteria for Information Technology Security Evaluation, for the current version see www.commoncriteriaportal.org (October 2012: Version 3.1 Release 4)

CC-AC CCIMB-2004-02-009, Assurance Continuity, CCRA Requirements, for current version see www.commoncriteriaportal.org

CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000, see www.commoncriteriaportal.org

CEM Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, for the current version see www.commoncriteriaportal.org (October 2012: Version 3.1 Release 4)

ITSEC German version: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Vorläufige Form der harmonisierten Kriterien, Version 1.2, June 1991, published by the European Union, Bundesanzeiger-Verlag Köln (1991), ISBN 92-826-3003-X
(English version:) Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonised Criteria, Version 1.2, June 1991, ISBN 92-826-3004-8

ITSEM German version: Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik, Vorläufige Form der harmonisierten Methodik, Version 1.0, September 1993, published by the European Union, Bundesanzeiger Verlag Köln, ISBN 92-826-7078-2
(English version:) Information Technology Security Evaluation Manual (ITSEM), Version 1.0, 1993

JIL Joint Interpretation Library, part of the AIS documents

Sig-AlgoKat Übersicht über geeignete Algorithmen, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen [Overview of suitable Algorithms, Announcements on the Electronic Signature under the Signature Act and the Signature Regulation, Federal Network Agency for Electricity, Gas, Telecommunication, Post and Rail], for the current version see www.bundesnetzagentur.de

SigG Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG): Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) [Act on the Framework Conditions for Electronic Signatures and Amendment of further Regulations (Signature Act - SigG): Signature Act of 16 May 2001 (Federal Law Gazette I page 876), last amendment by article 4 of the Act of 17 July 2009 (Federal Law Gazette I page 2091)], for the current version see www.bundesnetzagentur.de

SigV Verordnung zur elektronischen Signatur: "Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 17. Dezember 2009 (BGBl. I S. 3932) [Regulation on the Electronic Signature: Signature Regulation of 16 November 2001 (Federal Law Gazette I page 3074), last amended by the Regulation of 17 December 2009 (Federal Law Gazette I page 3932)], for current version see www.bundesnetzagentur.de

SOGIS-MRA Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3.0, January 2010, SOG-IS, see www.sogisportal.eu

SupDoc-SC Supporting Document Site Certification, CCDB-2007-11-001, see www.commoncriteriaportal.org

VB-Stellen Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern [Process Description on the Recognition of Evaluation Facilities and Certification of IT Security Service Providers], for the current version see www.bsi.bund.de/zertifizierung