BSI IT Certificates
Information for consumers

The BSI Security Certificate for IT products - what does it mean?

The BSI Security Certificate makes the security performance of an information technology (IT) product…

- **… transparent**

  The security performance of the IT product in relation to the threats it protects against is described precisely and an assessment is provided as to how strongly the security functions defend against these threats.

- **… trustworthy**

  Aspects such as confidentiality, integrity and availability are tested, from design through production and delivery to operation of the IT product.

- **… directly usable**

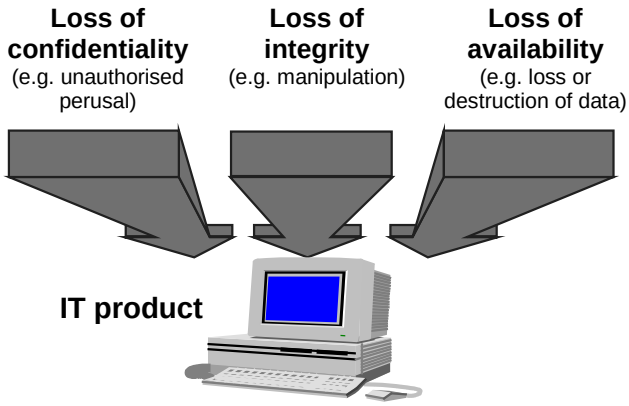
  The administration and operational environment of the IT product are described in detail and any vulnerabilities are identified, along with advice on how possible effects can be prevented.

- **… suitable for use by you**

  The certificate confirms that the IT product matches the security profile of your application and operational environment.

But how can one create confidence in technology?

Various security criteria serve as the basis for testing the assurance of IT products. Assurance is derived from correctness of implementation of the security functions and the effectiveness of these functions (for example, these functions include authentication, access control and error protection). The security functions act against the following three basic threats:



What criteria can be certificated?

ITS IT security criteria (the first national German set of criteria)

ITSEC Information Technology Security Evaluation Criteria (harmonised European security criteria)

CC Common Criteria (harmonisation of all relevant security criteria and an internationally recognised standard ISO/IEC 15048)

The BSI Security Certificate as confirmation of test results

The BSI Security Certificate confirms the results of testing according to the CC (security functionality, evaluation assurance level, strength of security functions) or ITSEC. The certificate applies only to the version of the product that was tested. The certificate can be upgraded to include new versions of the product or kept up-to-date through a re-certification process or maintenance process.

Common Criteria (CC)

The CC is based on

- the European ITSEC (Information Technology Security Devaluation Criteria)
- the US TCSEC (Trusted Computer Security Evaluation Criteria, "Orange Book")
- and the Canadian CTCPEC (Canadian Trusted Computer Product Evaluation Criteria).

Now that they have been turned into standard ISO/IEC 15048, for the first time they offer a comprehensive catalogue of predefined security functions and hence an internationally recognised language for the specification of IT security. International agreements guarantee world-wide recognition of certification results according to the CC.

How can security be measured?

The CC or ITSEC serve as the basis for the evaluation of the assurance of IT products.

The security criteria permit comparability between the results of independent security tests and evaluations. This is achieved through provision of a common set of requirements regarding the security functions of IT products and the assurance measures that are tested. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures meet the requirements.

The security criteria impose detailed test requirements, including on the IT product, development, the development environment, user documentation, delivery and operation. The capability of the security functions of an IT product to withstand the threats under consideration is also tested.

The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.

The assurance of IT products can be measured in so-called assurance levels. A series of levels is defined - EAL1 to EAL7 in the case of the CC and E1 to E6 for ITSEC - whereby the higher the number in the code the greater the level of assurance.

What does the certification report contain?

The certification report is issued following successful completion of testing and certification. As well as the **Security Certificate** itself, it contains a report publishing details of the evaluation and certification. The report

- describes the security behaviour of the product in relation to the threats listed;
- states the assurance level of the product;
- specifies the requirements regarding installation and the operational environment;
- states any inherent vulnerabilities and appropriate countermeasures.

Where can one obtain the certification report?

The manufacturer of a certified IT product will be happy to issue copies of the certification report. The certification reports published by the BSI can be retrieved on the Internet from: http://www.bsi.bund.de/zertifiz.

How do you obtain the appropriate certificate?

The *Common Criteria* (CC) provides full details of how to create protection profiles (PP) and incorporate these into a standardisation procedure. A PP is a set of requirements which specifies the security requirements for products of a similar kind in a generic, product-neutral manner, normally from the manufacturer's point of view. It is also an aim of the CC to orient this standardisation approach to use by users.

As far as the user is concerned, a protection profile should not be oriented to conventional security solutions but solely to user requirements. In addition, the legal and other requirements that users are required to adhere to must also be considered. Technical implementation of this security lies with the manufacturer, for whom the protection profile is intended to serve as a specification for further product developments. It can, moreover, be developed into a product class-specific protection profile.

Does IT security necessarily cost a lot of money?

Security measures only implemented retroactively will make a significant dent in your budget. However, it is generally a lot cheaper to use IT products that incorporate trusted security functions. If, as a user, you ask for a security certificate that matches the security profile appropriate to your requirements, you have the possibility of reducing the cost of supplementary security measures such as, for example, infrastructural measures.

Is there a list of BSI Security Certificates?

You can request a list of the BSI Security Certificates that have been issued from the address below. You will receive an up-to-date list of certified IT products with technical data and manufacturer addresses.

This list and other information are also available online at http://www.bsi.bund.de/zertifiz.

Bundesamt für Sicherheit in der Informationstechnik
Referat III 2.2
P.O. Box 20 03 63
53133 Bonn
GERMANY

Do you have any further questions?

BSI-Infoline:	+49 228 99 9582-111
Fax:	+49 228 99 9582-5455
e-mail:	zerti@bsi.bund.de
Internet:	http://www.bsi.bund.de