

brightsight®



Common Criteria Explained Series

**Common Criteria Guidance for
Developers –
Evaluation Assurance Level 4**



June 2010, v 1.40

© 2010 Brightsight. All rights reserved.

No part of this publication may be reproduced and/or published by print, photo print, microfilm or any other means without the previous written consent of Brightsight.

Contact information

If you have any questions that this document does not answer, additions, errors or whatever please contact:

Brightsight
Delftechpark 1
2628 XJ Delft
the Netherlands

Phone: +31 15 2692500
Fax: +31 15 2692555
Email: out@brightsight.com
Web: www.brightsight.com

References

- [CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, version 3.1
- [CEM] Common Methodology for Information Technology Security Evaluation, version 3.1
- [ISO-CoP] ISO - International Organization for Standardization Information Technology – Code of practice for information security management ISO 17799

Official versions of the Common Criteria can be found on:
www.commoncriteriaportal.org

Abbreviations

BSI	Bundesamt für Sicherheit in der Informationstechnik (German National Certification Body)
CC	Common Criteria
EAL	Evaluation Assurance Level
ISO	International Organization for Standardization
NSCIB	Netherlands Scheme for Certification in the Area of IT Security (Dutch National Certification Body)
PP	Protection Profile
SERTIT	Sertifiseringsmyndigheten for IT-sikkerhet (Norwegian National Certification Body)
ST	Security Target
TOE	Target Of Evaluation

Content

1	Introduction.....	4
1.1	About this document.....	4
1.2	Contents of this document.....	5
2	Claim requirements (Security Target)	7
3	Life-cycle support requirements (development process).....	9
3.1	Requirements	9
3.2	Frequently asked questions on Development Process requirements	10
4	Development requirements (product design).....	11
4.1	Requirements	11
4.2	Frequently asked questions on Product Design descriptions	12
5	Tests and vulnerability analysis requirements	14
6	Deployment requirements (guidance).....	15
7	The evaluation process.....	16
7.1	The evaluation process	16
7.1.1	Initial Phase	16
7.1.2	Evaluation Phase.....	16
7.1.3	Conclusion Phase.....	17
7.1.4	The certificate	17
7.2	Frequently asked questions on the evaluation process	17

1 Introduction

1.1 About this document

The Common Criteria / ISO 15408 is a *standard for the evaluation of security of IT systems*. It is currently at version 3.1 of which the latest revision was published in September 2007. Common Criteria (CC) was created to solve the question: how can I be sure that an IT product has the security I need? In the past, each country had their own ways to ensure the security of the IT products. CC is the first standard for IT security evaluation that is recognized internationally.

The *strength of CC* lies in the fact that it provides a complete and unambiguous method for the developer to describe and for the evaluation lab to evaluate the security of a product. However, to be able to achieve this completeness and unambiguity, CC becomes less accessible, especially to the product developers. Too many specialized terms and abbreviations are used; too broad and flexible to find out what you exactly need if you're not familiar with the philosophy hidden inside.

One *source of flexibility* is that the CC allows a developer to tailor an evaluation to his product. He can choose how his product is to be evaluated by selecting a set of security tests from a large list of possible security tests in the standard. The number of possible sets is therefore huge. To combat this, the Common Criteria defines seven sets of tests, called Evaluation Assurance Levels or EALs to help developers in making a choice. These levels range from EAL 1, which is a simple, brief examination of the product, to EAL 7, an extremely detailed examination of the product, its documentation and its design process. In essence, the EAL determines how sure you want to be that the product conforms to its specification.

The aim of this document is to provide, briefly, a general overview of what is being required of a developer to have his product CC evaluated at the level EAL4. EAL4 evaluation gives a reasonably complete view of all the aspects covered in CC. A CC evaluation is, compared to other evaluations, very much a joint effort of a developer and an evaluation lab.

This document supports help a developer **understand** what is being required from him on this level of evaluation. This document is therefore written in a very informal style. The goal of this document is **not** to make him a Common Criteria expert, precisely tell him what to do (that is what the CC does in almost a thousand pages) or help him design a secure product.

1.2 Contents of this document

Evaluation Assurance Level 4 contains various security requirements on your product and its supporting design processes and documentation. These requirements can be subdivided into five areas:

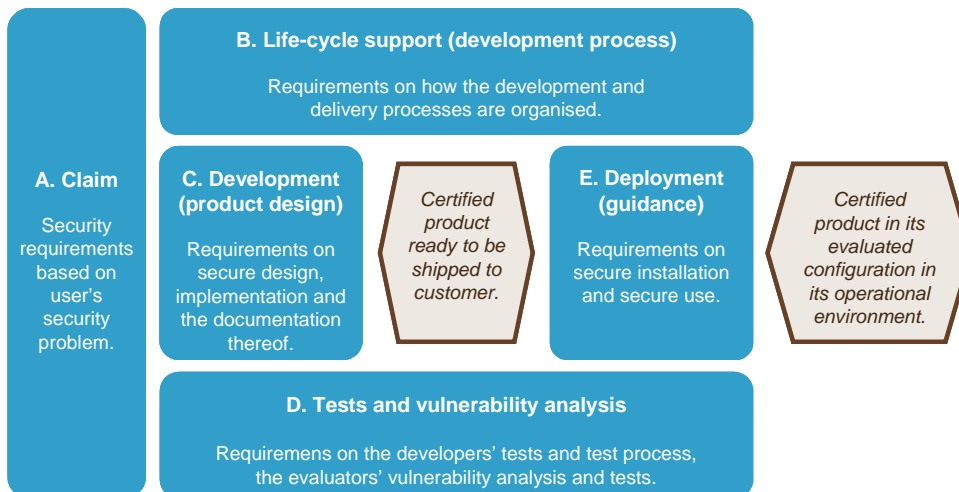


Figure 1 Overview of process requirements.

- A. Claim (Security Target):** These requirements focus on how you should describe what your product does, the threats it protects against, the security functionality it provides, the assistance and protection it requires from its environment.
- B. Life-cycle support (development process):** These requirements focus on how you should arrange and organize your development process. This addresses areas such as product life cycle, configuration management, site security, tools and delivery.
- C. Development (product design):** These requirements focus on the design documentation of your product: what types of design documentation are needed, what information they should contain, and how they should be related.
- D. Tests and vulnerability analysis:** These requirements focus on how you test the security aspects of your product: requirements for your test plan and processes. These requirements also indicate evaluators how to assess possible weaknesses and vulnerabilities in the product.
- E. Deployment (guidance):** These requirements focus on the post-production part of your product and how you guarantee that it can be securely shipped to customers and, once received, can be securely installed and used.

Each of these groups is described in its separate chapter. In these chapters we show you what you should deliver, how we may be able to assist you (some features of the Common Criteria are really hard to do yourself), and in some cases we provide a mini-FAQ.

The final chapter of this document is a chapter describing the general procedure of a Common Criteria evaluation from the beginning to the end, the certificate.

2 Claim requirements (Security Target)

One of the important phases in an evaluation is to determine what security functionality will be evaluated. A Common Criteria evaluation does **not** take your product, examine it, and pronounce, “This is a good product” or “This is a bad product”.

Rather, in a Common Criteria evaluation:

- you** determine what security functionality you claim your product has;
- we determine whether your claim is valid by examining your product.

The security functionality claim you make must be in a special format, called a Security Target. The Common Criteria gives strict criteria for the content of the Security Target, and we provide only the briefest possible overview here.

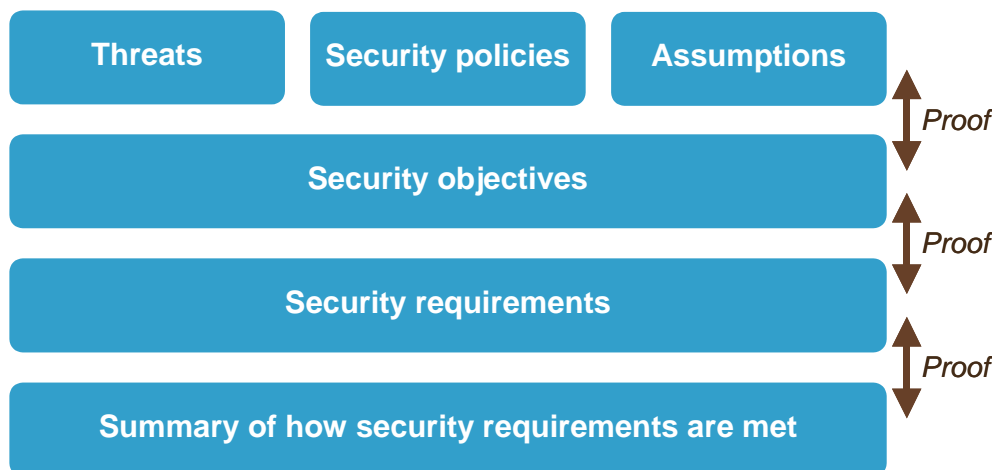


Figure 2 Brief overview of contents of a Security Target.

The Security Target must contain:

- 1) A description of the security problem that you are trying to solve. This must contain:
 - a list of *threats* that your product protects against;
 - a list of *security policies* that your product implements or conforms to (examples: National Banking Law Article X, Regulations for National Security Article Y);
 - assumptions*: a description of the intended environment that your product needs to function (example: connections with other products, trained personnel, regular backup).

- 2) A high-level description of the solution to this security problem, consisting of a set of objectives that together counter the threats and implement the policies in the intended environment.
- 3) A set of security requirements: a description of your solution formulated in a set of formal CC dedicated requirements. A complete list of these formal CC dedicated requirements is defined in [CC]. The requirements address the security functionality of the product and the assurance level with which it will be evaluated.
- 4) A description how your product implements the security requirements, but still on a relatively high level.
- 5) A “proof” that your objectives indeed protect against threats and implement objectives in the intended environment, a “proof” that your requirements implement your objectives and another “proof” that the security functionality implements your security requirements. These “proofs” are necessary to show that all descriptions are consistent.

As indicated under point 3 the Security Target defines an assurance level: how “sure” do you want to be that your product indeed corresponds with the Security Target. In general this is defined with an Evaluation Assurance Level (see section 1.1 About this document). Security Targets for an EAL2 up to EAL7 have identical types of contents. A Security Target for EAL1 is more limited.

The product that is described in the Security Target is called TOE (Target Of Evaluation).

Writing a Security Target is a fairly difficult task, mainly because formal CC dedicated requirements must be used. Choices made in the Security Target can dramatically influence cost and duration of the rest of the evaluation. The Security Target is therefore normally written as a co-operative effort between you and us.

3 Life-cycle support requirements (development process)

3.1 Requirements

Evaluation Assurance Level 4 has the following requirements on your development process:

You must use a **Life-Cycle Model** encompassing the procedures, tools, and techniques that you use to develop and maintain your product. Aspects of the process that may be covered by your model include design methods, review procedures, project management controls, change control procedures, test methods and acceptance procedures. An effective life-cycle model will address these aspects of the development and maintenance process within an overall management structure that assigns responsibilities and monitors progress.

You must use a **Configuration Management System** and this system must assign unique references to each version of your product and to all your configuration items¹. It must provide measures to prevent unauthorized changes and have procedures to accept new or modified configuration items. The Configuration System must be at least partly automated and have automated means to prevent unauthorized changes to the implementation and it must have automated means to “generate” your product (e.g. compile your product from the source code, generate masks from an HDL description etc.). Finally, the Configuration Management System must manage at least: all Design Descriptions, the test documentation, the user and administrator guidance, the Configuration management documentation itself and all information on security flaws discovered and reported.

You must provide **Site Security Documentation** that describes all the physical, procedural, personnel and other security measures that you use to protect your design and development process. Did you screen your personnel? Is your development environment connected to the Internet? Can anyone walk in and out of your building at will?

You must show that the **Development Tools** that you use for your product are well-defined (confirm to recognized standards, well known industry standard tools) and well documented (manuals describing all statements, options etc.).

¹ This is basically all your design documentation, source code, bug reports, process documentation etc.

3.2 Frequently asked questions on Development Process requirements

Configuration Management System and Development Security Documentation talks about procedures. What kind of procedures? How strict should they be? At this level you are mostly just required to a) have reasonably effective procedures² that you think are suitable for your product and b) follow them. So you could have poor procedures, but in our experience good procedures make for better products.

We already have procedures! We found a Life-Cycle model in the literature and use it "straight from the box". Great! It will probably save you (and us) a lot of time if you use a good existing Life Cycle model rather than trying to write it yourself.

So we could use any Life-Cycle model from literature? Not quite. Some may be less applicable to the type of product you develop, and some Life Cycle models allow choices or contain lots of optional sections. For the latter you will have to "instantiate" the Life-Cycle model, by making the choices beforehand, or stating which optional sections you will use beforehand. Otherwise you could just use the model and change it every time you liked, which is identical to not using a model at all.

You provided an overview of many deliverables, both for process and for design document requirements. Are there any examples that I can examine to see what they look like in real life?

No.³ (see section 2). For some reason developers do not want to publish their design documents and vulnerability analyses for other people to see. In other parts of this "CC explained series" we provide examples of deliverables, but these parts are not publicly available.

² The procedures should not contain rules like "throw all bug reports away as soon as you receive them", or "our source code repository can be directly accessed from the Internet by everyone"

³ With the sole exception of Security Targets.

4 Development requirements (product design)

4.1 Requirements

These requirements focus on the design documentation of your product: what types of design documentation are needed, what information they should contain, and how they should be related.

Evaluation Assurance Level 4 requires that you have at least the following design descriptions of your product:

- A functional specification;
- TOE design;
- Security Architecture
- The implementation.

The **Functional Specification** describes your product and all of its external interfaces in natural language. For each interface you must provide details, such as purpose, method of use, parameters, associated actions and error messages. You must also show that your functional specification describes all parts of your product that may be relevant for security. You must also "proof" that your Functional Specification is consistent with the security requirements made in the Security Target.

The **TOE Design** describes your product as a relatively small number of subsystems (parts, layers, domains, servers or whatever). You must describe the security functionality provided by each subsystem and describe all their interfaces, giving details of the purpose, method of use, parameters, actions, and error messages. You must also identify all underlying hardware, software and/or firmware that your product requires, and describe the protection mechanisms provided by them. The **TOE Design** further details your product as a number of modules (sub subsystems). The same characteristics as for subsystems have to be described for the modules. You must also "proof" that the TOE Design is consistent with the security requirements of the Security Target and correctly and completely maps on the Functional Specification.

The **Security Architecture** requires that you demonstrate that your product is structured in such a way that it cannot be tampered with and that its security mechanisms cannot be bypassed. If your product can be separated into different security relevant parts, these parts should be constructed such that they cannot be influenced by each other. Also, when it is turned on, all settings and parameters must be initialised securely and correctly.

The **Implementation** of your product: its source code, hardware drawings etc. During the evaluation selected parts of the implementation will be examined. You must also “proof” that the Implementation is consistent with the security requirements of the Security Target and correctly and completely maps on the TOE Design.

4.2 Frequently asked questions on Product Design descriptions

The design descriptions list seems to mandate a “waterfall” approach to design, but we use <fill in blank>? How do I tailor the CC to my design method? The design descriptions must only be complete at the end of your design process. If, for instance, you use “rapid prototyping” you can make as many cycles as you wish, but in the end you are required to have a functional specification, a high level design, and a low-level design for the final iteration, and they are required to match.

But our design process must be able to incorporate requirements made at a very late stage! How can we do this if we have to update all these descriptions? Haven't you ever heard of time-to-market? We have heard of time-to-market, often as a cause why a product with a lot of bugs, security holes and unwanted “features” was unleashed on unsuspecting customers. Adding requirements in a late stage of the design process without taking time to assess what it does to your design (i.e. update your design descriptions) is a recipe for trouble. Remember, a product may work when most of its features “kinda work”, but a product is only secure when all of its security features work correctly.

Don't all these layers describe the same product in slightly different ways? Why take all the trouble to write the same thing down multiple times?

Basically because it forces a designer to think about and structure his design, rather than produce code straight from the functional specification.

My design has less layers than the four that you describe, what do I do? You are out of luck. The CC mandates having at least four. You will have to create another one and sandwich it in between. Or you could cheat, and go to Evaluation Assurance Level 3 (EAL3) instead of the EAL4, since you do not need to provide module (lowest design layer of the TOE Design) and Implementation on EAL3. It may be a lower level and marketing may complain, but it is probably better than making up a lot of stuff just to satisfy a standard.

My design has more layers than you describe, what do I do?

You just select your “best” layers and give them the names described earlier. However, you must make the cross-tables to show correspondence between the layers that you provide. Of course, you could always leave the extra layers out if you think that is better or less work. You don't have to give the evaluator everything

you have.

I have a document describing all interfaces of my SmartCard, and another document describing all interfaces of my SmartCard reader. Do I need to combine them to produce a Functional Specification of the combination?

No. You could put all design documentation into a single document, or distribute it over a hundred documents, some of which also include stuff that is not design documentation. As long as it is clear which is which, and what information can be found where.

5 Tests and vulnerability analysis requirements

Evaluation Assurance Level 4 requires that you provide the following:

Test Documentation consisting of test plans, test procedure descriptions, expected test results and actual test results. Of course this test documentation must show that each tested function behaved as specified. The tests are only focused on the security aspects as defined in the Security Target.

A **Test Analysis** that analyses your Test Documentation and demonstrates that the “width” of your tests corresponds with what you have written in your Functional Specification (see section 3.1) by showing that every element in your Functional Specification is addressed by at least one test. The Test Analysis must also demonstrate that the “depth” of your tests is at least that of the Sub system level of the TOE Design (see section 3.1), as at EAL4 it is not sufficient to test only the external interfaces from the Functional Specification.

The **TOE, suitable for testing**. You must provide us with one or more copies of your TOE (or access to your TOE if you only have one). Where necessary, you must also provide us with (access to) testing tools and libraries that may be necessary for us to test your TOE.

The evaluator will perform a sample of the tests performed by you. In addition the evaluator will extend your tests set on places where more insight in the behaviour is needed.

The evaluator will do a **Vulnerability Analysis** where a search for vulnerabilities is done and whether the product security mechanisms are sufficient to resist certain attackers. The evaluators will “proof” that the product is resistant by means of a series penetration tests.

6 Deployment requirements (guidance)

Even when your product is completely secure the moment that you produce it, it still has to overcome two major problems before it is completely secure at the customer: it has to get there, and once there, has to be securely installed. Evaluation Assurance Level 4 therefore requires that you provide the following:

Delivery Documentation showing that there is a secure manner for your product to get to the user (perhaps you deliver it in person, or you have some sort of construction with digital signatures). This manner must describe how one can detect differences between the “master copy” and the product a customer receives, and it must also be resistant against people masquerading as the developer (Customer: “The new version 1.1 you sent us sucks! We can’t read our debtor database anymore!” Developer: “We never sent you version 1.1. In fact, there is no version 1.1. Where did you get it?”).

Preparative guidance describing how the customer can create a securely operating version of your product from what he received from you. This can include processes for installing software and hardware, compiling source code into an executable, configuring, personalizing, generating keys, creating a secure physical environment etc.

When your product is completely secure after preparation, if the user does not know how to use/maintain it in a secure manner the end result will not be secure. Evaluation Assurance Level 4 therefore requires that you provide **Operational guidance**. For each user role the security guidance must be described. This includes day-to-day secure operations, errors and warnings, handling of users with privileges, modes of operation, security events (e.g. what happens when there is power shortage) and recognizing when the product is not in a secure state any more.

7 The evaluation process

7.1 The evaluation process

The evaluation process consists of three distinct phases⁴:

- 1) Initial Phase;
- 2) Evaluation Phase;
- 3) Conclusion Phase.

The evaluation process will lead to a series of reports of Brightsight and a Certificate of a Certification Body.

7.1.1 Initial Phase

In this phase the evaluators assess your current product and/or design process, and together with you decide on:

- which functionality of your product should be evaluated;
- which Evaluation Assurance Level (or other set of tests to use) should be used during the evaluation⁵

At the end of the initial phase a Security Target is drawn up. The Security Target will form the basis for the evaluation. It will show exactly the functionality of the product to be evaluated and how it will be assessed whether your product actually has this functionality. This process is under supervision of a so-called Certification Body.

7.1.2 Evaluation Phase

In this phase, the evaluators check your design documentation and processes (see sections 3 and 4) for compliance with the requirements of the Evaluation Assurance Level 4 that was chosen in the Initial Phase. This will entail checking a lot of documents, a site visit or two, and testing of your product.

For EAL 4, the testing is limited to repeating some of the tests that you already did (to see if you have performed these tests correctly. We will also do some additional testing on places where we think that this may be necessary. Finally we will also try to find vulnerabilities in your product, both in the concept “the wrong idea” and in the implementation “the right idea, but implemented in the wrong way”. On EAL 4, we check for vulnerabilities that take a reasonable time and reasonable amount of resources to exploit, not whether the US National Security Agency can break your product, given unlimited budget and time.

⁴ Note: This is how we (Brightsight) do it. Other labs may do it in another way.

⁵ In this document we chose EAL 4 as an example, but you may choose otherwise.

7.1.3 Conclusion Phase

If we are satisfied that your product meets the requirements that we set out in the Security Target, we notify our Certification Body. The Certification Body reviews our work and might ask additional questions or require additional tests.

7.1.4 The certificate

When the Certification Body agrees with the reports of Brightsight they write a Certification Report and will give you a certificate. The certificate demonstrates that your product for the security functional requirements defined in the Security Target satisfies the EAL4 assurance requirements, in other words showing that your product meets the requirements.

The Security Target and the Certification Report are published on the website of the Certification Body and on the official CC website www.commoncriteriaportal.org.

7.2 Frequently asked questions on the evaluation process

And what do I do with this certificate? Anybody can publish a piece of paper saying anything, right?

Correct. You may get a reaction such as “Brightsight? Never heard of!” And this is a normal reaction. You may point to the official Common Criteria website www.commoncriteriaportal.org. But there is more.

Brightsight has therefore joined the

- German National Certification Body BSI (Bundesamt für Sicherheit in der Informationstechnik),
- Dutch National Certification Body TNO-Certification (Netherlands Scheme for Certification in the Area of IT Security),
- Norwegian National Certification Body SERTIT (Sertifiseringsmyndigheten for IT-sikkerhet).

All three are internationally recognized (Mutual Recognition). Joining a Certification Body is not a trivial matter: it requires an ISO 17025 certification and a strenuous entry test (it took us about four man months to pass).

In other words, Brightsight does not provide the certificates, but the Certification Bodies do. These Certification Bodies check whether Brightsight does a decent job, instead of just taking your money.

But I have never heard of these Certification Bodies either! And I doubt that my customer in <insert country> has.

The Certification Bodies are member of a group of governmental Certification Bodies, with members in Australia and New Zealand, Canada, France, Germany, Italy, Japan, the Republic of Korea, The Netherlands, Norway, Spain, Sweden,

United Kingdom and the United States. This group recognizes each others' certificates and also checks whether the Certification Body does a decent job, instead of just taking your money.

Additionally, Common Criteria certificates are recognized (though these countries do not yet produce certificates themselves) by the governments of Austria, Czech Republic, Denmark, Finland, Greece, Hungary, India, Israel, Malaysia, Pakistan, Singapore, Turkey. This list is expected to grow in the coming years.

This means that it no longer matters where you have your product evaluated (though we would prefer it if you had it done at Brightsight), your certificate is worth the same.

And why do I need a certificate anyway? If you don't know this, you don't. If both you and your customers trust your products, why spend money on having them certified?

Other companies have their product certified for various reasons:

- Some companies want to sell their product abroad, and their customers hardly know them, let alone have blind faith that the product will do a good job in protecting their valuable assets;
- Certificates are mandatory for some applications in some countries (e.g. certificates for Secure Signature Creation Devices under the European Digital Signature Law);
- Some companies want to prove to their customers that they have taken all possible care in preventing security holes and bugs;
- Some companies want to make a better product. In most evaluations we did so far, we pointed out serious flaws in either the security concept of the product and/or in the implementation of that concept.

The answers to all three previous questions feature a word I'm very much interested in, and which has been suspiciously lacking in the rest of this document: money. How much is this going to cost me? The certification costs are negligible, a few thousand Euro⁶. Our costs are more substantial, but depend strongly on:

- how much and which functionality you want to have certified;
- how much testing we have to do (the EAL);
- how good your product is, and how good your current design documentation is.

And there are always your own costs, to adapt your product, to adapt your design documentation etc.

⁶ 1 Euro ≈ 1 US\$. The costs for the Certification Bodies are similar.

I get the picture. Can't you give me an estimate anyway?

This may be completely off, but given a small to average sized⁷ product, an EAL4 evaluation, with “good” design documentation⁸, you are looking at about 32 KEuro for the Initial Phase and about 125 - 200 KEuro for the Evaluation Phase. During the Initial Phase we will refine our estimate for the Evaluation Phase. The costs you are going to make to write the documentation and set up/maintain a development process are not included.

That much money? We are a small company!

Unfortunately that is what an EAL4 evaluation is going to cost. The Common Criteria tell us what criteria your product should meet, and there is a Common Evaluation Methodology that tells us how to apply these criteria. Even what and how we report is standardized. This means: no shortcuts and no room to cut corners (it also adds substantially to the value of the evaluation: your competitor will also be unable to cut corners). It is comparable to what other evaluation facilities in the world charge, though your mileage may vary....

If it is too much, you may want to check out EAL3. In this evaluation less is checked. An initial phase is again about 32KEuro, whereas the Evaluation Phase is about 80 - 140 KEuro⁹.

And it is also just an estimate. So it could be much more?

Remember, you determine what functionality we will evaluate and which tests (the EAL) that we will use.

- If we discover substantial problems early in the evaluation, we can stop;
- If we discover problems late, we can usually adjust either the functionality, or lower the EAL;
- If we discover problems late and we cannot adjust, this means that there is something fundamentally wrong: your product has bugs that cannot be repaired, or your process has fundamental shortcomings that cannot be repaired. If this happens, failing the evaluation will not be your biggest problem....

How long will the Initial Phase take?

About one month, if we plan it two - three month in advance.

How long will the Evaluation Phase take?

On EAL4 about six to nine months if we plan it perfectly, both product and design documentation is right the first time and was made by a security expert who knows his way around the Common Criteria keeping in mind that it would be evaluated someday. More if it wasn't.

Much more if you didn't have anything resembling a design process to start with.

⁷ I don't know what this means, but just for the sake of discussion.

⁸ See the previous footnote

⁹ These estimates are based on the same firm assumptions as the estimates for EAL4.

Much, much more if you want EAL7. It could also be more if we are busy with a lot of other evaluations at that time.

What happens if it isn't right the first time?

We tell you that it is wrong, and it has to be fixed. If the problem is due to some misinterpretation or difficulty of the Common Criteria, we can help you fix it. If, however, the problem is due to deficiencies in your product and/or its associated documentation, you have to fix it yourself. After the problem has been fixed, we determine the impact on the evaluation, and this may entail that some parts will have to be redone.

Why don't you help me with deficiency-related problems?

Because we also evaluate related products of your competitors, and we think that it is unfair to them if we use the knowledge that we gained from these evaluations in improving your product. You would probably feel the same if it was the other way around....

What are my alternatives to Common Criteria evaluation?

This depends on what you want to have certified. If you want to have:

- your **product** certified, there are not many alternatives. There are older standards (mainly the European ITSEC and the US Orange Book) but these are dated and localized (ITSEC is not recognized in the US, Orange Book is not recognized in Europe). Both standards are currently in the process of being replaced by the Common Criteria. For certification of some **specific products**, such as Security Modules, specific methods such as FIPS 140 exist, and may be preferable;
- your **company** certified, the ISO9000 series or the BS7799/ISO17799 (Code of Practice) [ISO-CoP] may be a better alternative;
- your **design/development process** certified, you could use ISO 15504 (Software Process Assessment) or CMM and/or SSE-CMM (the security version of CMM).

And can you help me with these alternatives?

No. We may provide you with some advice, or an address, but we only do Common Criteria certifications.

I have sold 100.000 copies of my product already. Can it still be evaluated?

Sure. You may or may not be able to reach the EAL that you want, but one of the lower levels is usually perfectly feasible. Or we can always evaluate the new and upcoming version...

I have more questions....

Ask us about them. Our address information is on page 2.

Brightsight – the synonym for leading security evaluation technology

Our company is built on a stable foundation of expertise, reputation and discretion. Established knowledge and continuous dialogue with our market partners enable us to face the challenges of dynamic developments in the field of IT security with confidence, and to adapt these to the individual requirements of our customers. We enjoy the highest reputation as one of the leading security evaluation laboratories. We support more than 100 internationally active companies as a reliable partner - many of these already for decades, with:

Security Evaluation and Audits

Analyses, tests, inspection and audit of all relevant security criteria for IT products and systems within the scope of product approvals.

(i.e. smart cards, electronic ID cards, micro controllers, payment terminals, security tokens, mobile communication devices, set top boxes, access control systems, car equipment, taximeters, tachographs, alcohol interlocks etc.)

Training

Development and implementation of training courses and workshops in the area of IT security and security testing both for standard methods and customized security solutions.

Consultancy

Individual support to manufacturers before and during product development, in all aspects of the underlying evaluation requirements and guidelines, to help them improve product security. Support of organizations and stakeholders during definition and specification of dedicated security criteria required for the approval of new IT products.

Tools

Development, sales and distribution of unique analysis and testing tools which are used in high quality Common Criteria evaluations and have stood the test of time.

Full-service security evaluation – an asset to our customers

Our customers benefit from our many years of sound experience as an independent expert and from our extensive expertise. Our unique analysis techniques and tools ensure a precise preparation for the comprehensive product approval process. Furthermore, the close collaboration during the product development phase enables us to understand individual security needs. In return, we deliver the knowledge that is necessary to satisfy the certification requirements. With our help possible security gaps can be identified and closed at an early stage. As a result the formal security approval process becomes smooth and efficient, which is reflected in valuable time and cost saving benefits.