Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

BEST PRACTICES FOR ISS RISK MANAGEMENT

Use of the EBIOS® method to write a product security target

10 November 2004 Version

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tel 01 71 75 84 15 - Fax 01 71 75 84 00

What is a product security target?

A security target (ST), in the sense of standard ISO 15408 - Common Criteria for the Evaluation of Information Technology Security - is a "set of security requirements and specifications to be used as the basis for evaluation of an identified TOE" (the TOE - *Target Of Evaluation* - is the product under study).

It consists of a document with standardised content, that can be used as a specification refining the content of a protection profile (PP) and that can also be evaluated. In particular, this ST proposes a justified refinement of the security requirements formalised in the PP. It allows the TOE user to understand how adequate the TOE is for his needs.

Outside the context of technical evaluation (certified product evaluation by the DCSSI), it is possible to write ISS specifications in the form of an ST, primarily to ensure that a recognised framework and terminology are used.

What are the advantages of the EBIOS method when writing a product ST?

A product ST must be totally complete and consistent. It must therefore be written with the greatest rigour, but the standard does not propose any method for writing. The EBIOS method identifies all the elements required for writing an ST, and ensures that they remain consistent. It provides several other advantages:

- relevant security objectives covering the threats, assumptions, security policy rules and security requirements,
- justification of objectives and requirements by assessing ISS risks,
- a structured approach that ensures the study is exhaustive,
- involvement of interested parties (top management, contracting authority, prime contractor, users, etc.).

How is EBIOS used to write an ST?

An effective solution for writing an ST consists in:

- conducting an EBIOS study (with a scope of study that will be the scope of the ST) and refining the security requirements,
- writing a PP and having it validated on the basis of the study,
- extracting the necessary data from the study (a large part of the study),
- writing the introduction (identification of the ST and overview),
- reorganising the security objectives (classified according to their scope),
- reorganising the security requirements (classified according to their scope),
- writing the claims of PP conformance.

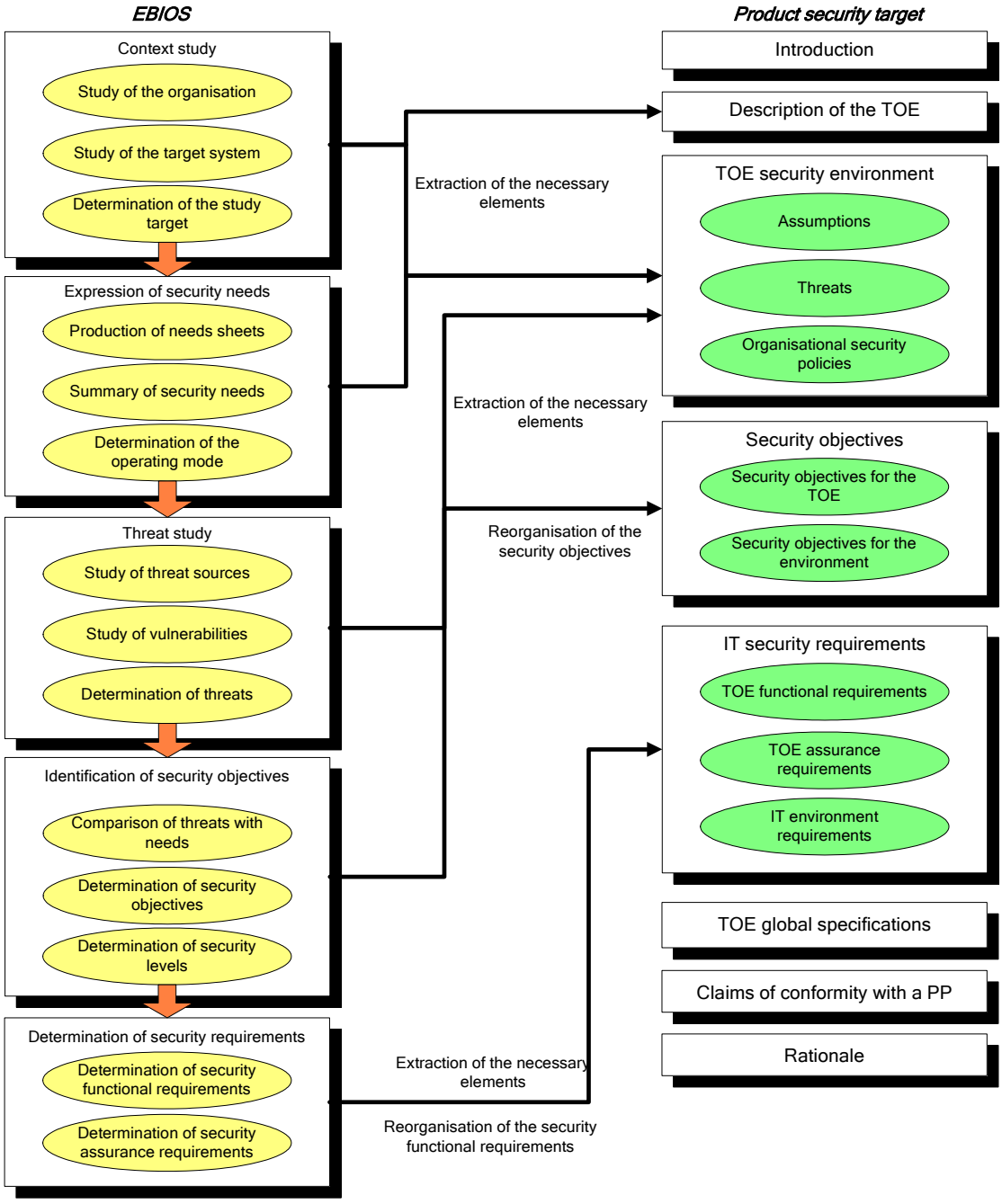
To achieve this, the activities of the EBIOS method are used as follows:

EBIOS activities	Implementation for the purposes of writing a product ST
STEP 1 Context study	Summary: the context study is only based on the information required for writing a security target
1.1 – Study of the organisation	It may be useful to describe the organisations or types of organisation in which it is intended to use the security product, in order to define the environment assumptions. However, this activity is generally not used.
1.2 - Study of the target system	The emphasis is on collecting the information required for writing an ST: - presentation of the TOE and functional description, - list of essential elements, - list of assumptions, - list of security rules. The other elements of this activity should only be studied if they add to the list above.
1.3 - Determination of the security study target	This activity must be detailed and complete, although generally it is only the technical entities such as software, hardware and networks that are of interest.
STEP 2 Expression of security needs	Summary: the security needs are determined using a straightforward scale of needs
2.1 - Creation of needs sheets	The chosen security criteria, scale of needs and impacts must be straightforward, for example, by defining: - the three usual security criteria (availability, integrity and confidentiality), - possibly one or two impacts (essentially linked to the loss of reliability of the mechanisms), - a binary scale.
2.2 - Summary of the security needs	The summary of security needs can be produced directly without having to use individual security needs sheets.

EBIOS activities	Implementation for the purposes of writing a product ST
STEP 3 Study of threats	Summary: the threat study is detailed
3.1 - Study of threat sources	The activity must be detailed and complete. The attack methods and threat agents must be characterised with the greatest clarity and accuracy. The attack potential of each threat agent must be indicated, explained and justified. The justified list of non-retained attack methods must be produced.
3.2 - Study of vulnerabilities	The vulnerabilties can be taken from the EBIOS method knowledge bases, but other more technical and detailed baselines are generally used. Determining vulnerability levels is only useful for prioritising threats later in the study.
3.3 - Formalisation of the threats	This activity must be clear (for communication purposes) and accurate. It is preferable to formulate individual, uniform and specific threats (one vulnerability per threat) that conform to the existing protection profiles and ST.
STEP 4 Identification of the security objectives	Summary: the risks explain the consequences of the threats; residual risks should "disappear" by making changes to the context
4.1 - Comparison of threats with needs	The risks must be identified and formulated uniformly on the basis of the threat formulation. It may be possible to integrate these risks into the ST in place of threats (less precise concerning the consequences).
4.2 - Formalisation of the security objectives	Security objectives must be written in a clear, accurate and uniform manner so that they are justified by their content. They must be classified into two categories: - those concerning the TOE, - those concerning the TOE environment. Any identified residual risks must result in a change to the context (mainly during activity 1.2) so that none remain at this level of the study. There must be a detailed demonstration showing that the study elements are covered by the security objectives.
4.3 - Determination of the security levels	The security levels must be explicit and duly justified.

EBIOS activities	Implementation for the purposes of writing a product ST
STEP 5 Determination of security requirements	
5.1 - Determination of the security functional requirements	The security functional requirements should be taken from ISO 15408 or created according to the recommendations of the standard and refined so that the specifications are directly applicable. Any identified residual risks must result in a change to the context (mainly during activity 1.2) so that not a single risk remains at this level of the study. The security requirements must be classified into two categories: - those concerning the TOE, - if appropriate, those concerning the TOE environment. There must be a detailed demonstration showing that the security objectives are covered by the security functional requirements.
5.2 – Determination of security assurance requirements	The security assurance requirements should be taken from ISO 15408 or created according to the recommendations of the standard. The rationale behind the security assurance requirements must be detailed.

To summarise, the data used are as follows:



(for any additional information: ebios.dcssi@sgdn.pm.gouv.fr)