Education and Society, R. Aiken (ed.), Proc. 12th IFIP World Computer Congress 1992,
Information Processing 92, Vol. II, Elsevier Science Publishers B.V. (North-Holland), 1992

Information Technology Security Evaluation Criteria (ITSEC) – a Contribution to Vulnerability?

Michael Gehrke[a], Andreas Pfitzmann[b], and Kai Rannenberg[c]

[a]Institute for Applied Informatics, Sekr. FR 5-9, Technical University Berlin, Franklinstr. 28/29, W-1000 Berlin 10, Germany, E-Mail: micky@cs.tu-berlin.de

[b]Institute for Informatics, University Hildesheim, Samelsonplatz 1, W-3200 Hildesheim, Germany, E-Mail: pfitza@informatik.uni-hildesheim.de

[c]Institute for Applied Informatics, Sekr. FR 5-10, Technical University Berlin, Franklinstr. 28/29, W-1000 Berlin 10, Germany, E-Mail: kara@cs.tu-berlin.de

Abstract

On initiative of the Commission of the European Communities, the Information Technology Security Evaluation Criteria (ITSEC) are designed to provide a yardstick for the evaluation and certification of the security of IT systems. To improve the usefulness of resulting evaluations and certificates for procurers, users, and manufacturers the ITSEC are intended to undergo further extensive review. We discuss weaknesses, remaining questions, and possible improvements concerning the current version 1.2 of ITSEC. Our criticism focusses on the intended scope, the functionality aspects, the assessment of effectiveness and correctness, and problems arising after the evaluation of IT systems. Additionally, the ITSEC development and the accompanying discussion are criticized and improvements are proposed.

Keyword Codes: K.7.3; K.6.5; D.4.6

Keywords: The Computing Profession, Certification, and Licensing; Management of Computing and Information Systems, Security and Protection; Operating Systems, Security and Protection

1 INTRODUCTION

The information society becomes more and more dependent on information infrastructures like telephone or data exchange networks. This trend is advanced by the permanent technological development and growing power of computer equipment. New applications like multimedia systems, computer-based medical systems, or electronic mail increase the needs of flexible, powerful, and secure information exchange.

Two threats have to be pointed out. First, with the expansion of information technology (IT) the dependency of society on the reliable operation of this technology is rising. Secondly, increasing information flow enhances the possibilities for misuse, e.g., by eaves-dropping, modification of information, or information flow analysis. In the following, we understand "security" as the property of IT to withstand accidental and intentional threats. To increase the security of IT systems the ITSEC [CEC 1991_1] have been developed.

This paper deals with weaknesses, remaining questions, and possible improvements found during review of the current version of ITSEC. Its purpose is to stimulate the discussion about the intended scope, the functionality aspects, assurance of effectiveness and correctness, and post-evaluation problems of ITSEC. Sect. 2 gives a short overview over aims, history, and approach of ITSEC and discusses related evaluation criteria. Sect. 3 briefly summarizes former criticism. Sect. 4 treats additional weaknesses, remaining questions, and possible improvements of ITSEC, and Sect. 5 discusses possibilities for further development.

2 THE ITSEC

The ITSEC shall provide a yardstick to measure the security of IT and to make users confident thereof. They are harmonized evaluation criteria of and by four nations (France, Germany, the Netherlands, and the United Kingdom). The ITSEC ought to be used within an evaluation process resulting in a certificate stating the degree of confidence that can be placed in an IT product or system. This section gives an overview over the history and the approach of ITSEC.

2.1 History of ITSEC

The first version of ITSEC (V1.0) was published in May 1990 and was reviewed and discussed on an international conference with about 500 participants in Brussels in Sept. 1990. After the discussion V1.1 was published in Jan. 1991 together with a paper of the 4 nations working group answering to the major issues of the discussion. In April 1991 about 50 experts who contributed substantially to the review of V1.0 were invited to a second workshop. The current version (V1.2) was issued in June 1991 and is intended to be used in evaluation and certification for two years. The experience gained shall then be used to further develop ITSEC.

As is indicated by the participation of four countries in publishing ITSEC several documents preceded and provided input to the ITSEC. These documents are:

- Catal. de Crit. Dest. à évaluer le Degré de Confiance d. Syst. d'Info. [SCSSI 1989]
- UK Systems Security Confidence Levels [CESG 1989]
- DTI Commercial Computer Security Centre Evaluation Manual [DTI 1989_1]
- DTI Commercial Computer Security Centre Functionality Manual [DTI 1989_2]
- IT-Security Criteria (ZSISEC) [GISA 1989].

Additionally, the Netherlands contributed to ITSEC. The U.S. catalogue, the "Trusted Computer Systems Evaluation Criteria" (TCSEC) of the Department of Defense [US_DOD 1983, 1985], is a predecessor which influenced all documents above. Despite several similarities between different national evaluation criteria a couple of main differences can be extracted. For readers familiar with the above evaluation criteria the differences are compiled in Table 1.

Table 1: Evolution of Security Evaluation Criteria

	TCSEC	ZSISEC	ITSEC
Dates of Publication	1983/85	1989	1990/91
Security Approach	confidentiality	confidentiality + integrity + availability	confidentiality + integrity + availability
Functionality & Quality	linked	separated	separated
Classification	7 Functionality-Quality-levels (F-Q-levels)	8 Q-levels 10 F-classes as guidelines in the document	7 E-levels 10 example F-classes in the annex Recommended generic headings for own definition of F-classes
Certification Bodies	1	1	≥ 4
Evaluation Bodies	1 (certification body)	≥ 1	≥ 1
Bandwidth of Covert Channels	≤ 0.1 bit/s	≤ 1 bit/s	the annex specifies "not unacceptably high"

The harmonization of evaluation criteria by the four nations was generally applauded as a first step in the right direction. In 1990 the standardization project "Evaluation criteria for IT security" was initiated in ISO/IEC JTC1/SC27. The project consists of 3 subprojects "Introduction and model", "Functionality", and "Assurance". The ITSEC are expected to be the basis for this standardization project. This is obvious by a textual comparison of the current working draft of the "Assurance" document with chapter 3 and 4 and the description of "E-levels" in the ITSEC. Hence it is very important to stimulate discussion about weaknesses, open questions, and possible improvements of ITSEC.

2.2 The ITSEC Approach

The ITSEC shall be used as a guideline for evaluation and certification of the security of IT. "Security" in the ITSEC context means confidentiality, integrity, and availability. It is supposed that some threats to security can already be excluded by non IT measures like physical access control. Remaining threats are countered by IT measures which are the subject of evaluation.

Systems and Products: ITSEC differentiate between systems and products. A "system" is a combination of hard- and software tailored to the needs of a specific operational environment. A "product" is a piece of standard hard- and/or software that can be incorporated into systems. The main difference regarding security is: For a system the operational environment is known, for a product usually not. Systems and products are commonly referred to as "targets of evaluation" (TOEs).

Evaluation and Certification: The basis of an evaluation is the "security target" that consists of specific security objectives, threats, a definition of security enforcing functions, and all security mechanisms employed by a TOE. Additionally, the desired evaluation level is specified (see below). Security enforcing functions may be either specified individually or by referencing one of 10 predefined "functionality classes" [CEC 1991_1, Annex A]. If security enforcing functions are individually specified it is recommended to present them under the following "generic headings":

(1) Identification and Authentication
(2) Access Control
(3) Accountability
(4) Audit
(5) Object Reuse
(6) Accuracy
(7) Reliability of Service
(8) Data Exchange

The sponsor of an evaluation provides the security target together with the TOE to an independent evaluator and pays the evaluation. The main task of evaluation is to give assurance that the security objectives are achieved by the selected security enforcing functions.

Assurance is divided into confidence in the "correctness" of the implementation of security enforcing functions and mechanisms and confidence in their "effectiveness". Thus, evaluation has two phases that may proceed interleaved.

1) Assessment of Correctness: The TOE lifecycle for the security enforcing functions from their top-level specification down to operation including the development process is investigated. The result is a (preliminary) evaluation level between E0 ("no confidence") and E6 ("highest confidence").

2) Assessment of Effectiveness: It is checked whether the security enforcing functions satisfy the security objectives. Additionally, assessment of effectiveness deals with the strength of mechanisms of the TOE. Three strength ratings classify mechanisms: "basic", "medium", and "high". If during assessment of effectiveness the security enforcing functions turn out not to satisfy the security objectives the whole TOE is degraded to evaluation level E0.

As result of the evaluation the evaluator forwards a report to the national certification authority, which will provide a certificate to the sponsor at least stating the evaluation level reached.

3 SUMMARY OF FORMER CRITICISMS ON ITSEC

This section summarizes criticism already published and hence not repeated in detail.

3.1 Criticism by Karl Rihaczek

Karl Rihaczek [Rihaczek 1991] pointed out that standardization of evaluation criteria despite all advantages has the drawback that manufacturers will try to adhere to a standard because of marketing reasons. Vulnerabilities that are not covered by the criteria could be detected and systematically exploited by an attacker. This would be especially severe after the evaluation criteria gave rise to a security monoculture. He criticizes that ITSEC mainly takes into account closed systems where the interests of a system's management dominate over interests of single users. He states that non-repudiation, which can be seen as a fourth basic security property at the side of confidentiality, integrity, and availability, is not really covered. This makes ITSEC unsuitable for Open Systems. Moreover, he raises the question of the legal relevance of evaluation certificates. Although [Rihaczek 1991] is related to ITSEC V1.0, at the level of its treatment, all critical remarks remain true for V1.2.

3.2 Criticism by Rüdiger Dierstein

Although Rüdiger Dierstein does not mention ITSEC at all (since [Dierstein 1990] has been written before the first publication of ITSEC), this is an implicit, but especially severe criticism. He derives six functions as a possible set of basic security functions:

(1) Authentication (identification and verification)

(2) Administration of rights (assignment of rights and administration of rights)

(3) Verification of rights (= control of rights = control of authorization)

(4) Registration (protocolling for audit and recovery)

(5) Error Recovery (error detection and error compensation)

(6) Supervision (recursive application of the above).

This means at least two kinds of criticsm: Basic functions are *derived* (and not just stated) and his set differs from the corresponding set of ITSEC, i.e., the generic headings, cf. Sect. 4.2.

4 OUR ADDITIONAL CRITICISM ON ITSEC

This section summarizes our criticism on ITSEC V1.2. The first 4 subsections are oriented along the structure of the ITSEC dealing with the title and scope (4.1), the functionality aspects (4.2), and the two aspects of assurance – effectiveness (4.3) and correctness (4.4). Post-evaluation problems are addressed in 4.5, weaknesses of the ITSEC development and discussion process in 4.6. More detailed criticism [Pfitzmann 1991] can be obtained from the authors.

4.1 Title and Scope

The ITSEC do not address the scope suggested by their title and their scope section and needed in an information society. They tend to define a criteria framework and they do not take into account different kinds of potential attackers and decentrally managed IT systems. Moreover, the definitions of confidentiality and integrity are insufficient. An appropriate title for V1.2 of ITSEC might be: *A Framework of Security Evaluation Criteria for hierarchically managed IT Systems*.

Criteria or Criteria Framework? During the revisions the criteria became more and more general: ITSEC V1.2 are even less security evaluation criteria than V1.0. They define a *framework* to formulate security evaluation criteria, as the sponsors can define the functionality of their TOEs by themselves. This is less obligatory than criteria would be.

Different Kinds of Potential Attackers: The ITSEC do not cover problems of different kinds of potential attackers. This is obvious by reading, e.g., §2.37 of ITSEC V1.2 (p. 25):

> *In many TOEs there will be requirements to ensure that users and processes acting on their behalf are prevented from gaining access to information or resources that they are not authorised to access or have no need to access. Similarly, there will be requirements concerning the unauthorised creation or amendment (including deletion) of information.*

There and in the following two paragraphs on access control only "users" are mentioned. Not only users, but also designers, manufacturers, and operators can cause threats to a system (the same has to be considered for development tools, too). Additionally, even in centrally managed systems a difference has to be made between potential attackers of different parts of the TOE.

Especially risks caused by the operator of the system are not considered or are not considered any longer. An example is §E4.35 of ITSEC V1.2 or V1.1 in comparison with the associated paragraph in V1.0 (p. 62): "Unrecognized loss of functionality of the security functions" caused by errors of the system operator is treated in V1.0 but left out in V1.1 and V1.2.

Decentrally Managed IT Systems: The ITSEC do not address *decentrally managed* IT systems, i.e., connected IT systems with multiple administrations with potentially conflicting interests. There are at least two deficits which show that decentrally managed IT systems are not covered: Different kinds of attackers are not covered (cf. Sect. 4.1); the aspect "Non-repudiation" is neglected. Reference to "Non-repudiation" under the generic heading "Data Exchange" is by far not enough and raises problems of systematics (cf. Sect. 3.1 and Sect. 4.2).

Definitions of Confidentiality and Integrity: These definitions are insufficient for 2 reasons:

(1) The best – and at least against strong attackers in today's systems, only – way to keep information confidential in a provable way is to avoid that it can be gathered. In theory nearly any application can be realized that way [Chaum 1990 and references there] and in practice many essential applications can, e.g., communication networks, payment systems, authorization systems or value exchange systems [Chaum 1985; Pfitzmann, Pfitzmann, Waidner 1991; Bürk, Pfitzmann 1990].

(2) In distributed systems one cannot prevent unauthorized modification of data, e.g., in transit on a network, but one can detect unauthorized modification with cryptographical means.

Therefore, the following definitions (changes in italics) are proposed:

confidentiality	prevention of the unauthorized disclosure of information*, or, if possible, avoidance of unnecessary information*.
integrity	prevention of *undetected* unauthorized modification of information.

Additionally, the changed definition of integrity provides for a cleaner separation of integrity and availability. Without that change, unauthorized overwriting of data would be both an integrity and availability violation. Changing the definition of integrity makes integrity correspond to the well established notion of *partial correctness* in program verification, and integrity and availability together correspond to the well established notion *total correctness*.

4.2 Functionality

The ITSEC divide the functionality aspects of secure systems in two levels of abstraction – generic headings and functionality classes – but do not treat the aspects of user protection in IT systems. The generic headings do not give an adequate structure to the issue of computer security. The example functionality classes cover a smaller range than they seem to do at first sight.

Protection of Users in Communication Systems: Neither the generic headings nor the proposed functionality classes give guidance for the adequate classification and certification of TOEs which provide anonymity, pseudonymity, and freeness from observability to their users [Chaum 1985; Pfitzmann, Pfitzmann, Waidner 1991; Bürk, Pfitzmann 1990]. ITSEC V1.2 do not give any help for evaluation and certification of TOEs which work without the need or enforcement of any gathering of unnecessary person-related information. TOEs which protect users by keeping their data confidential can only be classified by negating the generic headings. The same is true for TOEs which protect usees by making them users operating their own individual computers [Chaum 1985] ("Usees" are people, whose data "users" are working with, potentially putting them at risk). So the ITSEC seem to be focussed neither on the issues of the users nor of the usees.

Generic Headings: The 8 generic headings for the security enforcing functions are incomplete and unsystematic. They are incomplete as essential counterparts to the given classes are missing. For some services, *Identification* and *Authentication* are wanted, for other services, one needs the corresponding counterparts *Anonymity* and *Pseudonymity*, cf. [Chaum 1985]. The same relationship exists between *Audit* and its counterpart *Freeness from observability*.

The generic headings are unsystematic as "Data Exchange" is no generic heading at the same level of abstraction as the other 7 generic headings given, e.g., there is no generic heading "Data Storage". The unsystematic approach is obvious as "Authentication" and "Access Control" which are subissues to "Data Exchange" are issues treated as generic headings as well. Assigning to that eighth generic heading such important aspects as non-repudiation makes this unsystematic approach even worse, cf. Sect. 3.1.

The Example Functionality Classes: The 10 example functionality classes leave out the aspects of anonymity, pseudonymity, and unobservability and so give the false impression every relevant security problem is covered. Even the possibility to define additional functionality classes does not solve the following problem: Without guidance by the ITSEC themselves users, customers, and procurers will not be supported in specifying their security needs.

4.3 Assurance of Effectiveness

The effectiveness of security functions is strongly dependent on the strength of the mechanisms used. Therefore a well-contrived scale to classify mechanisms according to their strength has to exist. Additionally, for an international rating of security mechanisms to be objective, algorithms should be published. If they are secret this should become distinct in the rating. Third, determinations of acceptable bandwidths of covert channels are missing.

Strength of Mechanisms: "Beyond normal practicality" as the highest rating for the strength of mechanisms is too low. This is a trivial condition and only suited to characterize *basic* and not at all *high*. The highest rating has to be called, e.g., "unbreakable". One gets it from the highest rating in [GISA 1989], "virtually unbreakable", which "prevents all violations of the security policy and according to the present state of the art it is practically impossible to overcome. […]". Omitting "according to […] art" results in a time-independent definition for "unbreakable". Examples of mechanisms rated "unbreakable" are the one-time pad [Shannon 1949] or information-theoretic authentication codes [Simmons 1988].

The discrimination between strengths of mechanisms in only three ratings (basic, medium, or high) is very poor and not adequate. There must be more ratings, see, e.g., [GISA 1989] for more ratings and good definitions. Few ratings imply relatively big rounding errors which stimulates subjectivity. With many classes one can handle the problem of subjectivity by giving one class as expectation and two further classes as an upper and lower bound. This accords with confidence intervals which have a good tradition in engineering.

Public Discussion of Cryptographic Mechanisms: Opposed to ITSEC V1.2 §3.23 (p. 39) and §E6.32 (p. 106), the rating of cryptographic mechanisms has to be international and as objective and reproducible as possible. An open and international discussion increases the probability to detect possible weaknesses in an algorithm. It requires that all mechanisms be published in any detail. Any secret mechanisms are not suitable for certified secure systems. This has to be stated in the rating of cryptographic mechanisms to avoid national attitudes to employ secret cryptographic mechanisms.

Covert Channels: The use of covert channels can circumvent every security policy dealing with confidentiality and therefore has to be considered as an aspect of effectiveness. It is also an aspect of the correctness as Covert Channels can be introduced into a system during the implementation. Neither in the Chapters 0-6 of ITSEC, nor in the proposed functionality classes, there are limits imposed on the bandwidth of covert channels. Compared with [US_DOD 1983, 1985] and [GISA 1989] this is a large step backward.

To protect people from risks caused by information leaks the highest security class has to restrict the bandwidth of all covert channels together well below $4 \cdot 10^{-10}$ bit/s as the following example shows: One can imagine a database including information on the attribute "AIDS, yes or no". This bit of information has to be kept secret for the lifetime of the patient, e.g., 80 years. This yields an upper bound of the bandwidth of 1/80 bit/year $\approx 4 \cdot 10^{-10}$ bit/s. An acceptable bandwidth should be considerably lower.

The very least is that higher evaluation levels require a determination of the bandwidth of covert channels. It is then for the accreditor or procurer of a TOE to decide whether the possible bandwidth is acceptable or not. If the ITSEC do not require to evaluate this bandwidth for, e.g., products, many procurers will have to do that which is a multiplication of effort.

4.4 Assurance of Correctness

Considering the vulnerability of software development tools through, e.g., Trojan Horses six evaluation levels are not enough. Further on the current definition of E4 might restrict the evaluation of all TOEs of the near future to only three levels.

Evaluation Levels beyond E6 – Consideration of Tools: As in [GISA 1989], it must be stated clearly that evaluation levels beyond E6 are possible, very desirable, and might be defined in the future. One reason for this is the existence of transitive Trojan Horses [Thompson 1984]. Examples for evaluation levels beyond E6 are E7 (Verified design history of all tools used to develop the TOE) and E8 (Verified design history of all tools used to develop tools used to develop the TOE). The ultimate level would require verified design for all used tools (recursive definition!), i.e., one needs some form of secure bootstrap in generating these tools.

Even if the suggested levels E7 and E8 might be not achievable considering today's "state of the art" [CEC 1991_2] criteria should define or at least mention possible targets. What the criteria makers believe to be "the state of the art" might be more a matter of expense than "art". Even if it was "art" hopefully the "state of the art" emerges faster than (hopefully stable) criteria. Not mentioning what some users of ITSEC might desire because it is deemed not to be "state of the art" is very dangerous as it gives them a false impression of security.

TOEs without Formal Specification: A formal security policy for *all* aspects of security has to exist for the levels E4 and above (§E4.2 ITSEC). This is a major (at least short term) weakness of ITSEC because at present only 3 evaluation levels are possible for nearly all relevant TOEs (the argument of Sect. 4.3 that 3 ratings are much too less applies).

4.5 Post-Evaluation Problems

Evaluation and certification of TOEs do not stay valid forever and evaluated TOEs are going to be connected. This subsection addresses the problems after a TOE has been evaluated.

Re-Rating and Re-Evaluation: The re-rating and re-evaluation have to be harmonized internationally. The current document presents no concept to solve this problem. Reference to national certification bodies or a statement that this task is "beyond the scope of these criteria" as stated in §1.34 of V1.2 is a bad excuse for not addressing that issue.

Security Flaws in Certified Products: There are no concepts in the ITSEC, what shall happen if someone discovers – and possibly publishes – a security flaw allowing a break of security for a certified TOE. Maybe the certificate becomes invalid by discovery of a security flaw but there are no concepts to inform all users (not to speak about usees) of the TOE.

Rating of TOEs consisting of Evaluated Components: Evaluated TOEs often are not used stand-alone. An example is the connection of two computers by a network. ITSEC do not contain concepts what functionality class and evaluation level should be assigned to systems consisting of evaluated TOEs. Is in this case a complete, partial, or no re-evaluation required?

4.6 Development and Discussion of the ITSEC

The organization of ITSEC development and discussion must be improved to enable a public review and a constructive scientific discussion adequate to a project of this size and importance.

Need for a Rationale: To stimulate a constructive discussion it is not enough to publish the criteria themselves, but necessary to publish a detailed rationale, e.g., all options and suggestions and the reasons for their selection. This has been asked for unanimously at VIS'91, an international scientific conference on dependable computer systems organized by the GI (German IFIP Full Member) in March 1991 [Rannenberg 1991]. [CEC 1991_2] and its predecessor are only a first step as they do not contain all critical points and give very few answers.

Avoidance of Critical Points: The comparison between ITSEC V1.1 and V1.2 gives the impression that critical points are neither discussed nor clarified but left out in the course of the document's development. Examples are:

§4.24 in V1.1 was criticized because it did not cover the need for configuration control for tools to ensure that insecure functionality is not added. As a result in V1.2 the aspect of additional insecure functionality vanished from §4.24.

§E6.5 and §E6.11 in V1.1 were criticized as the vulnerability analysis mentioned there covered the circumvention of the security of a TOE only with respect to users and left out the risks caused by operators and designers. As a result in V1.2 the vulnerability analysis is not mentioned any longer.

Risks caused by the operators are left out since V1.1 of ITSEC (see Sect. 4.1).

5 CONCLUSIONS

The ITSEC and their use could both increase and decrease the vulnerability of society. Vulnerability increases if the ITSEC are used by unexperienced persons as certain threats are ignored without any documentation of this fact. An example are the recommended generic headings in combination with the 10 example functionality classes derived from the ZSISEC [GISA 1989] which can give the false impression every security issue is covered. A decrease of vulnerability caused by ITSEC is only possible if experienced people knowing the weaknesses of ITSEC use the criteria. Besides this aspect the criteria amplify the trend to systems which need a centralized and trusted instance sometimes called "big brother systems“.

At least the following measures are needed to make ITSEC a real contribution to security instead of vulnerability.

(1) The title and the scope section have to be narrowed or much more and much broader work is required. In any case, it does not help to re-define "evaluation criteria" in a way that the ITSEC title becomes correct.

(2) Functionality classes useful for a democratic society must be developed. They have to reflect the complex relations between the individual, the society, and the state, i.e., they must consider citizens rights on data protection and privacy in general and on unobservable communication in particular. The definition of functionality classes by independent bodies has to be sponsored to promote the consideration of human rights.

(3) The problems and risks of computer aided software engineering (CASE) have to be considered in the field of assurance. Especially the risks of transitive Trojan Horses in CASE tools, e.g., editors and compilers should be treated.

(4) A complete and detailed synopsis of the criticism and a rationale for the reaction to it have to be published.

(5) The criteria have to be tested by IT users in public administrations needing open systems.

(6) Only cryptographic mechanisms whose complete construction and design decisions are internationally known and discussed are eligible for high ratings.

The development process of the criteria, also in the standardization has to be organized publicly and openly and with a public rationale. The process must empower the issues of "usees" who normally lack the ability to appear for their interests. During the classical ISO standardization process "usee" representatives must be sponsored to visit *and* prepare the meetings.

Further on, concepts for at least the following problems are needed additionally to the ITSEC:

(1) TOEs must be re-evaluated continuously, e.g., to cover new arising threats.

(2) The evaluation and certification instances have to be evaluated, too. If many instances will evaluate and certificate TOEs a common basis for the legitimation and evaluation of these instances is needed.

(3) The public and international rating of cryptographic mechanisms has to be *organized* internationally.

6 REFERENCES

[Bürk, Pfitzmann 1990] Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721

[CEC 1991_1] (Informal) EC advisory group SOG-IS: Information Technology Security Evaluation Criteria (ITSEC) – Provisional Harmonised Criteria; Version 1.2, 28 June 1991, 163 pages (obtainable free of charge from CEC; Directorate XIII/F; SOG-IS Secretariat; Rue de la Loi, 200; B-1049 Brussels; Belgium)

[CEC 1991_2] (Informal) EC advisory group SOG-IS: ITSEC V1.1 Revision: Adressing the Main Issues, June 1991, 9 pages (obtainable free of charge like [CEC 1991_1])

[CESG 1989] UK Systems Security Confidence Levels, CESG Memorandum No.3, Communications-Electronics Security Group, United Kingdom, January 1989

[Chaum 1985] David Chaum, Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044

[Chaum 1990] David Chaum: The Spymasters double-agent problem: Multiparty computations secure unconditionally from minorities and cryptographically from majorities; Crypto '89, LNCS 435, Springer-Verlag, Heidelberg 1990, 591-602

[Dierstein 1990] Rüdiger Dierstein: The Concept of Secure Information Processing Systems and their Basic Functions; IFIP/Sec'90, Helsinki, May 1990; North-Holland; Amsterdam 1990

[DTI 1989_1] DTI Commercial Computer Security Centre Evaluation Manual, V22; DTI, UK, February 1989

[DTI 1989_2] DTI Commercial Computer Security Centre Functionality Manual, V21; DTI, UK, February 1989

[GISA 1989] IT-Security Criteria, Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems, ISBN 3-88784-200-6, German Information Security Agency, FR of Germany, January 1989

[Pfitzmann 1991] Andreas Pfitzmann: Statement of Observations concerning the Information Technology Security Evaluation Criteria (ITSEC) Version 1.2, 28 June 1991; Institut für Informatik, University of Hildesheim, Germany, November 29, 1991

[Pfitzmann, Pfitzmann, Waidner 1991] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes – Untraceable Communication with very small Bandwidth Overhead; Proc. IFIP/Sec'91, Brighton, UK, May 1991; North-Holland; Amsterdam 1991; 245-258

[Rannenberg 1991] Kai Rannenberg: VIS'91: IT-Sicherheit – Bewertungskriterien; Computer & Recht 7/11 (1991) 699-701

[Rihaczek 1991] Karl Rihaczek: The Harmonized ITSEC Evaluation Criteria; Comp. & Sec. 10 (1991) 101-110

[SCSSI 1989] Catalogue de Critères Destinés à évaluer le Degré de Confiance des Systèmes d'Information, 692/SGDN/DISSI/SCSSI, Service Central de la Sécurité des Systèmes d'Information, Juillet 1989.

[Shannon 1949] Claude E. Shannon, Communication Theory of Secrecy Systems; The Bell System Technical Journal 28/4 (1949) 656-715

[Simmons 1988] G. J. Simmons, A Survey of Information Authentication; Proc. IEEE 76/5 (1988) 603-620

[Thompson 1984] Ken Thompson, Reflections on Trusting Trust; CACM 27/8 (1984) 761-763

[US_DOD 1983, 1985] DoD Standard: Department of Defense Trusted Computer System Evaluation Criteria; December 1985, DOD 5200.28-STD, Supersedes CSC-STD-001-83, dtd 15 Aug 83, Library No. S225,711