Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, April 23rd, 2014

No. 1690 /ANSSI/SDE/PSS/CCN

Reference: ANSSI-CSPN-NOTE-01/2

APPLICATION NOTE

METHODOLOGY FOR EVALUATION FOR A FIRST LEVEL SECURITY CERTIFICATION - ETR CONTENT

Application : As soon as approved.

Circulation : Public.

COURTESY TRANSLATION

Version history

Edition	Date	Modifications
Experimental phase	January 30th, 2008	First edition for the experimental phase, repealed by this procedure.
1	May 30th, 2011	End of the experimental phase. Change in name for the certification body (ANSSI) and editorial improvements.
2	April 23rd, 2014	Modification of a document classification domain: change from an instruction to an application note. Removal of the redundancies in relation to [CRITERIA]. Establishment of conformity in relation to the procedure ANSSI-CSPN-CER-P-01.

This application note is available online on the ANSSI's institutional website (www.ssi.gouv.fr).

TABLE OF CONTENTS

1 Subject of the application note

This application note sets the information expected in the first level security certification (CSPN) evaluation technical reports (ETR). It provides a complement to the description of the CSPN evaluation criteria described by [CRITERIA].

This methodology may be refined according to the type of product to be evaluated. In this case, the specific methodology must be used.

2 Introduction

The evaluation of a product must check that it provides the security functions indicated in its security target, that all the security functions reach at least an "elementary" intrinsic resistance level and that no vulnerability may be exploited during the evaluation. This final conclusion must be taken with all due care in the field of information technology security. In fact, it is impossible to guarantee that there will be no exploitable vulnerabilities in the product.

3 Evaluation technical report identification

Evaluation project name	Unique identifier provided by the ANSSI
ETR reference	Unique identifier provided by the ITSEF
Author	Name of the expert(s) involved in carrying out the analysis
Approver	Name of the technical inspector
ETR creation date	ETR creation date
ETR update date	ETR update date
ETR version No.	
Miscellaneous	Free text

4 Evaluated product identification

Editor's name	
Product name	Commercial name
Analysed version No.	Exact No. (version, release)
Any corrections applied	
CSPN technical domain	
Miscellaneous	

5 Functionalities, usage and security environment

To have a reference base to guide the security analyses, the evaluator must first carry out the following tasks:

- Analyse the available documentation;
- Identify the requirements in terms of test platforms.

The evaluator must then fill in the following chapters in the ETR.

5.1 Product specification of need

This responds to three questions:

- For which use has the product been developed?
- Which threats relate to the sensitive assets handled by the product?
- Which security functions enable the identified threats to be countered?

5.2 Typical users

This involves describing the typical users of the analysed product, for example:

- General public user: no specific IT skills;
- Experienced user: knowledge of the main IT concepts;
- Administrator: fine knowledge of the main IT and network concepts, ability to configure and administer a park of computers connected as a network;
- Expert: expert in the product domain (typically, the evaluator).

5.3 Typical usage environment / Product argument

This involves identifying:

- How the product is planned to be used;
- The environment planned for its use and the supposed threats in this environment.

The evaluator must provide a summary of the product's security characteristics and define all the identifiable hypotheses concerning the environment and how the product will be used. This includes the logical, physical and organisational security measures related to the personnel and information technology (IT) required to support the product, as well as the product's dependencies in relation to hardware, software and/or microprograms which are not supplied with the product.

A description of the typical information system architecture in which the product is normally used may be provided if it can be identified.

5.4 Functional description of the product

This involves describing the product's security functions.

5.5 Inventory of the security functions identified

The security functions identified must be described and classified by functionality in the following table.

Key: - Function exists in the product:

- Yes (Y) ;
- No (N);
- Information not available (NA);
- Not applicable (N/A);

- Critical nature of the function for the product:

- Critical (C);
- Important (I);
- Optional (O).

The following table specifies in italics the meanings of the titles proposed for the security functions.

Title	**Existence (Y / N / NA / N/A)**	**Criticality for the product (C / I / O)**	**Description and comment on the security function**
Security audit			
Alarm management			*Measures taken if events indicating a potential security violation are detected.*
Security log			*Record of the occurrences of events which affect security.*
Intrusion detection			*Automated resources which analyse the system's activity and the audit data, searching for possible or actual security violations.*
Audit log review			*Audit tools which should be provided to authorised users to help them review audit data.*
Audit log selection			*Defines the requirements to include or exclude events from all the events that may be audited.*
Audit log storage			*Ability to create and maintain a secure audit trace.*
Communication			
Non repudiation of origin			*Guarantees that the person who sends information cannot deny having sent it.*
Non repudiation of reception			*Guarantees that the person who receives information cannot deny having received it.*
Cryptographic support			
Key management			*Cryptographic key generation, distribution, access and destruction.*
Cryptographic operation			*Typical cryptographic operations (data encryption or decryption, digital signature generation or verification, cryptographic message integrity code generation for integrity requirements or to verify an integrity code, secured chopping, cryptographic key encryption or decryption and cryptographic key negotiation).*
User data protection			
Access control policy			
Access control functions			
User data authentication			
Export outside the evaluation scope			*Functions to certify that the security attributes and the user data protection may be either explicitly preserved, or be ignored, after it has been exported.*
Data flow control policy			
Data flow control functions			
Import from a zone outside the evaluation scope			
Transfer within the evaluation scope			
Temporary data deletion			*Need to guarantee that the information destroyed will no longer be accessible and that the objects which have just been created do not contain any information which should not be accessible.*
Stored data confidentiality and integrity			

Title	**Existence (Y / N / NA / N/A)**	**Criticality for the product (C / I / O)**	**Description and comment on the security function**
User traffic confidentiality and integrity			
User data integrity during an internal flow			
Identification and authentication			
Authentication failure management			*Function to define parameters for a certain number of unsuccessful authentication attempts and the product actions in the event of failed authentication attempts.*
User attribute definition			*User security attributes other than their identity.*
Password generation			
Authentication mechanisms			
Identification mechanisms			
Security management			
Security function administration			*Functions that enable authorised users to control the administration of security functions.*
Security attribute administration			*Functions that enable authorised users to control the administration of security attributes.*
Security data administration			*Functions that enable authorised users to control the administration of security data.*
Revocation/ compromise of secret elements			
User profile management			*Assignment of different roles to users.*
Privacy protection			
Anonymity			*Guarantees that a user may use a resource or service without revealing their user identity.*
Possibility of acting under a pseudonym.			*Guarantees that a user may use a resource or service without revealing their user identity, but may still need to respond for this use.*
Impossibility of establishing a link			*Guarantees that a user may use resources or services several times without other people being able to establish a link between these uses.*
Non-observability			*Guarantees that a user may use a resource or service without other people, in particular third parties, being able to see that the resource or service is being used.*
Product security function protection			
High availability			
Exported data protection (availability, integrity, confidentiality)			
Physical product protection			*Functions to restrict unauthorised physical accesses to the product and prevent unauthorised physical modification or a product substitution.*
Breakdown management and recovery after incident			
Replay detection			

Title	Existence (Y / N / NA / N/A)	Criticality for the product (C / I / O)	Description and comment on the security function
Time and date stamping			
Self-tests			*Detect the alteration of the product's executable code and data due to various failures which do not necessary generate a stoppage in its operation.*
Use of resources			
Tolerance to breakdowns			*Function that enables degraded mode.*
Quota/quality of service management			
Access to the evaluation scope			
User session management			*Limit on the number of parallel sessions, access history, session locking, etc.*

6 Product installation

The content expected is detailed in the "Evaluator's tasks" section in paragraph 4.2 in instruction ANSSI-CSPN-CER-I.02 (see [CRITERIA]).

The information must be entered in the sub-chapters that deal with the following points:

- Specific environment configuration features;
- Installation options retained for the product;
- Description of the installation and any non-conformities;
- Installation time;
- Notes and various remarks.

7 Conformity analysis

7.1 Documentation analysis

The content expected is detailed in the "Evaluator's tasks" section in paragraph 4.3 in instruction ANSSI-CSPN-CER-I.02 (see [CRITERIA]).

7.2 Source code review (if available)

The content expected is detailed in the "Evaluator's tasks" section in paragraph 4.4 in instruction ANSSI-CSPN-CER-I.02 (see [CRITERIA]).

7.3 Functionalities tested

The content expected is detailed in the "Evaluator's tasks" section in paragraph 4.5 in instruction ANSSI-CSPN-CER-I.02 (see [CRITERIA]).

For each analysed function, the evaluator fills in a "Conformity analysis" sheet (see Appendix). These sheets must be provided as appendices to the ETR. The evaluator only indicates the references to these sheets at this point.

7.3.1 Summary of the functions tested / not tested and non-conformities

7.3.2 Expert opinion on the product

7.3.3 Duration of the analysis

7.3.4 Notes and various remarks

8 Analysis of the resistance of functions and mechanisms

The objective is to have an expert opinion on the functions' theoretical resistance, according to the attacker's resources.

The content expected is detailed in the "Evaluator's tasks" section in paragraph 4.6 in instruction ANSSI-CSPN-CER-I.02 (see [CRITERIA]).

8.1 List of mechanisms and scoring for their resistance

8.2 Expert opinion on the mechanisms' resistance

8.3 Duration of the analysis

8.4 Notes and various remarks

9 Analysis of the vulnerabilities (intrinsic, construction, exploitation, etc.)

The content expected is detailed in the "Evaluator's tasks" section in paragraph 4.7 in instruction ANSSI-CSPN-CER-I.02 (see [CRITERIA]).

9.1 List of known or potential vulnerabilities in the sub-category

9.2 List of vulnerabilities actually tested

If specific tools or methodologies are needed to exploit the vulnerability, they will be described. If third party tools are required, they will be delivered with the product if they are rights-free (freeware or software developed to order as part of the contract).

Examples of standard vulnerabilities:

- The mechanisms may be robust in principle but be poorly implemented;
- The software architecture itself may encourage attacks;
- There may be hidden channels introduced intentionally or not;
- Certain implementations do not prevent keys being swapped on the disk;
- Certain implementations do not erase the files securely.

9.3 List of vulnerabilities discovered during the analysis and not known to the bases used

9.4 Expert opinion on the vulnerabilities

9.5 Duration of the analysis

9.6 Notes and various remarks

10 Analysis of the vulnerabilities induced into the host system (if applicable).

The objective is to have an expert opinion on the impact of installing the product on the host system's security, according to the attacker's resources, when this installation requires specific privileges on the host system.

The content expected is detailed in the "Evaluator's tasks" section in paragraph 4.8 in instruction ANSSI-CSPN-CER-I.02 (see [CRITERIA]).

11 Ease of use analysis

The content expected is detailed in the "Evaluator's tasks" section in paragraph 4.9 in instruction ANSSI-CSPN-CER-I.02 (see [CRITERIA]).

The ETR will indicate the cases where the product's security may be called into question in certain product user modes or configurations. In this case, if such an option exists, a configuration must be recommended which enables the best level of security to be achieved to counter the identified threats. A reduction in the product's functional scope (in terms of security) may be proposed.

11.1 Case where security is called into question

11.2 Recommendations for secure use of the product

11.3 Expert opinion on the ease of use

11.4 Notes and various remarks

12 Meetings with the developers

This task is optional.

12.1 Result of the interviews

The expert in charge of the analysis indicates the elements which they feel are useful to mention for the reader.

12.2 Opinion on the developer

The content expected is detailed in the "Evaluator's tasks" section in paragraph 4.10 in instruction ANSSI-CSPN-CER-I.02 (see [CRITERIA]).

13 Cryptography evaluation (if the product implements cryptographic mechanisms)

The content expected is detailed in the "Evaluator's tasks" section in paragraph 4.11 in instruction ANSSI-CSPN-CER-I.02 (see [CRITERIA]).

14 Summary

Here the evaluator provides an expert opinion which summarises the results of the previous tasks for a technical reader.

15 References

[CEM] : *Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, current version.

[RGS_B] : General security reference base, appendix B:

[RGS_B1]: Rules and recommendations concerning the choice and dimensioning of cryptographic mechanisms.

[RGS_B2]: Rules and recommendations concerning the management of the keys used in cryptographic mechanisms.

[RGS_B3]: Rules and recommendations concerning authentication mechanisms.

[CRITERIA]: Criteria for evaluation for first level security certification, reference ANSSI-CSPN-CER-I-02, current version.

APPENDIX

Security function conformity analysis sheet template

Blank sheet

Objective of the analysis:	*Product reference*	
Security function:	*Sheet ref.*	*Author*
	Subject of the test:	
Test scenario:		
Operations to be carried out	**Expected results**	**Observed results**
Conclusion:		

Example

Objective of the analysis:	PPP software version 3.5	
Security function: IP filtering	Ref. : Test-PPP-1	Author: XXXXX
	Subject of the test: A firewall should drop all traffic which is not explicitly authorised. This test checks that the *PPP* software is in this case.	
Test scenario: machine just installed		
Operations to be carried out	**Expected results**	**Observed results**
Deactivate the default replay rule and scan the internal network with, for example netwox 67 --ips 10.2.0.1-10.2.0.2 --ports 20-55 for TCP and the same thing for UDP with command No. 69. Reactivate the rule.	No TCP connection succeeds. For UDP, only port 53 must be accessible.	The TCP scan declares all the attempts in "timeout" except for the authorised port which corresponds to SMTP. The UDP scan declares "timeout" for everything including port 53 which corresponds to the DNS, which is unexpected.
Conclusion:		
Results ok, the replay of the UDP packet to port 53 was due, according to the firewall log, to the fact that it is not a correct DNS packet.		