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 30th, 2014

No. 1760 /ANSSI/SDE/PSS/CCN

Reference: ANSSI-CSPN-NOTE-02/1.0

APPLICATION NOTE

METHODOLOGY FOR THE SOFTWARE EVALUATION OF SET-TOP BOX FOR FIRST LEVEL SECURITY CERTIFICATION

Application : As soon as approved.

Circulation : Public.

COURTESY TRANSLATION

Version history

Editions	Date	Modifications
1.0	April 30th, 2014	Creation of the document in the context of the SEMS working group, from the documents [CDS-STB] and the evaluation methodology for CSPN [MET_CSPN]. Acknowledgement of pilot evaluations.

Pursuant to decree No. 2002-535 of 18th April 2002, this procedure has been submitted to the certification management committee, which delivered a favourable opinion.

This instruction is available online at the ANSSI's institutional website (www.ssi.gouv.fr).

Acknowledgements

This methodology was produced by the work of the members of the SEMS (*Security Evaluation Methodology for Set top boxes*) group based on a document drafted by Sogeti for Canal +.

The following bodies were involved in drafting this document:

- Amossys;
- Bouygues Telecom;
- Canal +;
- GIE-CB;
- Orange;
- Sagemcom;
- Sogeti;
- Thales (TCS – CNES);
- Viaccess.

TABLE OF CONTENTS

1. Introduction

1.1. Definitions

Chipset	Integrated circuit which manages the data flow between the processor, the memory and the peripherals.
Conditional Access System (CAS)	Security system used to limit access to Service content to authorised subscribers.
Control Word (CW)	Service content encryption key
Digital Right Management (DRM)	Technical measures to control the use made of digital work.
Personal Video Recorder (PVR)	System used to record video, such as a digital video recorder.
Service	Group of channels.
Connected service	Service available for the subscriber from their Terminal and requiring the connection of the terminal to a remote server which provides the services.
Catch-up television (*Catch-up TV*)	Service which provides a subscriber with the possibility of watching a programme after it is first broadcast over a fixed period.
Set top box (STB)	Hardware and software system to receive, unscramble, decode and send to viewing/sound equipment the content distributed over a platform.
Video on demand (VOD)	Possibility of viewing a service's programme after its broadcast, generally by downloading content from a server (*Pull VoD*).

1.2. Subject of the note and products targeted

This application note describes the software security evaluation method for a digital reception terminal (STB – *Set Top Box*) in the context of first level security certification (CSPN, Certification de sécurité de premier niveau). This methodology does not cover hardware security.

This methodology targets digital reception terminals which handle secrets while Pay-TV content is displayed on a TV. It does not target directly the network "boxes" of operators, but may be used as a methodological base for the evaluation of this equipment and, more generally, for the evaluation of various types of connected box.

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

More specifically, the evaluation is intended to check the correct software handling of the secrets contained in the STB. This comprises the operator content and the user data, but also the secrets used to authentication of the user with third party services. Conversely, the

evaluation does not take into account the hardware threats to the STB's components, nor to the interception of the secrets contained in the STB during transfers between these components.

1.3. Evaluation workload

The workload scheduled to evaluate the STB is **40 man*days for the box** and **an extra 10 man*days for the cryptographic part** (compared with 25 + 10 in the CSPN methodology).

DRM is not part of the scope of this methodology. If the sponsor wants to evaluate it, an additional workload of 10 man*days must be given over to it. DRM evaluation is not covered by this methodology.

The workload may be reviewed downwards in the event of a re-evaluation of a differential evaluation. In general, all workload modifications must be justified and validated by the certification body before the start of the evaluation is accepted.

1.4. Specific aspects of this methodology in relation to the CSPN methodology

This methodology may be used without referring to the CSPN methodology [MET_CSPN]. To do so, certain tasks to be performed are taken from the generic methodology and others have been added or refined in relation to the products targeted.

2. Specific evaluation work

This chapter describes the content of the evaluation technical report (ETR), whose framework it reuses, and lists the specific evaluation tasks expected.

2.1. Identification of the technical evaluation report

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

2.2. Evaluated product identification

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

2.3. Functionalities, usage and security environment

This chapter and its sub-chapters will contain a brief description of the STB evaluated and the different services concerned by the evaluation. They will also restate the most important elements from the security target.

The security target, which is provided by the evaluation's sponsor, must be based on the generic target for STB [CDS-STB] and clearly define the scope of the analysis in particular in relation to the third party remote services which may be the subject of investigations without prior authorisation.

2.3.1. General description of the product

The evaluator must provide a reminder of the product's general architecture. In particular, they will specify the following points:

Chipset	*supplier and reference*
Start-up program	*name and version*
Operating systems	*name and version*
Middleware	*name and version*
Browser	*name and version*
Libraries	
CAS	*name and version*
DRM	*name and version*
Video on demand	*name and version*

If available, a general architecture diagram for the STB must be provided by the sponsor when the evaluation starts. This diagram will identify the STB's main hardware and software entities, as well as their interconnections.

2.3.2. Product operating modes

In this section, the evaluator will specify the product's operating mode, more particularly:

- The operation of the embedded software update, specifying:
  - The resources to detect the existence of a new version;
  - How the change to a new version is performed;
  - The update protection systems;
- The secure start-up procedure, specifying the protection systems put in place.

2.3.3. Description of how to use the product

This section will contain a description of how the product is used and how it matches the supplied documentation.

2.3.4. Description of the planned usage environment

By default, the planned usage environment must correspond to standard use (use by a subscriber in their home). If this is a specific environment, the evaluator may detail it in this section.

2.3.5. Description of the environment hypotheses

Here, the evaluator must enter all the environmental hypotheses indicated in the security target, indicate whether some of these hypotheses do not appear relevant to them and identify the hypotheses that cover vulnerabilities discovered during the evaluation.

2.3.6. Description of the dependencies

The dependencies with hardware or software elements which are not supplied with the product must be indicated. In particular, the evaluation shall indicate the content reception method (satellite, via an Internet access provider's network, etc.), the equipment needed for reception (dish, network box, etc.) and the resource to connect the evaluated product to the equipment mentioned above.

2.3.7. Description of the typical users concerned

The typical user is the subscriber to the services of the operator who distributes the terminal.

2.3.8. Definition of the evaluation scope

The evaluation scope is the STB with its external interfaces enabling Pay-TV functionalities to be used and access to the connected services.

The hardware attacks on the STB's components or the interception of secrets between these components do not enter the scope of the evaluation.

2.3.9. Inventory of the identified security functions

The evaluator shall carry over all the security functions described in the security target and identify the functions which failed during the evaluation.

2.3.10. Inventory of the sensitive assets that the product must protect

The evaluator shall carry over all the sensitive assets described in the security target and identify those they managed to compromise.

2.3.11. Inventory of the threats to the product

The evaluator shall carry over all the threats described in the security target and identify those they managed to implement.

2.4. Product installation

To enable the product to be evaluated, at least the hardware, software, documents and services accessible to the STB must be available. The sponsor must ensure that the evaluator has these elements.

2.4.1. Equipment needed to carry out the evaluation

The evaluator shall have the following elements to carry out their evaluation:

- A digital reception terminal (hereafter referred to as the "production" STB);
- A digital reception terminal in debug mode offering series console access, a JTAG debugger, etc. (hereafter referred to as the "development" STB).

The debug terminal is required to check whether unplanned behaviour by the box may be exploited to harm the availability, integrity or confidentiality of the goods to be protected.

In addition, in order to evaluate the software security of the STB's operating system, access in console mode with administrator rights (SSH type) is necessary for the development STB.

Certain operations may cause the STB to become unstable. A reconditioning procedure shall also be provided (reset to the status prior to the evaluation, from an installation image, for example).
A reconditioning procedure following intrusion into the box shall also be provided if the STB's operation is blocked by any sensors.

2.4.2. Software and documents needed to carry out the evaluation

The evaluator shall have the following elements to carry out their evaluation:

- Embedded software in raw, unencrypted format (binary file) and the file system comprising the configuration elements;
- Functional documentation (specifications, hardware information, cryptographic mechanisms, list of components and version numbers);
- A functional compilation chain.

Ten days are set aside to evaluate the cryptographic mechanisms. It is therefore important for the evaluator to have all the information they need to verify the implementation made of them. The expectations concerning the cryptographic mechanism documentation are specified in chapter 3.3. of the document [CRI_CSPN].

2.4.3. Services needed to carry out the evaluation

The evaluator shall have the following elements to carry out their evaluation:

- One account per STB provided to access the encrypted and protected channels;
- One *Video on demand* account per STB provided to purchase and rent films;
- Access to the satellite/network flow;
- Accounts to access all the services which are part of the evaluation scope.

More generally, as the evaluation takes account of the user authentication with the third party service, the sponsor shall ensure that the evaluator has all the elements that enable them to study these mechanisms.

2.4.4. Evaluator's position

To verify the conformity of the functionalities and the resistance of the mechanisms implemented in the product, the evaluator may position themselves on the test platform between the terminal and the Internet access. To do so, the evaluator's machine must be placed between the two boxes using, for example, an Ethernet hub to analyse the traffic (network bridge or network *tap* type solutions may be considered). In all cases, the evaluator shall precisely describe the evaluation platform.

2.5. Conformity analysis

2.5.1. 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 [CRI_CSPN]).

2.5.2. Source code review (if possible)

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

2.5.3. 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 [CRI_CSPN]).

2.6. Analysis of the resistance of functions and mechanisms and vulnerabilities

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

For this type of equipment, specific mechanism and interface identification work shall be carried out by the evaluator. This work, which is described in the following paragraphs, may be carried out on the *debug* STB. The tasks in paragraph 2.6.2 shall be validated on a production STB.

In addition, the mechanism resistance scoring will be carried out on the *debug* STB and on the production STB.

2.6.1. Service analysis

2.6.1.1. Entry point identification

All entry points must be identified to list the user's methods for interaction with the box.
The entry points may be divided into several categories:

- The logical entry points: these are mainly network connections. The following will be checked, for example:
  - The network connections supported: Ethernet, Wi-Fi, ADSL, Satellite, modem;
  - The services exposed: TCP/IP, UDP;
  - The applications used: FTP, Web browser, etc.;
- The physical entry points: these are mainly the ports available on the STB to connect external peripherals. For example, the following available ports will be checked: USB, RS-232 (serial), Infrared, Firewire;
- The physical entry points that require intrusion into the box: these are mainly entry points that are only accessible after the box is opened and are not normally accessible to the subscriber. The following will be checked, for example:
  - The ports available: JTAG ports;
  - The mass storage media: hard disk, flash drive.

2.6.1.2. Service identification

To protect the sensitive data, whether the data related to a user or a video flow, the evaluator shall identify all the flow transfers.

To do so, all the functionalities that relate to the available services must be listed (channels, video on demand, etc.):

- Account creation;
- Authentication;
- Access to personal areas;
- Payment systems;
- Content location;
- Content recording.

For each service, the evaluator shall note at least the following information:

- The type of service exposure:
  - Incoming service (from the STB's point of view) accessible from the Internet;
  - Incoming service (from the STB's point of view) accessible from the local network;
  - Outgoing service (from the STB's point of view);

- The box, user and server identification process;
- The data transfer method (format, protocol, encryption method, etc.).

2.6.1.3. Terminal update

The installation by an attacker of software on the terminal constitutes a critical threat. The **update management**, the **signature verification** for the embedded software and the **start-up validation chain** shall be analysed by the evaluator. The evaluator shall study the mechanisms relative to the start-up chain and more particularly the presence of integrity verification based on a cryptographic signature. This mechanism must not be able to be compromised without making the equipment unusable.

2.6.1.4. Service analysis summary

At the end of this stage to recover the services running on the STB, the evaluator shall fill in a file identifying the points to be checked as priority. The items in the tables below are presented for information purposes and must be completed according to the product evaluated.

Entry	**Present?**
Ethernet	Yes/No
Wi-Fi	Yes/No
Satellite	Yes/No
JTAG	Yes/No
RS-232	Yes/No

Network service	**Port**	**Notes**	**Public vulnerability?**
Web	80	Apache X.Y	Yes/No
…	…	…	Yes/No

Action	**Trigger event**	**Security**		
		Client authentication	**Server authentication**	**Encryption**
DNS	Network Start-up and Configuration			
DHCP	Network Start-up and Configuration			
FTP	Factory setting reset			
Update by satellite	Start-up + 24-hour verification			
Hard disk mounting	USB connection			

Services	Functionalities	Security		
		Client authentication	Server authentication	Encryption
Catch-up TV				
	Account creation			
	Authentication			
	Personal area			
	Viewing			
	…			
Video on demand				

2.6.2. Flow analysis

Here, the evaluator shall verify the effectiveness of the protection measures implemented by the terminal.
The following points must be verified, for example:

- The possibility for a user to pretend to be someone else:
  - To recover content free of charge;
  - To pass a bill onto another user;
  - To recover confidential information;
  - To falsify logs;
- The possibility of automating requests:
  - To test weak passwords by brute force;
  - To find valid card numbers by brute force;
  - To recover user information.

2.6.2.1. Service-related flow analysis

The evaluator shall list the flows exchanged, without forgetting the flows activated automatically:

- When the ADSL link starts up;
- When the TV box starts up;
- During access to the different services available:
  - Change of channel;
  - Subscription;
  - Rental of a Video on demand film;
  - Rebroadcast via the catch-up TV service;
  - Access to the customer area;
- During a factory setting reset.

2.6.2.2. Video flow analysis

Two types of content must be protected. If this is a channel, then the flow will be recovered as it is broadcast. In the case of a video file, the file may be downloaded in full or in several parts to enable it to be viewed as it is downloaded. In both cases, the evaluator shall verify whether it is possible to access the content unscrambled.

In particular, the evaluator shall list the content provided and the protection mechanisms, including:

- The presence of an encrypted tunnel (VPN) protecting the video flow;
- The use of DRM (unscrambled RTP flow with the encrypted content).

Note: While third party server security is not part of the evaluation scope, the evaluator will report to the sponsor, after agreement from the ANSSI, any abnormal behaviour that may suppose the existence of vulnerabilities associated with the server.

2.6.2.3. Flow analysis summary

The evaluator shall provide a detailed description of the operation of each service in the form of a summary table as proposed below (the responses in italics are examples):

Action	Trigger event	Security		
		Box authentication	Server authentication	Encryption
DNS	Network Start-up and Configuration	*none*	*none*	*no*
DHCP	Network Start-up and Configuration	*none*	*none*	*no*
FTP	Factory setting reset	*none*	*certificate + embedded software signature*	*no*
Update by satellite	Start-up + 24-hour verification	*none*	*embedded software signature*	*no*

Service	Functionalities	Security		
		Client authentication	Server authentication	Encryption
Catch-up TV				
	Account creation	*no*	***no***	***no***
	Authentication	*login + password*	***no***	***no***
	Personal area	*session cookie*	***no***	***no***
	Viewing	*session cookie*	***certificate***	***AES***
	…			
Video on demand				
	…			

2.6.3. Software analysis

The objective of the embedded software evaluation is to obtain a precise view of the different information processing mechanisms for the goods to be protected in order to determine whether these assets may be compromised in terms of availability, integrity and confidentiality from a software attack.

2.6.3.1. Cryptographic aspects

In that the evaluation relates to the software aspects of the STB, the chipset and the content protection system, once this system is based on chipset hardware protection, are outside the scope of the cryptographic scoring (conformity with the RGS) of the STB.

The cryptographic study that the evaluator shall carry out comprises the analysis and scoring of the standard cryptological mechanisms for the embedded software, such as, for example:

- The encryption of the content on the disk;
- The communication with the remote servers;
- The embedded software signature.

The analysis must enable understanding of the mechanisms related to the use and storage of cryptographic secrets associated with protected content processing.

The evaluator shall:

- Detail the software or hardware components in charge of this processing;
- Detail the actual processing;
- Detail the operation of the random event generator used (in particular the entropy sources used);
- Validate the conformity of the cryptographic mechanisms in relation to appendix B of the General Security Reference Base [RGS];
- Validate the correct use of a trusted component for the storage and use of secrets;
- Validate the presence or absence of vulnerabilities in relation to the state of the art.

For each cryptographic weakness identified, the evaluator shall develop evidence of a concept that uses the weak mechanism; they will propose one or more correcting actions.

These cryptographic aspects cover the protocol and algorithm weaknesses (example: attack by oracle on the CBC "padding" in TLS) and the weaknesses related to the implementation (example: weakening of the signature due to the use of an *strncmp* instead of *memcmp*, or incorrect use of ECDSA).

The evaluator shall provide a detailed description for each vulnerability identified, using the example below.

Data	Component used	Protocol	Correct processing of the secrets in the memory	RGS conformity	Public vulnerabilities
Video flow to TV	*Trusted component*	*X.Y.Z*	***OK***	***OK***	
Bank card number	*OpenSSL 0.9.6 + libCB 1.1*	*TLS*	***NOK***	***OK***	*Bleichenbacher oracle*
USB disk encryption					

2.6.3.2. System aspects

2.6.3.2.1 Verification of proper hardening practices

The evaluator will verify the presence of mechanisms to harden the binary protection:

- Stack protection with canaris;
- Stack not executable;
- Memory randomisation;
- Application of the minimality principle: only the services, applications and core models necessary for the STB to operate must be deployed on the system;
- Use of process isolation mechanisms: chroot, containers (VZ or Vserver for example), process execution rights, SECCOMP, process capabilities;
- Network protection: against spoofing IP/MAC, DoS, IP stack protection.

2.6.3.2.2 Public vulnerability identification

The evaluator shall examine the programs and libraries provided in unencrypted format to identify the components and their associated version number (for example: zlib 1.2.3), as well as the potential absence of the planned counter-measures ("stack cookies", "randomisation", input processing white list, etc.).

They will then look for the public vulnerabilities which affect these components. For each vulnerability, they will study the exploitation path to determine whether the vulnerability is accessible from one of the entry points quoted above. The writing of concept evidence to highlight the vulnerability and its impact on the goods to be protected and the supply of one or more corrective actions to protect against the vulnerabilities identified are not compulsory.

It should be noted that this section may require the development of tools specific to the environment studied. The evaluator may provide the sponsor and the developer, after agreement from the ANSSI, with all or some of the tools developed to enable them to reproduce the vulnerability and to verify its correction in a later phase.

The evaluator shall provide a detailed description for each vulnerability identified, using the example below:

Binary and library	Notes	Vulnerable CVE	Restricted privilege	Protection of the stack	Signed code
Web server	*Apache X.Y.Z*				
Browser	*Webfront 3.5*	***no***	***yes***	***no***	***no***
libpng	...				

2.6.3.2.3 Non-public vulnerability search

This phase is based on the evaluator's expertise to identify the potential non-public vulnerabilities on the components present or specific to the proprietary architecture in place, particularly those that deal with the data controlled by the attacker.

Examples:

- Use of IPv6 to avoid the filtering policy;
- The exploitation of a vulnerability in processing the metadata associated with a download;
- A vulnerability in a Web interface (directory crossing, sending of arbitrary files, etc.).

The development of concept evidence and the proposal of corrective actions are not required for the evaluator.

It should be noted that this phase may require the evaluation duration to be extended according to the size of the scope and the difficulty in analysing the system's components.

2.7. 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 [CRI_CSPN]).

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.

2.8. Meetings with the developers

This task is optional.

2.8.1. Result of the interviews

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

2.8.2. 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 [CRI_CSPN]).

2.9. Summary

An **expert opinion** summarises the results of the previous tasks for a technical reader.

Annexe 1 : References

[CRI_CSPN]	Instruction – Criteria for evaluation for a First level security certification, Reference: ANSSI-CSPN-CER-I-02, current version.
[MET_CSPN]	Application note – Methodology for evaluation for a First level security certification - ETR content, Reference: ANSSI-CSPN-NOTE-01, current version.
[CDS-STB]	STB general security requirements conforming to the CSPN methodology. Version: 1.2, dated 26/12/2012. Canal+.
[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.