Analysis and comparison of lightweight evaluation methodologies

This analysis has been carried out by Jose Ruiz – CTO at jtsec.

This document will examine the national lightweight methodologies from four different countries:

- Spain (*LINCE*)
- Germany (*BSZ*)
- France (*CSP*N)
- Netherlands (*BSPA*)

The analysis will take into account the technical aspects of each of them.

Background

Lightweight certifications arise to solve the issue related to duration and cost of the existing certifications, such as *Common Criteria,* that are not suitable for low assurance products.

To solve this problem, France was one of the first countries to create a light methodology (CSPN) in 2008. Other countries have created similar methodologies afterwards.

These certifications make possible to evaluate products that require low assurance using a cost-effective approach in a predictable time frame.

Analysis

The analysis takes into account different aspects:

- Evaluation Methodology General aspects and Process
- Requirements for Developers
- Evaluation Activities

Evaluation Methodology General aspects and Process

	LINCE	CSPN	BSPA	BSZ
Workload	25 man/days	25 man/days	25 man/days	25 man/days

Additional Workload	5 man/days per additional optional module	10 man/days if crypto implemented.	No	10 man/days if crypto.
Customization of Workload	No	Yes, when another specific workload is recommended in a particular methodology or if agreed between the parties but no specific rules are specified.	Yes (Only under special circumstances), but no specific rules are specified.	Yes. Customization depending on different factors. Details rules for calculation.
Calendar Duration	8 weeks 2 additional weeks per module (Mandatory)	8 weeks (Recommendation)	8 weeks (Recommendation)	No constraint
Optional Modules	- Crypto Evaluation Module (MEC) - Source Code Review Module (MCF)	No	No	No
ETR Template	Yes	Yes	No The content is outlined in the methodology.	Yes
Lab Accreditation	Follow the CC Process. ISO17025 and Pilot evaluation are required. No Licensing Domains.	Specific Procedure. ISO17025 is not required. Pilot evaluation is required. 13 different Licensing domains	Specific Procedure. ISO17025 is not required. Pilot evaluation is required. 8 Different Licensing domains	Specific Procedure. ISO17025 is required. Pilot evaluation is required. Licensing domains are under preparation.

Requirements for Developers

	LINCE	CSPN	BSPA	BSZ
Required Evidences	- ST - Operational and installation Guidance - Testing Environment - Product Samples - Source Code (if module chosen) - Crypto Information (if module chosen)	- ST - Operational and installation Guidance - Crypto Information - Product Samples - Source code (Not clear if optional or depending on the case)	- ST - Operational and installation Guidance - Testing Environment - Product Samples - Public Information	- ST - Operational and installation Guidance - Product Samples (3 copies) - Crypto Information - copy of the unencrypted firmware (optional) - an overview of the principle design of the TOE and the libraries used - a brief technical description of the update mechanism
ST Type	ST Template Available - TOE Identification - TOE Usage - TOE Description - Operational Environment - Assumptions, Assets and threats - Security Functions Specification	ST Template Available - TOE Identification - TOE Usage - TOE Description - Operational Environment - Assumptions, Assets and threats - Security Functions Specification	ST Template Available - TOE Identification - TOE Usage - TOE Description - Operational Environment - Assets and threats - Security Functions Specification	ST Template Available - TOE Identification - TOE Usage - TOE Description - Operational Environment - Assumptions, Assets, Attackers and threats - Security Functions Specification - Limits of evaluation

Evaluation Activities

	LINCE	CSPN	BSPA	BSZ
Evaluation Type (Personal View)	BlackBox Evaluation (If modules are not chosen) Gray/White Box depending on the modules chosen	Gray/White Box Evaluation (Crypto information is required) (Source code may be required)	BlackBox Evaluation	Gray/White Box Evaluation (Crypto information is required) (Source or pseudo source code of the cryptographic functions is required)
Steps	- SECURITY TARGET ASSESSMENT - TOE PREPARATION AND CONFIGURATION - DOCUMENTATION ANALYSIS - FUNCTIONAL TESTS - VULNERABILITY ANALYSIS - TOE PENETRATION TESTING	- SECURITY TARGET ANALYSIS - PRODUCT INSTALLATION - DOCUMENTATION ANALYSIS - SOURCE CODE REVIEW (IF AVAILABLE) - PRODUCT TESTING - RESISTANCE OF THE MECHANISMS/FUNCTIONS - VULNERABILITY ANALYSIS (INTRINSIC, CONSTRUCTION, EXPLOITATION, ETC.) - HOST SYSTEM VULNERABILITY ANALYSIS - EASE OF USE ANALYSIS - CRYPTOGRAPHY EVALUATION (IF THE PRODUCT IMPLEMENTS CRYPTOGRAPHIC MECHANISMS)	- CONFORMANCE ANALYSIS - STRENGTH ANÁLISIS - IMPACT ASSESSMENT ON THE SECURITY OF THE HOST SYSTEM - DEPLOYMENT ADVISORY	- REVIEW THE TOE, THE CRYPTOGRAPHY AND THE ST - ESTIMATE THE EVALUATION - EVALUATE THE SECURE USER GUIDE - EVALUATE THE CONFORMITY - EVALUATE THE RESISTANCE (VA and Testing) - CRYPTOGRAPHIC EVALUATION
ST Review	Yes	Yes	Yes	Yes
Guidance Doc Review	Yes	Yes	Yes (implicitly)	Yes
Product Installation	Yes	Yes	Yes	Yes

Other Documentation Analysis	No	Yes	No	Yes
Source Code Review	Optional	Yes (Not clear under which circumstances)	No	Yes (For Crypto)
Security Functionality Testing	Yes	Yes	Yes	Yes
Analysis of the resistance of the mechanisms	During the Vuln. Analysis Phase	Yes	Yes	Yes
Vulnerability Analysis	Yes	Yes	Yes	Yes
Penetration Testing	Yes	Yes (Testing is mentioned During Vuln. Analysis phase)	Yes (Testing is mentioned During Strength Analysis phase)	Yes (Testing is mentioned During Evaluate the Resistance phase)
Ease of Use Analysis	No	Yes	No	No
Impact assessment on the security of the host system	No	Yes	Yes	No
Crypto Evaluation	Included as an Optional module – Conformance testing	Mandatory if the product implements crypto – Conformity & Vuln. Analysis – No Penetration Testing is specified	No additional information is provided.	Mandatory if the product implements crypto – Vuln. Analysis & Penetration Testing Note: The evaluation of crypto is currently under discussion and most likely will change to what is documented now.

Further work

Define a common methodology with different modules that would allow to fulfil the current requirements of all the national methodologies.

In a first step, I would focus only on evaluation methodologies and would keep the evaluation process out of the scope.

Conclusions

All the national methodologies are similar with slight differences. It should be affordable to create a common methodology that could be re-used in different CSA schemes.

CSA requests methodology for the following activities:

- Technical Documentation Review
- Security Functional Testing
- Search for public/known vulnerabilities
- Penetration testing

The future methodology should address explicitly these points.

Disclaimer

The information contained in this report has used public sources. There could be some errors. Do not hesitate to comment it in order to solve them.