Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRIME MINISTER

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, 9 juillet 2013

N°2360/ANSSI/SDE/PSS/CCN
Reference:ANSSI-CC-NOTE-16/1.0EN

APPLICATION NOTE

COMPLEMENTARY EXPERTISE FOR BANKING PRODUCTS EVALUATION

Application : From date of publication.

Circulation : Public.

COURTESY TRANSLATION

Version history

Version	Date	Modifications
1.0	9 July 2013	Creation

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

This application note is available online at the following sites:

- The ANSSI institutional site (www.ssi.gouv.fr);
- The SGDSN institutional site (www.sgdsn.gouv.fr);
- The site specified in decree No. 2008-1281 of 8th December 2008 for the publication of instructions and circulars (www.circulaires.gouv.fr).

TABLE OF CONTENTS

1. Subject of the note

The purpose of this note is to highlight the complementary expertise for banking products that may be implemented at the same time as a Common Criteria evaluation in the context of the French scheme.

2. References

- Amended decree No. 2002-535 of 18th April 2002 relating to the evaluation and certification of the security provided by information technology products and systems.
- Expertise convention for security evaluations between CB EIG, MPS, SFPMEI et ANSSI.

3. Issue

The GIE CB[1], SFPMEI[2] and MPS[3] inter-bank entities manage market release authorisations (also called banking licences) for banking applications on smart cards, as follows

- GIE CB processes CB-EMV applications;
- SFPMEI and MPS process Moneo applications.

The security aspect of this banking licence is based on the following two types of evaluation:

- Common Criteria (CC) evaluations, carried out in the context of the French certification scheme;
- Optional complementary expertise.

The inter-bank entities and the ANSSI have agreed to entrust the ANSSI with coordinating these two types of evaluation, where applicable, to ensure their successful implementation.

4. Presentation of the complementary expertise approach

The laboratories responsible for carrying out the complementary expertise are named "excellence laboratories" to distinguish them from the ITSEF. Chapter 7 describes how these excellence laboratories are referenced. The list of these excellence laboratories is maintained by the ANSSI and the inter-bank entities. Appendix A features this list when this note is drafted. It is updated when needed, according to the reference convention and in agreement with the convention signatories.

Complementary expertise corresponds to a "black box" evaluation, i.e. an evaluation without provision of the design details for the banking application in question. Neither the test methods nor the equipment used are predetermined.

A complementary expertise corresponds to a maximum workload of two men x month. This workload is dedicated to carrying out penetration tests and to drafting an expertise report. The expertise report describes the penetration tests carried out and the vulnerabilities detected. This report is the sole responsibility of the excellence laboratory which carried out the complementary expertise. However, it is reviewed by the ANSSI to confirm the ratings for any attacks identified by the excellence laboratory.

[1] Bank Card Economic Interest Group.

[2] Société Financière du Porte-Monnaie Electronique Interbancaire.

[3] MONEO PAYMENT SOLUTIONS.

To enable the complementary expertise to be carried out, the inter-bank entities make a contractual commitment to the excellence laboratories responsible for carrying out this expertise. In particular, these contracts include the clauses needed to carry out and report on the complementary expertise. They also specify that the ANSSI must be informed by the excellence laboratory of the conduct of the expertise work and the results as the work progresses to enable the ANSSI to coordinate as best as possible the complementary expertise and the CC evaluation carried out in parallel.

5. Expertise proposal

5.1. Complementary expertise proposed by the ANSSI

5.1.1. Introduction

Each banking application CC evaluation may only be associated with one complementary expertise. Consequently, choices must be made to identify the products submitted for expertise.

The decision has therefore been made for the ANSSI to propose to the inter-bank entities:

- The products which might be the subject of a complementary expertise;
- The excellence laboratories which would carry out this expertise.

These proposals are made based on the criteria presented below.

5.1.2. Product selection criteria

The ANSSI proposes the products that are eligible for complementary expertise based on the following main criteria, presented in descending order of importance:

- The innovative nature of the product: priority is given to the most innovative products (for example: new microcircuit, new operating system, new application, etc.) in order to enhance developers' skills in terms of "future" product security;
- Developer rotation: if two developers present eligible products which cannot both be the subject of complementary expertise, priority is given to the developer whose lastest expertise dates back the furthest;
- The products' sensitivity to certain attacks: priority is given to products for which it is felt that certain types of attack would have a high probability of success and that these access would enable the most sensitive banking elements to be reached.

5.1.3. Laboratory selection criteria

The ANSSI proposes the excellence laboratories based on the following main criteria, presented in descending order of importance:

- The laboratory's technical resources and competence: priority is given to the laboratory that has the technical test resources and skills that are the best suited to the product submitted for expertise;
- The laboratory's availability; the laboratory selected must be able to carry out the complementary expertise within a time frame that is compatible with the scheduled or estimated end of the CC evaluation;

- Laboratory rotation: if several laboratories meet the conditions to carry out the expertise, priority is given to the laboratory whose lastest expertise dates back the furthest.

5.2. Contract agreement

The inter-bank entities validate the ANSSI's proposals based on their financial commitment, at the latest during the product's CC evaluation launch meeting. The inter-bank entities must then sign a contract with the selected laboratory within a time frame to enable the complementary expertise to be carried out before the scheduled end of the CC evaluation.

As soon as the ANSSI is informed that the contract agreement process has been finalised, it informs the developer of the decision to submit the product for complementary expertise, the laboratory which will carry it out and the date selected for the expertise work.

6. Coordination of the complementary expertise and the CC evaluation

6.1. Introduction

To enable the ANSSI to identify as soon as possible the products likely to be submitted for complementary expertise and so minimise the impact of the complementary expertise on the CC evaluation, the developers must send the ANSSI each year the list of all their banking products which may be submitted for a CC evaluation over the year within the French scheme. This list must be combined with a technical description, the provisional date for the CC evaluation request and provisional ability dates for each of these products. All modifications must be communicated to the certification centre. If this commitment is not respected by the developers, the coordination objective between the complementary expertise and the CC evaluation may not be met. This problem may not be attributed to the inter-bank entities or to the ANSSI.

The complementary expertise is carried out independently of the CC evaluation. If exchanges are necessary between the excellence laboratory and the ITSEF, they will be made under the control of the ANSSI.

6.2. Supplies

The developer delivers the product samples and corresponding profiles to the excellence laboratory.

The developer guarantees the consistency between the product samples delivered to the laboratory which carries out the complementary expertise and the samples delivered to the ITSEF for the CC evaluation. When the samples delivered to the excellence laboratory and the ITSEF correspond to different product versions, the developer must provide a detailed impact analysis between the two product versions and undertakes in any event to keep sufficient quantities of each version of the samples to enable the ITSEF to carry out the verifications it considers necessary.

6.3. Distribution of the complementary expertise reports

The inter-bank entities, the developer and the ANSSI receive the expertise report. The information in the expertise report is not revealed either by the inter-bank entities or by the developer to the laboratory in charge of the CC evaluation.

6.4. Results of the complementary expertise

When the ANSSI considers that certain vulnerabilities highlighted by the complementary expertise may have an impact on the level of security targeted by the CC evaluation, it asks the developer to correct their product (as for any vulnerability discovered during a CC evaluation) and the ITSEF will make a declaration on the effectiveness of the counter-measure in the context of the CC evaluation.

7. Excellence laboratory referencing

The inter-bank entities and the ANSSI reference the candidate laboratories based on the following criteria:

- Excellent reputation in terms of ethics;
- Technical competence guaranteeing the relevance of the black box penetration test results. Concerning the ITSEF, this competence is verified in the context of the procedures laid down by the French certification scheme, which informs the inter-bank entities of the ITSEF's areas of excellence. Concerning the other laboratories, competence equivalent to that of the ITSEF in their specific area of expertise must be recognised;
- Ability to maintain the confidentiality and independence of their work, including in relation to their shareholders or their control structure. Global (laboratory's legal representative) and individual (experts who carry out the penetration tests) confidentiality agreements may be demanded. For the ITSEF, this ability is certified by the ANSSI in the context of the procedures laid down by the national certification scheme. For the other laboratories, this ability is certified by the inter-bank entities which inform the ANSSI of the confidentiality agreements that are signed;
- Ability to work with the ANSSI in the context of this expertise process.

Annexe A List of referenced excellence laboratories

CEA/LETI
MINATEC – 17, rue des Martyrs, 38054 Grenoble Cedex 8, France

EDSI
1, rue de Paris, 35510 Cesson-Sévigné, France

SERMA Technologies
30, avenue Gustave Eiffel, 33608 Pessac Cedex, France

THALES (TCS/CNES)
BPI1414 – 18, avenue Edouard Belin, 31401 Toulouse Cedex 9, France

Annexe B Frequently Asked Questions

1 *What is the maximum workload allocated to the excellence laboratory for these tests?*

The maximum expertise workload is set by the inter-bank entities and is 2 men x month (see chapter 4).

2 *Is this workload independent of the number of applications embedded on the card?*

Yes, the maximum workload is 2 men x month independently of the number of applications embedded on the card.

3 *Who defines the profiles (personalisation) to be provided for these tests?*

If the personalisation profiles have an impact on the evaluation, the inter-bank entities validate the choice of the profiles selected.

4 *How is the excellence laboratory's work monitored during the expertise?*

No interaction between the ANSSI and the excellence laboratory is specially planned outside the following cases:

- Administrative difficulty during the work;
- Discovery of a vulnerability. The excellence laboratory then alerts the ANSSI, which then informs the developer.

5 *What are the consequences for the CC evaluation if the excellence laboratory is late?*

The implementation of this procedure is intended to guarantee the synchronisation between the two evaluations (i.e. that the expertise must be finished before the end of the CC evaluation).

If, however, the excellence laboratory cannot deliver its results on time, only the expertise results available before the certification are taken into account.

6 *How and by whom would a potential late sample delivery be managed (following a delay in the project for example) in relation to the time slot reserved for the excellence laboratory?*

The ANSSI refers this to the inter-bank entities who identify the follow-up. One option would be to freeze the CC certification process until the expertise results are obtained.

7 *What are the consequences for the CC evaluation if the rules described in paragraph 6.1 are not respected?*

The ANSSI refers this to the inter-bank entities who identify the follow-up. One option would be to force an expertise or even to impose deadlines on the CC evaluation.

8 *If a vulnerability is detected by the ITSEF then corrected by the developer, does the corrected product need to undergo the excellence laboratory's tests again?*

No.

9 Concerning the samples, in which context may the developer formalise a confidentiality commitment with the excellence laboratory?

The excellence laboratory sets up a contract with the inter-bank entities who finance its expertise and signs the expertise convention which binds it to the other actors involved in this evaluation. The confidentiality of the excellence laboratory's work is covered by these contracts.

However, if the developer desires, they may put in place a secure sample delivery and return contract with the excellence laboratory (which is also bound to guarantee confidentiality by the clauses in the inter-bank entities' contract). This contract, if deemed necessary, must be limited to these aspects only and must not interfere with the conduct of the expertise.

10 What is the process if a vulnerability is detected by the excellence laboratory?

As soon as a problem that affects the results of the CC evaluation is validated by the certification centre, the developer if informed of it so that they can determine as quickly as possible the changes necessary to this product (see chapter 6.4).

The correction of the problems identified by the excellence laboratory is validated by the ITSEF in charge of the CC evaluation (see chapter 6.4).

11 What is the impact on the evaluation being carried out by the ITSEF?

The impact is the same as if the vulnerability had been found during the CC evaluation, by the ITSEF or by anyone else.

12 Does the excellence laboratory keep the samples after its expertise?

No, the laboratory promises to return or destroy all the samples at the end of the expertise.