Requirements and procedure for security evaluations of chip card products and digital signature creation device for the Taiwanese payment system

Version 1.4

Table of contents

1 Introduction

In order to make sure that chip cards and digital signature creation device(DSCD) used in payment systems fulfil minimal functional as well as security requirements, BAROC governs the chip card and DSCD approval scheme for Taiwan (see [ApprScheme] and www.ba.org.tw). Within BAROC, the Financial Chip Card Authorisation and Verification Team is responsible for setting up and maintaining the scheme.

Experience with the chip card deployment in Taiwan showed that security considerations are becoming more and more important. Therefore, BAROC decided to add explicit security requirements to the existing requirement set for chip cards and DSCD to fight counterfeit, fakes and other attacks on the chip card and DSCD itself.

Due to the inherent dynamic nature of security threats and based on international experience with security evaluations, BAROC decided to enhance its scheme with an additional security evaluation procedure for the chip cards and DSCD. However, BAROC reserves the right to make security evaluations of chip card products a mandatory part of the approval process in the nearer future.

The procedure of security evaluation is detailed in the following document. It involves an independent third party doing the evaluation based on the security requirements put forward by BAROC. The evaluation results are reported to BAROC for approval decision.

2 Security requirements

The security requirements valid for chip card products and DSCD in Taiwan are described in [SecReq]. Chip card products or DSCD undergoing security evaluations have to fulfil this requirement set in order to achieve a positive evaluation.

3 Security evaluation procedure

BAROC puts forward the following security evaluation procedure:

1. The applicant registers with BAROC that he wants to conduct a security evaluation for his product. The applicant uses the form from annex of this document.
2. The applicant contracts a security evaluation laboratory from the list of accredited laboratories maintained by BAROC. The list is sent to the applicant when he applies for security evaluation.
3. The applicant submits his product for evaluation to the laboratory. He provides the documentation and items required in section 4 to the laboratory.
4. The security evaluation laboratory conducts the evaluation. When completed, the laboratory provides an evaluation report and submits this report to BAROC. A copy of the report goes to the applicant.

4 Documents and items required

4.1 Security requirements of the chip hardware used

4.1.1 IC documentation of the IC manufacturer

The security evaluation laboratory needs the full documentation of the HW used.

4.1.2 Implementation guidance documents from the IC manufacturer

Since the security of the chip card product or DSCD depends on the proper use of the HW security features, the security evaluation laboratory needs to be informed about implementation guidance given by the IC manufacturer.

4.2 Chip hardware security evaluation certificate

If the IC HW was successfully evaluated according to an internationally recognised security standard, the results of this evaluation process have to be provided by the applicant.

4.2.1 Evaluation certificate

The certificate itself is needed for reference. It is required to use an IC with CC 2.x evaluation according to EAL 4+ augmented with AVA_VLA.4 or CC 3.1 evaluation according to EAL 4+ augmented with AVA_VAN.5.

4.2.2 Certified HW configuration

In many cases, the security certification authority granted its certification for a certain configuration of HW used for chip card products. The applicant has to provide a description of this configuration, of parameter values used, etc.

4.2.3 Guidance documents from the HW certification

From a certificate restricted to a particular HW configuration it may follow that the certifier gives additional guidance documents on the proper use of the HW for chip card products. If available, these guidance documents have to be supplied.

4.3 Source code

4.3.1 Code itself

The source code has to be provided in plain text.

The source code has to be sufficiently commented so that the evaluator can understand what specific parts of the code stand for and how they function.

4.3.2 Evidence on the production status of the source code

The security evaluation laboratory needs to have evidence that the source code provided by the applicant is the code actually used in the production version of the

chip card. This requirement applies to all kind of code implemented in or loaded into the chip card.

The evidence can be provided on three different ways:

- Manufacturers written declaration that the production version of the code is a one-to-one compilation of the source code and naming of the tools used for compiling the production code – or –
- Provision of the production code to the security evaluation laboratory, comparison with a production code generated from the source code by the security evaluation laboratory – or –
- Audit of the production code compilation facilities in use at the chip card production site by personnel of the security evaluation laboratory.

4.4 Functional specification

Documentation of chip card commands for initialisation, pre-personalisation, personalisation and usage phases:

- Command APDUs
- Return codes
- Functional description of commands

4.5 Mapping between functional specification and source code

Document describing the mapping between the functional specification and the source code. With this document, the security evaluation laboratory should be able to find code parts related to a certain command or to a security functionality required by the BAROC security requirement document [SecReq].

4.6 Mapping between HW requirements and source code

Document describing the mapping between the HW requirements put forward by the HW manufacturer and the certification of the HW and the source code.

4.7 Samples

Security evaluation laboratories need at least ten samples of the chip card product or DSCD to do the security testing. Based on experience with other evaluation work the following tentative list is provided.

- Three chip cards or DSCD with SPA/DPA/DFA preparation (the security evaluation laboratory will provide detailed description of the required features).
- Seven additional cards or DSCD in initialisation or personalisation state (depending on the initialisation/personalisation concept and functionality and according to detailed description from the security evaluation laboratory)

For the test samples, a documentation with keys loaded, life-cycle status of the card, etc. has to be provided by the applicant.

The above list may be modified by the security evaluation laboratory according to (future) testing requirements.

5 References

[ApprScheme] Financial chip card related specification authorisation and product verification guideline. BAROC, December 2003, see www.ba.org.tw

[SecReq] Security requirements of BAROC for Financial chip card and Digital Signature Creation Device (FDSCD) approval and implementation, Version 1.1 Date 2009-09-16

6 Glossary

APDU	Application protocol data unit
BAROC	The Bankers Association of the Republic of China
CC	Common criteria
IC	Integrated circuit used as basis for a chip card product or DSCD
HW	Hardware
SW	Software

7 Annex: Forms and templates

7.1 Application form for security evaluation

Registration form for security evaluation of a chip card product or digital signature creation device

Name of the applicant	Organisation and department name
Organisational affiliation	Legal status of organisation
Status of the applicant	SW developer – Issuer – Other party
Contact person	Name
Address	Street
	Zip code
	Town
	Country
	Phone
	Email
Product to be evaluated	Product name, version number(s), completion date(s)
Status of the product	Under development – Completed
Issuer to use the product	Issuer(s) using the product (if already known)
Status of intended security evaluation	First security evaluation of the product – Re-evaluation of changes to the product*
Other evaluations already conducted	If applicable, list of preceding security evaluations (e.g. former BAROC or CC evaluations)**
Security evaluation laboratory	Name of the accredited security evaluation laboratory to be contracted for the evaluation***
Publication policy on BAROC website during evaluation	Publication when product is under evaluation – Publication only when product was evaluated successfully
Publication policy on BAROC website after successful evaluation	Publication – No publication
Signature of applicant	Place, date and signature
Documents provided with this application	List of documents

* A list of changes to the product has to be attached to the registration form
** Evaluation reports have to be included with the application
*** See list on BAROC website under www.ba.org.tw/...

7.2 Security evaluation report

1 General information

The following information has to be provided by the applicant:

- Approval registration number
- Security evaluation laboratory
- ID of the evaluation report
- Approval applicant
- Approval object
- Payment scheme and/or functionality under evaluation
- Payment scheme and/or functionality available on approval object
- Short summary of approval object

2 References

References used in the evaluation report, for example

- BAROC chip card or digital signature creation device functional specification
- BAROC chip card or digital signature creation device security requirements
- Former evaluation reports used for this report
- Data sheets
- Application notes

3 Management summary

Overall statement of fulfilment of BAROC chip card or digital signature creation device security requirements.

4 Results according to requirements

Statements on fulfilment of any single item from the BAROC security requirements. Short description of the evaluation methods used.

5 Full description of analysis results

Detailed description of the analysis done, methods used and results achieved.

6 Glossary

Definition of abbreviations.

7 Appendix

Additional documents (if necessary)