Accreditation of security evaluation laboratories to the BAROC approval scheme

Version 1.4

Table of contents

1 Introduction

In order to make sure that Financial chip card and Digital Signature Creation Device (FDSCD) used in payment systems fulfil minimal functional as well as security requirements, BAROC governs the chip card and FDSCD 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 schemes.

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 FDSCD to fight counterfeit, fraud and other attacks on the chip card and FDSCD itself (see [SecReq]).

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 FDSCD. This procedure which is specified in [SecEval], 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.

Parties interested in doing security evaluations for chip card and FDSCD approvals in Taiwan are invited to apply for accreditation according to the BAROC approval scheme. In order to receive an accreditation, it has to be proven to BAROC that security evaluation laboratories (also called lab applicants hereafter) are capable of doing such evaluations according to international standards and that they have the necessary project experience in the chip card business.

2 Criteria for security evaluators

2.1 Testing laboratory working procedures

Laboratories doing security evaluations have to work according to internationally established procedures for test laboratories. This requirement is to make sure that testing procedures and test documentation are reliably performed according to the standards for which the laboratory is accredited. Measurement tools and evaluators' knowledge have to reflect the state of the art in the respective security technologies as well as known attacks on payment systems and cards in particular.

A laboratory working according to the international norm [ISO17025] is regarded as fulfilling this requirement. ***Fulfilment of this norm can be established with an audit of the laboratory, its staff and procedure documentation.***

2.2 Common criteria accreditation

Due to its international scope and generic approach, BAROC has decided to adopt the Common Criteria (CC) security evaluation and certification scheme [ComCrit] respectively [CC] as basis for the security evaluation procedure of chip cards. Currently, a number of steps are being undertaken to state CC conformance security

requirements for chip cards on the Taiwanese market. These requirements will be put into force in the nearer future.

Therefore, a laboratory doing security evaluations within the BAROC approval scheme must have working experience with CC evaluations and certifications. ***Laboratories with CC accreditation by a CC accreditation body fulfil this requirement.***

2.3 Project experience with payment card evaluation

Effective security evaluation of chip card products requires the laboratory to have knowledge of up-to-date chip card hard- and software and knowledge of common attacks on chip cards.

It is therefore mandatory that the laboratory has project experience with evaluation projects in the area of payment chip cards. ***Laboratories with at least one documented project fulfil this requirement.***

3 Required documents

BAROC requires the following documents as part of an application:

- A completed application form that is available on the web site and upon request.
- A description the laboratory and its profile (organisational description, number of evaluators, professional backgrounds, physical security, testing equipment).
- A document providing evidence that the laboratory has implemented its working procedures according to the [ISO17025]. This evidence is usually given as part of a CC or ITSEC accreditation by national accreditation bodies in the area of information security.
- An accreditation certificate for CC security evaluation and certification by an internationally recognised national information security body.
- A document providing evidence that the security evaluation laboratory has professional experience with at least one evaluation project in chip card or FDSCD security in the financial business (statement of the projects, project scope and work carried out).

4 Accreditation procedure

Security evaluation laboratories interested in becoming listed as security evaluators within the BAROC approval scheme can apply for this at the BAROC approval office.

1. Lab applicants have to state their interest becoming accredited with a completed application form to BAROC and the documents described in section 3.
2. BAROC will answer to an application with a registration note and request further evidence on some or all of the above topics when needed.
3. BAROC can require an on-site audit of the lab applicants premises, its personnel, testing equipment, working procedures and manuals, in support of its evaluation of the documents.

4. When BAROC reaches the decision that the lab applicant is capable of carrying out security evaluations according to its approval scheme, the accreditation is granted in a formal letter together with the current version of the BAROC security requirements for FDSCD.

With the accreditation, the lab applicant is entitled to perform security evaluations according to the BAROC approval scheme. Evaluation working procedures are described in [SecEval].

5. The accreditation is granted for 2 years. After this period, the laboratory has to apply for a prolongation which is granted without further consideration when at least one security evaluation has been performed during the accreditation period. The accreditation can be withdrawn when the laboratory did not actively perform evaluations during the accreditation period.

Laboratories have to regularly report on their evaluation experiences.

BAROC reserves the right to withdraw an accreditation when there is evidence that the laboratory no longer fulfils the requirements stated above.

5 Fees

Accreditation fee is NT $ 1,500,000.00 (including tax) excluding travel expenses for audit if required.

Additional fee will be charged for NT$100,000.00 (including tax) of evaluation fee for each application case.

6 References

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

[SecEval] Requirements and procedure for security evaluations of chip card products and digital signature creation device for the Taiwanese payment system, Version 1.4 Date 2009-09-16.

[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

[ComCrit] ISO/IEC 15408:1999 Information technology -- Security techniques – Evaluation criteria for IT security, Part 1 to 3 (CC 2.1) and including final interpretations for compliance with CommonCriteria Version 2.2 and Common Methodology Part 2, Version 2.2; and in addition ISO/IEC 15408:2005 (CC Version 2.3)

[CC] *Common Criteria, Common Criteria for Information Technology Security Evaluation,*

Part 1: Introduction and General Model, Version 3.1, Revision 1, June 2006, CCMB-2006-06-001

Part 2: Security Functional Requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-002

Part 3: Security Assurance Requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-003

And/or

Part 1: Introduction and general model, July 2009, Version 3.1, Revision 3, Final, CCMB-2009-07-001

Part 2: Security functional components, July 2009, Version 3.1, Revision 3, Final, CCMB-2009-07-002

Part 3: Security assurance components, July 2009, Version 3.1, Revision 3 Final, CCMB-2009-07-003

[ISO17025] DIN EN ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories

7 Annex: Application form

Application form for security evaluation laboratories

Name of the applicant	Organisation and department name
Organisational affiliation	Legal status of organisation
Contact person	Name
Address	Street
	Zip code
	Town
	Country
	Phone
	Email
Accreditations already received	List of accreditations the laboratory received from other organisations (e.g. other payment scheme approval offices, security evaluation schemes)
Evaluations already conducted	List of security evaluations conducted (former payment chip card evaluations, former CC evaluations, other evaluation projects)
Signature of applicant	Place, date and signature
Documents provided with this application	Laboratory description*, CC accreditation certificate, Evidence on ISO 17025 compliance**, Full reports on former chip card evaluations***

* Names of evaluators, professional background, physical security of laboratory building, test equipment available.

** If not given as part of a CC accreditation.

*** If the reports of chip card evaluations are confidential information, the laboratory can anonymise project details as product codes, manufacturers etc.