Security requirements of BAROC for financial chip card approval and implementation

Version 2.1

Table of contents

1 Introduction

For the payment system in Taiwan the specifications of BAROC are obligatory. In addition to these functional requirements, the following security requirements have to be applied by

- Card Issuers,
- Financial Chip Card Software Developer,
- IC Manufacturers.

2 Chip card and terminal authentication (CCT_AUTH)

A chip card actively taking part in the communication process of a payment system has to authenticate itself to the Card Issuer on a one-to-one basis with the help of cryptographic procedures.

The chip card also has to provide functionality for terminal authentication.

2.1 Explanations:

2.1.1 CCT_AUTH_Expl_1

The permissible cryptographic algorithms for use within the cryptographic procedures should be selected from the list of approved cryptographic algorithms provided in *Encryption procedure* section 11.

2.1.2 CCT_AUTH_Expl_2

This requirement does not specify a particular authentication procedure for the initialisation and personalisation phase. Generally verifying the ownership of a secret piece of information authenticates the components. Using the terminal authentication functionality (see [FCOS] section 3.14) would be sufficient to fulfil this requirement.

2.1.3 CCT_AUTH_Expl_3

This requirement specifies the TAC authentication procedure and the terminal authentication procedure for the usage phase. Using the terminal authentication functionality and the TAC generation functionality (see [FCOS] section 3.14 & 3.8) would be sufficient to fulfil this requirement.

2.1.4 CCT_AUTH_Expl_4

Security related information includes the ICC Serial Number (TSEF S/N) and the Transaction Authentication Code (TAC). The serial number is a sequence counter for

transactions which is incremented by one upon each successful transaction signed by the chip card.

3 Message integrity (MES_INT)

As long as stored on the chip card, all security-relevant information included in the messages has to be protected with appropriate functionality against alteration.

Alterations of security-relevant information occurring during the transmission from the chip card to the Card Issuer have to be detected. The chip card should provide functionality to enable the payment system to detect unauthorised input of messages.

3.1 Explanations:

3.1.1 MES_INT_1

In particular, security-relevant information in messages includes TAC and ICC serial number.

3.1.2 MES_INT_2

Besides using software functionality, the protection of the security-relevant information on the chip card should also be done using appropriate hardware functionality (e.g. provided by the IC, see Hardware requirements section 8).

3.1.3 MES_INT_3

This requirement specifies the TAC generation and the ICC serial number generation functionality for the usage phase. Using the TAC generation functionality and the ICC serial number generation functionality (see [FCOS] section 3.8) would be sufficient to fulfil this requirement.

In addition, the basic integrity mechanisms of the file system management have to be used for securing the integrity of the input data for the TAC generation.

3.1.4 MES_INT_4

Before the usage phase the Card Issuer is responsible for the integrity of the security-relevant information. This includes all key data with related information and the initialisation / personalisation data. For verification of the fulfilment of this requirement the approval applicant has to provide appropriate documentary evidence that allows a judgement about the effectiveness of the procedures applied within the intended environment. Requirements Hardware requirements section 8, Encryption procedure section 11 and Personnel requirements section 13 have to be taken into account for this documentary evidence. Also see section 14 Approval applicants responsibility for approval documentation.

4 User authentication (USER_AUTH)

If the chip card based payment system requires user authentication by means of his PIN, it has to be ensured that specific functions can be executed only if the correct PIN is known.

4.1 Explanations:

4.1.1 USER_AUTH_EXP_1

If necessary, the user has to authenticate himself towards his chip card by typing in his PIN correctly. The chip card has to provide a function for PIN verification as described in [FCOS section 3.12].

Explanations SECRECY_1 and SECRECY_3 of section 5 have to be considered.

5 Secrecy of PINs and keys (SECRECY)

If the PIN or keys are processed or stored in the chip card, they have to be protected against any readout and unauthorised change.

Cryptographic keys must never be translated into plain text on electronic transmission paths. After the initialisation phase, which has to take place in a secure environment, keys have to be imported using secure channel.

No chip card must allow a PIN or key to be identified as the result of an exhaustive search.

5.1 Explanations:

5.1.1 SECRECY_1

This requirement has to be fulfilled at any time during usage phase, starting with the moment the PIN is keyed in. It is then permissible to pass the PIN in plain text on to the user's chip card via the keyboard, if it is ensured that the entered plain text PIN can never leave the physically secured area, which also includes the contacts of the chip card, and that the plain text PIN cannot be recorded within this area. The owner or user of the interface device used for the transaction (i.e. the acquirer, the merchant, the card holder) is responsible for the security of the used IFD.

5.1.2 SECRECY_2

For hardware components in which PINs or keys are stored and processed, the Hardware requirements section 8 also have to be considered before and during usage phase. Especially those keys are regarded as cryptographic keys, which are used for generating TACs and for terminal authentication.

5.1.3 SECRECY_3

It should not be allowed to guess PINs or keys by means of an exhaustive search. Especially the PIN verification has to be implemented according to [FCOS section 3.12] with the related error counter. The error counter handling (increasing or decreasing the error counter value before verification – resetting the value to default value after successful verification) should be done before the PIN verification in order to prevent an attack with DFA (power interruption).

5.1.4 SECRECY_4

The PIN has to be changeable during the usage phase by means of an appropriate command (for implementation details see [FCOS section 3.9 or 3.19]).

5.1.5 SECRECY_5

The cryptographic keys have to be changeable during the usage phase by means of an appropriate command (for implementation details see [FCOS section 3.19]).

Note: Before the usage phase keys must also be changeable by means of an appropriate command. The implementation details for this functionality are left to the approval applicants. However, in all cases the use of a secure channel is mandatory which includes the transfer of the keys in encrypted form.

6 Logging (LOG)

All transaction data within the chip card which is available for the reconstruction of the applicable transaction has to be logged.

It has to be made sure that the logged data can be evaluated in a controlled way.

Logged data must be protected against unauthorised changes.

6.1 Explanations:

6.1.1 LOG_1

Implementation of the logging functionality as described in [FCOS section 3.8] including the transaction data, the TAC and the ICC serial number would fulfil this requirement. At least the last 10 transactions should be logged. The approval applicant is free to log more than 10 transactions with ICC serial number on the chip card.

6.1.2 LOG_2

The functionality for controlled evaluation is given by the controlled reading of the transaction data through the interface of the chip card (with command described in [FCOS section 3.5]).

6.1.3 LOG_3

Authorised changes to transaction data are only allowed by the chip card itself. An authorised change is possible by overwriting the transaction data with new transaction data (new transaction number is larger than old transaction number, difference of transaction numbers depends on the number of transactions which can be stored). Deletion and modification of transaction data is not allowed.

7 Key management (KEY_MNG)

The chip card has to provide functionality for the purpose of distribution, management and, if applicable, the change and replacement of keys at regular intervals before and during usage phase.

7.1 Explanations:

7.1.1 KEY_MNG_1

Before the usage phase the chip card has to provide appropriate functionality to support the key distribution techniques specified by the Card Issuer. The usage of the key management functionality as described in [FCOS section 4.2] would fulfil this requirement. Nevertheless the Card Issuer is allowed to specify similar key distribution procedures and functionality to be provided by the chip card with an equivalent level of security. *Personnel requirements* section 13 have to be considered in this context.

7.1.2 KEY_MNG_2

During the usage phase the chip card has to provide appropriate functionality to support the key management procedures as specified by [FCOS section 3.19].

8 Hardware requirements (HW_REQ)

All encryption and decoding, recoding, the generation of TACs and cryptographic check procedures are conducted within Integrated Circuits (IC), which are specifically protected against unauthorised access. The appropriate keys are also stored in those IC.

In IC, security-relevant data and sequences (e.g. keys, programs) have to be protected against unauthorised amendment. Secret data (e.g. keys) must be protected against unauthorised readout. This must be guaranteed by the following means:

- The design of the IC, possibly in co-operation with the security mechanisms of the chip card software,
- Loading of programs into IC only during the production or cryptographic protection of the loading procedure,

- Cryptographic protection of the loading of security-relevant data, especially of cryptographic keys.

8.1 Explanations:

8.1.1 HW_REQ_1

The protection of data and programs in IC against amendment and/or readout has to be such that attacks carried out with a reasonable amount of time and effort become impossible during the operating life of the module. In this context the amount of time and effort needed to carry out a successful attack and the profit resulting from it have to result in a reasonable trade-off.

8.1.2 HW_REQ_2

To secure data and sequences, mechanical as well as electronic data memory protection should be provided.

8.1.3 HW_REQ_3

Undesirable functions must not be executable by an IC and the chip card.

8.1.4 HW_REQ_4

The recommendations from HW to SW for secure usage of the IC have to be fulfilled by the chip card (e. g. initialisation of SFRs for usage of HW features like side channel attacks countermeasures, active shielding, memory scrambling). Especially the specific application notes provided by the IC manufacturer and the evaluation results of HW certifications have to be followed by the chip card SW design. 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**. Additional augmentations are allowed.

8.1.5 HW_REQ_5

It is also recommended to use chip card HW for storage and processing of the sensitive data (especially the keys) that provide an equivalent level of security.

For verification of this recommendation the approval applicant shall provide appropriate documentary evidence to the approval office.

8.1.6 HW_REQ_6

In order to prevent the program to be tampered in any shape or form, the card operating system (COS) including the Financial application SW of Financial Chip Card shall be stored in NVM(Non-Volatile Memory), i.e., ROM or Flash memory which shall be irreversibly locked as read-only memory.

9 Sequence safeguarding (SEQ_SG)

It has to be ensured that the sequences of specific transaction steps and the simultaneously applied security-relevant data of a chip card based payment system cannot be manipulated.

The components involved, especially the user, must not be deceived concerning the transaction sequences.

It has to be ensured that once the usage phase of the chip card is reached, a phase earlier in life-cycle is no longer accessible.

9.1 Explanations:

9.1.1 SEQ_SG_1

As part of the access control functionality of the chip card some commands are allowed to be processed only after successfully performing previous commands. For example the terminal authentication is only allowed after a get challenge command has been successfully performed.

For a list of commands with sequence control see the following table:

Command under Sequence Safeguarding	**Condition (previously processed command)**	**Reference [FCOS]**
Terminal authentication	Generate random	Section 3.13 & 3.14
Generate TAC	Verify PIN	Section 3.12 , 3.8 & 4 (after usage phase)
Update key cipher	Set secure channel	Section 3.18 & 3.19

Table 1: Commands with Sequence safeguarding

9.1.2 SEQ_SG_2

The software developer is free to choose among available mechanisms for sequence control of the life-cycle (e.g. global chip card states, dedicated values, access control mechanisms). He has however to document the functionality implemented in the chip card.

9.1.3 SEQ_SG_3

The components involved, especially the user, must not be deceived concerning the transaction sequences. For fulfilling this requirement it is sufficient to implement the return codes as specified in [FCOS section 3.8].

10 Processing of other applications (PRO_APP)

If other than payment system related applications are processed in the chip card, this must not affect the security of the chip card use in payment systems.

10.1 Explanations:

10.1.1 PRO_APP_1

It has to be ruled out, for example, that the functions performing other applications cannot be misused in a compromising way in the payment system.

10.1.2 PRO_APP_2

If various applications can be carried out within a chip card, no application may affect the security of any other application.

10.1.3 PRO_APP_3

The software developer has to use an appropriate platform (e.g. MULTOS, GP) to prevent application specific data from one application being changed added or compromised by another application.

10.1.4 PRO_APP_4

Every time when security related functions for payment systems are carried out, the SW has to check whether the appropriate HW security settings for use of the HW security features of the IC are still valid. It is recommended that other applications should not change HW security settings.

11 Encryption procedure (ALGO)

Only encryption procedures that withstand a crypto analysis with selected plain text may be used.

11.1 Explanations:

11.1.1 ALGO_1

The security must not depend on the secrecy of the procedure or the cryptographic algorithm, but must be guaranteed by keeping the keys secret.

11.1.2 ALGO_2

For TAC generation at least one of the following cryptographic algorithms with related parameters' values should be used:

Algorithm	Reference	Parameters / key length
RSA	ANSI X9.31 PKCS 1	1024 bit
Triple-DES	FIPS 46-3	112 bit
AES	FIPS 197	128 bit

Table 2: List of approved algorithms for TAC generation

11.1.3 ALGO_3

Appropriate information should be provided about countermeasures implemented in SW and the use of the HW features for secure usage (also see HW_REQ_4 in section 8.1.4). Also see section 14 Approval applicants responsibility for approval documentation.

12 Clear representation (REPR)

Every chip card has to be clearly identifiable within the payment system.

12.1 Explanations:

12.1.1 REPR_1

The identification data have to be used to provide security-relevant messages with information about the sender and the receiver. This requirement is fulfilled with the inclusion of the Card Issuer bank ID and the ICC ID in messages as specified by [FCOS section 4].

13 Personnel requirements (PERS_REQ)

Trustworthy individuals are to be appointed for responsibility in the case of changes to approved system components for ensuring that either the security-relevant features of the components are maintained or that BAROC is notified about these changes respectively.

13.1 Explanations:

13.1.1 PERS_REQ_1

A change notice about the change of constituent parts of the chip card (IC, SW) has to be assigned to the approval office. The approval office will decide about the

appropriate action especially about the need for full or partial re-approval of the chip card.

14 Approval applicants responsibility for approval documentation

The approval applicant is requesting the approval for the chip card. Therefore he is also responsible for the appliance of the procedures as required by section 13, 3, 7, 8 and 11. For verification of the fulfilment of these requirements the approval applicant has to provide appropriate documentary evidence. The documentation has to allow a judgement about whether or not procedures applied by the vendors and developers fulfil the security requirements.

15 References

[FCOS] Functional Specification FISC COS, Version 2.2, date 2005-08-01

16 Glossary

AES	Short for the “Advanced Encryption Standard“ algorithm for symmetric cryptography
Approval applicant	Organisation that applies for a chip card security approval by BAROC.
Acquirer	Organisation that accepts chip cards as means for payment or for other purposes.
ATM	Automatic teller machine
BAROC	Bankers Association of the Republic of China
Card Issuer	Organisation that issues the chip card to a customer, the card holder. Usually banks function as Card Issuers.
Card Holder	Customer of a card issuer holding a personal chip card for payment or other applications.
DES	Short for the “Data Encryption Standard“ algorithm for symmetric cryptography
DFA	Differential fault analysis
DPA	Differential power analysis
ECC	Elliptic curve cryptography
FCOS	FISC Card Operating System
Functionality	Features of a chip card, terminal or payment network realized in hard- and software.

FISC	Financial Information Service Co. Ltd
IC	Integrated circuit
ICC	Integrated circuit chip card, also referred to as chip card
IFD	Interface device
MOB	Mobile banking terminal
MOD	Media on demand
PIN	Personal identification number
Procedure	Generic term for functionality, command, process etc.
RSA	Short for the “Rivest-Shamir-Adleman” algorithm for asymmetric cryptography
SFR	Special function register
SPA	Single power analysis
TAC	Transaction authentication code
Triple-DES	Variant of DES, the threefold application of DES with different keys for obtaining stronger encryption.