Security requirements of BAROC for Financial chip card and Digital Signature Creation Device (FDSCD) approval and implementation

Version 1.1

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

- Financial chip card and Digital Signature Creation Device (FDSCD) Issuers,
- Financial chip card and Digital Signature Creation Device Software Developer,
- Integrated Circuits (IC) Manufacturers.

2 FDSCD and terminal authentication (CCT_AUTH)

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

The FDSCD also has to provide functionality for transaction authentication code (TAC) generation, terminal authentication, signature creation, public key export authentication; certificate import authentication and remote unlock PIN (RUP) 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 [FS section 2.9]) would be sufficient to fulfil this requirement.

2.1.3 CCT_AUTH_Expl_3

This requirement specifies TAC generation procedure, the terminal authentication procedure and signature creation procedure for the usage phase. Using the TAC Generation functionality (see [FS section 2.5]), *Terminal Authentication* functionality and the signature creation functionality *RSA Cipher* (see [FS section 2.21]) 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 ICC serial number is a sequence counter for transactions which is incremented by one upon each successful transaction signed by the FDSCD.

2.1.5 CCT_AUTH_Expl_5

This requirement specifies the public key export authentication procedure for the usage phase. Using the *Read Public Key with MAC* functionality (see [FS section 2.19]) would be sufficient to fulfil this requirement.

2.1.6 CCT_AUTH_Expl_6

This requirement specifies the remote unlock PIN authentication procedure and certificate import authentication procedure for the usage phase. Using the *Remote Unlock PIN* functionality (see [FS section 2.22]) and *Write Certificate With MAC* functionality (see [FS section 2.18]) would be sufficient to fulfil this requirement.

3 Message integrity (MES_INT)

As long as stored on the FDSCD, 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 FDSCD to the verification entity have to be detected. The FDSCD should provide functionality to enable the verification entity to detect unauthorised input of messages.

Alterations of public key and certificate occurring during the transmission between the FDSCD and interface device (IFD) have to be detected. The FDSCD should provide functionality to enable the issuer or FDSCD itself 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 FDSCD 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 [FS] section 2.5) 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

This requirement specifies the signature creation functionality for the usage phase. Using the *RSA Cipher* functionality (see [FS section 2.21]) would be sufficient to fulfil this requirement.

In addition, the basic integrity mechanisms have to be used for securing the integrity of the input data from FDSCD edge for the signature creation.

3.1.5 MES_INT_5

This requirement specifies the public key export functionality and certificate import functionality for the usage phase. Using the *Read Public Key With MAC* functionality (see [FS section 2.19]) and W*rite Certificate With MAC* functionality (see [FS section 2.18]) would be sufficient to fulfil this requirement.

3.1.6 MES_INT_6

Before the usage phase the FDSCD 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 Random Number Generation.

4 User authentication (USER_AUTH)

If the FDSCD 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 FDSCD by typing in his PIN correctly. The FDSCD has to provide a function for PIN verification as described in [FS sections 2.7 and 2.23].

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

5 Secrecy of PINs and sensitive keys (SECRECY)

If the PIN or cryptographic keys (private key and secret key) are processed or stored in the FDSCD, they have to be protected against any readout.

Sensitive 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, secret keys have to be imported using secure channel.

No FDSCD must allow a PIN or sensitive 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 FDSCD 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 FDSCD, and that the plain text PIN cannot be recorded within this area. The owner or user of the interface device used for the transaction (e.g. the acquirer, the FDSCD issuer, the merchant, the FDSCD User) is responsible for the security of the used IFD.

5.1.2 SECRECY_2

For hardware components in which PINs or sensitive keys are stored and processed, the *Hardware requirements* section 8 also have to be considered before and during usage phase. Especially those sensitive keys are regarded as cryptographic keys, which are used for TAC generation authentication, public key export authentication, signature creation authentication, certificate import authentication, RUP authentication and terminal authentication.

5.1.3 SECRECY_3

It should not be allowed to guess PINs and sensitive keys by means of an exhaustive search or DFA. Especially the PIN verification has to be implemented according to [FS sections 2.7 and 2.23] 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 accordingly in order to prevent an attack with timing analysis (TA) or 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 [FS section 2.6]).

5.1.5 SECRECY_5

The secret keys have to be changeable during the usage phase by means of an appropriate command (for implementation details see [FS section 2.13).

Note: Before the usage phase secret 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 FDSCD 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 should include the transaction data, the TAC and the ICC serial number. 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 FDSCD.

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 [FS section 2.3]).

6.1.3 LOG_3

Authorised changes to transaction data are only allowed by the FDSCD 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 FDSCD has to provide functionality for the purpose of distribution, management and, if applicable, the change and replacement of secret keys at regular intervals before and during usage phase.

The FDSCD has to provide functionality for the purpose of creation and destruction of private and public keys at regular intervals during usage phase.

7.1 Explanations:

7.1.1 KEY_MNG_1

Before the usage phase the FDSCD has to provide appropriate functionality to support the secret key distribution techniques specified by the FDSCD Issuer. The usage of the Terminal Authentication functionality as described in [FS section 2.9] would fulfil this requirement. Nevertheless the FDSCD Issuer is allowed to specify similar secret key distribution procedures and functionality to be provided by the FDSCD with an equivalent level of security. Personnel requirements section 13 has to be considered in this context.

7.1.2 KEY_MNG_2

During the usage phase the FDSCD has to provide appropriate functionality to support the secret key management procedures as specified by Terminal Authentication functionality [FS section 2.9].

7.1.3 KEY_MNG_3

During the usage phase the FDSCD has to provide appropriate functionality to support the key pair creation procedures as specified by Generate RSA Key [FS section 2.16]. The private key used for signature creation can practically occur only once and cannot be reconstructed from the public key or any other public data. In that context ‘practically occur once’ means that the probability of equal private key is negligible low.

For generation of keys some requirements should be considered carefully:

- If using a number sieve for generation of prime numbers and the prime candidates are strong cohering (e. g. by addition of 2) then it must not be possible by side channel analysis to investigate by which prime factors the prime candidate are divisible.
- During Fermat and Miller-Rabin test modular exponentiations are done. They have to be resistant against SPA. Otherwise the prime candidates can be spied out.
- The probability that a chosen prime number is not prime has to be less than 2-100. This is normally fulfilled by combination of several prime tests. Therefore it s required that the probability cannot be reduced by fault attacks, e. g. breaking the loop of different Miller-Rabin-tests.
- It must not be possible to force short prime numbers.
- If dp, dq and qinv are generated, then the inversion of q respective e for calculation of dp, dq and qinv must be resistant to SPA since information about q respective p might be gathered.
- The generated key pair should be tested for consistency. E. g. a trial en- and decryption with the key pair could be done in order to show consistency of parameters.

7.1.4 KEY_MNG_4

During the usage phase the FDSCD has to provide appropriate functionality to support the key pair destruction procedures as specified by [FS section 2.16, option p1 = 01h], The FDSCD shall provide safe destruction techniques for the private key. It must be assured that private keys are destroyed securely e.g. by overwriting with new keys or zeroizing.

8 Hardware requirements (HW_REQ)

All crypto operations and key pair generation, which are conducted within Integrated Circuits (IC), shall be 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 FDSCD 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 FDSCD.

8.1.4 HW_REQ_4

The recommendations from HW to SW for secure usage of the IC have to be fulfilled by the FDSCD (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 FDSCD 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 FDSCD 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) of FDSCD shall be stored in ROM, i.e. ROM mask.

9 Sequence safeguarding (SEQ_SG)

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

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

It has to be ensured that once the usage phase of the FDSCD 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 FDSCD 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.

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 FDSCD states, dedicated values, access control mechanisms). He has however to document the functionality implemented in the FDSCD.

9.1.3 SEQ_SG_3

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

10 Processing of other applications (PRO_APP)

If other than payment system related applications are processed in the FDSCD, this must not affect the security of the FDSCD 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 FDSCD, 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, signature generation, public key export authentication, certificate import authentication, RUP authentication and terminal authentication 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	2048 bit
Triple-DES	FIPS 46-3	112 bit
AES	FIPS 197	128 bit

ECC	ANSI X9.62 FIPS 186-3	160 bit

Table 1: List of approved algorithms

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, Random Number Generation.

12 Clear representation (REPR)

Every FDSCD 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 FDSCD Issuer bank ID and the ICC ID in messages as specified by FDSCD Issuer during personalization.

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 FDSCD (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 FDSCD.

14 Random Number Generation

The quality of the RND generated should be as minimum that it is practically impossible for an adversary with high attack potential to work out or guess the numbers which precede or follow a random number subsequence ri,ri+1,…,ri+j or to work out or guess an internal state.

A physical RNG (TRNG) with class P2 and strength of mechanism and functionality high according to [AIS31] would fulfill these requirements.

Also a deterministic RNG according to [AIS20] Class K3 with entropy H(pA) ≥ 100 would fulfill these requirements. For future use of the products after 2010 more entropy H(pA) ≥ 120 is recommended.

15 Approval applicant's responsibility for approval documentation

The approval applicant is requesting the approval for the FDSCD. 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.

16 References

[AIS20] Application Notes and Interpretation of the Scheme (AIS) AIS 20, Version 1, 1999-12-02, Status: Mandatory, Subject: Functionality classes and evaluation methodology for deterministic random number generators, Publisher: Certification body of the BSI, Section II 2, as part of the certification scheme

[AIS31] Application Notes and Interpretation of the Scheme (AIS), AIS 31, Functionality classes and evaluation methodology for physical random number generators, Version 1, 2001-09-25, Bundesamt für Sicherheit in der Informationstechnik.

[FS] Annex 2, Financial chip card and DSCD (FDSCD) Functional Specification, Version 1.1 Date 2009-09-16

17 Glossary

AES — Short for the "Advanced Encryption Standard" algorithm for symmetric cryptography

Approval applicant	Organisation that applies for a FDSCD security approval by BAROC.
BAROC	The **B**ankers **A**ssociation of the **R**epublic **O**f **C**hina
FDSCD Issuer	Organisation that issues the FDSCD to a customer, the FDSCD holder. Usually banks function as Card Issuers.
FDSCD User	Customer of a FDSCD holding a personal FDSCD 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 FDSCD, terminal or signature network realized in hard- and software.
FISC	Financial Information Service Co. Ltd
HW	Hardware
IC	Integrated circuit
ICC	Integrated circuit chip card, also referred to as chip card
IFD	Interface device
PIN	Personal identification number
Procedure	Generic term for functionality, command, process etc.
RSA	Short for the “Rivest-Shamir-Adleman” algorithm for asymmetric cryptography
RUP	Remote Unlock PIN
SFR	Special function register
SPA	Single power analysis
SW	Software / Firmware
Triple-DES	Variant of DES, the threefold application of DES with different keys for obtaining stronger encryption.