Common Security Evaluation &
Certification Consortium
of GBIC and UKF

Common.SECC

Security Evaluation & Certification Consortium

Rule Book

Annex 8

Evaluation of the POI Payment Application

Version 0.9

30.03.2020

1 Introduction

In addition to the POI platform (for the definition see the current version of the Common.SECC Rule Book) the Payment Application of the POI plays an important role regarding POI security.

This is mainly due to the security requirement of a “secure process flow” to be provided by the application software, which is signed by the vendor and thus ensures the authenticity of the payment application and its processing activity. The “secure process flow” can be looked at as a state machine ensuring the proper usage of security services. The proper and evaluated security services provided by the POI firmware only meet their purpose if they are used by the application as defined by this mechanism implemented in the application software.

Without an evaluation of the payment application the risk owner can at best only assume that the POI’s proper platform services being evaluated are indeed used by the payment application. Evidence can only be provided by a sound application software analysis.

Therefore the Common.SECC Consortium enhances its services and offers the optional security certification of the POI payment application. An approval body may choose to mandate this certification.

This document describes the security requirements to be evaluated and the requirements to perform the security evaluation.

2 The POI Payment Application

The POI Payment Application is the software which is responsible for the processing of the different card services, the processing of the different interfaces of the POI (e.g. customer, acquirer, card reader, terminal management), the POI configuration, error handling and usage of the services provided by the POI platform. There will be a Payment Application loaded into the POI when it is evaluated, but that may not be the Payment Application that is loaded into the POI when it is deployed. The Common.SECC application certification targets at any application that is suitable for deployment.

3 Security Requirements for the POI Payment Application

The security requirements for the POI Payment Application are defined as follows. For a high level version of these requirements, see the SEPA Card Standardization Book of Requirements “Volume” (www.e-csg.eu, Book 4 “Security Requirements,, chapter 3.7.1, section N-Requirements for the POI payment application).

1. The platform provides security functions. These security functions *shall* be called by the payment application according to a secure process flow as defined by the pay-

ment application. This secure process flow is not part of the platform evaluation. The following security functions are considered as part of the secure process flow.

a) PIN entry
b) confirmation of the amount
c) verification of the online and offline authorisation result
d) prompting of the transaction result and
e) maintaining security related transaction data

1.1 The above mentioned secure process flow shall be controlled by the POI in order that it cannot be bypassed by logical means.

1.2 Online and offline (EMV kernel) process order shall not be allowed to be manipulated. A state machine (or other solutions) that controls the online and offline process steps and the final status screen prompt in the application *shall* be present.

1.3 A state machine *shall* control the secure process flow even if the POI is cut from the message exchange or from power supply. If there is no response on a request or keys are not pressed according to expected time outs the secure process flow *shall* react in an adequate way.

2. Security functions of the platform implementing authentication and integrity for the online messages, including transaction data, *shall* be called according to the secure process flow.

3. Any secure process flow *shall* only use random numbers generated by the random number generator which has been verified in the platform evaluation.

4. The following requirements *shall* hold for the EMV related part of the secure process:
   a) Authenticity and integrity of the Root CA public key *shall* be preserved (during loading and transaction)
   b) Authenticity and integrity of the EMV management data *shall* be preserved.
   c) Only authorized entities *shall* be able to change the EMV code, root keys and management data.
   d) The EMV related parts *shall* not be abused via logical anomalies.
   e) The amount *shall* not be manipulated during the transaction.
   f) Cryptographic functions of the platform *shall* be used if applicable.

5. It *shall* not be possible to bypass the display of the transaction amount by logical means. The cardholder *shall* not be deceived about the secure process flow showing another amount than the amount being authorised. This holds also for the key the

cardholder is pressing to confirm or to cancel a transaction. The execution of functions depending on the user authentication *shall* only be allowed, e.g. the authorisation of a transaction, if the user authentication has been performed successfully.

Table 1 allocates the typical contributions to meet these requirements to the POI platform, the payment application and the EMV kernel for guidance and support.

Table 1: Contribution of the different POI parts to meet the security requirements for a payment application

Security Requirement	**Platform part only supporting but not implementing the secure process flow (in scope of the Common.SECC platform security certification)**	**Payment application part which implements the secure process flow (in scope of the Common.SECC application security certification)**	**EMV kernel part which implements the secure process flow (out of scope of the Common.SECC security evaluation)**
The platform provides security functions. These security functions *shall* be called by the payment application according to a secure process flow as defined by the payment application. This secure process flow is not part of the platform evaluation. The following security functions are considered as part of the secure process flow. The secure process flow consists of	The platform evaluation at best assumes that the secure process flow is implemented in a payment application running on the platform as well as in the EMV kernel. Thus the secure process flow is <u>not</u> covered by the platform evaluation.		
a) PIN entry	PIN entry is processed by the platform (asking for PIN entry at the display, PIN entry and PIN processing, feedback to the display).	Initiating PIN entry and processing the result of the PIN verification (verification successful, verification failed) are assumed to be processed by the payment applica-	Processing VERIFY command and related retry counters are assumed to be processed by the EMV kernel.

Security Requirement	Platform part only supporting but not implementing the secure process flow (in scope of the Common.SECC platform security certification)	Payment application part which implements the secure process flow (in scope of the Common.SECC application security certification)	EMV kernel part which implements the secure process flow (out of scope of the Common.SECC security evaluation)
		tion.	
b) confirmation of the amount	See requirement 5.		
c) verification of the online and offline authorisation result	See requirement 2. for online. See requirement 4. for offline.		
d) prompting of the transaction result and	See requirement 5.		
e) maintaining security related transaction data	Platform, payment application and EMV kernel may process security related transaction data. The platform, the payment application and the EMV kernel have to counter attacks on transaction data e.g. attacks on the integrity of the data.		

Security Requirement	**Platform part only supporting but not implementing the secure process flow (in scope of the Common.SECC platform security certification)**	**Payment application part which implements the secure process flow (in scope of the Common.SECC application security certification)**	**EMV kernel part which implements the secure process flow (out of scope of the Common.SECC security evaluation)**
The above mentioned secure process flow *shall* be controlled by the POI in order that it cannot be bypassed by logical means.	Platform, payment application and EMV kernel *shall* control the secure process flow.		
Online and offline (EMV kernel) process order shall not be allowed to be manipulated. A state machine (or other solutions) that controls the online and offline process steps and the final status screen prompt in the application *shall* be present.	No state machine is assumed to be part of the platform.	The (general) state machine is part of the payment application.	The EMV kernel is expected to include the EMV Terminal Risk Management as state machine.
A state machine *shall* control the secure process flow even if the POI is cut from the message exchange or from power supply.	Transport layers are provided by the platform.	The application layer is part of the payment application.	N/A
If there is no response on a request or keys are not pressed according to expected time outs the secure process flow *shall* react in an adequate way.			
6. Security functions of the platform implementing authentication and integrity for the online messages, including transaction data, *shall* be called	Cryptographic signature/ authentication code key management and signature/ authentication code key usage are	The calls for the calculation and verification of signatures/ authentication codes of online messages (re-	N/A

Security Requirement	**Platform part only supporting but not implementing the secure process flow** **(in scope of the Common.SECC platform security certification)**	**Payment application part which implements the secure process flow** **(in scope of the Common.SECC application security certification)**	**EMV kernel part which implements the secure process flow** **(out of scope of the Common.SECC security evaluation)**
according to the secure process flow. For a platform not covering all security functions for key derivation the missing functions *shall* be part of the payment application.	part of the platform.	quests, responses) are part of the payment application. Especially signature/ authentication codes are verified before the received online message is used.	
Any secure process flow *shall* only use random numbers generated by the random number generator which have been verified in the platform evaluation.	The random number generator is provided by the platform.	The payment application uses the evaluated random generator provided by the platform.	The EMV kernel uses the evaluated random number generator provided by the platform.
The following requirements *shall* hold for the EMV related part of the secure process flow: a) Authenticity and integrity of the Root CA public key *shall* be preserved (during loading and transaction) b) Authenticity and integrity of the EMV management data *shall* be preserved. c) Only authorized entities *shall* be able to change the EMV code, root keys	Note: The POI does not apply cryptography with confidential keys for EMV transactions. Only public key cryptography is applied in the EMV part of the POI.		
	Ad a), b) c) The platform itself may process the root key and other EMV management data. In such a case authenticity and integrity (e.g. during a download) is expected to be protected by the platform.	The results of the EMV kernel are processed by the payment application. E.g. the rejection of an offline transaction, the rejection of an offline PIN verification, …	Ad a), b) c) The EMV kernel itself may process the root key and other EMV management data. In such a case authenticity and integrity (e.g. during a download) is expected to be protected by the EMV kernel.

Security Requirement	Platform part only supporting but not implementing the secure process flow (in scope of the Common.SECC platform security certification)	Payment application part which implements the secure process flow (in scope of the Common.SECC application security certification)	EMV kernel part which implements the secure process flow (out of scope of the Common.SECC security evaluation)
and management data. d) The EMV related parts *shall* not be abused via logical anomalies. e) The amount *shall* not be manipulated during the transaction. f) Cryptographic functions of the platform *shall* be used if applicable.	Depending on the design the platform may have the EMV kernel integrated or may run the EMV kernel as a separated application. In both case the EMV kernel needs to be protected by the platform against manipulation. Ad d) Transport layers are provided by the platform. Ad f) Cryptographic functions of the EMV kernel are the public key algorithms for EMV. These functions are expected to be provided by the platform. This holds especially for the cryptographic functions used to encrypt the PIN in case of an offline PIN encryption.		Ad d) The application layer is part of the EMV kernel. Ad e) The amount is sent to the card.
It *shall* not be possible to bypass the display of the	Access to the display and information	The payment application completes	N/A

Security Requirement	Platform part only supporting but not implementing the secure process flow (in scope of the Common.SECC platform security certification)	Payment application part which implements the secure process flow (in scope of the Common.SECC application security certification)	EMV kernel part which implements the secure process flow (out of scope of the Common.SECC security evaluation)
transaction amount by logical means. The cardholder *shall* not be deceived about the secure process flow showing him another amount than the amount being authorised. This holds also for the key the cardholder is pressing to confirm or to cancel a transaction. The execution of functions depending on the user authentication *shall* only be allowed, e.g. the authorisation of a transaction, if the user authentication has been performed successfully.	about pressed keys (showing texts/amount and amount confirmation) are provided by the platform. The amount is received by an external interface of the platform (e.g. cash register) or entered via the keypad of the platform. Keypad status and display status are controlled by the platform. Secure mechanisms to download applications as well as secure application separation are part of the platform.	the transaction (approved, declined or aborted) depending on the pressed key (confirm or cancel/abort). The payment application processes the received amount. Which texts are shown at the display is controlled by the payment application. The secure process flow of the payment application considers the results of the PIN verification as well as amount confirmation/rejection.	

4 Requirements for the Security Evaluation of the POI Payment Application

The evaluation of the payment application according to the security requirements defined in chapter 3 must be performed by a source code analysis of the payment application ("platform" and "payment application" as indicated to be in scope in Table 1). The results have to be integrated in the AVA Class of the ETR.

The EMV Kernel is indicated to be out of scope of the evaluation of the payment application because it is sufficiently tested within the functional part of the certification being covered outside of Common.SECC.

Within the evaluation the requirements for a source code analysis defined in Annex 4 of the Rule Book must be met.

5 Certification Service

Common.SECC offers the security certification of the POI Payment Application according to this document as an option.

Name and version of the certified application will be published on the Common.SECC web site.