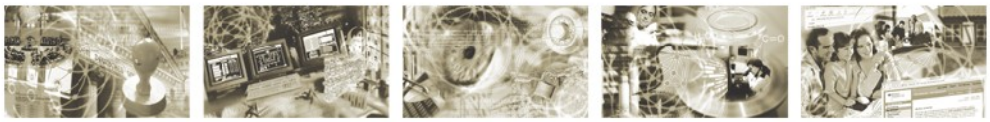
Bundesamt
für Sicherheit in der
Informationstechnik



Amendment to BSI TR-03105 Part 5.2 V1.1

Version: **Release 1**

Status: **final**

Date: **30.05.2012**

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de

Content

Amendment to BSI TR-03105 Part 5.2 V1.1 1

1 Introduction 4

2 Test cases 4

2.1 Terminal Authentication 4

2.1.1 Test case R_TA_2.1.1 4

2.1.2 Test case R_TA_2.1.2 4

2.1.3 Test case R_TA_4.3.2 5

2.2 Access to the eID Application 6

2.2.1 Test case R_eID_5.1.1 6

2.2.2 Test case R_eID_5.1.2 7

2.2.3 Test case R_eID_5.2.1 8

2.2.4 Test case R_eID_5.3.1 8

1 Introduction

This amendment defines changes of test cases in BSI TR-03105 Part 5.2 Version 1.1. The amendment replaces the herein described test cases. The purpose of this amendment is to collect corrections and clarifications of the BSI TR-03105 Part 5.2 to provide a systematic and formal document in addition. The changes defined in this document will be taken as comments and eventually be adopted to a new version of the BSI TR-03105 Part 5.2.

2 Test cases

All test cases described in this chapter replace the test cases with the same Test-ID in the BSI TR-03105 Part 5.2. The changes are highlighted.

2.1 Terminal Authentication

2.1.1 Test case R_TA_2.1.1

Deleted in Amendment Release 1

2.1.2 Test case R_TA_2.1.2

Test ID	R_TA_2.1.2
Purpose	Check that reader aborts terminal authentication if the terminal certificate description used in the terminal authentication protocol is different from the terminal certificate description used in the PACE protocol.
References	[TR-03110], 4.4, B.3, C.4.1; [TR-03119],
Profiles	R_PACE ~~AND R_TA~~
Preconditions	Certificate with role authentication terminal and access rights according to Table 28, No. 1; CA certificates according to Table 31, No. 1, 2 The PACE protocol has been executed successfully with CAN in the reader. EstablishPACEChannel must contain a complete certificate description (CERT_DESC) as described in chapter 5.2.3. After PACE protocol especially the following eCard data are available in UT: • PK_PICC (public key of the eCard) • D_PICC (static domain parameters of the eCard) • ID_PICC (identification of the eCard) A Secure Messaging Channel (SM) is established between reader and LT after PACE protocol.
Test scenario	The execution steps have to be performed as described in chapter 5.3.2: UT sends command APDUs to the test object reader via PC/SC (without SM). LT receives command APDUs (with SM) from the reader and sends response

	APDUs (with SM) back to the reader. UT receives response APDUs from the reader via PC/SC (without SM). The return codes in all response APDUs are positive ('90 00'). The hash value of the terminal certificate description submitted by UT in the command APDU to PSO: Verify Certificate is different from the hash value which the reader had to calculate from the terminal certificate description (CERT_DESC) used in the PACE protocol.
Expected results	Each command APDU received at LT is correctly coded and secured by SM and coincides apart from SM with the command APDU sent by UT directly before. The SM in the command APDU generated by the reader and received by LT is correct. UT receives response APDUs to the commands MSE: Set DST and PSO: Verify Certificate for all certificates of the certificate chain which are correctly coded without SM. The response APDUs to MSE: Set DST and PSO: Verify Certificate (for the CV certificates) coincide apart from SM with the response APDU sent by LT directly before. The response APDU to PSO: Verify for the terminal certificate received by UT consists of the negative return code '69 85'. It is expected that the reader aborts protocol execution after sending this return code.
Post processing	Reset of eCard and reader

2.1.3 Test case R_TA_4.3.2

Test ID	R_TA_4.3.2
Purpose	The reader aborts terminal authentication if it receives an incorrect SM data objects from LT in response APDU to command MSE: Set DST (tag '8E' has false length, '07' instead if '08'). Check that the session keys are deleted after error in secure messaging handling. The PACE protocol is executed with password CAN
References	[TR-03110]
Profiles	R_PACE
Preconditions	Certificate with role signature terminal and access rights according to Table 29, No. 1; CA certificates according to Table 32, No. 1, 2 Make certificates and the password CAN available in UT. The PACE protocol has been executed successfully with password-IDs CAN in the reader. After PACE protocol especially the following eCard data are available in UT: -PK_PICC (public key of the eCard) -D_PICC (static domain parameters of the eCard) -ID_PICC (identification of the eCard) A Secure Messaging Channel (SM) is established between reader and LT after PACE protocol.
Test scenario	1. LT receives command MSE: Set DST with SM as described in chapter 5.3.2 and sends response APDUs with incorrect SM (MAC tag '8E' has

	only 7 bytes data) back to the reader for this command. Response APDU: 99 02 <SW1SW2> 8E 07 <MAC> <SW1SW2> The return code in response APDU to MSE: Set DST is positive ('9000'). 2. UT calls PC/SC function SCardControl with InBuffer for EstablishPACEChannel (see chapter 5.2.3), where the positions in InBuffer are defined as follows: • <PIN-ID>: '02' (CAN is used) • <CHAT>: Restricted CHAT for terminal certificate as specified in Profiles • <PIN>: value of the password • <CERT_DESC>: certificates description 3. LT receives command APDUs without SM from the test object reader and sends response APDUs without SM back to the reader as described in chapter 5.3.1. The return codes in all response APDUs are positive ('90 00'). 4. UT receives OutBuffer of SCardControl (see chapter 5.2.4).
Expected results	1. UT received error code 'F0 10 00 01' (Communication abort). 2. – 3. The command APDUs which LT receives from the reader are built up as described in chapter 5.3.1 with the following additions: • The <PIN-ID> in command APDU to MSE: Set AT is '02', CAN is used. • The role in <OID-Role> in command APDU to MSE: Set AT is '02' (authentication terminal). • The <access rights> in command APDU to MSE: Set AT are as defined in Table 28, No. 1. 4. For the OutBuffer of SCardControl, that UT receives (see chapter 5.2.4), the following holds: • <Result_Code>: The result code is positive (i. e. '00 00 00 00'). • <status_mse>: The status code for command MSE: Set AT is '90 00'. • <data_card_acc>: The transmitted eCard data for card access coincide with the data of EF.CardAccess in LT. • <CAR1> and <CAR2>: The current and previous CAR are as defined in the eCard. • <IDPICC>: The field contains the correct ID_PICC.
Post processing	Reset of eCard and reader

2.2 Access to the eID Application

2.2.1 Test case R_eID_5.1.1

Test ID	R_eID_5.1.1
Purpose	Check that an unauthenticated terminal supports the password management function to change the PIN. The current PIN is *not* a transport PIN.

References	[TR-03110], 3.5.1; [PCSC10]
Profiles	R_PACE AND R_eID
Preconditions	The PACE protocol has been executed successfully with PIN as user input via PIN-Pad, where the PIN is not a transport PIN. After execution of this protocol, a Secure Messaging Channel (SM) is established between reader and LT.
Test scenario	UT sends command FEATURE_MODIFY_PIN_DIRECT to the test object reader via PC/SC. Since the SM channel is a established with the current active PIN, only the new PIN shall be requested as user input. LT receives command APDUs with SM from the reader and sends response APDUs with SM back to the reader. UT receives response APDUs from the reader via PC/SC. The return codes in all response APDUs are positive ('90 00').
Expected results	Each command APDU received at LT is correctly coded and secured by SM and coincides with the command APDU sent by UT directly before. Each response APDU received at UT is correctly coded and coincides with the response APDU sent by LT directly before.
Post processing	The original PIN is restored in the eCard. Reset of eCard and reader

2.2.2 Test case R_eID_5.1.2

Test ID	R_eID_5.1.2
Purpose	Check that an unauthenticated terminal supports the password management function to change the PIN. The current PIN is a transport PIN.
References	[TR-03110], 3.5.1; [PCSC10]
Profiles	R_PACE AND R_eID
Preconditions	The PACE protocol has been executed successfully with PIN as user input via PIN-Pad, where the PIN is a transport PIN. After execution of this protocol, a Secure Messaging Channel (SM) is established between reader and LT.
Test scenario	UT sends command FEATURE_MODIFY_PIN_DIRECT to the test object reader via PC/SC. Since the SM channel is a established with the transport PIN, only the new PIN shall be requested as user input. LT receives command APDUs with SM from the reader and sends response APDUs with SM back to the reader. UT receives response APDUs from the reader via PC/SC. The return codes in all response APDUs are positive ('90 00').
Expected results	Each command APDU received at LT is correctly coded and secured by SM and coincides with the command APDU sent by UT directly before. Each response APDU received at UT is correctly coded and coincides with the response APDU sent by LT directly before.
Post processing	Reset of eCard and reader

2.2.3 Test case R_eID_5.2.1

Test ID	R_eID_5.2.1
Purpose	Check that an unauthenticated terminal supports the password management function to reset the retry counter for the PIN using the PUK.
References	[TR-03110], 3.5.1; [PCSC10]
Profiles	R_PACE AND R_eID
Preconditions	The PIN is blocked in the eCard. The PACE protocol has been executed successfully with PUK as user input via PIN-Pad. After execution of this protocol, a Secure Messaging Channel (SM) is established between reader and LT.
Test scenario	UT sends command APDU “Reset Retry Counter” without SM to the test object reader. LT receives command APDUs with SM from the reader and sends response APDUs with SM back to the reader. UT receives response APDUs from the reader via PC/SC. The return codes in all response APDUs are positive (SW '90 00').
Expected results	Each command APDU received at LT is correctly coded and secured by SM and coincides with the command APDU sent by UT directly before. Each response APDU received at UT is correctly coded and coincides with the response APDU sent by LT directly before.
Post processing	Reset of eCard and reader

2.2.4 Test case R_eID_5.3.1

Test ID	R_eID_5.3.1
Purpose	Check that an unauthenticated terminal supports the password management function to set a new PIN using the PUK.
References	[TR-03110], 3.5.1; [PCSC10]
Profiles	R_PACE AND R_eID AND R_Chg_PIN_PUK
Preconditions	The PACE protocol has been executed successfully with PUK as user input via PIN-Pad. After execution of this protocol, a Secure Messaging Channel (SM) is established between reader and LT.
Test scenario	UT sends command FEATURE_MODIFY_PIN_DIRECT to the test object reader via PC/SC. Since the SM channel is a established with the PUK, only the new PIN shall be requested as user input. LT receives command APDUs with SM from the reader and sends response APDUs with SM back to the reader. UT receives response APDUs from the reader via PC/SC. The return codes in all response APDUs are positive ('90 00').
Expected results	Each command APDU received at LT is correctly coded and secured by SM and coincides with the command APDU sent by UT directly before. Each response APDU received at UT is correctly coded and coincides with the response APDU sent by LT directly before.

Post processing	The original PIN is restored in the eCard. Reset of eCard and reader