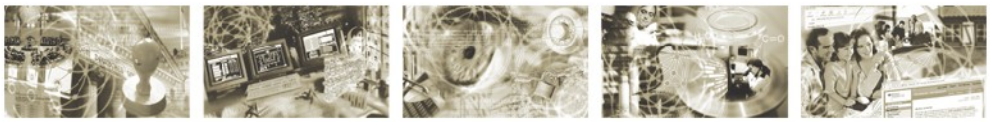
Bundesamt
für Sicherheit in der
Informationstechnik



Amendment to BSI TR-03105 Part 3.3

Version: **Release 3**

Status: **final**

Date: **04.06.2012**

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

Content

1 Introduction

This amendment defines changes of test cases and certificate descriptions of **BSI TR-03105 Part 3.3 Version 1.03**. The amendment does add or replace the herein described test case and certificates. The purpose of this amendment is to collect corrections and clarifications of the TR-03105 Part 3.3 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 TR-03105 Part 3.3.

2 Profiles

2.1 Protocol profiles

Add the following profile to the protocol profile table (chapter 2.2.2 in TR-03105 Part 3.3):

Profile-ID	Profile	Remark
CS	Chip Security	A MRTD which which stores a ChipSecurity file containing PrivilegedTerminalInfo with chip-individual keys and eIDSecurityInfo.

Annex A shall be extended in order to declare the support of this new profile.

3 Certificates

All certificates described in this chapter replace the certificates with the same ID in the BSI TR-03105 Part 3.3.

3.1 Certificate Set 17

3.1.1 DV_CERT_17

ID	DV_CERT_17
Purpose	This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits access to all eID special functions. It also permits read access to DG1 for testing access permissions.
Version	Am_3
Referred by	Test case EAC2_ISO7816_L_17, Test case EAC2_ISO7816_L_18, Test case EAC2_ISO7816_L_19, Test case EAC2_ISO7816_L_20, Test case EAC2_ISO7816_L_21, Test case EAC2_ISO7816_L_22, Test case EAC2_ISO7816_L_23, Test case EAC2_ISO7816_L_24, Test case EAC2_ISO7816_L_25, Test case EAC2_ISO7816_L_26, Test case EAC2_ISO7816_L_27, Test case EAC2_ISO7816_L_28, Test case EAC2_ISO7816_M_6, Test case EAC2_ISO7816_O_9, Test case EAC2_ISO7816_O_10, Test case EAC2_ISO7816_O_11, Test case EAC2_ISO7816_O_12, Test case EAC2_ISO7816_P_15, Test case EAC2_ISO7816_P_16, Test case EAC2_ISO7816_P_17, Test case EAC2_ISO7816_P_18, Test case EAC2_ISO7816_Q_1, Test case EAC2_ISO7816_Q_2, Test case EAC2_ISO7816_Q_3, Test case EAC2_ISO7816_Q_4, Test case EAC2_ISO7816_Q_6, Test case EAC2_ISO7816_Q_7, Test case EAC2_ISO7816_Q_8, Test case EAC2_ISO7816_Q_10, Test case EAC2_ISO7816_Q_11, Test case EAC2_ISO7816_Q_12, Test case EAC2_ISO7816_Q_13, Test case EAC2_ISO7816_Q_15, Test case EAC2_ISO7816_R_1, Test case EAC2_ISO7816_R_3, Test case EAC2_ISO7816_R_5, Test case EAC2_ISO7816_R_6

Content definition	**7F 21** *aa*
	  7F 4E *bb*
	  5F 29 01 00
	  42 *cc dd*
	  7F 49 *ee ff*
	  5F 20 *xx yy*
	  7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 00 00 01 FF
	  5F 25 06 *gg*
	  5F 24 06 *hh*
	  5F 37 *ii jj*
	
	aa is the encoded combined length of certificate body and signature objects
	bb is the encoded length the certificate body object
	cc is the encoded length of the Certificate Authority Reference

	dd is the placeholder for the Certificate Authority Reference (cc bytes) *ee* is the encoded length of the certificate's public key, *ff* is the placeholder for the certificate's public key bytes (ee bytes), *xx* is the encoded length of the Certificate Holder Reference *yy* is the placeholder for the Certificate Holder Reference (xx bytes) *gg* is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETESTDVDE017
	Certificate Holder Authorization	Official domestic DV, read DG1, eID-Specials (all)
	Certificate effective date	$CVCA_{eff}$
	Certificate expiration date	$CVCA_{eff}$+ 1 month
	Public Key reference	Public key of key pair DV_KEY_17
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17

3.1.2 AT_CERT_17h

This certificate was added in release 3 of this amendment.

ID	AT_CERT_17h
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_17. It encodes access rights for the eID special function “CAN allowed” and “Privileged Terminal”.
Version	Am_3
Referred by	Test case EAC2_ISO7816_L_37
Content definition	**7F 21** *aa* **7F 4E** *bb* **5F 29** 01 00 **42** *cc dd* **7F 49** *ee ff* **5F 20** *xx yy* **7F 4C** 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 00 18 **5F 25** 06 *gg* **5F 24** 06 *hh* **5F 37** *ii jj* *aa* is the encoded combined length of certificate body and signature objects *bb* is the encoded length the certificate body object *cc* is the encoded length of the Certificate Authority Reference *dd* is the placeholder for the Certificate Authority Reference (cc bytes) *ee* is the encoded length of the certificate's public key, *ff* is the placeholder for the certificate's public key bytes (ee bytes), *xx* is the encoded length of the Certificate Holder Reference

	yy is the placeholder for the Certificate Holder Reference (xx bytes) *gg* is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	DETESTDVDE017
	Certificate Holder Reference	DETESTATDE017
	Certificate Holder Authorization	Terminal, CAN allowed, Privileged Terminal
	Certificate effective date	$CVCA_{eff}$
	Certificate expiration date	$CVCA_{eff}$+ 1 month
	Public Key reference	Public key of key pair AT_KEY_17
	Signing Key reference	Signed with the private key of key pair DV_KEY_17

3.2 Certificate Set 21

3.2.1 DV_CERT_21

ID	DV_CERT_21
Purpose	This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits write access to all elementary files
Version	Am_1
Referred by	Test case EAC2_ISO7816_L_15 Template, Test case EAC2_ISO7816_O_7 Template
Content definition	**7F 21** *aa* **7F 4E** *bb* **5F 29** 01 00 **42** *cc dd* **7F 49** *ee ff* **5F 20** *xx yy* **7F 4C** 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 BE 1F FF FF 10 **5F 25** 06 *gg* **5F 24** 06 *hh* **5F 37** *ii jj* *aa* is the encoded combined length of certificate body and signature objects *bb* is the encoded length the certificate body object *cc* is the encoded length of the Certificate Authority Reference *dd* is the placeholder for the Certificate Authority Reference (cc bytes) *ee* is the encoded length of the certificate's public key, *ff* is the placeholder for the certificate's public key bytes (ee bytes), *xx* is the encoded length of the Certificate Holder Reference *yy* is the placeholder for the Certificate Holder Reference (xx bytes) *gg* is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object,

	jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETESTDVDE021
	Certificate Holder Authorization	Official domestic DV, write access (all), CAN allowed
	Certificate effective date	$CVCA_{eff}$
	Certificate expiration date	$CVCA_{eff}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_21
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17

3.3 Certificate Set 22

3.3.1 DV_CERT_22

ID	DV_CERT_22
Purpose	This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits write access to all elementary files
Version	Am_1
Referred by	Test case EAC2_ISO7816_L_16 Template, Test case EAC2_ISO7816_O_8 Template

Content definition	**7F 21** *aa*
	  7F 4E *bb*
	  5F 29 01 00
	  42 *cc dd*
	  7F 49 *ee ff*
	  5F 20 *xx yy*
	  7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 7E 1F FF FF 10
	  5F 25 06 *gg*
	  5F 24 06 *hh*
	  5F 37 *ii jj*
	
	aa is the encoded combined length of certificate body and signature objects
	bb is the encoded length the certificate body object
	cc is the encoded length of the Certificate Authority Reference
	dd is the placeholder for the Certificate Authority Reference (cc bytes)
	ee is the encoded length of the certificate's public key,
	ff is the placeholder for the certificate's public key bytes (ee bytes),
	xx is the encoded length of the Certificate Holder Reference
	yy is the placeholder for the Certificate Holder Reference (xx bytes)
	gg is the placeholder for the BCD encoded effective date of the certificate
	hh is the placeholder for the BCD encoded expiration date of the certificate
	ii is the encoded length of the certificates signature object,
	jj is the placeholder for the certificates signature (ii bytes)

Parameter	Certificate Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETESTDVDE022
	Certificate Holder Authorization	Commercial DV, write access (all), CAN allowed
	Certificate effective date	$CVCA_{eff}$
	Certificate expiration date	$CVCA_{eff}$ + 1 month
	Public Key reference	Public key of key pair DV_KEY_22
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17

3.4 Certificate Set 23

3.4.1 LINK_CERT_23a

ID	LINK_CERT_23a	
Purpose	This certificate is a link certificate, which validity period starts one day before the original CVCA certificate expires.	
Version	Am_3	
Referred by	Test case EAC2_ISO7816_M_7	
Content definition	**7F 21** *aa* **7F 4E** *bb* **5F 29** 01 00 **42** *cc dd* **7F 49** *ee ff* **5F 20** *xx yy* **7F 4C** 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 FE 1F FF FF FF **5F 25** 06 *gg* **5F 24** 06 *hh* **5F 37** *ii jj* *aa* is the encoded combined length of certificate body and signature objects *bb* is the encoded length the certificate body object *cc* is the encoded length of the Certificate Authority Reference *dd* is the placeholder for the Certificate Authority Reference (cc bytes) *ee* is the encoded length of the certificate's public key, *ff* is the placeholder for the certificate's public key bytes (ee bytes), *xx* is the encoded length of the Certificate Holder Reference *yy* is the placeholder for the Certificate Holder Reference (xx bytes) *gg* is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	As defined by the initial AT CVCA reference

	Certificate Holder Reference	DETESTLINKDE23A
	Certificate Holder Authorization	CVCA, Unrestricted rights
	Certificate effective date	$CVCA_{exp}$ - 1 day
	Certificate expiration date	$CVCA_{exp}$ + 3 month
	Public Key reference	Public key of key pair AT_CVCA_KEY_23a
	Signing Key reference	Signed with the private key of key pair AT_CVCA_KEY_17

3.4.2 LINK_CERT_23b

ID	LINK_CERT_23b	
Purpose	This certificate is a link certificate, which validity period starts one month before the previous CVCA certificate expires.	
Version	Am_3	
Referred by	Test case EAC2_ISO7816_M_7	
Content definition	**7F 21** *aa* **7F 4E** *bb* **5F 29** 01 00 **42** *cc dd* **7F 49** *ee ff* **5F 20** *xx yy* **7F 4C** 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 FE 1F FF FF FF **5F 25** 06 *gg* **5F 24** 06 *hh* **5F 37** *ii jj* *aa* is the encoded combined length of certificate body and signature objects *bb* is the encoded length the certificate body object *cc* is the encoded length of the Certificate Authority Reference *dd* is the placeholder for the Certificate Authority Reference (cc bytes) *ee* is the encoded length of the certificate's public key, *ff* is the placeholder for the certificate's public key bytes (ee bytes), *xx* is the encoded length of the Certificate Holder Reference *yy* is the placeholder for the Certificate Holder Reference (xx bytes) *gg* is the placeholder for the BCD encoded effective date of the certificate *hh* is the placeholder for the BCD encoded expiration date of the certificate *ii* is the encoded length of the certificates signature object, *jj* is the placeholder for the certificates signature (ii bytes)	
Parameter	Certificate Authority Reference	DETESTLINKDE23A
	Certificate Holder Reference	DETESTLINKDE23B
	Certificate Holder Authorization	CVCA, Unrestricted rights
	Certificate effective date	$CVCA_{exp}$ + 2 month
	Certificate expiration date	$CVCA_{exp}$ + 5 month
	Public Key reference	Public key of key pair AT_CVCA_KEY_23b

	Signing Key reference	Signed with the private key of key pair AT_CVCA_KEY_23a

4 Test cases

All test cases described in this chapter replace the test cases with the same Test-ID in the BSI TR-03105 Part 3.3. Test cases with new Test-ID have to be performed in addition.

4.1 Unit EAC2_ISO7816_I Chip Authentication

4.1.1 Test case EAC2_ISO7816_I_17

This test case was added in release 3 of this amendment.

Test - ID	EAC2_ISO7816_I_17
Purpose	MSE:Set AT / General Authenticate commands with correct ephemeral public key using ChipAuthenticationPublicKeyInfo encapsulate in PrivilegedTerminalInfo
Version	Am_3
Profile	PACE, TA2, CA2, CS
Preconditions	1. The PACE mechanism MUST have been performed. 2. The Terminal Authentication MUST have been performed (DV_CERT_1, IS_CERT_1) 3. The ChipAuthenticationPublicKeyInfo encapsulated in PrivilegedTerminalInfo stored in ChipSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	1. Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 80 <L_{80}> <cryptographic mechanism reference> 84 <L_{84}> <private key reference> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure encapsulated in the PriviledTerminalInfo stored in EF.ChipSecurity file. 2. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 97 <L_{97}> <Ne> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L_{80}> <ephemeral public key> 3. Verify the returned authentication token TPICC 4. To verify the chips ability to continue the Secure Messaging with the new session keys, an arbitrary SM APDU is send to the chip. '0C B0 (80 || <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys.

	2. 7C <L_{7C}> '81 <L_{81}> <Nonce> 82 <L_{82}> <Authentication Token> 90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 3. True 4. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the NEW session keys.

4.2 Unit EAC2_ISO7816_K Terminal Authentication

4.2.1 Test case EAC2_ISO7816_K_13

Test - ID	EAC2_ISO7816_K_13
Purpose	This test case checks if the eID card does not accept more than one execution of Terminal Authentication within the same session, same certificate set.
Version	Am_2
Profile	PACE, TA2
Preconditions	1. The PACE mechanism MUST have been performed. 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_15, IS_CERT_15a). 3. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <certificate authority reference> • The Certificate Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 15" chapter as DV_CERT_15. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <certificate authority reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the "Certificate Set 15" chapter as IS_CERT_15. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>

	5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted terminal generated signature
Expected results	1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' or Checking error within a valid SM response. If this step returns Checking error the following steps don't need to be performed. 6. '<Eight bytes of random data> 90 00' within an SM response 7. Checking error within a valid SM response

4.2.2 Test case EAC2_ISO7816_K_14

Test - ID	EAC2_ISO7816_K_14
Purpose	This test case checks if the eID card does not accept more than one execution of Terminal Authentication within the same session, different certificate sets.
Version	Am_2
Profile	PACE, TA2
Preconditions	1. The PACE mechanism MUST have been performed. 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_1, IS_CERT_1). 3. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <certificate authority reference> • The Certificate Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 15" chapter as DV_CERT_15. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects

	7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <certificate authority reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the "Certificate Set 15" chapter as IS_CERT_15b. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted terminal generated signature
Expected results	1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' or Checking error within a valid SM response. If this step returns Checking error the following steps don't need to be performed. 6. '<Eight bytes of random data> 90 00' within an SM response 7. Checking error within a valid SM response

4.2.3 Test case EAC2_ISO7816_K_15

Test - ID	EAC2_ISO7816_K_15
Purpose	This test case checks if the eID card does not accept more than one execution of Terminal Authentication within the same session, different auxiliary data.
Version	Am_2
Profile	PACE, TA2
Preconditions	1. The PACE mechanism MUST have been performed.

	2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_15, IS_CERT_15b). 3. Auxiliary data with valid Date of Birth data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. DOB MUST NOT fit the required age. 4. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <certificate authority reference> • The Certificate Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 15" chapter as DV_CERT_15. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <certificate authority reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the "Certificate Set 15" chapter as IS_CERT_15b. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference> 91 <L91> <Compressed Ephemeral Public Key> 67 <L67> <Auxiliary Data> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. • Auxiliary data with valid Date of Birth data object DOB MUST fit the required age. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08

	<Checksum> 00’ • <Cryptogram> contains the encrypted terminal generated signature
Expected results	1. ’90 00’ within a valid SM response 2. ’90 00’ within a valid SM response 3. ’90 00’ within a valid SM response 4. ’90 00’ within a valid SM response 5. ’90 00’ or Checking error within a valid SM response. If this step returns Checking error the following steps don't need to be performed. 6. ‘<Eight bytes of random data> 90 00’ within an SM response 7. Checking error within a valid SM response

4.3 Unit EAC2_ISO7816_L Effective Access Conditions

4.3.1 Test case EAC2_ISO7816_L_29

Deleted in Amendment Release 1

4.3.2 Test case EAC2_ISO7816_L_30

Deleted in Amendment Release 1

4.3.3 Test case EAC2_ISO7816_L_31

Deleted in Amendment Release 1

4.3.4 Test case EAC2_ISO7816_L_32

Deleted in Amendment Release 1

4.3.5 Test case EAC2_ISO7816_L_33

Deleted in Amendment Release 1

4.3.6 Test case EAC2_ISO7816_L_34

Deleted in Amendment Release 1

4.3.7 Test case EAC2_ISO7816_L_37

This test case was added in release 3 of this amendment.

Test - ID	EAC2_ISO7816_L_37
Purpose	Positive test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is “Privileged Terminal”.

Version	Am_3
Profile	eID, TA2, CS
Preconditions	1. The PACE mechanism MUST have been performed (CAN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <certificate authority reference> • The Certificate Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 17" chapter as DV_CERT_17. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to all eID special functions. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L_{83}> <certificate authority reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the "Certificate Set 17" chapter as AT_CERT_17h. '0C 2A 00 BE <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function "Privileged Terminal" 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 80 <L_{80}> <Cryptographic Mechanism Reference> 83 <L_{83}> <Certificate Holder Reference > 91 <L_{91}> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00'

	• <Cryptogram> contains the encrypted terminal generated signature 8. Send the given Read Binary APDU to the eID Card. '0C B0 (80 || <sfi.EF.ChipSecurity>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. '<One byte content of EF.ChipSecurity> 90 00' within a valid Secure Messaging response.

4.4 Unit EAC2_EIDDATA_B eID Data Groups

4.4.1 Test case EAC2_EIDDATA_B_18

This test cases was added in release 3 of this amendment.

Test - ID	EAC2_EIDDATA_B_18
Purpose	Test the ASN.1 encoding of the eID DG13 elementary file
Version	Am_3
Profile	eID, DG13
Preconditions	1. DG13 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the BirthName syntax definition.
Expected results	1. true

4.5 Unit EAC2_DATA_C EF.ChipSecurity

This test unit was added in release 3 of this amendment.

This unit covers all tests about the coding of the optional file EF.ChipSecurity containing the signed SecurityInfos supported by the chip.

4.5.1 Test case EAC2_DATA_C_1

Test - ID	EAC2_DATA_C_1
Purpose	Test the ASN.1 encoding of the SecurityInfos in EF.ChipSecurity
Version	Am_3
Profile	PACE, TA2, CA2, CS
Preconditions	1. EF.ChipSecurity MUST have been read from the eID Card

Test scenario	1. The content of the SecurityInfos object MUST be encoded according to the SecurityInfos syntax definition. 2. EF.ChipSecurity MUST be implemented as SignedData according to the EAC specification [R9]. 3. The signature MUST be verified. 4. At least one PACEInfo object MUST exist 5. For each supported set of proprietary PACE domain parameters a PACEDomainParameterInfo object MUST exist 6. At least one ChipAuthenticationInfo object MUST exist 7. At least one ChipAuthenticationDomainParameterInfo MUST exist 8. At least one ChipAuthenticationPublicKeyInfo MUST exist 9. At least one TerminalAuthenticationInfo MUST exist 10. Exactly one CardInfoLocator SHOULD be present.
Expected results	1. true 2. true 3. true 4. true 5. true 6. true 7. true 8. true 9. true 10. true

4.5.2 Test cases EAC2_DATA_C_2 to EAC2_DATA_C_7

Test cases EAC2_DATA_C_2 to EAC2_DATA_C_7 are equally performed on SecurityInfo objects from EF.CardSecurity like test cases EAC2_DATA_A_2 to EAC2_DATA_A_7 were performed on SecurityInfo objects EF.CardAccess before. References to EAC2_DATA_A_1 are replaced by references to EAC2_DATA_C_1.

4.5.3 Test case EAC2_DATA_C_8

Test - ID	EAC2_DATA_C_8
Purpose	Test the ASN.1 encoding of the PrivilegedTerminalInfo
Version	Am_3
Profile	CS
Preconditions	1. Test case EAC2_DATA_C_1 MUST have been performed and exactly one PrivilegedTerminalInfo object MUST exist. 2. The data object containing SecurityInfos is parsed.
Test scenario	1. The PrivilegedTerminalInfo element must follow the ASN.1 syntax definition in the EAC specification [R9]. 2. For each ChipAuthenticationInfo encapsulated in PrivilegedTerminalInfo, the corresponding ChipAuthenticationPublicKeyInfo MUST be also included in PrivilegedTerminalInfo.
Expected	1. true

results	2. true

4.5.4 Test case EAC2_DATA_C_9

Test - ID	EAC2_DATA_C_9
Purpose	Test the ASN.1 encoding of the eIDSecurityInfo
Version	Am_3
Profile	CS
Preconditions	1. Test case EAC2_DATA_C_1 MUST have been performed and exactly one eIDSecurityInfo object MUST exist 2. The data object containing SecurityInfos is parsed
Test scenario	1. The eIDSecurityInfo element must follow the ASN.1 syntax definition in the EAC specification [R9].
Expected results	1. true