INTERNATIONAL STANDARD ISO/IEC 18013-4:2011
TECHNICAL CORRIGENDUM 1

Published 2013-11-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Personal identification — ISO-compliant driving licence —

Part 4: **Test methods**

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Identification des personnes — Permis de conduire conforme à l'ISO —

Partie 4: Méthodes d'essai

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 18013-4:2011 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

Page 2, Clause 4 Terms and Definitions

Insert the following definition:

4.3
CL protocol
protocol defined in ISO/IEC 14443-4:2008

ICS 35.240.15 **Ref. No. ISO/IEC 18013-4:2011/Cor.1:2013(E)**

Published in Switzerland

Page 24, A.3.2.15 Test Case SE_LDS_D G1_015

Replace the entire table with the following table:

Test Case-ID	SE_LDS_DG1_015
Purpose	This test checks the Vehicle Category Code of each "Category of Vehicle/Restriction/Condition" entry in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.1
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	Perform the following checks for each of the "Category of Vehicle/Restriction/Condition" entries: 1. Check the format of the Vehicle Category Code (sub-field #1).
Expected Results	1. The Vehicle Category Code contains Alpha-Numeric characters only.

Page 25, A.3.2.18 Test Case SE_LDS_DG1_018

Replace the entire table with the following table:

Test Case-ID	SE_LDS_DG1_018
Purpose	This test checks the Code field (if present) of each "Category of Vehicle/Restriction/Condition" entry in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.1
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, A.5.1 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	Perform the following checks for each of the "Category of Vehicle/Restriction/Condition" entries: 1. Check the format of the Code. 2. Check the value of the Code.
Expected Results	1. Code shall be encoded in ANS characters. 2. The value of the Code is one of the values specified in ISO/IEC 18013-2:2008, A.5.1 (i.e. "01", "03", "78", "S01", "S02", "S03", "S04" or "S05").

Page 26, A.3.2.19 Test Case SE_LDS_DG1_019

Replace the entire table with the following table:

Test Case-ID	SE_LDS_DG1_019
Purpose	This test checks the Sign field (if present) of each "Category of Vehicle/Restriction/Condition" entry in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.1
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, A.5.1 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	Perform the following checks for each of the "Category of Vehicle/Restriction/Condition" entries: 1. Check the format of the Sign. 2. Check the value of the Sign. 3. Check the Sign only occurs in combination with an applicable Code. 4. Check the Sign only occurs in combination with a Value field.
Expected Results	1. Sign shall be encoded in Special characters. 2. The value of the Sign is one of the values specified in ISO/IEC 18013-2:2008, A.5.1 (i.e. "<","=",">","<=","=<","<>","><",">=","=>","=="). 3. The value of the Code is one of the following values specified in ISO/IEC 18013-2:2008, A.5.1 (i.e. "S01", "S02", "S03" or "S04"). 4. The Value field is not empty.

Page 26, A.3.2.20 Test Case SE_LDS_DG1_020

Replace the entire table with the following table:

Test Case-ID	SE_LDS_DG1_020
Purpose	This test checks the Value field (if present) of each "Category of Vehicle/Restriction/Condition" entry in the "Categories of Vehicles/Restrictions/Conditions" DO (Tag '7F63') in EF.DG1.
Version	1.1
References	ISO/IEC 18013-2:2008, A.4 ISO/IEC 18013-2:2008, A.5.1 ISO/IEC 18013-2:2008, Annex C
Profile	
Preconditions	1. EF.DG1 has been retrieved from the IDL. 2. The Categories of Vehicles/Restrictions/Conditions object has been retrieved from EF.DG1.
Test Scenario	Perform the following checks for each of the "Category of Vehicle/Restriction/Condition" entries: 1. Check the format of the Value. 2. Check the Value only occurs in combination with a Code. 3. Check the Value only occurs in combination with a Sign.
Expected Results	1. The Value field shall be encoded in ANS format. 2. The Code field is not empty. 3. The Sign field is not empty.

Page 78, A.3.11.3 Test Case SE_LDS_SOD_003

In step 2 of Expected Results, delete "the" before "EF.SOD".

Page 80, A.3.11.7 Test Case SE_LDS_SOD_007

In step 9 of Test Scenario, delete "the" before " SubjectKeyIdentifier".

Page 94, B.2.6 Certificate specification

Add following text after the example:

"The trust point certificate shall be an authoritative time source certificate."

Page 144, B.2.6.7.1 CERT_LF_07a

Replace the entire table with the following table:

Cert ID	CERT_LF_07a	
Purpose	This is a regular certificate. Its effective date equals the Trust Root’s effective date plus five days and the expiration date equals the Trust Root’s effective date plus two months. Path length constraint is set to ‘Fh’ This is not an authoritative time source certificate.	
Version	1.1	
Content definition	7F 21 *aa* 7F 4E *bb* **5F 29** 01 00 **42** *cc dd* **7F 49** *ee ff* **5F 20** 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 0F 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 AKID *dd* is the placeholder for the AKID (cc bytes) *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee 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	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF007
	Relative authorization	Non authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Point$_{eff}$ + 5 days
	Certificate expiration date	Trust Point$_{eff}$ + 2 months
	Public Key reference	Public key of key pair CERT_LF_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

Page 145, B.2.6.7.2 CERT_LF_07b

Replace the entire table with the following table:

<table>
<tr><td>Cert ID</td><td colspan="2">CERT_LF_07b</td></tr>
<tr><td>Purpose</td><td colspan="2">This is a regular certificate. Its effective date equals the Trust Root's effective date and the expiration date equals the Trust Root's effective date plus four days.
Path length constraint is set to ‘Fh’
This is not an authoritative time source certificate.</td></tr>
<tr><td>Version</td><td colspan="2">1.1</td></tr>
<tr><td>Content definition</td><td colspan="2">7F 21 *aa*
7F 4E *bb*
5F 29 01 00
42 *cc dd*
7F 49 *ee ff*
5F 20 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37
7F 4C 0F 06 07 28 81 8C 5D 03 03 01 53 04 0F 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 AKID
dd is the placeholder for the AKID (cc bytes)
ee is the encoded length of the certificates public key,
ff is the placeholder for the certificates public key bytes (ee 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)</td></tr>
<tr><td>Parameter</td><td>Authority Key Identifier</td><td>As defined by the Trust point</td></tr>
<tr><td></td><td>Subject Key Identifier</td><td>TESTCERTLF007</td></tr>
<tr><td></td><td>Relative authorization</td><td>Non authoritative time source
Path length constraint set to F
Grant read access to all DGs</td></tr>
<tr><td></td><td>Certificate effective date</td><td>Trust Point$_{eff}$</td></tr>
<tr><td></td><td>Certificate expiration date</td><td>Trust Point$_{eff}$ + 4 days</td></tr>
<tr><td></td><td>Public Key reference</td><td>Public key of key pair CERT_LF_KEY_07</td></tr>
<tr><td></td><td>Signing Key reference</td><td>Signed with the private key of key pair TRUSTPOINT_KEY_00</td></tr>
</table>

Page 146, B.2.6.7.3 CERT_LF_07c

Replace the entire table with the following table:

Cert ID	CERT_LF_07c	
Purpose	This is a regular certificate. Its effective date equals the Trust Root's effective date plus five days and the expiration date equals the Trust Root's effective date plus two months. Path length constraint is set to ‘Fh’ This is an authoritative time source certificate.	
Version	1.1	
Content definition	7F 21 *aa* 7F 4E *bb* **5F 29** 01 00 **42** *cc dd* **7F 49** *ee ff* **5F 20** 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 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 AKID *dd* is the placeholder for the AKID (cc bytes) *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee 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	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF007
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Point$_{eff}$ + 5 days
	Certificate expiration date	Trust Point$_{eff}$ + 2 months
	Public Key reference	Public key of key pair CERT_LF_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

Page 147, B.2.6.7.4 CERT_LF_07d

Replace the entire table with the following table:

Cert ID	CERT_LF_07d	
Purpose	This is a regular certificate. Its effective date equals the Trust Root's effective date plus ten days and the expiration date equals the Trust Root's effective date plus two months. Path length constraint is set to 'Fh' This is not an authoritative time source certificate.	
Version	1.1	
Content definition	7F 21 *aa* 7F 4E *bb* **5F 29** 01 00 **42** *cc dd* **7F 49** *ee ff* **5F 20** 0E 54 45 53 54 43 45 52 54 4C 46 30 30 37 64 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 0F 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 AKID *dd* is the placeholder for the AKID (cc bytes) *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee 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	Authority Key Identifier	TESTCERTLF007
	Subject Key Identifier	TESTCERTLF007d
	Relative authorization	Non authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Point$_{\text{eff}}$ + 10 days
	Certificate expiration date	Trust Point$_{\text{eff}}$ + 2 months
	Public Key reference	Public key of key pair CERT_LF_KEY_07d
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_07

Page 148, B.2.6.7.5 CERT_L1_07e

Replace the entire table with the following table:

Cert ID	CERT_LF_07e	
Purpose	This is a regular certificate. Its effective date equals the Trust Root's effective date and the expiration date equals the Trust Root's effective date plus nine days. Path length constraint is set to 'Fh' This is not an authoritative time source certificate.	
Version	1.1	
Content definition	7F 21 *aa* 7F 4E *bb* **5F 29** 01 00 **42** *cc dd* **7F 49** *ee ff* **5F 20** 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 0F 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 AKID *dd* is the placeholder for the AKID (cc bytes) *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee 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	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF007
	Relative authorization	Non authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Point$_{eff}$
	Certificate expiration date	Trust Point$_{eff}$ + 9 days
	Public Key reference	Public key of key pair CERT_LF_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

Page 149, B.2.6.7.6 CERT_L1_07f

Replace the entire table with the following table:

Cert ID	CERT_LF_07f	
Purpose	This is a regular certificate. Its effective date equals the Trust Root's effective date plus twenty days and the expiration date equals the Trust Root's effective date plus two months. Path length constraint is set to 'Fh' This is an authoritative time source certificate.	
Version	1.1	
Content definition	7F 21 *aa* 7F 4E *bb* **5F 29** 01 00 **42** *cc dd* **7F 49** *ee ff* **5F 20** 0E 54 45 53 54 43 45 52 54 4C 46 30 30 37 66 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 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 AKID *dd* is the placeholder for the AKID (cc bytes) *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee 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	Authority Key Identifier	TESTCERTLF007
	Subject Key Identifier	TESTCERTLF007f
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Point$_{eff}$ + 20 days
	Certificate expiration date	Trust Point$_{eff}$ + 2 months
	Public Key reference	Public key of key pair CERT_LF_KEY_07f
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_07

Page 150, B.2.6.7.7 CERT_L1_07g

Replace the entire table with the following table:

Cert ID	CERT_LF_07g	
Purpose	This is a regular certificate. Its effective date equals the Trust Root's effective date and the expiration date equals the Trust Root's effective date plus fifteen days. Path length constraint is set to ‘Fh’ This is an authoritative time source certificate.	
Version	1.1	
Content definition	7F 21 *aa* 7F 4E *bb* **5F 29** 01 00 **42** *cc dd* **7F 49** *ee ff* **5F 20** 0D 54 45 53 54 43 45 52 54 4C 46 30 30 37 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 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 AKID *dd* is the placeholder for the AKID (cc bytes) *ee* is the encoded length of the certificates public key, *ff* is the placeholder for the certificates public key bytes (ee 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	Authority Key Identifier	As defined by the Trust point
	Subject Key Identifier	TESTCERTLF007
	Relative authorization	Authoritative time source Path length constraint set to F Grant read access to all DGs
	Certificate effective date	Trust Point$_{\text{eff}}$
	Certificate expiration date	Trust Point$_{\text{eff}}$ + 15 days
	Public Key reference	Public key of key pair CERT_LF_KEY_07
	Signing Key reference	Signed with the private key of key pair TRUSTPOINT_KEY_00

Page 156, B.2.6.8.3 CERT_L1_08c

Replace the entire table with the following table:

Cert ID	CERT_L1_08c	
Purpose	This certificate is a regular certificate, of which the validity period starts at the expiration date plus three months of the Trust root and expires one month later. Path length constraint is set to ‘1h. This certificate is an authoritative time source certificate.	
Version	1.1	
Content definition	7F 21 aa 7F 4E bb **5F 29** 01 00 **42** cc dd **7F 49** ee ff **5F 20** 0E 54 45 53 54 43 45 52 54 4C 31 30 30 38 63 **7F 4C** 0F 06 07 28 81 8C 5D 03 03 01 53 04 11 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 AKID, *dd* is the placeholder for the AKID (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), *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 certificate's signature object, *jj* is the placeholder for the certificate's signature (ii bytes).	
Parameter	Authority Key Identifier	TESTCERTLF008b
	Subject Key Identifier	TESTCERTL1008c
	Relative authorization	Authoritative time source Path length constraint set to 1
	Certificate effective date	Trust Point$_{exp}$ + 3 months
	Certificate expiration date	Trust Point$_{exp}$ + 4 months
	Public Key reference	Public key of key pair CERT_L1_KEY_08c
	Signing Key reference	Signed with the private key of key pair CERT_LF_KEY_08b

Page162, B.3.1.6 Test case SE_ISO7816_SelDF_6

Replace the entire table with the following table:

Test – ID	SE_ISO7816_SelDF_6
Purpose	Selecting the LDS application using wrong Lc byte.
Version	1.1
Profile	
Preconditions	1. LDS application shall not be selected. 2. Test is applicable for T=1 and CL protocol only.
Test scenario	1. The tester shall ensure that the command with an incorrect Lc byte can be transmitted from the reader to the IDL under test. 2. Send the given SELECT APDU to the IDL (wrong Lc). ’00 A4 04 0C 08 A0 00 00 02 48 02 00’
Expected results	1. The reader should be able to transmit the command with an incorrect Lc byte. If not, the test result shall be recorded as inconclusive. 2. The IDL shall return an ISO Checking Error.

Page 162, B.3.2 Test Unit SE_ISO7816_SecBAP– Security conditions of BAP protected IDL

Delete "the" before "certificates" in the second line of the Note.

Page 190, B.3.4 Test Unit SE_ISO7816_SelEFSM – Protected SELECT EF Command

Delete "the" at the end of the first line of the Note.

Page 243, B.3.9.33 Test case SE_ISO7816_SecEAP_33

Replace the entire table with the following table:

Test – ID	SE_ISO7816_SecEAP_33
Purpose	READ BINARY command with odd instruction and with short EF ID for EF.DG14 without BAP on a plain profile (Positive test).
Version	1.1
Profile	EAP, Plain, OddIns
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall not have been performed.
Test scenario	1. Send the given READ BINARY APDU for EF.DG14 (short EF ID ‘0E’) to the IDL. ’00 B1 00 0E 03 54 01 00 06’ 2. Verify the DG14 data returned.
Expected results	1. 6 bytes of data, and ’90 00’ as a plain text response without Secure Messaging. 2. The data shall consist of a DO ‘53’. The value field (DG14 data) shall start with '6E'.

Page 270, B.3.11.13 Test case SE_ISO7816_ CertVer_13

Replace the entire table with the following table:

Test - ID	SE_ISO7816_CertVer_13
Purpose	Test the MSE:Set DST command with an invalid class byte.
Version	1.1
Profile	EAP
Preconditions	1. The LDS application shall have been selected. 2. The BAP mechanism shall have been performed. 3. The CA mechanism shall have been performed as well. 4. The Certification Authority Reference shall have been read from the EF.COM file (Current trust root). 5. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	1. Send the given MSE: Set DST APDU to the IDL. '8C 22 81 B6 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted DOs 83 <L_{83}> <AKID> • The Certification Authority Reference shall be used as read from the EF.COM file. • The class byte is set to an invalid value. 2. If the error code in step 1 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped. Send an arbitrary SM APDU to the chip. '0C B0 81 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	1. Checking error. Note that the behaviour of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 2. Skipped or '90 00' in a valid SM response.

Page 308, B.3.13 Test Unit SE_ISO7816_AccCond - Effective Access Conditions

Delete "the" before "certificates" in the second last line of the first paragraph.

Page 321, B.3.14 Test Unit SE_ISO7816_Update - Update mechanism

Add following text at the end of the paragraph:

"The initial Trust Point shall be an authoritative time source"

Page 321, B.3.14.1 Test case SE_ISO7816_Update_1

Replace the entire table with the following table:

Test - ID	SE_ISO7816_Update_1
Purpose	Test the “Current Date” update mechanism with a non-authoritative time source certificate signed by an authoritative time source entity.
Version	1.1
Profile	EAP
Preconditions	1. The LDS application shall have been selected. 2. The CA mechanism shall have been performed as well. 3. The Certification Authority Reference shall have been read from the EF.COM file (trust root). 4. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the “Certificate set 7” chapter as CERT_LF_07a. ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • The certificate is marked as non-authoritative time source but is signed by an authoritative time source entity so the chip shall update its current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 2. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the “Certificate set 7” chapter as CERT_LF_07b. ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • This certificate has an expiry date BEFORE the current date. Therefore this certificate shall be rejected.
Expected results	1. ’90 00’ in a valid SM response. 2. Checking error.

Add following text after the table:

"After this test case, the chip current date is ‘Trust Point$_{\text{eff}}$ + 5 days’."

Page 322, B.3.14.2 Test case SE_ISO7816_Update_2

Replace the entire table with the following table:

Test - ID	SE_ISO7816_Update_2
Purpose	Test the “Current Date” update mechanism with authoritative time source certificates.
Version	1.1
Profile	EAP
Preconditions	1. The LDS application shall have been selected. 2. The CA mechanism shall have been performed as well. 3. The Certification Authority Reference shall have been read from the EF.COM file (trust root). 4. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the “Certificate set 7” chapter as CERT_LF_07c. ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • The certificate is marked as authoritative time source. 2. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the “Certificate set 7” chapter as CERT_LF_07d. ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • The certificate is marked as non-authoritative time source but as this certificate has an effective date AFTER the current date and the parent certificate is marked as authoritative time source, the chip shall update its current date • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the “Certificate set 7” chapter as CERT_LF_07e. ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • This certificate has an expiry date BEFORE the current date. Therefore this certificate shall be rejected.
Expected results	1. ’90 00’ in a valid SM response. 2. ’90 00’ in a valid SM response. 3. Checking error.

Add following text after the table:

"After this test case, the chip current date is ‘Trust Point$_{eff}$ + 10 days’."

Page 322, B.3.14.3 Test case SE_ISO7816_Update_3

Replace the entire table with the following table:

Test - ID	SE_ISO7816_Update_3
Purpose	Test the "Current Date" update mechanism with authoritative time source certificate signed by a non-authoritative time source entity.
Version	1.1
Profile	EAP
Preconditions	1. The LDS application shall have been selected. 2. The CA mechanism shall have been performed as well. 3. The Certification Authority Reference shall have been read from the EF.COM file (trust root). 4. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the "Certificate set 7" chapter as CERT_LF_07a. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • The certificate is marked as non-authoritative time source. 2. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the "Certificate set 7" chapter as CERT_LF_07f. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • The certificate is marked as authoritative time source but signed by a non-authoritative time source. Therefore the current date is not updated. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the "Certificate set 7" chapter as CERT_LF_07g. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • This certificate has an expiry date BEFORE the effective date of the previous certificate but the current date has not been updated.
Expected results	1. '90 00' in a valid SM response. 2. '90 00' in a valid SM response. 3. '90 00' in a valid SM response.

Add following text after the table:

"After this test case, the chip current date is unchanged and therefore equal to 'Trust Point$_{eff}$ + 10 days'."

Page 323, B.3.14.4 Test case SE_ISO7816_Update_4

Replace the entire table the following text:

"Test Case removed."

Page 324, B.3.14.5 Test case SE_ISO7816_Update_5

Replace the entire table with the following table:

Test - ID	SE_ISO7816_Update_5
Purpose	Test the “Trust root” update mechanism with a new link certificate.
Version	1.1
Profile	EAP
Preconditions	1. The LDS application shall have been selected. 2. The CA mechanism shall have been performed as well. 3. The Certification Authority Reference shall have been read from the EF.COM file (trust root). 4. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. PSO – VERIFY CERTIFICATE command: Send the appropriate Link Certificate as specified in the «Certificate set 7” chapter as CERT_LF_07i: ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • The certificate is a trust root marked as an authoritative time source. • The IDL shall update the trust root with this new certificate. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 2. Power down the field or remove the IDL from the reader, so that the chip loses all temporary information. This is done to prove, that the new trust point has been stored in persistent memory. • Power up the chip. • Re-establish the preconditions. • Read the EF.COM using the SELECT EF and READ BINARY command. • Check that EF.COM file contains now two trust points and verify that the new trust point is at the first position and the previous one has been moved to the second position. 3. MSE – SET DST command '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted DO 83 <L83> Subject Key Identifier of original Trust Root 4. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the «Certificate set 7” chapter as CERT_LF_07j. ‘0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ • <Cryptogram> contains the following encrypted DOs 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • Since the previous trust point is still valid, the certificate shall be verified successfully. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed.

	5. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the «Certificate set 7" chapter as CERT_LF_07k. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted DOs 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • Since the effective date of this certificate is after the expiration date of the original trust point, the chip shall update the current date and shall also disable the original trust point. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 6. MSE – SET DST command: '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted DO 83 <L83> Subject Key Identifier of original Trust Root 7. PSO – VERIFY CERTIFICATE command: Send the appropriate Certificate as specified in the «Certificate set 7" chapter as CERT_LF_07j. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted DOs 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • Since the trust point has been disabled, the certificate verification shall fail.
Expected results	1. '90 00' in a valid SM response. 2. True. 3. '90 00' in a valid SM response. 4. '90 00' in a valid SM response. 5. '90 00' in a valid SM response. 6. '90 00' or checking error in a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 7. Checking error or '6300' in a valid SM response. This certificate shall no longer be valid, since the current date of the chip has been updated.

Page 325, B.3.14.6 Test case SE_ISO7816_Update_6

In step 3 of the Test Scenario, delete "the" before "EF.COM".