



INTERNATIONAL STANDARD ISO/IEC 18013-3:2009

TECHNICAL CORRIGENDUM 2

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 3: Access control, authentication and integrity validation

TECHNICAL CORRIGENDUM 2

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

Partie 3: Contrôle d'accès, authentification et validation d'intégrité

RECTIFICATIF TECHNIQUE 2

Technical Corrigendum 1 to ISO/IEC 18013-3:2009 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

ICS 35.240.15

Ref. No. ISO/IEC 18013-3:2009/Cor.2:2013(E)

© ISO/IEC 2013 – All rights reserved

Published in Switzerland

Replace clause B.10.4 with the following:

B.10.4 Example Using Configuration 4

Static document keying material:

$$K_{\text{doc}} = \text{'348D2F25C266CC8068F99391BF0F5CCB876B5F5DDB004D0E5C8BCD1D3ACF2FDADA'}$$

Compute Basic Access Keys:

$$\begin{aligned} \text{Input: } K_{\text{seed}} &= H_{\text{SHA-256}}(K_{\text{doc}}) \\ K_{\text{seed}} &= \text{'2E3AB26DC47C4BA6724E58514492ABF3B2B92BD21A40BEBFAF0D7A52D291EA98'} \end{aligned}$$

Encryption Key (K_{enc}) computation:

1. Concatenate K_{seed} and c ($c = 1$):
 $D = \text{'2E3AB26DC47C4BA6724E58514492ABF300000001'}$
2. Calculate the hash of D :
 $H_{\text{SHA-256}}(D) = \text{'0AFD72514422FD43622BB3F1680F62435A6F9B8E83C92A299D3B89124D89B611'}$
3. Form key:
 $K_{\text{enc}} = \text{'0AFD72514422FD43622BB3F1680F62435A6F9B8E83C92A299D3B89124D89B611'}$

Message Authentication Key (K_{mac}) computation:

4. Concatenate K_{seed} and c ($c = 2$):
 $D = \text{'2E3AB26DC47C4BA6724E58514492ABF300000002'}$
5. Calculate the hash of D :
 $H_{\text{SHA-256}}(D) = \text{'F3BC7313E7D34BB3BE0EB07B4DF9DE6AE73A4CA604FE1516AEBFB4140115A5A6'}$
6. Form key:
 $K_{\text{mac}} = \text{'F3BC7313E7D34BB3BE0EB07B4DF9DE6AE73A4CA604FE1516AEBFB4140115A5A6'}$

Authentication and Establishment of Session Keys:

IS:

1. Request an 8 byte random challenge from the document's SIC:

Command APDU:

CLA	INS	P1	P2	Le
'00'	'84'	'00'	'00'	'08'

Document SIC:

2. Generate random challenge and return it to IS:
 $\text{RND.ICC} = \text{'E880AAE12EB3A5FB'}$

Response APDU:

Response Data Field	SW1	SW2
RND.ICC	'90'	'00'

IS:

3. Generate an 8-byte random challenge and 24-byte random keying material:
 $\text{RND.IFD} = \text{'B962840EFBFE80C9'}$
 $\text{K.IFD} = \text{'1D05B3E621AC7BB4786AC1657D0C4C1158875525EB21659D905674FCAFF94421'}$
4. Concatenate RND.IFD, RND.ICC and K.IFD:
 $\text{S} = \text{'B962840EFBFE80C9E880AAE12EB3A5FB1D05B3E621AC7BB4786AC1657D0C4C1158875525EB21659D905674FCAFF94421'}$
5. Encrypt S using AES with key K_{enc} :
 $\text{E_IFD} = \text{'DA020143D3816ACB4EF104FDAAFA30A7BC49BFE6B616D9D061F728EB063362A1C435F95DDACBE36C37A09472BBCD464B'}$
6. Compute CMAC over E_IFD with key K_{mac} :
 $\text{M_IFD} = \text{'4F3B9205ADB2DD20'}$
7. Construct command data for MUTUAL AUTHENTICATE and send command to the document's SIC:
 $\text{cmd_data} = \text{'DA020143D3816ACB4EF104FDAAFA30A7BC49BFE6B616D9D061F728EB063362A1C435F95DDACBE36C37A09472BBCD464B4F3B9205ADB2DD20'}$

Command APDU:

CLA	INS	P1	P2	Lc	Command Data Field	Le
'00'	'82'	'00'	'00'	'38'	cmd_data	'38'

Document SIC:

8. Generate 16-byte random keying material:
 $\text{K.ICC} = \text{'56F1510FDCC2B01787E80D2D5E34084020C93698AF4599C9B9B7D68EB2E958B7'}$
9. Calculate XOR of K.IFD and K.ICC:
 $\text{K}_{\text{seed}} = \text{'4BF4E2E9FD6ECBA3FF82CC4823384451784E63BD4464FC5429E1A2721D101C96'}$

10. Derive session keys:
 $KS_{enc} = \text{'60BDD38EE1B27EEAC7AF9907889F2E0474C7AF231C71705BB2A84BF87BA825FF'}$
 $KS_{mac} = \text{'978E2D4BFC62716966B215A28980ED041756A53EBC56AE7CE9F8341167210C33'}$
11. Initialize send sequence counter:
 $SSC = \text{'2EB3A5FBFBFE80C9'}$
12. Concatenate RND.ICC, RND.IFD and K.ICC; and add padding:
 $R = \text{'E880AAE12EB3A5FBB962840EFBFE80C956F1510FDCC2B01787E80D2D5E34084020C93698AF4599C9B9B7D68EB2E958B7'}$
13. Encrypt R using AES with key K_{enc} :
 $E_ICC = \text{'2918E899CF1B797F5F869521B1B942B78F72C19AA8162C82BA5295733D33C2F72BABED4C7687E8D2A58E9C4F109F92A2'}$
14. Compute CMAC over E_ICC with key K_{mac} :
 $M_ICC = \text{'2FDBF985C7DA7CCF'}$
15. Construct response data and send response APDU to the IS:
 $resp_data = \text{'2918E899CF1B797F5F869521B1B942B78F72C19AA8162C82BA5295733D33C2F72BABED4C7687E8D2A58E9C4F109F92A22FDBF985C7DA7CCF'}$

Response APDU:

Response Data Field	SW1	SW2
resp_data	'90'	'00'

IS:

16. Calculate XOR of K.IFD and K.ICC:
 $K_{seed} = \text{'4BF4E2E9FD6ECBA3FF82CC4823384451784E63BD4464FC5429E1A2721D101C96'}$
17. Derive session keys:
 $KS_{enc} = \text{'60BDD38EE1B27EEAC7AF9907889F2E0474C7AF231C71705BB2A84BF87BA825FF'}$
 $KS_{mac} = \text{'978E2D4BFC62716966B215A28980ED041756A53EBC56AE7CE9F8341167210C33'}$
18. Initialize send sequence counter:
 $SSC = \text{'2EB3A5FBFBFE80C9'}$