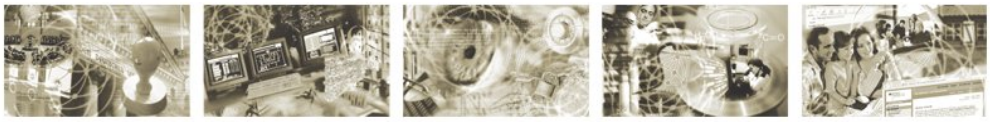
Bundesamt
für Sicherheit in der
Informationstechnik



Worked Example for Extended Access Control (EAC)

PACE, Chip Authentication and Terminal Authentication

Version 1.02

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

E-Mail: ExtendedAccessControl@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1. Introduction

This document provides two worked examples for the EAC protocols as defined in [TR-03110]. The first example of this document is based on ECDH / ECDSA while the second one uses DH / RSA. All numbers contained in the APDUs are noted hexadecimal. The notation follows [TR-03110] and [Doc9303]. The example is based on the log file attached to this document. The log file was generated with the tool GlobalTester (www.globaltester.org) provided by HJP Consulting GmbH (www.hjp-consulting.com).

2. Settings for ECDH/ECDSA

In this example based on elliptic curves the two following certificates are use: Cert_DV and Cert_AT from test case EAC2_EIDDATA_B_01 of [TR-03105] part 3.3. Both certificates allow the terminal to read the data of the eID application.

2.1 Certificate DV

The **DV certificate** stores the information below:

Certificate Body:

```
0000  7F 4E 81 DE 5F 29 01 00 42 0D 44 45 43 56 43 41  .N.._)..B.DECVCA
0010  41 54 30 30 30 30 31 7F 49 81 90 06 0A 04 00 7F  AT00001.I.......
0020  00 07 02 02 02 02 05 86 81 81 04 5B 6E C0 28 FA  ...........[n.(.
0030  BA A3 88 53 1E 46 DA 2D 1E 4D F2 DA 21 90 3A A2  ...S.F.-.M..!.:.
0040  FF 00 BD 22 32 5C 25 D7 CD 46 24 C5 52 4E E1 EC  ..."2\%..F$.RN..
0050  35 F3 15 18 45 EF 29 AC 40 BF 71 F4 57 6B 82 7F  5...E.).@.q.Wk..
0060  79 EB EC BB 54 60 E2 2C 2F 38 72 0E B6 A0 5A CA  y...T`.,/8r...Z.
0070  69 43 88 88 5F 53 D4 62 30 6F 98 CE CC 5D DC B6  iC.._S.b0o...]..
0080  43 4F 81 BE 01 53 FC 1E 4E 6B A2 71 16 F7 FB 06  CO...S..Nk.q....
0090  FE 5C B6 F4 A3 A2 87 A4 9B F4 A4 DA F9 DB BD 8A  .\..............
00A0  B6 38 EE 8E 66 AC 72 FA 76 98 AF 5F 20 0D 44 45  .8..f.r.v.._ .DE
00B0  54 45 53 54 44 56 44 45 30 31 39 7F 4C 12 06 09  TESTDVDE019.L...
00C0  04 00 7F 00 07 03 01 02 02 53 05 80 1F FF FF 10  .........S......
00D0  5F 25 06 01 00 00 09 03 00 5F 24 06 01 00 01 00  _%......._$.....
00E0  03 00                                           ..
```

Tag	*Length*	*Value*	*ASN1.Type*	*Comment*
7F 4E	DE		SEQUENCE	Certificate Body
5F 29	01	00	UNSIGNED INTEGER	Certificate Profile Identifier
42	0D	44 45 43 56 43 41 41 54 30 30 30 30 31	CHARACTER STRING	Certification Authority Reference DECVCAAT00001
7F 49	90		SEQUENCE	Public Key
06	0A	04 00 7F 00 07 02 02 02 02 05	OID	id-TA-ECDSA-SHA-512
86	81	04 5B 6E C0 ... ... FA 76 98 AF	ELLIPTIC CURVE POINT	Public Point
5F 20	0D	44 45 54 45 53 54 44 56 44 45 30 31 39	CHARACTER STRING	Certificate Holder Reference

					DETESTDVDE019
7F 4C	12			SEQUENCE	Certificate Holder Authorization Template
06	09	04 00 7F 00 07 03 01 02 02		OID	id-AT
53	05	80 1F FF FF 10		OCTET STRING	Discretionary Data (official DV with all access rights)
5F 25	06	01 00 00 09 03 00		DATE	Certificate Effective Date
5F 24	06	01 00 01 00 03 00		DATE	Certificate Expiration Date

Certification information:

Authority Reference:	44 45 43 56 43 41 41 54 30 30 30 30 31 (DECVCAAT00001)
Public Key:	OID: 0.4.0.127.0.7.2.2.2.2.5 (ECDSA with SHA-512) Public point Y: 0000 04 5B 6E C0 28 FA BA A3 88 53 1E 46 DA 2D 1E 4D 0010 F2 DA 21 90 3A A2 FF 00 BD 22 32 5C 25 D7 CD 46 0020 24 C5 52 4E E1 EC 35 F3 15 18 45 EF 29 AC 40 BF 0030 71 F4 57 6B 82 7F 79 EB EC BB 54 60 E2 2C 2F 38 0040 72 0E B6 A0 5A CA 69 43 88 88 5F 53 D4 62 30 6F 0050 98 CE CC 5D DC B6 43 4F 81 BE 01 53 FC 1E 4E 6B 0060 A2 71 16 F7 FB 06 FE 5C B6 F4 A3 A2 87 A4 9B F4 0070 A4 DA F9 DB BD 8A B6 38 EE 8E 66 AC 72 FA 76 98 0080 AF
Certificate Holder Reference:	44 45 54 45 53 54 44 56 44 45 30 31 39 (DETESTDVDE019)
Certificate Holder Authorization:	OID: 0.4.0.127.0.7.3.1.2.2 (Authentication Terminal) Discretionary Data: 80 1F FF FF 10 Role: DV (official domestic) Access Rights: CAN allowed Read Access(eID) DG1

	Read Access(eID) DG2 Read Access(eID) DG3 Read Access(eID) DG4 Read Access(eID) DG5 Read Access(eID) DG6 Read Access(eID) DG7 Read Access(eID) DG8 Read Access(eID) DG9 Read Access(eID) DG10 Read Access(eID) DG11 Read Access(eID) DG12 Read Access(eID) DG13 Read Access(eID) DG14 Read Access(eID) DG15 Read Access(eID) DG16 Read Access(eID) DG17 Read Access(eID) DG18 Read Access(eID) DG19 Read Access(eID) DG20 Read Access(eID) DG21
Effective Date:	01 00 00 09 03 00 (2010.09.30)
Expiration Date:	01 00 01 00 03 00 (2010.10.30)

Certificate AT

The **AT certificate** stores the following data:

Certificate Body:

```
0000  7F 4E 81 DE 5F 29 01 00 42 0D 44 45 54 45 53 54  .N.._)..B.DETEST
0010  44 56 44 45 30 31 39 7F 49 81 90 06 0A 04 00 7F  DVDE019.I.......
0020  00 07 02 02 02 02 05 86 81 81 04 16 6D 8F 5E FC  ............m.^.
0030  C6 E2 36 14 86 90 7C 52 4F 8A 9A 50 63 34 F8 43  ..6...|RO..Pc4.C
0040  09 8D A1 DB 83 D1 3E 10 9A F8 89 E7 26 71 0F B0  ......>.....&q..
0050  AF 3E A5 7E 76 09 86 05 A0 43 6F E0 7B 75 3A 75  .>.~v....Co.{u:u
0060  7A 04 6D 30 DA 7D 99 C0 7E 7C AD 34 D1 39 FD 40  z.m0.}..~|.4.9.@
0070  02 53 EF B7 FB DD DD 0B 3D 80 A0 BC 48 14 D3 05  .S......=...H...
0080  5A 3C D3 81 B5 B3 BE 1C D3 F7 45 6D 91 BA B1 6D  Z<........Em...m
0090  D0 54 E4 03 EC 1A 93 93 F7 06 0B 2B 10 E0 1E 3C  .T.........+...<
00A0  BA 5D D4 57 C1 3F 21 D7 C5 4C 2E 5F 20 0D 44 45  .].W.?!..L._ .DE
```

```
00B0  54 45 53 54 41 54 44 45 30 31 39 7F 4C 12 06 09  TESTATDE019.L...
00C0  04 00 7F 00 07 03 01 02 02 53 05 00 00 00 01 10  .........S......
00D0  5F 25 06 01 00 00 09 03 00 5F 24 06 01 00 01 00  _%......._$.....
00E0  03 00                                            ..
```

Tag	*Length*	*Value*	*ASN1.Type*	*Comment*
7F 4E	DE		SEQUENCE	Certificate body
5F 29	01	00	UNSIGNED INTEGER	Certificate Profile Identifier
42	0D	44 45 54 45 53 54 44 56 44 45 30 31 39	CHARACTER STRING	Certification Authority Reference DETESTDVDE019
7F 49	90		SEQUENCE	Public Key
06	0A	04 00 7F 00 07 02 02 02 02 05	OID	id-TA-ECDSA-SHA-512
86	81	04 16 6D 8F D7 C5 4C 2E	ELLIPTIC CURVE POINT	Public Point
5F 20	0D	44 45 54 45 53 54 41 54 44 45 30 31 39	CHARACTER STRING	Certificate Holder Reference DETESTATDE019
7F 4C	12		SEQUENCE	Certificate Holder Authorization Template
06	09	04 00 7F 00 07 03 01 02 02	OID	id-AT
53	05	00 00 00 01 10	OCTET STRING	Discretionary Data (AT with read access for DG1)
5F 25	06	01 00 00 09 03 00	DATE	Certificate Effective Date
5F 24	06	01 00 01 00 03 00	DATE	Certificate Expiration Date

Certification information:

Authority	44 45 54 45 53 54 44 56 44 45 30 31 39

Reference:	(DETESTDVDE019)
Public Key:	OID: 0.4.0.127.0.7.2.2.2.2.5 (ECDSA with SHA-512) Public point Y: 0000 04 16 6D 8F 5E FC C6 E2 36 14 86 90 7C 52 4F 8A 0010 9A 50 63 34 F8 43 09 8D A1 DB 83 D1 3E 10 9A F8 0020 89 E7 26 71 0F B0 AF 3E A5 7E 76 09 86 05 A0 43 0030 6F E0 7B 75 3A 75 7A 04 6D 30 DA 7D 99 C0 7E 7C 0040 AD 34 D1 39 FD 40 02 53 EF B7 FB DD DD 0B 3D 80 0050 A0 BC 48 14 D3 05 5A 3C D3 81 B5 B3 BE 1C D3 F7 0060 45 6D 91 BA B1 6D D0 54 E4 03 EC 1A 93 93 F7 06 0070 0B 2B 10 E0 1E 3C BA 5D D4 57 C1 3F 21 D7 C5 4C 0080 2E
Certificate Holder Reference:	44 45 54 45 53 54 41 54 44 45 30 31 39 (DETESTATDE019)
Certificate Holder Authorization:	OID: 0.4.0.127.0.7.3.1.2.2 (Authentication Terminal) Discretionary Data: 00 00 00 01 10 Role: AT Access Rights: CAN allowed Read Access(eID) DG1
Effective Date:	01 00 00 09 03 00 (2010.09.30)
Expiration Date:	01 00 01 00 03 00 (2010.10.30)

Passwords

In this example the following passwords are used:

CAN	500540
PIN	123456
MRZ	TPD<<T220001293<<<<<<<<<<<<<<< 6408125<1010318D<<<<<<<<<<<<<<6 MUSTERMANN<<ERIKA<<<<<<<<<<<<<

2.2 CHAT

The following CHAT is used in this worked example:

CHAT	0000 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 .....S.... 0010 01 10 ..

Tag	***Length***	***Value***	***ASN1.Type***	***Comment***
06	09	04 00 7F 00 07 03 01 02 02	OID	id-AT OBJECT IDENTIFIER Authentication Terminal
53	05	00 00 00 01 10	OCTET STRING	Discretionary Data Access rights: • Read Access DG1 • CAN allowed

3. PACE Example (ECDH/ECDSA)

In this chapter the protocol PACE is described. PACE establishes Secure Messaging between an MRTD chip and a terminal based on weak (short) passwords. PACE is an alternative to Basic Access Control, i.e. it enables the MRTD chip to verify that the terminal is authorized to access stored less-sensitive data. At the beginning the file EF.CardAccess must be read by the terminal. This file is defined as followed:

```
SET SIZE( 198 )
  SEQUENCE SIZE( 13 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 2 }
    INTEGER SIZE( 1 )
      0000  02                                                .
  SEQUENCE SIZE( 18 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 3 2 2 }
    INTEGER SIZE( 1 )
      0000  02                                                .
    INTEGER SIZE( 1 )
      0000  01                                                .
  SEQUENCE SIZE( 18 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 4 2 2 }
    INTEGER SIZE( 1 )
      0000  02                                                .
    INTEGER SIZE( 1 )
      0000  0D                                                .
  SEQUENCE SIZE( 28 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 3 2 }
    SEQUENCE SIZE( 12 )
      OBJECT IDENTIFIER = { 0 4 0 127 0 7 1 2 }
      INTEGER SIZE( 1 )
        0000  0D                                                .
    INTEGER SIZE( 1 )
      0000  01                                                .
  SEQUENCE SIZE( 47 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 6 }
    IA5-STRING SIZE( 35 )
      0000  68 74 74 70 73 3A 2F 2F 77 77 77 2E 68 6A 70 2D  https://www.hjp-
      0010  63 6F 6E 73 75 6C 74 69 6E 67 2E 63 6F 6D 2F 68  consulting.com/h
      0020  6F 6D 65                                        ome
  SEQUENCE SIZE( 62 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 8 }
    SET SIZE( 50 )
      SEQUENCE SIZE( 18 )
        OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 3 2 2 }
        INTEGER SIZE( 1 )
          0000  02                                                .
        INTEGER SIZE( 1 )
          0000  02                                                .
      SEQUENCE SIZE( 28 )
        OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 3 2 }
        SEQUENCE SIZE( 12 )
          OBJECT IDENTIFIER = { 0 4 0 127 0 7 1 2 }
          INTEGER SIZE( 1 )
            0000  0D                                                .
        INTEGER SIZE( 1 )
          0000  02                                                .
```

The content of EF.CardAccess is described in the following table:

Tag	*Length*	*Value*	*ASN1.Type*	*Comment*
31	81 C6		SET	
30	0D		SEQUENCE	
06	08	04 00 7F 00 07 02 02 02	OID	id-TA OBJECT IDENTIFIER TerminnalAuthentication Info
02	01	02	INTEGER	Version of protocol
30	12		SEQUENCE	
06	0A	04 00 7F 00 07 02 02 03 02 02	OID	id-CA-ECDH-AES-CBC-CMAC-128 ChipAuthenticationInfo
02	01	02	INTEGER	Version
02	01	01	INTEGER	keyId
30	12		SEQUENCE	
06	0A	04 00 7F 00 07 02 02 04 02 02	OID	id-PACE-ECDH-GM-AES-CBC-CMAC-128 PACEInfo
02	01	02	INTEGER	Version
02	01	0D	INTEGER	parameterID identifier for standardized domain parameter
30	1C		SEQUENCE	
06	09	04 00 7F 00 07 02 02 03 02	OID	id-CA-ECDH ChipAuthentication DomainParameterInfo
30	0C		SEQUENCE	
06	07	04 00 7F 00 07 01 02	OID	OID_StandaradizedDomainParameters

02	01	0D			INTEGER	parameterID
02	01	01			INTEGER	keyId
30	2F			SEQUENCE		
06	08	04 00 7F 00 07 02 02 06			OID	id-CI OBJECT IDENTIFIER
16	23	68 74 74 70 73 3A 2F 2F 77 77 77 2E 68 6A 70 2D 63 6F 6E 73 75 6C 74 69 6E 67 2E 63 6F 6D 2F 68 6F 6D 65			IA5STRING	URL of CardInfo file
30	3E			SEQUENCE		
06	08	04 00 7F 00 07 02 02 08			OID	id-PT
31	32				SET	
30	12			SEQUENCE		
06	0A	04 00 7F 00 07 02 02 03 02 02			OID	id-CA-ECDH-AES-CBC-CMAC-128
02	01	02			INTEGER	Version
02	01	02			INTEGER	keyId
30	1C			SEQUENCE		
06	09	04 00 7F 00 07 02 02 03 02			OID	id-CA-ECDH
30	0C			SEQUENCE		
06	07	04 00 7F 00 07 01 02			OID	OID_StandaradizedDomainParameters
02	01	0D			INTEGER	parameterID
02	01	02			INTEGER	keyId

The relevant information for PACE are:

Version	02
Algorithm Identifier (parameterID)	0D (BrainpoolP256r1)
PACE Info OID	0.4.0.127.0.7.2.2.4.2.2 (PACE-ECDH-GM-AES-CBC-CMAC128)
First key derived from PIN (K_π)	59 14 68 CD A8 3D 65 21 9C CC B8 56 02 33 60 0F

3.1 Command MSE:Set AT

To initialize PACE the terminal sends the following command MSE:Set AT to the chip.

T→C	0000 00 22 C1 A4 27 80 0A 04 00 7F 00 07 02 02 04 02 ."..'..... 0010 02 83 01 03 7F 4C 12 06 09 04 00 7F 00 07 03 01 .....L..... 0020 02 02 53 05 00 00 00 01 10 84 01 0D ..S.....
C→T	0000 90 00

Here T→C is an abbreviation for an APDU sent from terminal (T or PCD) to chip (C or PICC) while C→T denotes the corresponding response sent by the chip to the terminal. The encoding of the command is explained in the next table.

C-APDU				
CLA	00		Plain	
INS	22		Manage Security Environment	
P1/P2	C1 A4		Set Authentication Template for Mutual Authentication	
L_c	27		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	80	0A	04 00 7F 00 07 02 02 04 02 02	Cryptographic mechanism: PACE with ECDH, generic mapping and AES 128 session keys
	83	01	03	Password: PIN
	7F 4C	12	06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 01 10	Certificate Holder Authorization Template (CHAT)

	84	01	0D	Reference of domain parameters (BrainpoolP256r1)

R-APDU		
SW	90 00	Normal operation

3.2 Command Get Nonce

The chip randomly generates a nonce s and encrypts it with the key K_π

Nonce decrypted (s)	0000 CE 83 4C DE 69 FF BB 1D 1E B2 15 85 CD 70 9F 18 ..L.i........p..
Nonce encrypted (z)	0000 7D 98 C0 0F C6 C9 E9 54 3B BF 94 A8 70 73 A1 23 }......T;...ps.#

The encrypted nonce is queried by the terminal:

T→C	0000 10 86 00 00 02 7C 00 00 .....|..
C→T	0000 7C 12 80 10 CE 83 4C DE 69 FF BB 1D 1E B2 15 85 |.....L.i..... 0010 CD 70 9F 18 90 00 .p..

C-APDU				
CLA	10		Plain, Command Chaining	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	02		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	00	–	-
L_e	00			Expected maximal byte length of the response data field

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	12		Dynamic Authentication Data
	80	10	CE 83 4C DE 69 FF BB 1D 1E B2 15 85 CD 70 9F 18	Encrypted Nonce
SW	90 00		Normal operation	

3.3 Command Map Nonce

The nonce is mapped to an ephemeral group generator via generic mapping. The required randomly chosen ephemeral keys are also collected in the next table.

PCD Private Key $\widetilde{SK}_{PCD}$	0000 75 22 87 F5 B0 2D E3 C4 BC 3E 17 94 51 18 C5 1B u"...-...>..Q... 0010 23 C9 72 78 E4 CD 74 80 48 AC 56 BA 5B DC 3D 46 #.rx..t.H.V.[.=F
PCD Public Key $\widetilde{PK}_{PCD}$	0000 04 3D D2 9B BE 59 07 FD 21 A1 52 AD A4 89 5F AA .=...Y..!.R..._. 0010 E7 AC C5 5F 5E 50 EF BF DE 5A B0 C6 EB 54 F1 98 ..._^P...Z...T.. 0020 D6 15 91 36 35 F0 FD F5 BE B3 83 E0 03 55 F8 2D ...65........U.- 0030 3C 41 ED 0D F2 E2 83 63 43 3D FB 73 85 6A 15 DC <A.....cC=.s.j.. 0040 9F . 0000 19 C4 28 71 56 63 DE 74 5D 18 24 B8 55 D2 B9 67 ..(qVc.t].$.U..g 0010 89 0C 99 D6 8E D5 FE EE 9D CD F8 D7 BB A2 89 D2 .....
PICC Private Key $\widetilde{SK}_{PICC}$	
PICC Public Key $\widetilde{PK}_{PICC}$	0000 04 9C FC F7 58 2A C9 86 D0 DD 52 FA 53 12 34 14 ....X*....R.S.4. 0010 C3 E1 B9 6B 4D 00 AB A8 E5 74 67 9B 70 EF B5 BC ...kM....tg.p... 0020 3B 45 D2 F1 37 29 CC 2A E1 78 E7 E2 41 B4 43 21 ;E..7).*.x..A.C! 0030 35 33 B7 7D BB 44 64 9A 81 5D DC 4A 23 84 BA 42 53.}.Dd..].J#..B 0040 2A *
Shared Secret H	0010 04 71 85 0C FD 80 FB 47 59 47 E5 B1 AF 10 FE 8E .q.....GYG..... 0020 66 63 96 7C 2D 26 49 35 B3 19 51 F7 63 A4 B0 3A fc.|-&I5..Q.c..: 0030 57 49 16 73 88 F8 8F 52 A1 09 16 7E 3E 65 92 CA WI.s...R...~>e.. 0040 08 20 46 8D 11 57 A8 E7 81 D2 F7 04 91 79 B1 D1 . F..W.......y.. 0050 14 .
Mapped generator $\tilde{G}$	0000 04 39 29 D2 8B A1 E5 33 9D 6C 5D AD E5 E3 3B D3 .9)....3.l]...;. 0010 C2 F0 BD 14 DD 77 C7 52 15 32 26 16 59 C9 18 FA .....w.R.2&.Y... 0020 60 14 DD 48 FA 84 E6 2B DE 43 8E DB 4C 97 71 D0 `..H...+.C..L.q. 0030 42 CD B2 4B 77 88 BD BA B2 03 1C 45 75 1E 77 7F B..Kw......Eu.w. 0040 66 f

The following APDUs are exchanged by terminal and chip to map the nonce.

T→C	0000 10 86 00 00 45 7C 43 81 41 04 3D D2 9B BE 59 07 ....E|C.A.=...Y. 0010 FD 21 A1 52 AD A4 89 5F AA E7 AC C5 5F 5E 50 EF .!.R..._...._^P. 0020 BF DE 5A B0 C6 EB 54 F1 98 D6 15 91 36 35 F0 FD ..Z...T.....65.. 0030 F5 BE B3 83 E0 03 55 F8 2D 3C 41 ED 0D F2 E2 83 ......U.-<A..... 0040 63 43 3D FB 73 85 6A 15 DC 9F 00 cC=.s.j....
C→T	0000 7C 43 82 41 04 9C FC F7 58 2A C9 86 D0 DD 52 FA |C.A....X*....R. 0010 53 12 34 14 C3 E1 B9 6B 4D 00 AB A8 E5 74 67 9B S.4....kM....tg. 0020 70 EF B5 BC 3B 45 D2 F1 37 29 CC 2A E1 78 E7 E2 p...;E..7).*.x.. 0030 41 B4 43 21 35 33 B7 7D BB 44 64 9A 81 5D DC 4A A.C!53.}.Dd..].J 0040 23 84 BA 42 2A 90 00 #..B*..

C-APDU				
CLA	10		Plain, Command Chaining	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	45		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	43	–	Dynamic Authentication Data
	81	41		Mapping Data
			04	Uncompressed Point
			3D D2 9B BE 59 07 FD 21 A1 52 AD A4 89 5F AA E7 AC C5 5F 5E 50 EF BF DE 5A B0 C6 EB 54 F1 98 D6	X-Coordinate
			15 91 36 35 F0 FD F5 BE B3 83 E0 03 55 F8 2D 3C 41 ED 0D F2 E2 83 63 43 3D FB 73 85 6A 15 DC 9F	Y-Coordinate
L_e	00			Expected maximal byte length of the response data field

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***

	7C	43		Dynamic Authentication Data
	82	41		Mapping data
			04	Uncompressed Point
			9C FC F7 58 2A C9 86 D0 DD 52 FA 53 12 34 14 C3 E1 B9 6B 4D 00 AB A8 E5 74 67 9B 70 EF B5 BC 3B	X-Coordinate
			45 D2 F1 37 29 CC 2A E1 78 E7 E2 41 B4 43 21 35 33 B7 7D BB 44 64 9A 81 5D DC 4A 23 84 BA 42 2A	Y-Coordinate
SW	90 00		Normal operation	

3.4 Command Perform Key Agreement

In the third step chip and terminal perform an anonymous ECDH key agreement using the new domain parameters determined by the ephemeral group generator $\tilde{G}$ of the previous step. As shared secret only the first coordinate is required.

PCD Private Key (SK_{PCD})	0000 00 9D 9A 32 DF 93 A5 7C CE 33 CA 3C DD 34 57 E3 ...2...|.3.<.4W. 0010 3A 97 6F 29 35 46 C7 35 50 F3 97 25 9C 93 BE 01 :.o)5F.5P..%.... 0020 20
PCD Public Key (PK_{PCD})	0000 04 51 8B C4 E5 32 AD 2A 9B D6 52 78 04 D5 D6 65 .Q...2.*..Rx...e 0010 AB D5 10 41 03 7A 0C C8 AA 92 28 04 EB 50 1C 22 ...A.z....(..P." 0020 2B 34 27 38 85 99 AF AA E9 FB AC E2 DF 93 E1 3C +4'8...........< 0030 3C 49 79 CD 12 F0 AE 3E 3C 01 26 02 83 91 55 45 <Iy....><.&...UE 0040 82 .
PICC Private Key (SK_{PICC})	0000 15 87 2C 56 90 8C 14 40 02 17 79 94 CF AA ED D5 ..,V...@..y..... 0010 46 7C E1 50 85 3C 44 53 50 51 FF 24 18 30 39 D8 F|.P.<DSPQ.$.09.
PICC Public Key (PK_{PICC})	0000 04 28 2C F3 80 73 03 6A FA C2 16 AF 13 5B D9 94 .(,..s.j.....[.. 0010 DA 0C 35 7F 10 BD 4C 34 AF EA 10 42 B2 EB 0F D6 ..5...L4...B.... 0020 80 4D F3 65 8B 83 5A C2 E7 13 3F 13 69 11 84 54 .M.e..Z...?.i..T 0030 2B B5 0B 10 99 63 A4 66 2A BD C0 8B 97 63 AF 4B +....c.f*....c.K 0040 5B [
Shared Secret K	0000 6E 7D 07 7C CD 36 7C 2E AA 68 3F 1E 8E C5 34 30 n}.|.6|..h?...40 0010 2E 2D 00 B6 AD AF 8A 87 A6 ED A7 87 40 F1 76 06 .-..........@.v.

The key agreement is performed as following.

T→C	0000 10 86 00 00 45 7C 43 83 41 04 51 8B C4 E5 32 AD ....E|C.A.Q...2. 0010 2A 9B D6 52 78 04 D5 D6 65 AB D5 10 41 03 7A 0C *..Rx...e...A.z. 0020 C8 AA 92 28 04 EB 50 1C 22 2B 34 27 38 85 99 AF ...(..P."+4'8... 0030 AA E9 FB AC E2 DF 93 E1 3C 3C 49 79 CD 12 F0 AE ....<<Iy.... 0040 3E 3C 01 26 02 83 91 55 45 82 00 ><.&...UE..
C→T	0000 7C 43 84 41 04 28 2C F3 80 73 03 6A FA C2 16 AF |C.A.(,..s.j.... 0010 13 5B D9 94 DA 0C 35 7F 10 BD 4C 34 AF EA 10 42 .[....5...L4...B 0020 B2 EB 0F D6 80 4D F3 65 8B 83 5A C2 E7 13 3F 13 .....M.e..Z...?. 0030 69 11 84 54 2B B5 0B 10 99 63 A4 66 2A BD C0 8B i..T+....c.f*... 0040 97 63 AF 4B 5B 90 00 .c.K[

C-APDU				
CLA	10		Plain, Command Chaining	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	45		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	43	–	Dynamic Authentication Data
	83	41		Terminal's Ephemeral Public Key
			04	Uncompressed Point
			51 8B C4 E5 32 AD 2A 9B D6 52 78 04 D5 D6 65 AB D5 10 41 03 7A 0C C8 AA 92 28 04 EB 50 1C 22 2B	X-coordinate
			34 27 38 85 99 AF AA E9 FB AC E2 DF 93 E1 3C 3C 49 79 CD 12 F0 AE 3E 3C 01 26 02 83 91 55 45 82	Y-coordinate
L_e	00			Expected maximal byte length of the response data field

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***

	7C	43		Dynamic Authentication Data
	84	41		Chip's Ephemeral Public Key
			04	Uncompressed Point
			28 2C F3 80 73 03 6A FA C2 16 AF 13 5B D9 94 DA 0C 35 7F 10 BD 4C 34 AF EA 10 42 B2 EB 0F D6 80	X-Coordinate
			4D F3 65 8B 83 5A C2 E7 13 3F 13 69 11 84 54 2B B5 0B 10 99 63 A4 66 2A BD C0 8B 97 63 AF 4B 5B	Y-Coordinate
SW	90 00		Normal operation	

By means of the KDF specified in [TR-03110] the AES 128 session keys are derived from the shared secret as following.

K_{Enc}	0000 68 40 6B 41 62 10 05 63 D9 C9 01 A6 15 4D 29 01 h@kAb..c.....M).
K_{Mac}	0000 73 FF 26 87 84 F7 2A F8 33 FD C9 46 40 49 AF C9 s.&...*.3..F@I..

3.5 Command Mutual Authentication

The authentication token is constructed by OID and public key on both sides, PICC and PCD.

Construction of input data for Authentication Token T_{PCD}:

Tag	*Length*	*Value*	*ASN1.Type*	*Comment*
7F 49	4F		PUBLIC KEY	Input data for PCD Authentication Token
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Chip's ephemeral public point
		04		Uncompressed Point
		28 2C F3 80 73 03 6A FA C2 16 AF 13 5B D9 94 DA 0C 35 7F 10 BD 4C 34 AF EA 10 42 B2 EB 0F D6 80		X-coordinate
		4D F3 65 8B 83 5A C2 E7 13 3F 13 69 11 84 54 2B B5 0B 10 99 63 A4 66 2A BD C0 8B 97 63 AF 4B 5B		Y-coordinate

Construction of input data for Authentication Token T_{PICC}:

Tag	*Length*	*Value*	*ASN1.Type*	*Comment*
7F 49	4F		PUBLIC KEY	Input data for PICC Authentication Token
06	0A	04 00 7F 00 07 02 02 04 02 02	OBJECT IDENTIFIER	PACE with ECDH, generic mapping and AES 128 session keys
86	41		ELLIPTIC CURVE POINT	Terminal's ephemeral public point
		04		Uncompressed Point

		51 8B C4 E5 32 AD 2A 9B D6 52 78 04 D5 D6 65 AB D5 10 41 03 7A 0C C8 AA 92 28 04 EB 50 1C 22 2B		X-coordinate
		34 27 38 85 99 AF AA E9 FB AC E2 DF 93 E1 3C 3C 49 79 CD 12 F0 AE 3E 3C 01 26 02 83 91 55 45 82		Y-coordinate

Computed Authentication Tokens

T_{PICC}	0000 A2 7A E7 B3 65 73 C1 D9 .z..es..
T_{PCD}	0000 A2 65 8C 2F 38 60 0B 0F .e./8`..

Finally these tokens are exchanged and verified.

T→C	0000 00 86 00 00 0C 7C 0A 85 08 A2 7A E7 B3 65 73 C1 .....|....z..es. 0010 D9 00 ..
C→T	0000 7C 19 86 08 A2 65 8C 2F 38 60 0B 0F 87 0D 44 45 |....e./8`....DE 0010 43 56 43 41 41 54 30 30 30 30 31 CVCAAT00001

C-APDU				
CLA	00		Plain	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	0C		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	0A	–	Dynamic Authentication Data
	85	08	A2 7A E7 B3 65 73 C1 D9	Terminal's Authentication Token MAC
L_e	00			Expected maximal byte length of the response data field

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	19		Dynamic Authentication Data
	86	08	A2 65 8C 2F 38 60 0B 0F	Chip's Authentication Token MAC
	87	0D	44 45 43 56 43 41 41 54 30 30 30 30 31	Certification Authority Reference (CAR)
SW	90 00		Normal operation	

With this successful exchange a secure channel based on PACE has been established.

4. Terminal Authentication Example (ECDH/ECDSA)

Terminal Authentication enables the chip to verify that the terminal is entitled to access sensitive data.

4.1 Command MSE: Set DST

The command MSE:Set DST is used to send the CAR from the terminal to the chip. The CAR is delivered by PACE before (see 3.5).

CAR	0000 44 45 41 54 43 56 43 41 30 30 30 30 31

The terminal sends a certificate chain to the chip. From this point the communication is encrypted by Secure Messaging with the keys derived during PACE. The chain starts with a certificate verifiable with the CVCA public key stored on the chip as following.

T→C plain	0000 00 22 81 B6 0F 83 0D 44 45 43 56 43 41 41 54 30 ."....DECVCAAT0 0010 30 30 30 31 0001
T→C coded	0000 0C 22 81 B6 1D 87 11 01 BE 90 23 7E EB 4B A0 FF ."........#~.K.. 0010 25 3E A2 46 AE 31 C8 B8 8E 08 92 D2 1C 73 A1 DF %>.F.1.......s.. 0020 E9 99 00 ...
C→T coded	0000 99 02 90 00 8E 08 A8 95 70 A6 86 64 A7 D6 ....p..d..
C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	22		Manage Security Environment	
P1/P2	81 B6		Set Digital Signature Template for verification	
L_c	0F		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	83	0D	44 45 43 56 43 41 41 54	Reference of a public key, CAR

			30 30 30 30 31	

R-APDU		
SW	90 00	Normal operation

4.2 Command PSO: Verify Certificate

The DV certificate is send to the chip by the terminal as following.

T→C plain

```
0000  00 2A 00 BE 00 01 66 7F 4E 81 DE 5F 29 01 00 42  .*....f.N._)..B
0010  0D 44 45 43 56 43 41 41 54 30 30 30 30 31 7F 49  .DECVCAAT00001.I
0020  81 90 06 0A 04 00 7F 00 07 02 02 02 02 05 86 81  ................
0030  81 04 5B 6E C0 28 FA BA A3 88 53 1E 46 DA 2D 1E  ..[n.(....S.F.-.
0040  4D F2 DA 21 90 3A A2 FF 00 BD 22 32 5C 25 D7 CD  M..!.:....."2\%..
0050  46 24 C5 52 4E E1 EC 35 F3 15 18 45 EF 29 AC 40  F$.RN..5...E.).@
0060  BF 71 F4 57 6B 82 7F 79 EB EC BB 54 60 E2 2C 2F  .q.Wk..y...T`.,/
0070  38 72 0E B6 A0 5A CA 69 43 88 88 5F 53 D4 62 30  8r...Z.iC.._S.b0
0080  6F 98 CE CC 5D DC B6 43 4F 81 BE 01 53 FC 1E 4E  o...]..CO...S..N
0090  6B A2 71 16 F7 FB 06 FE 5C B6 F4 A3 A2 87 A4 9B  k.q.....\.......
00A0  F4 A4 DA F9 DB BD 8A B6 38 EE 8E 66 AC 72 FA 76  ........8..f.r.v
00B0  98 AF 5F 20 0D 44 45 54 45 53 54 44 56 44 45 30  .._ .DETESTDVDE0
00C0  31 39 7F 4C 12 06 09 04 00 7F 00 07 03 01 02 02  19.L............
00D0  53 05 80 1F FF FF 10 5F 25 06 01 00 00 09 03 00  S......_%.......
00E0  5F 24 06 01 00 01 00 03 00 5F 37 81 80 34 EA 28  _$......._7..4.(
00F0  28 25 23 1B F9 EF 84 DC D1 5A F7 72 A9 26 B0 A4  (%#......Z.r.&..
0100  78 CA 96 5A 7F 8E 9E 0D 90 CD 7D E6 18 30 53 0F  x..Z......}..0S.
0110  D9 15 47 8E 68 56 39 9F E7 8A B2 D6 F3 BD E5 0D  ..G.hV9.........
0120  9A 56 25 EC B6 51 D7 58 77 34 77 13 6F 70 A5 90  .V%..Q.Xw4w.op..
0130  81 E5 30 D8 29 28 C7 34 AF 02 BA A9 E3 03 E9 6B  ..0.)(.4.......k
0140  BD A6 06 DC 6E F9 9A 40 28 62 DD 72 7E 96 4E 19  ....n..@(b.r~.N.
0150  64 DA 09 49 B5 84 60 20 C3 26 7A EA 6C F0 26 E5  d..I..` .&z.l.&.
0160  4C 7E 9E 83 73 67 DF 17 1C C7 B2 C8 91           L~..sg.......
```

T→C coded

```
0000  0C 2A 00 BE 00 01 7F 87 82 01 71 01 BB 99 CB 14  .*........q.....
0010  CA 8D AB 03 80 8E 10 A4 05 24 A8 A6 5C 86 FD 7B  .........$..\..{
0020  67 4A E4 3B 2A FE 41 94 47 B1 EB AD 05 D8 AE 6E  gJ.;*.A.G......n
0030  34 7E E1 81 A8 36 28 F5 C1 79 B4 91 37 A2 E6 78  4~...6(..y..7..x
0040  B9 81 8D 86 79 99 C6 E3 7E F7 F3 F6 8D AB 41 36  ....y...~.....A6
0050  A1 49 1C 91 5B 61 6B EB 83 5A FE DE A7 92 61 C7  .I..[ak..Z....a.
0060  F5 CE 5C 63 87 BD 72 06 90 AB 90 9D 13 CE 36 15  ..\c..r.......6.
0070  C9 CD A7 16 70 26 B3 D8 28 13 5B 8C 54 F0 F1 1A  ....p&..(.[.T...
0080  F8 DB 65 B9 F4 35 BB 2C CF 41 71 F8 2C 45 72 3A  ..e..5.,.Aq.,Er:
0090  88 B5 FF A3 40 9F 09 ED F9 A2 46 E8 4C 21 5F 0E  ....@.....F.L!_.
00A0  F1 A8 BB 27 18 35 0A 4F 96 32 C7 06 8C B9 C9 FA  ...'.5.O.2......
00B0  4E 0A 75 40 87 5D 4B 73 D2 8A E0 5C 28 D5 23 B4  N.u@.]Ks...\(.#.
00C0  2C 6D 4C 1A 4F 64 78 F6 6E 86 EE 42 1B C8 DB 68  ,mL.Odx.n..B...h
00D0  34 12 0B EC B9 12 B1 50 AB AC 9D 80 6D 66 AC 1F  4......P....mf..
00E0  7B EF 14 C5 40 F0 A2 53 E1 C1 83 03 27 B9 37 5F  {...@..S....'.7_
00F0  6B DA 79 A8 B2 77 DD EF 63 D7 EE 25 52 53 1E 2C  k.y..w..c..%RS.,
0100  9E 44 B7 15 29 84 A5 77 E2 E8 A5 C3 21 3F BC B4  .D..)..w....!?..
0110  BF 7F 0D F3 EC F9 EB D5 0C 48 EF 2D 01 C3 B3 03  .........H.-....
0120  AF 58 39 26 4A A5 34 D5 58 76 AF 81 CA B1 73 F7  .X9&J.4.Xv....s.
```

	0130 08 4E BF 46 3D 8F 0A F1 6A B9 7A DB 9D 4C 65 68 .N.F=...j.z..Leh 0140 8D D4 32 A9 EC 3B 3F 8D 9A 68 5B A8 48 4B 5E A2 ..2..;?..h[.HK^. 0150 1A F7 39 CD A4 D6 3C 2A 98 74 B9 61 F5 30 06 97 ..9...<*.t.a.0.. 0160 70 64 83 05 90 E2 76 1F 88 AA 6E 4D 65 08 8A E4 pd....v...nMe... 0170 C7 C8 4D E8 AE 62 B6 8E 55 7D CD F5 8E 08 E3 8A ..M..b..U}...... 0180 CD A4 4E 50 3C E5 00 00 ..NP<...
C→T coded	0000 99 02 90 00 8E 08 2B 06 86 4A EA 1A 10 13 ......+..J....
C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	2A		Perform Security Operation	
P1/P2	00 BE		Verify self-descriptive certificate	
L_c	00 01 66		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7F 4E	81 DE	5F 29 01 00 42 0D 44 45 43 56 43 41 41 54 … … 00 00 09 03 00 5F 24 06 01 00 01 00 03 00	Certificate Body
	5F 37	81 80	34 EA 28 28 25 23 1B F9 EF 84 DC D1 5A F7 … … E5 4C 7E 9E 83 73 67 DF 17 1C C7 B2 C8 91	Signature

R-APDU		
SW	90 00	Normal operation

4.3 Command MSE: Set DST

The following CAR of the DV certificate is used by the command MSE:Set DST.

CAR	0000 44 45 54 45 53 54 44 56 44 45 30 31 39

The reference of the public key (CAR) is send from the terminal to the chip as following.

T→C plain	0000 00 22 81 B6 0F 83 0D 44 45 54 45 53 54 44 56 44 ."".....DETESTDVD 0010 45 30 31 39 E019
T→C coded	0000 0C 22 81 B6 1D 87 11 01 A7 BB 8F 23 0F FF 92 21 ."".....#...! 0010 16 2A D6 73 B9 F3 19 A8 8E 08 D8 71 3E 9B 7A 60 .*.s.....q>.z` 0020 0B 49 00 .I.
C→T coded	0000 99 02 90 00 8E 08 C8 48 8F 79 FE F3 86 C7 .....H.y....
C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	22		Manage Security Environment	
P1/P2	81 B6		Set Digital Signature Template for verification	
L_c	0F		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	83	0D	44 45 54 45 53 54 44 56 44 45 30 31 39	Reference of a public key, CAR

R-APDU		
SW	90 00	Normal operation

4.4 Command PSO: Verify Certificate

The AT certificate is send to the chip by the terminal as following.

T→C plain

```
0000  00 2A 00 BE 00 01 66 7F 4E 81 DE 5F 29 01 00 42  .*....f.N.._)..B
0010  0D 44 45 54 45 53 54 44 56 44 45 30 31 39 7F 49  .DETESTDVDE019.I
0020  81 90 06 0A 04 00 7F 00 07 02 02 02 02 05 86 81  ................
0030  81 04 16 6D 8F 5E FC C6 E2 36 14 86 90 7C 52 4F  ...m.^...6...|RO
0040  8A 9A 50 63 34 F8 43 09 8D A1 DB 83 D1 3E 10 9A  ..Pc4.C......>..
0050  F8 89 E7 26 71 0F B0 AF 3E A5 7E 76 09 86 05 A0  ...&q...>.~v....
0060  43 6F E0 7B 75 3A 75 7A 04 6D 30 DA 7D 99 C0 7E  Co.{u:uz.m0.}..~
0070  7C AD 34 D1 39 FD 40 02 53 EF B7 FB DD DD 0B 3D  |.4.9.@.S......=
0080  80 A0 BC 48 14 D3 05 5A 3C D3 81 B5 B3 BE 1C D3  ...H...Z<.......
0090  F7 45 6D 91 BA B1 6D D0 54 E4 03 EC 1A 93 93 F7  .Em...m.T.......
00A0  06 0B 2B 10 E0 1E 3C BA 5D D4 57 C1 3F 21 D7 C5  ..+...<.].W.?!..
00B0  4C 2E 5F 20 0D 44 45 54 45 53 54 41 54 44 45 30  L._ .DETESTATDE0
00C0  31 39 7F 4C 12 06 09 04 00 7F 00 07 03 01 02 02  19.L............
00D0  53 05 00 00 00 01 10 5F 25 06 01 00 00 09 03 00  S......_%.......
00E0  5F 24 06 01 00 01 00 03 00 5F 37 81 80 29 F8 17  _$......._7..)..
00F0  6A 03 D2 AE 3F 7C FF E1 A5 9B 28 75 50 DC 05 16  j...?|....(uP...
0100  92 C5 E1 D8 1B E8 53 26 54 01 E0 FF A5 D8 C4 6B  ......S&T......k
0110  FC A4 0C AD 72 D1 0D AA A6 14 34 2D 4F 3D C5 BA  ....r.....4-O=..
0120  F7 4A 54 F9 4A F6 2A A1 DC 86 7F 15 A9 59 AA A5  .JT.J.*......Y..
0130  6C 82 57 DA 5E 2F E5 55 8B 9E 59 25 72 E4 C1 C2  l.W.^/.U..Y%r...
0140  1E FC 91 6B AC 5A 92 42 BD BD B8 E1 8F 19 0C 3F  ...k.Z.B.......?
0150  A1 CA 2E F8 61 EB B9 18 F8 CB EE E8 F6 7E FB F0  ....a........~..
0160  26 14 D5 47 E3 02 AC 63 8E 51 45 38 AB           &..G...c.QE8.
```

T→C coded

```
0000  0C 2A 00 BE 00 01 7F 87 82 01 71 01 EF 27 17 6D  .*........q..'.m
0010  74 26 F3 41 10 23 61 8E 47 D7 35 CB FC A4 35 50  t&.A.#a.G.5...5P
0020  87 90 DC 5E 99 AE 80 37 F7 8A 0A 29 BC 88 6C 5D  ...^...7...)..l]
0030  FD 3B 86 85 2A C8 C6 20 B5 ED 8D 0E BC CD C7 E2  .;..*.. ........
0040  79 FC 60 E1 AE 14 25 0F B8 F0 EF F2 E9 69 DC 13  y.`...%......i..
0050  43 1E BF 0B 6F AC D7 D9 1F BF 1A 0F 58 1D 6A 6A  C...o.......X.jj
0060  BE E7 ED 81 01 5B 7E F6 B0 0F EE 25 B1 75 9B B5  .....[~....%.u..
0070  E7 97 84 37 AC 09 47 9D 6F F2 FF D1 2B 16 AB E3  ...7..G.o...+...
0080  0C 53 DA 41 60 F3 67 DB 1D 7C 1D 8F D2 28 BA A9  .S.A`.g..|...(..
0090  D4 D3 C9 F1 B0 2A 5F 94 3A 8B 9C A3 63 47 59 84  .....*_.:...cGY.
00A0  85 86 FE 35 1A 83 BF 73 39 58 D4 29 49 D2 7D FC  ...5...s9X.)I.}.
00B0  85 3B 23 70 FE 41 7C 84 9B A1 B0 43 55 72 97 40  .;#p.A|....CUr.@
00C0  A1 60 CF 06 50 CB 37 78 3E 4F 8C E4 CF F1 D9 B4  .`..P.7x>O......
00D0  11 8F 46 76 AE F1 3A 8C 89 19 8A B8 33 10 48 B7  ..Fv..:.....3.H.
00E0  0C 68 6F 94 30 10 37 82 24 C6 2C 91 E4 AA 95 7F  .ho.0.7.$.,.....
00F0  72 3F 5E 5D B3 41 1A C9 E7 B2 AC 5E FF D8 72 6A  r?^].A.....^..rj
0100  38 BE 5A 1B 1E 06 78 92 E1 8D 6E 43 C4 C2 9D 5C  8.Z...x...nC...\
0110  2C F9 5F F3 BD 14 2E E6 48 BD 15 44 42 69 6D 6D  ,._.....H..DBimm
0120  F0 F6 F2 5C 43 C1 DA AA 41 09 46 E5 5E E1 6D 6F  ...\C...A.F.^.mo
0130  DC 18 53 D8 43 4E 6F F7 C7 84 15 01 0C 8E EC C9  ..S.CNo.........
0140  C2 EE 3D 53 AF 0D CF C9 0D 0A 43 6A F7 C4 E3 64  ..=S......Cj...d
0150  53 A5 59 12 2E 52 20 F5 C0 99 4D DF 5D 6A 95 3C  S.Y..R ...M.]j.<
0160  60 7C 4C 39 87 B5 97 E3 D4 68 5C 83 37 E9 AA B9  `|L9.....h\.7...
0170  5C 23 39 02 8B AB B9 AC AD ED 11 3D 8E 08 06 80  \#9........=....
0180  77 2F B3 9D 76 61 00 00                          w/..va..
```

C→T coded

```
0000  99 02 90 00 8E 08 A7 F7 F0 42 EB D0 92 33        .........B...3
```

C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	2A		Perform Security Operation	
P1/P2	00 BE		Verify self-descriptive certificate	
L_c	00 01 66		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7F 4E	81 DE	5F 29 01 00 42 0D 44 45 54 45 53 54 44 56 … … 00 00 09 03 00 5F 24 06 01 00 01 00 03 00	Certificate Body
	5F 37	81 80	29 F8 17 6A 03 D2 AE 3F 7C FF E1 A5 9B 28 … … F0 26 14 D5 47 E3 02 AC 63 8E 51 45 38 AB	Signature

R-APDU		
SW	90 00	Normal operation

4.5 Command MSE: Set AT

Extract the following relevant information from EF.CardAccess. In EF.CardAccess there are two key references for CA defined: 01 and 02. Both use the curve BrainpoolP256r1 (0D).

The terminal generates an ephemeral Diffie-Hellman key pair and sends the compressed ephemeral public key to the chip.

D_{PICC}	0D
ECDH Ephemeral public key ($\widetilde{PK}_{PCD}$)	0000 04 5A 7A 37 7F C9 CA FC 03 AC 7F F4 54 41 A8 B2 .Zz7........TA.. 0010 90 9D 88 EA B8 E6 B0 17 38 47 AB 49 B9 49 DF 37 ....8G.I.I.7 0020 99 A3 4E E5 7E C5 52 68 CF 8B 1C 3E C4 89 F8 BF ..N.~.Rh...>.... 0030 4C F4 C6 8D 3F D9 67 0E 89 C0 D5 D3 FF F1 AA F8 L...?.g......... 0040 9F .
ECDH	0000 00 A6 A4 D2 55 C5 BF 7A 77 EC 3D 05 53 DB 74 F6 ....U..zw.=.S.t.

Ephemeral private key ($\widetilde{SK}_{PCD}$)	0010 93 CF 04 4E 18 C9 83 64 D4 97 7A 29 61 08 AF 19 ...N...d..z)a... 0020 BD .
OID for TA	0.4.0.127.0.7.2.2.2.2.5
CHR	44 45 54 45 53 54 41 54 44 45 30 31 39

T→C plain	0000 00 22 81 A4 3D 80 0A 04 00 7F 00 07 02 02 02 02 ."..=..... 0010 05 83 0D 44 45 54 45 53 54 41 54 44 45 30 31 39 ...DETESTATDE019 0020 91 20 5A 7A 37 7F C9 CA FC 03 AC 7F F4 54 41 A8 . Zz7.....TA. 0030 B2 90 9D 88 EA B8 E6 B0 17 38 47 AB 49 B9 49 DF .....8G.I.I. 0040 37 99 7.
T→C coded	0000 0C 22 81 A4 4D 87 41 01 FE 3F 02 34 E5 EF E6 6B ."..M.A..?.4...k 0010 9C 56 FD 23 D6 02 EE A5 9C 25 1E 1E 86 04 C4 6B .V.#.....%.....k 0020 33 FA 60 C7 D0 95 70 EE 88 17 91 C8 9F B8 15 9E 3.`...p..... 0030 71 C6 35 43 A9 BB 54 6F 6F 74 6F A8 83 7B C3 99 q.5C..Tooto..{.. 0040 0A 60 CA A5 8A 5A 5A B5 8E 08 D1 73 6F 1E 72 5B .`...ZZ....so.r[0050 C5 F8 00 ...
C→T coded	0000 99 02 90 00 8E 08 7D 47 C4 5B 27 DE DB 5C ......}G.['..\
C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	22		Manage Security Environment	
P1/P2	81 A4		Terminal Authentication: Set Authentication Template for external authentication	
L_c	3D		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	80	0A	04 00 7F 00 07 02 02 02 02 05	Cryptograhic mechanism reference, OID
	83	0D	44 45 54 45 53 54 41 54 44 45 30 31 39	Reference of public key
	91	20	5A 7A 37 7F C9 CA FC	Ephemeral public key

			03 AC 7F F4 54 41 A8 B2 90 9D 88 EA B8 E6 B0 17 38 47 AB 49 B9 49 DF 37 99	

4.6 Command Get Challenge

The chip is randomly chosing a r_{PICC} and this r_{PICC} is queried by the terminal.

r_{PICC}	54 7E 4E AB 03 B2 35 D2

T→C plain	0000 00 84 00 00 08
T→C coded	0000 0C 84 00 00 0D 97 01 08 8E 08 1D 21 EB BE 73 8F ....!..s. 0010 F4 FD 00 ...
C→T coded	0000 87 11 01 12 4E BD D5 70 FE 8E 05 FD 04 8B 2A 76 ....N..p......*v 0010 5C 5E 75 99 02 90 00 8E 08 C9 40 9B 30 57 B1 B4 \^u.......@.0W.. 0020 3F ?
C→T plain	0000 54 7E 4E AB 03 B2 35 D2 T~N...5.

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	84		Get Challenge	
P1/P2	00 00		-	
L_e	08			8 byte length of the response expected

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***
			54 7E 4E AB 03 B2 35 D2	8 bytes of randomness
SW	90 00		Normal operation	

4.7 Command External Authenticate

The data to be signed is constructed of the key, the challenge and the hash. The resulting signature is used in the command EXTERNAL AUTHENTICATE. The defined algorithm here is SHA512withECDSA.

Key (SK_{PCD})	0000 00 9D 9A 32 DF 93 A5 7C CE 33 CA 3C DD 34 57 E3 ...2...|.3.<.4W. 0010 3A 97 6F 29 35 46 C7 35 50 F3 97 25 9C 93 BE 01 :.o)5F.5P..%.... 0020 20
Challenge (r_{PICC})	0000 54 7E 4E AB 03 B2 35 D2 T~N...5.
Hash (ID_{PICC})	0000 5A 7A 37 7F C9 CA FC 03 AC 7F F4 54 41 A8 B2 90 Zz7........TA... 0010 9D 88 EA B8 E6 B0 17 38 47 AB 49 B9 49 DF 37 99 ....8G.I.I.7.
Data to be signed	0000 28 2C F3 80 73 03 6A FA C2 16 AF 13 5B D9 94 DA (,..s.j.....[... 0010 0C 35 7F 10 BD 4C 34 AF EA 10 42 B2 EB 0F D6 80 .5...L4...B..... 0020 54 7E 4E AB 03 B2 35 D2 5A 7A 37 7F C9 CA FC 03 T~N...5.Zz7..... 0030 AC 7F F4 54 41 A8 B2 90 9D 88 EA B8 E6 B0 17 38 ...TA..........8 0040 47 AB 49 B9 49 DF 37 99 G.I.I.7.

Signature (S_{PCD})	0000 81 A2 D9 E5 89 1B 86 A0 F0 1A DD 03 41 C8 9D 6E ....A..n 0010 9E F3 E2 0C 22 38 84 F2 7B 2F 20 40 E9 72 1C 46 ....."8..{/ @.r.F 0020 C9 C3 CF 7C 0E E0 A4 22 26 3B A6 F1 EA FC 69 3B ...|..."&;....i; 0030 D8 73 8F 34 76 0B 59 98 58 4F 58 DD 25 B8 D6 0D .s.4v.Y.XOX.%... 0040 99 D7 C4 59 57 C2 E2 F1 0C 0E 5F 91 A8 DC 88 BD ...YW....._..... 0050 7C FA 33 CB F7 84 A9 DA 83 C8 00 32 41 65 17 9D |.3........2Ae.. 0060 BE 71 C6 9B 2C 0F D8 11 27 0E 43 6C 43 27 81 84 .q..,...'.ClC'.. 0070 DD B5 42 14 23 42 DB F1 56 E8 2D 2A 1B C1 90 85 ..B.#B..V.-*....

T→C plain	0000 00 82 00 00 80 81 A2 D9 E5 89 1B 86 A0 F0 1A DD .... 0010 03 41 C8 9D 6E 9E F3 E2 0C 22 38 84 F2 7B 2F 20 .A..n...."8..{/ 0020 40 E9 72 1C 46 C9 C3 CF 7C 0E E0 A4 22 26 3B A6 @.r.F...|..."&;. 0030 F1 EA FC 69 3B D8 73 8F 34 76 0B 59 98 58 4F 58 ...i;.s.4v.Y.XOX 0040 DD 25 B8 D6 0D 99 D7 C4 59 57 C2 E2 F1 0C 0E 5F .%......YW....._ 0050 91 A8 DC 88 BD 7C FA 33 CB F7 84 A9 DA 83 C8 00 .....|.3........ 0060 32 41 65 17 9D BE 71 C6 9B 2C 0F D8 11 27 0E 43 2Ae...q..,...'.C 0070 6C 43 27 81 84 DD B5 42 14 23 42 DB F1 56 E8 2D lC'....B.#B..V.- 0080 2A 1B C1 90 85 *....
T→C coded	0000 0C 82 00 00 9E 87 81 91 01 18 61 40 90 D8 1A 79 ....a@...y 0010 F0 97 6A FA CB 5B 5C C6 DF 1B 11 13 11 56 5B 7F ..j..[\.......V[. 0020 17 40 57 69 F1 D5 7F 15 72 DD 03 B3 FE C9 32 77 .@Wi....r.....2w 0030 3C 34 68 AC 48 47 7C 28 AC 6C 46 AC 45 5C 7C 6F <4h.HG|(.lF.E|o 0040 99 3C 5C FA 7E D4 43 48 0D 89 84 48 C7 B1 9E CF .<\.~.CH...H.... 0050 DD 17 74 3C 86 A9 B0 8C 58 F4 B8 2B 7E E6 98 7A ..t<....X..+~..z 0060 7B C0 49 28 2B B1 35 E4 55 99 CC 5E DD 3B 8D EA {.I(+.5.U..^.;.. 0070 A5 70 EC 6D 71 F4 78 39 A8 B6 97 AB 9B FB E9 06 .p.mq.x9........ 0080 18 EA AC D7 F1 93 A8 93 D3 E2 29 54 19 CE A6 F5 ....)T....

	0090 37 AE 16 5F E0 CD 22 0D 8D 8E 08 B8 36 C6 48 0A 7.._.."".....6.H. 00A0 C6 3D C8 00 .=..
C→T coded	0000 99 02 90 00 8E 08 59 5C 11 F0 CD EC F1 F7 ......Y\......
C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	82		External Authenticate	
P1/P2	00 00		Keys and algorithms implicitly known	
L_c	80		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
			81 A2 D9 E5 89 1B 86 A0 F0 1A DD 03 41 C8 … … 42 14 23 42 DB F1 56 E8 2D 2A 1B C1 90 85	Signature generated by terminal

R-APDU		
SW	90 00	Normal operation

If the last command EXTERNAL AUTHENTICATE performs successfully the Terminal Authentication is established.

5. Chip Authentication Example (ECDH/ECDSA)

In this chapter the protocol Chip Authentication is described. Chip Authentication establishes Secure Messaging between a chip and a terminal based on a static key pair stored on the chip. Chip Authentication enables the terminal to verify that the chip is genuine. At first the file EF.CardSecurity must be read by the terminal. This file is defined as followed:

```
SEQUENCE SIZE( 2023 )
  OBJECT IDENTIFIER = { 1 2 840 113549 1 7 2 }
  A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 2008 )
    SEQUENCE SIZE( 2004 )
      INTEGER SIZE( 1 )
        0000  03                                                .
      SET SIZE( 15 )
        SEQUENCE SIZE( 13 )
          OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
          NULL SIZE( 0 )
      SEQUENCE SIZE( 333 )
        OBJECT IDENTIFIER = { 0 4 0 127 0 7 3 2 1 }
        A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 319 )
          OCTET-STRING SIZE( 315 )
            0000  31 82 01 37 30 0D 06 08 04 00 7F 00 07 02 02 02  1..70...........
            0010  02 01 02 30 12 06 0A 04 00 7F 00 07 02 02 03 02  ...0............
            0020  02 02 01 02 02 01 01 30 12 06 0A 04 00 7F 00 07  .......0........
            0030  02 02 04 02 02 02 01 02 02 01 0D 30 1C 06 09 04  ...........0....
            0040  00 7F 00 07 02 02 03 02 30 0C 06 07 04 00 7F 00  ........0.......
            0050  07 01 02 02 01 0D 02 01 01 30 2F 06 08 04 00 7F  .........0/.....
            0060  00 07 02 02 06 16 23 68 74 74 70 73 3A 2F 2F 77  ......#https://w
            0070  77 77 2E 68 6A 70 2D 63 6F 6E 73 75 6C 74 69 6E  ww.hjp-consultin
            0080  67 2E 63 6F 6D 2F 68 6F 6D 65 30 17 06 0A 04 00  g.com/home0.....
            0090  7F 00 07 02 02 05 02 03 30 09 02 01 01 02 01 01  ........0.......
            00A0  01 01 00 30 17 06 0A 04 00 7F 00 07 02 02 05 02  ...0............
            00B0  03 30 09 02 01 01 02 01 02 01 01 FF 30 19 06 09  .0..........0...
            00C0  04 00 7F 00 07 02 02 05 02 30 0C 06 07 04 00 7F  .........0......
            00D0  00 07 01 02 02 01 0D 30 62 06 09 04 00 7F 00 07  .......0b.......
            00E0  02 02 01 02 30 52 30 0C 06 07 04 00 7F 00 07 01  ....0R0.........
            00F0  02 02 01 0D 03 42 00 04 A4 4E BE 54 51 DF 7A AD  .....B...N.TQ.z.
            0100  B0 1E 45 9B 8C 92 8A 87 74 6A 57 92 7C 8C 28 A6  ..E.....tjW.|.(.
            0110  77 5C 97 A7 E1 FE 8D 9A 46 FF 4A 1C C7 E4 D1 38  w\......F.J....8
            0120  9A EA 19 75 8E 4F 75 C2 8C 59 8F D7 34 AE BE B1  ...u.Ou..Y..4...
            0130  35 33 7C F9 5B E1 2E 94 02 01 01                 53|.[......
      A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 1122 )
        SEQUENCE SIZE( 1118 )
          SEQUENCE SIZE( 658 )
            A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 3 )
              INTEGER SIZE( 1 )
                0000  02                                           .
            INTEGER SIZE( 3 )
              0000  01 63 26                                     .c&
            SEQUENCE SIZE( 65 )
              OBJECT IDENTIFIER = { 1 2 840 113549 1 1 10 }
              SEQUENCE SIZE( 52 )
                A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 15 )
                  SEQUENCE SIZE( 13 )
                    OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
                    NULL SIZE( 0 )
```

```
    A1 [ CONTEXT 1 ] IMPLICIT SEQUENCE SIZE( 28 )
      SEQUENCE SIZE( 26 )
        OBJECT IDENTIFIER = { 1 2 840 113549 1 1 8 }
        SEQUENCE SIZE( 13 )
          OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
          NULL SIZE( 0 )
    A2 [ CONTEXT 2 ] IMPLICIT SEQUENCE SIZE( 3 )
      INTEGER SIZE( 1 )
        0000  20
SEQUENCE SIZE( 83 )
  SET SIZE( 11 )
    SEQUENCE SIZE( 9 )
      OBJECT IDENTIFIER = { 2 5 4 6 }
      PRINTABLE-STRING SIZE( 2 )
        0000  44 45                                              DE
  SET SIZE( 23 )
    SEQUENCE SIZE( 21 )
      OBJECT IDENTIFIER = { 2 5 4 10 }
      UTF8-STRING SIZE( 14 )
        0000  48 4A 50 20 43 6F 6E 73 75 6C 74 69 6E 67          HJP Consulting
  SET SIZE( 23 )
    SEQUENCE SIZE( 21 )
      OBJECT IDENTIFIER = { 2 5 4 11 }
      UTF8-STRING SIZE( 14 )
        0000  43 6F 75 6E 74 72 79 20 53 69 67 6E 65 72          Country Signer
  SET SIZE( 18 )
    SEQUENCE SIZE( 16 )
      OBJECT IDENTIFIER = { 2 5 4 3 }
      UTF8-STRING SIZE( 9 )
        0000  48 4A 50 20 50 42 20 43 53                         HJP PB CS
SEQUENCE SIZE( 30 )
  UTC SIZE( 13 )
    0000  30 39 30 39 31 38 30 37 35 39 35 33 5A           090918075953Z
  UTC SIZE( 13 )
    0000  31 30 30 39 31 33 30 37 35 39 35 33 5A           100913075953Z
SEQUENCE SIZE( 84 )
  SET SIZE( 11 )
    SEQUENCE SIZE( 9 )
      OBJECT IDENTIFIER = { 2 5 4 6 }
      PRINTABLE-STRING SIZE( 2 )
        0000  44 45                                              DE
  SET SIZE( 23 )
    SEQUENCE SIZE( 21 )
      OBJECT IDENTIFIER = { 2 5 4 10 }
      UTF8-STRING SIZE( 14 )
        0000  48 4A 50 20 43 6F 6E 73 75 6C 74 69 6E 67          HJP Consulting
  SET SIZE( 24 )
    SEQUENCE SIZE( 22 )
      OBJECT IDENTIFIER = { 2 5 4 11 }
      UTF8-STRING SIZE( 15 )
        0000  44 6F 63 75 6D 65 6E 74 20 53 69 67 6E 65 72       Document Signer
  SET SIZE( 18 )
    SEQUENCE SIZE( 16 )
      OBJECT IDENTIFIER = { 2 5 4 3 }
      UTF8-STRING SIZE( 9 )
        0000  48 4A 50 20 50 42 20 44 53                         HJP PB DS
SEQUENCE SIZE( 290 )
  SEQUENCE SIZE( 13 )
```

```
      OBJECT IDENTIFIER = { 1 2 840 113549 1 1 1 }
      NULL SIZE( 0 )
    BIT-STRING SIZE( 271 )
      0000  00 30 82 01 0A 02 82 01 01 00 B6 C5 A8 EE 57 30  .0............W0
      0010  76 79 E3 64 E3 F7 E7 76 EA 64 07 4E 9A 72 F6 B3  vy.d...v.d.N.r..
      0020  76 C2 D2 31 89 63 1C 10 BA 65 EA 34 6F EF 70 3B  v..1.c...e.4o.p;
      0030  52 EF 75 93 D4 96 E1 50 0F 71 64 D0 38 E9 A8 80  R.u....P.qd.8...
      0040  D0 6E 90 FC F9 6F AD 5B 60 68 B3 42 CC A8 24 77  .n...o.[`h.B..$w
      0050  0B AD F1 42 9E BB DB 97 88 0A AE A4 31 14 62 CA  ...B........1.b.
      0060  CE 40 AA F2 24 78 35 AB C2 59 1E 18 80 AD D9 FD  .@..$x5..Y......
      0070  35 F2 C0 E4 3C C6 FE B9 1B 0F 13 7C C4 2A D8 34  5...<......|.*.4
      0080  73 24 93 FD 63 F7 8F C7 DA 75 CD B4 A1 BD 4C 7D  s$..c....u....L}
      0090  E1 E0 4A C1 B4 BD 4C 62 C4 6F 8D 83 EE 6B F1 AC  ..J...Lb.o...k..
      00A0  24 05 D5 A1 73 77 6A 58 96 0A 79 B1 B5 B9 0B 79  $...swjX..y....y
      00B0  7A 4A 7A 19 84 57 C7 A0 2A 72 A2 FF 9A 32 7E 55  zJz..W..*r...2~U
      00C0  88 19 67 42 C5 7C 8B 9D 5E E6 4B 8A 46 00 3B C5  ..gB.|..^.K.F.;.
      00D0  6D 24 93 C0 A6 58 82 37 94 AB 23 14 BC F9 79 C5  m$...X.7..#...y.
      00E0  EE DF 32 7C 6C 11 2E 9E DD 86 C6 E4 19 F9 AD 35  ..2|l..........5
      00F0  A9 46 56 FD E7 ED 89 6A F5 C3 46 43 5A B3 D7 BE  .FV....j..FCZ...
      0100  C0 F8 B9 02 56 A3 10 50 B3 97 02 03 01 00 01     ....V..P.......
  A3 [ CONTEXT 3 ] IMPLICIT SEQUENCE SIZE( 82 )
    SEQUENCE SIZE( 80 )
      SEQUENCE SIZE( 31 )
        OBJECT IDENTIFIER = { 2 5 29 35 }
        OCTET-STRING SIZE( 24 )
          0000  30 16 80 14 0D FD 5C 02 88 BF EC E0 B0 7A 5D 40  0.....\......z]@
          0010  FF 80 AC 8A 91 74 3A 9B                        .....t:.
      SEQUENCE SIZE( 29 )
        OBJECT IDENTIFIER = { 2 5 29 14 }
        OCTET-STRING SIZE( 22 )
          0000  04 14 91 93 F4 F0 AA 4A CA C0 D3 A1 B6 AC 83 B2  .......J........
          0010  4F 6F DC 8F F2 1B                              Oo....
      SEQUENCE SIZE( 14 )
        OBJECT IDENTIFIER = { 2 5 29 15 }
        BOOLEAN SIZE( 1 )
          0000  FF                                            .
        OCTET-STRING SIZE( 4 )
          0000  03 02 07 80                                   ....
SEQUENCE SIZE( 65 )
  OBJECT IDENTIFIER = { 1 2 840 113549 1 1 10 }
  SEQUENCE SIZE( 52 )
    A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 15 )
      SEQUENCE SIZE( 13 )
        OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
        NULL SIZE( 0 )
    A1 [ CONTEXT 1 ] IMPLICIT SEQUENCE SIZE( 28 )
      SEQUENCE SIZE( 26 )
        OBJECT IDENTIFIER = { 1 2 840 113549 1 1 8 }
        SEQUENCE SIZE( 13 )
          OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
          NULL SIZE( 0 )
    A2 [ CONTEXT 2 ] IMPLICIT SEQUENCE SIZE( 3 )
      INTEGER SIZE( 1 )
        0000  20
BIT-STRING SIZE( 385 )
  0000  00 A3 AF EC 3B C5 D3 66 E6 61 19 4A CA 8D FC 39  ....;..f.a.J...9
  0010  06 76 06 1D 6E 52 30 18 CA 13 93 0D 79 40 E6 CE  .v..nR0.....y@..
  0020  77 86 1D 18 F6 5F 3C EF 8C BF 44 E8 7D 59 AA FA  w...._<...D.}Y..
```

```
      0030  6F 29 EC 57 FB 19 DB 12 30 F0 F2 FC 1B F6 0D 1D  o).W....0.......
      0040  03 96 33 3C 89 A9 2B F2 31 3C 43 60 BA B2 18 DE  ..3<..+.1<C`....
      0050  57 71 3F 39 0C A5 BB B6 99 CD 1A 1E 27 3C 61 8B  Wq?9........'<a.
      0060  25 A7 EE DA B5 F0 BA B0 30 65 AA 74 9D 51 32 60  %.......0e.t.Q2`
      0070  BE 86 7E B0 11 29 1D CF 4A DC 83 33 F7 78 4F DD  ..~..)..J..3.xO.
      0080  E8 17 2F 46 C4 F7 90 42 15 FD C9 8F 5C DE 49 16  ../F...B....\.I.
      0090  F0 3E 24 9C D3 94 07 62 D2 F8 E9 2F 23 17 16 A6  .>$....b.../#...
      00A0  BF 74 2F ED C2 62 7E 62 F0 46 95 6D B9 7B AA D2  .t/..b~b.F.m.{..
      00B0  5C 04 62 47 54 D4 AF 3E 1A 7E C4 72 07 CC 08 BD  \.bGT..>.~.r....
      00C0  15 4E 83 9A 43 55 D0 1F 16 DA 2C C1 61 77 A9 14  .N..CU....,.aw..
      00D0  D4 42 87 E6 52 25 64 D0 00 53 9E C9 6A 2B 0E 1E  .B..R%d..S..j+..
      00E0  6E BB 89 63 81 86 8B 5A FE 0A 0F D3 C3 62 F4 19  n..c...Z.....b..
      00F0  AF FD FF 01 6A 71 17 0A C8 B3 78 A6 E3 99 5D 82  ....jq....x...].
      0100  EE 45 95 0E EB B4 C9 BB F6 31 13 24 82 A5 03 C3  .E.......1.$....
      0110  10 26 B4 C2 CD 94 26 E6 66 3D E4 C4 3E FE 54 01  .&....&.f=..>.T.
      0120  F4 D3 BA 76 E5 4F 66 3B 28 32 3E A3 33 1E 96 A7  ...v.Of;(2>.3...
      0130  08 12 F9 43 15 D6 08 A9 E8 CE 1B F0 2B 6E CF 07  ...C........+n..
      0140  01 5D 40 F4 73 DF E1 6F 5C 12 14 60 81 C4 4C 14  .]@.s..o\..`..L.
      0150  8D AB 09 83 50 46 57 A5 3C CA 16 BD 54 5D 5A D5  ....PFW.<...T]Z.
      0160  9A 21 AA 91 9E 7F 9B B7 B3 50 01 AB EF 61 E7 D5  .!.......P...a..
      0170  6E 21 C7 F1 13 73 42 55 71 A7 91 45 D4 46 2E B2  n!...sBUq..E.F..
      0180  6B                                              k
SET SIZE( 517 )
  SEQUENCE SIZE( 513 )
    INTEGER SIZE( 1 )
      0000  01                                              .
    SEQUENCE SIZE( 90 )
      SEQUENCE SIZE( 83 )
        SET SIZE( 11 )
          SEQUENCE SIZE( 9 )
            OBJECT IDENTIFIER = { 2 5 4 6 }
            PRINTABLE-STRING SIZE( 2 )
              0000  44 45                                       DE
        SET SIZE( 23 )
          SEQUENCE SIZE( 21 )
            OBJECT IDENTIFIER = { 2 5 4 10 }
            UTF8-STRING SIZE( 14 )
              0000  48 4A 50 20 43 6F 6E 73 75 6C 74 69 6E 67   HJP Consulting
        SET SIZE( 23 )
          SEQUENCE SIZE( 21 )
            OBJECT IDENTIFIER = { 2 5 4 11 }
            UTF8-STRING SIZE( 14 )
              0000  43 6F 75 6E 74 72 79 20 53 69 67 6E 65 72   Country Signer
        SET SIZE( 18 )
          SEQUENCE SIZE( 16 )
            OBJECT IDENTIFIER = { 2 5 4 3 }
            UTF8-STRING SIZE( 9 )
              0000  48 4A 50 20 50 42 20 43 53                  HJP PB CS
      INTEGER SIZE( 3 )
        0000  01 63 26                                        .c&
    SEQUENCE SIZE( 13 )
      OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
      NULL SIZE( 0 )
    A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 74 )
      SEQUENCE SIZE( 23 )
        OBJECT IDENTIFIER = { 1 2 840 113549 1 9 3 }
        SET SIZE( 10 )
          OBJECT IDENTIFIER = { 0 4 0 127 0 7 3 2 1 }
```

```
  SEQUENCE SIZE( 47 )
    OBJECT IDENTIFIER = { 1 2 840 113549 1 9 4 }
    SET SIZE( 34 )
      OCTET-STRING SIZE( 32 )
        0000  49 AE B9 37 52 8C 26 9E A7 23 BB C8 AA DC 38 5C  I..7R.&..#....8\
        0010  9D 6B 1A E3 75 16 A5 B8 92 1F F8 C4 59 18 72 93  .k..u.......Y.r.
SEQUENCE SIZE( 65 )
  OBJECT IDENTIFIER = { 1 2 840 113549 1 1 10 }
  SEQUENCE SIZE( 52 )
    A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 15 )
      SEQUENCE SIZE( 13 )
        OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
        NULL SIZE( 0 )
    A1 [ CONTEXT 1 ] IMPLICIT SEQUENCE SIZE( 28 )
      SEQUENCE SIZE( 26 )
        OBJECT IDENTIFIER = { 1 2 840 113549 1 1 8 }
        SEQUENCE SIZE( 13 )
          OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
          NULL SIZE( 0 )
    A2 [ CONTEXT 2 ] IMPLICIT SEQUENCE SIZE( 3 )
      INTEGER SIZE( 1 )
        0000  20
OCTET-STRING SIZE( 256 )
  0000  97 C2 2D 87 C3 13 D6 48 DF B9 DE 9D 9C CA 3A 41  ..-....H......:A
  0010  CB F8 52 22 E3 6D 3B 9C 7E B1 CC 0B 1A 8C AE 4C  ..R".m;.~......L
  0020  93 E0 F1 CA 02 8A 90 DD 2B 4F 5C B4 2C 9E 5B B5  ........+O\.,.[.
  0030  73 C0 39 77 3E 64 08 41 B3 28 30 DF 83 93 22 46  s.9w>d.A.(0..."F
  0040  FC 8B AF 92 8D 67 54 6E 8E 0C 06 65 A9 32 87 48  .....gTn...e.2.H
  0050  85 51 8E A3 D0 20 46 A6 18 CF 1A F5 A0 F5 E4 C4  .Q... F.........
  0060  05 62 4D 2D 66 D1 6B DA 18 A8 38 22 84 78 8E 81  .bM-f.k...8".x..
  0070  FE 1C B5 E2 17 01 CD D2 09 22 12 0E 68 20 30 E8  .........".h 0.
  0080  0D 12 DA 40 6B 01 36 E9 ED 8B 23 8F 65 3C 7D DC  ...@k.6...#.e<}.
  0090  A9 27 86 60 41 4E FA 93 73 82 50 CD 08 41 72 7E  .'.`AN..s.P..Ar~
  00A0  0F 68 C4 90 02 64 1D 7E 40 26 28 5B 9B 53 F2 70  .h...d.~@&([.S.p
  00B0  BB A5 05 8E 46 60 0B 84 35 54 60 5B F8 EC 2C 74  ....F`..5T`[..,t
  00C0  0A ED C8 B2 4E 2A 64 AC 78 F5 89 97 A1 88 33 A4  ....N*d.x.....3.
  00D0  05 CB 64 EA 6D D7 D7 11 5F D7 C3 51 76 72 65 4E  ..d.m..._..QvreN
  00E0  03 02 97 30 FA B7 25 65 A0 92 65 71 69 68 01 F3  ...0..%e..eqih..
  00F0  FE 5A 63 CF 70 92 0A 11 2F CF 69 29 1B AE 37 A3  .Zc.p.../.i)..7.
```

The relevant information for CA are:

Public Key (PK_{PICC})	0000 04 A4 4E BE 54 51 DF 7A AD B0 1E 45 9B 8C 92 8A ..N.TQ.z...E.... 0010 87 74 6A 57 92 7C 8C 28 A6 77 5C 97 A7 E1 FE 8D .tjW.|.(.w\..... 0020 9A 46 FF 4A 1C C7 E4 D1 38 9A EA 19 75 8E 4F 75 .F.J....8...u.Ou 0030 C2 8C 59 8F D7 34 AE BE B1 35 33 7C F9 5B E1 2E ..Y..4...53|.[.. 0040 94 .
CA OID	0.4.0.127.0.7.2.2.3.2.2
ECDH Shared Secret (K)	0000 79 1D A0 42 73 CC FE 86 2E 52 DF 60 34 7E 25 57 y..Bs....R.`4~%W 0010 19 2E 1F 8D 75 17 82 2C E3 D3 06 05 6C 1C DE B4 ....u..,....l...

5.1 Command MSE: Set AT

In the first step the following information extracted from EF.ChipSecurity are important.

CA OID	0.4.0.127.0.7.2.2.3.2.2
Key Reference	01

In the first step of Chip Authentication the terminal sends its OID for CA and the reference of the private key to the chip with the command MSE:Set AT as following.

T→C plain	0000 00 22 41 A4 0F 80 0A 04 00 7F 00 07 02 02 03 02 ."A..... 0010 02 84 01 01 ....
T→C coded	0000 0C 22 41 A4 1D 87 11 01 73 29 A5 63 CC C8 1D D1 ."A.....s).c.... 0010 98 18 79 EF 55 C3 5F F4 8E 08 2F C6 BD 55 A9 1D ..y.U._.../..U.. 0020 5E A1 00 ^..
C→T coded	0000 99 02 90 00 8E 08 28 3C F6 67 65 5C 33 A6 90 00 ......(<.ge\3...
C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	22		Manage Security Environment	
P1/P2	41 A4		Chip Authentication: Set Authentication Template for internal authentication	
L_c	0F		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	80	0A	04 00 7F 00 07 02 02 03 02 02	Cryptographic mechanism reference, OID
	84	01	01	Reference of private key

R-APDU		
SW	90 00	Normal operation

5.2 Command General Authenticate

The terminal send the ephemeral public key $\widetilde{PK}_{PCD}$ to the chip.

$\widetilde{PK}_{PCD}$	0000 04 5A 7A 37 7F C9 CA FC 03 AC 7F F4 54 41 A8 B2 .Zz7........TA.. 0010 90 9D 88 EA B8 E6 B0 17 38 47 AB 49 B9 49 DF 37 ....8G.I.I.7 0020 99 A3 4E E5 7E C5 52 68 CF 8B 1C 3E C4 89 F8 BF ..N.~.Rh...>.... 0030 4C F4 C6 8D 3F D9 67 0E 89 C0 D5 D3 FF F1 AA F8 L...?.g......... 0040 9F . .

The command is performed as following.

T→C plain	0000 00 86 00 00 45 7C 43 80 41 04 5A 7A 37 7F C9 CA ....E|C.A.Zz7... 0010 FC 03 AC 7F F4 54 41 A8 B2 90 9D 88 EA B8 E6 B0 .....TA......... 0020 17 38 47 AB 49 B9 49 DF 37 99 A3 4E E5 7E C5 52 .8G.I.I.7..N.~.R 0030 68 CF 8B 1C 3E C4 89 F8 BF 4C F4 C6 8D 3F D9 67 h...>....L...?.g 0040 0E 89 C0 D5 D3 FF F1 AA F8 9F 00 .....
T→C coded	0000 0C 86 00 00 60 87 51 01 20 43 9F E1 26 64 30 D1 ....`.Q. C..&d0. 0010 7B 9D EA A0 9E 6B A5 6B F9 DC 58 A4 7E 2E 08 F4 {....k.k..X.~... 0020 90 31 8B E4 90 6C 41 CD 67 6A 18 D0 D4 BF 99 52 .1...lA.gj.....R 0030 A4 EA 1E 81 DA FB F9 DE 89 10 2F 32 4F 14 DA A6 ..../2O... 0040 D6 D3 F1 67 6D 2E AA EF E6 D1 F9 AB 34 F1 4B 1D ...gm.......4.K. 0050 9D 27 35 C3 60 2D DC 0B 97 01 00 8E 08 E1 9B 47 .'5.`-.........G 0060 4E FE AF A6 EB 00 N.....
C→T coded	0000 87 21 01 DA 04 8A 9D D7 BA 3A 90 1B 3F 36 49 C0 .!.......:..?6I. 0010 9F E2 B6 9B 1A 4F D9 90 5A BD 51 95 78 95 EA 84 .....O..Z.Q.x... 0020 D5 CD 2B 99 02 90 00 8E 08 6C 9C CD 20 7F 35 DE ..+......l.. .5. 0030 AD .
C→T plain	0000 7C 14 81 08 42 87 B3 07 2A 3E DC 60 82 08 FF 01 |...B...*>.`.... 0010 17 D6 8D EE 8E 72 .....r

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	45		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	43		Dynamic Authentication Data
	80	41	04 A4 4E BE 54 51 DF 7A AD B0 1E 45 9B 8C 92 8A	Ephemeral public key of terminal

			87 74 6A 57 92 7C 8C 28 A6 77 5C 97 A7 E1 FE 8D 9A 46 FF 4A 1C C7 E4 D1 38 9A EA 19 75 8E 4F 75 C2 8C 59 8F D7 34 AE BE B1 35 33 7C F9 5B E1 2E 94	
L_e	00			Expected maximal byte length of the response data field

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	14		Dynamic Authentication Data
	81	08	42 87 B3 07 2A 3E DC 60	r_{PICC}
	82	08	FF 01 17 D6 8D EE 8E 72	T_{PICC}
SW	90 00		Normal operation	

Both the terminal and the chip calculate the shared secret K.

PICC:

SK_{PICC}	0000 79 84 67 4C F3 B3 A5 24 BF 92 9C E8 A6 7F CF 22 y.gL...$....... 0010 17 3D A0 BA D5 95 EE D6 DE B7 2D 22 C5 42 FA 9D .=........-".B..
$\widetilde{PK}_{PCD}$	0000 04 5A 7A 37 7F C9 CA FC 03 AC 7F F4 54 41 A8 B2 .Zz7........TA.. 0010 90 9D 88 EA B8 E6 B0 17 38 47 AB 49 B9 49 DF 37 ....8G.I.I.7 0020 99 A3 4E E5 7E C5 52 68 CF 8B 1C 3E C4 89 F8 BF ..N.~.Rh...>.... 0030 4C F4 C6 8D 3F D9 67 0E 89 C0 D5 D3 FF F1 AA F8 L...?.g......... 0040 9F .
D_{PICC}	0D
Shared Secret K	0000 79 1D A0 42 73 CC FE 86 2E 52 DF 60 34 7E 25 57 y..Bs....R.`4~%W 0010 19 2E 1F 8D 75 17 82 2C E3 D3 06 05 6C 1C DE B4 ....u..,....l... 0020 42 87 B3 07 2A 3E DC 60 B...*>.`

PCD:

$\widetilde{SK}_{PCD}$	0000 00 A6 A4 D2 55 C5 BF 7A 77 EC 3D 05 53 DB 74 F6 ....U..zw.=.S.t. 0010 93 CF 04 4E 18 C9 83 64 D4 97 7A 29 61 08 AF 19 ...N...d..z)a... 0020 BD .
PK_{PICC}	0000 04 A4 4E BE 54 51 DF 7A AD B0 1E 45 9B 8C 92 8A ..N.TQ.z...E.... 0010 87 74 6A 57 92 7C 8C 28 A6 77 5C 97 A7 E1 FE 8D .tjW.|.(.w\.....

	0020 9A 46 FF 4A 1C C7 E4 D1 38 9A EA 19 75 8E 4F 75 .F.J....8...u.Ou 0030 C2 8C 59 8F D7 34 AE BE B1 35 33 7C F9 5B E1 2E ..Y..4...53|.[.. 0040 94 .
D_{PICC}	0D
Shared Secret K	0000 79 1D A0 42 73 CC FE 86 2E 52 DF 60 34 7E 25 57 y..Bs....R.`4~%W 0010 19 2E 1F 8D 75 17 82 2C E3 D3 06 05 6C 1C DE B4 ....u..,....l... 0020 42 87 B3 07 2A 3E DC 60 B...*>.`

Input data for Authentication Token:

OID	0000 04 00 7F 00 07 02 02 03 02 02 ....
$\widetilde{PK}_{PCD}$	0000 04 5A 7A 37 7F C9 CA FC 03 AC 7F F4 54 41 A8 B2 .Zz7........TA.. 0010 90 9D 88 EA B8 E6 B0 17 38 47 AB 49 B9 49 DF 37 ....8G.I.I.7 0020 99 A3 4E E5 7E C5 52 68 CF 8B 1C 3E C4 89 F8 BF ..N.~.Rh...>.... 0030 4C F4 C6 8D 3F D9 67 0E 89 C0 D5 D3 FF F1 AA F8 L...?.g......... 0040 9F .
Complete input data for Token	0000 7F 49 4F 06 0A 04 00 7F 00 07 02 02 03 02 02 86 .IO............. 0010 41 04 5A 7A 37 7F C9 CA FC 03 AC 7F F4 54 41 A8 A.Zz7........TA. 0020 B2 90 9D 88 EA B8 E6 B0 17 38 47 AB 49 B9 49 DF ....8G.I.I. 0030 37 99 A3 4E E5 7E C5 52 68 CF 8B 1C 3E C4 89 F8 7..N.~.Rh...>... 0040 BF 4C F4 C6 8D 3F D9 67 0E 89 C0 D5 D3 FF F1 AA .L...?.g........ 0050 F8 9F ..
T_{PCD}	FF 01 17 D6 8D EE 8E 72

The authentication token T_{PCD} computed by the terminal is equal to the authentication T_{PICC} returned by the PICC in the previous command above. This means Chip Authentication has performed successfully.

The new session keys (AES 128) are derived from the shared secret by means of KDF specified in [TR-03110].

K_{Enc}	0000 94 AB CD 27 1A B7 D9 A5 59 0B A5 2C B5 18 B8 31 ...'....Y..,...1
K_{Mac}	0000 78 B5 70 9E 7A BE DB 18 5B 42 4D 0E E3 A8 24 99 x.p.z...[BM...$.

With an established Chip Authentication and the new session keys the data of the chip application can be read.

6. Settings for DH/RSA

In this example based on DH the two following certificates are use: Cert_DV and Cert_AT from test case EAC2_EIDDATA_B_01 of [TR-03105] part 3.3. Both certificates allow the terminal to read the data of the eID application.

6.1 Certificate DV

The **DV certificate** stores the information below:

Certificate Body:

```
0000  7F 4E 81 E4 5F 29 01 00 42 0F 44 45 54 45 53 54  .N.._)..B.DETEST
0010  43 56 43 41 30 30 30 30 33 7F 49 81 94 06 0A 04  CVCA00003.I.....
0020  00 7F 00 07 02 02 02 01 01 81 81 80 A0 8C 4D 11  ..............M.
0030  D6 99 F4 25 B0 E7 43 BB A4 F2 19 6E 05 BC 9E F2  ...%..C....n....
0040  4F 53 A6 74 42 90 E6 55 6E 83 E9 05 77 A9 30 EC  OS.tB..Un...w.0.
0050  31 4A 4F 9F 03 33 A0 A0 19 93 11 0E C6 34 86 DF  1JO..3.......4..
0060  60 7F D7 B3 04 74 79 B0 EC 09 04 AC F8 B6 26 5C  `....ty.......&\
0070  D0 AB C3 53 8F 4D 72 39 5D D5 F1 E7 A1 08 18 A7  ...S.Mr9].......
0080  FA A0 1D 25 FF 25 BC 6B F1 9C E8 6A 20 82 33 C5  ...%.%.k...j .3.
0090  43 7F F9 90 FE 94 D1 C2 5D 59 BE DB 6A E7 9E 4A  C.......]Y..j..J
00A0  76 DE 22 79 FC D6 A5 A3 D6 6F F5 F9 82 03 01 00  v."y.....o......
00B0  01 5F 20 0D 44 45 54 45 53 54 44 56 44 45 30 31  ._ .DETESTDVDE01
00C0  39 7F 4C 12 06 09 04 00 7F 00 07 03 01 02 02 53  9.L............S
00D0  05 80 1F FF FF 10 5F 25 06 01 00 00 03 02 04 5F  ......_%......._
00E0  24 06 01 00 00 04 02 04                          $.......
```

Tag	*Length*	*Value*	*ASN1.Type*	*Comment*
7F 4E	E4		SEQUENCE	Certificate Body
5F 29	01	00	UNSIGNED INTEGER	Certificate Profile Identifier
42	0F	44 45 54 45 53 54 43 56 43 41 30 30 30 30 33	CHARACTER STRING	Certification Authority Reference DETESTCVCA00003
7F 49	94		SEQUENCE	Public Key
06	0A	04 00 7F 00 07 02 02 02 01 01	OID	id-TA-RSA-v1-5-SHA-1
81	80	A0 8C 4D 11 ... ... D6 6F F5 F9	UNSIGNED INTEGER	Prime modulus
82	03	01 00 01	UNSIGNED INTEGER	First coefficient

5F 20	0D	44 45 54 45 53 54 44 56 44 45 30 31 39		CHARACTER STRING	Certificate Holder Reference DETESTDVDE019
7F 4C	12			SEQUENCE	Certificate Holder Authorization Template
06	09	04 00 7F 00 07 03 01 02 02		OID	id-AT
53	05	80 1F FF FF 10		OCTET STRING	Discretionary Data (DVwith all access rights)
5F 25	06	01 00 00 03 02 04		DATE	Certificate Effective Date
5F 24	06	01 00 00 04 02 04		DATE	Certificate Expiration Date

Certification information:

Authority Reference:	44 45 54 45 53 54 43 56 43 41 30 30 30 30 33 (DETESTCVCA00003)
Public Key:	0.4.0.127.0.7.2.2.2.1.1 (RSA v1.5 with SHA-1) Prime modulus: 0000 A0 8C 4D 11 D6 99 F4 25 B0 E7 43 BB A4 F2 19 6E 0010 05 BC 9E F2 4F 53 A6 74 42 90 E6 55 6E 83 E9 05 0020 77 A9 30 EC 31 4A 4F 9F 03 33 A0 A0 19 93 11 0E 0030 C6 34 86 DF 60 7F D7 B3 04 74 79 B0 EC 09 04 AC 0040 F8 B6 26 5C D0 AB C3 53 8F 4D 72 39 5D D5 F1 E7 0050 A1 08 18 A7 FA A0 1D 25 FF 25 BC 6B F1 9C E8 6A 0060 20 82 33 C5 43 7F F9 90 FE 94 D1 C2 5D 59 BE DB 0070 6A E7 9E 4A 76 DE 22 79 FC D6 A5 A3 D6 6F F5 F9 Public exponent e: 01 00 01
Certificate Holder Reference:	44 45 54 45 53 54 44 56 44 45 30 31 39 (DETESTDVDE019)
Certificate Holder Authorization:	OID: 0.4.0.127.0.7.3.1.2.2 (Authentication Terminal) Discretionary Data: 80 1F FF FF 10 Role: DV (official domestic)

	Access Rights: CAN allowed Read Access(eID) DG1 Read Access(eID) DG2 Read Access(eID) DG3 Read Access(eID) DG4 Read Access(eID) DG5 Read Access(eID) DG6 Read Access(eID) DG7 Read Access(eID) DG8 Read Access(eID) DG9 Read Access(eID) DG10 Read Access(eID) DG11 Read Access(eID) DG12 Read Access(eID) DG13 Read Access(eID) DG14 Read Access(eID) DG15 Read Access(eID) DG16 Read Access(eID) DG17 Read Access(eID) DG18 Read Access(eID) DG19 Read Access(eID) DG20 Read Access(eID) DG21
Effective Date:	01 00 00 03 02 04 (2010.03.24)
Expiration Date:	01 00 00 04 02 04 (2010.04.24)

Certificate AT

The **AT certificate** stores the following data:

Certificate Body:

```
0000  7F 4E 81 E2 5F 29 01 00 42 0D 44 45 54 45 53 54  .N.._)..B.DETEST
0010  44 56 44 45 30 31 39 7F 49 81 94 06 0A 04 00 7F  DVDE019.I.......
0020  00 07 02 02 02 01 01 81 81 80 9F 7E F6 8E 15 3D  ...........~...=
0030  B4 FD 10 84 DD ED BE AE 84 2C 55 6D 41 9F CB 5E  .........,UmA..^
0040  F6 21 AA 37 51 F0 FC 0C FD 71 4F C0 E7 68 86 6B  .!.7Q....qO..h.k
0050  3F 44 E2 72 5A F0 35 1A 97 ED B1 BA 88 DF DD 9B  ?D.rZ.5.........
```

```
0060  4D 81 D4 08 FE 07 63 34 6A 77 2C F6 46 16 46 5C  M.....c4jw,.F.F\
0070  8F D9 71 B7 75 D2 E1 34 26 C5 BC 11 89 47 95 C5  ..q.u..4&....G..
0080  AD 2C 3E 42 68 37 F3 A1 01 9F E9 51 24 EA 5D 43  .,>Bh7.....Q$.]C
0090  3E 90 6D 79 93 49 63 21 EF CB DB C3 2D 93 C0 68  >.my.Ic!....-..h
00A0  0B 45 F3 B8 F6 4A 5D AF CF B9 82 03 01 00 01 5F  .E...J].........
00B0  20 0D 44 45 54 45 53 54 41 54 44 45 30 31 39 7F   .DETESTATDE019.
00C0  4C 12 06 09 04 00 7F 00 07 03 01 02 02 53 05 00  L............S..
00D0  00 00 01 10 5F 25 06 01 00 00 03 02 04 5F 24 06  ....._%......._$.
00E0  01 00 00 04 02 04                                ......
```

Tag	*Length*	*Value*	*ASN1.Type*	*Comment*
7F 4E	E2		SEQUENCE	Certificate Body
5F 29	01	00	UNSIGNED INTEGER	Certificate Profile Identifier
42	0F	44 45 54 45 53 54 44 56 44 45 30 31 39	CHARACTER STRING	Certification Authority Reference DETESTDVDE019
7F 49	94		SEQUENCE	Public Key
06	0A	04 00 7F 00 07 02 02 02 01 01	OID	id-TA-RSA-v1-5-SHA-1
81	80	9F 7E F6 8E ... ... 5D AF CF B9	UNSIGNED INTEGER	Prime modulus
82	03	01 00 01	UNSIGNED INTEGER	First coefficient
5F 20	0D	44 45 54 45 53 54 41 54 44 45 30 31 39	CHARACTER STRING	Certificate Holder Reference DETESTATDE019
7F 4C	12		SEQUENCE	Certificate Holder Authorization Template
06	09	04 00 7F 00 07 03 01 02 02	OID	id-AT
53	05	00 00 00 01 10	OCTET STRING	Discretionary Data (AT with read access for DG1)
5F 25	06	01 00 00 03 02 04	DATE	Certificate Effective Date
5F 24	06	01 00 00 04 02 04	DATE	Certificate

					Expiration Date

Certification information:

Authority Reference:	44 45 54 45 53 54 44 56 44 45 30 31 39 (DETESTDVDE019)
Public Key:	0.4.0.127.0.7.2.2.2.1.1 (RSA v1.5 with SHA-1) Prime modulus: 0000 9F 7E F6 8E 15 3D B4 FD 10 84 DD ED BE AE 84 2C 0010 55 6D 41 9F CB 5E F6 21 AA 37 51 F0 FC 0C FD 71 0020 4F C0 E7 68 86 6B 3F 44 E2 72 5A F0 35 1A 97 ED 0030 B1 BA 88 DF DD 9B 4D 81 D4 08 FE 07 63 34 6A 77 0040 2C F6 46 16 46 5C 8F D9 71 B7 75 D2 E1 34 26 C5 0050 BC 11 89 47 95 C5 AD 2C 3E 42 68 37 F3 A1 01 9F 0060 E9 51 24 EA 5D 43 3E 90 6D 79 93 49 63 21 EF CB 0070 DB C3 2D 93 C0 68 0B 45 F3 B8 F6 4A 5D AF CF B9 Public exponent e: 01 00 01
Certificate Holder Reference:	44 45 54 45 53 54 41 54 44 45 30 31 39 (DETESTATDE019)
Certificate Holder Authorization:	OID: 0.4.0.127.0.7.3.1.2.2 (Authentication Terminal) Discretionary Data: 00 00 00 01 10 Role: AT Access Rights: CAN allowed Read Access(eID) DG1
Effective Date:	01 00 00 03 02 04 (2010.03.24)
Expiration Date:	01 00 00 04 02 04 (2010.04.24)

Passwords

In this example the following passwords are used:

CAN	500540
PIN	123456
MRZ	TPD<<T220001293<<<<<<<<<<<<<<

	6408125<1010318D<<<<<<<<<<<<<6 MUSTERMANN<<ERIKA<<<<<<<<<<<<<

6.2 CHAT

The following CHAT is used in this worked example:

CHAT	0000 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 .....S.... 0010 01 10 ..

Tag	*Length*	*Value*	*ASN1.Type*	*Comment*
06	09	04 00 7F 00 07 03 01 02 02	OID	id-AT OBJECT IDENTIFIER Authentication Terminal
53	05	00 00 00 01 10	OCTET STRING	Discretionary Data Access rights: • Read Access DG1 • CAN allowed

7. PACE Example (DH/RSA)

In this chapter the protocol PACE is described. PACE establishes Secure Messaging between an MRTD chip and a terminal based on weak (short) passwords. PACE is an alternative to Basic Access Control, i.e. it enables the MRTD chip to verify that the terminal is authorized to access stored less-sensitive data. At the beginning the file EF.CardAccess must be read by the terminal. This file is defined as followed:

```
SET SIZE( 198 )
  SEQUENCE SIZE( 13 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 2 }
    INTEGER SIZE( 1 )
      0000  02                                                .
  SEQUENCE SIZE( 18 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 3 1 2 }
    INTEGER SIZE( 1 )
      0000  02                                                .
    INTEGER SIZE( 1 )
      0000  01                                                .
  SEQUENCE SIZE( 18 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 4 1 2 }
    INTEGER SIZE( 1 )
      0000  02                                                .
    INTEGER SIZE( 1 )
      0000  00                                                .
  SEQUENCE SIZE( 28 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 3 1 }
    SEQUENCE SIZE( 12 )
      OBJECT IDENTIFIER = { 0 4 0 127 0 7 1 2 }
      INTEGER SIZE( 1 )
        0000  00                                                .
    INTEGER SIZE( 1 )
      0000  01                                                .
  SEQUENCE SIZE( 47 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 6 }
    IA5-STRING SIZE( 35 )
      0000  68 74 74 70 73 3A 2F 2F 77 77 77 2E 68 6A 70 2D  https://www.hjp-
      0010  63 6F 6E 73 75 6C 74 69 6E 67 2E 63 6F 6D 2F 68  consulting.com/h
      0020  6F 6D 65                                        ome
  SEQUENCE SIZE( 62 )
    OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 8 }
    SET SIZE( 50 )
      SEQUENCE SIZE( 18 )
        OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 3 1 2 }
        INTEGER SIZE( 1 )
          0000  02                                                .
        INTEGER SIZE( 1 )
          0000  02                                                .
      SEQUENCE SIZE( 28 )
        OBJECT IDENTIFIER = { 0 4 0 127 0 7 2 2 3 1 }
        SEQUENCE SIZE( 12 )
          OBJECT IDENTIFIER = { 0 4 0 127 0 7 1 2 }
          INTEGER SIZE( 1 )
            0000  00                                                .
        INTEGER SIZE( 1 )
          0000  02                                                .
```

The content of EF.CardAccess is described in the following table:

Tag	*Length*	*Value*	*ASN1.Type*	*Comment*
31	81 C6		SET	
30	0D		SEQUENCE	
06	08	04 00 7F 00 07 02 02 02	OID	id-TA OBJECT IDENTIFIER TerminalAuthenticationInfo
02	01	02	INTEGER	Version of protocol
30	12		SEQUENCE	
06	0A	04 00 7F 00 07 02 02 03 01 02	OID	id-CA-DH-AES-CBC-CMAC-128 ChipAuthenticationInfo
02	01	02	INTEGER	Version
02	01	01	INTEGER	keyId
30	12		SEQUENCE	
06	0A	04 00 7F 00 07 02 02 04 01 02	OID	id-PACE-DH-GM-AES-CBC-CMAC-128 PACEInfo
02	01	02	INTEGER	Version
02	01	00	INTEGER	parameterID
30	1C		SEQUENCE	
06	09	04 00 7F 00 07 02 02 03 01	OID	id-CA-DH
30	0C		SEQUENCE	
06	07	04 00 7F 00 07 01 02	OID	OID_StandaradizedDomainParameters
02	01	00	INTEGER	parameterID
02	01	01	INTEGER	keyId
30	2F		SEQUENCE	

06	08	04 00 7F 00 07 02 02 06			OID	id-CI OBJECT IDENTIFIER
		16 23 68 74 74 70 73 3A 2F 2F 77 77 77 2E 68 6A 70 2D 63 6F 6E 73 75 6C 74 69 6E 67 2E 63 6F 6D 2F 68 6F 6D 65			-	
30	3E			SEQUENCE		
06	08	04 00 7F 00 07 02 02 08			OID	id-PT
31	32				SET	
30	12			SEQUENCE		
06	0A	04 00 7F 00 07 02 02 03 01 02			OID	id-CA-DH-AES-CBC-CMAC-128
02	01	02			INTEGER	Version
02	01	02			INTEGER	keyId
30	1C			SEQUENCE		
06	09	04 00 7F 00 07 02 02 03 01			OID	id-CA-DH
30	0C			SEQUENCE		
06	07	04 00 7F 00 07 01 02			OID	OID_StandaradizedDomainParameters
02	01	00			INTEGER	parameterID
02	01	02			INTEGER	keyId

The relevant information for PACE are:

Version	02
Algorithm Identifier (parameterID)	00 (1024-bit MODP Group with 160-bit Prime Order Subgroup specified by [RFC5114])
PACE Info OID	0.4.0.127.0.7.2.2.4.1.2

	(PACE-DH-GM-AES-CBC-CMAC128)

First key derived from PIN (K_π)	59 14 68 CD A8 3D 65 21 9C CC B8 56 02 33 60 0F

7.1 Command MSE:Set AT

To initialize PACE the terminal sends the following command MSE:Set AT to the chip.

T→C	0000 00 22 C1 A4 27 80 0A 04 00 7F 00 07 02 02 04 01 ."..'..... 0010 02 83 01 03 7F 4C 12 06 09 04 00 7F 00 07 03 01 .....L..... 0020 02 02 53 05 00 00 00 01 10 84 01 00 ..S.....
C→T	0000 90 00

Here T→C is an abbreviation for an APDU sent from terminal (T or PCD) to chip (C or PICC) while C→T denotes the corresponding response sent by the chip to the terminal. The encoding of the command is explained in the next table.

C-APDU				
CLA	00		Plain	
INS	22		Manage Security Environment	
P1/P2	C1 A4		Set Authentication Template for Mutual Authentication	
L_c	27		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	80	0A	04 00 7F 00 07 02 02 04 01 02	Cryptographic mechanism: PACE with DH, generic mapping and AES 128 session keys
	83	01	03	Password: PIN
	7F 4C	12	06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 01 10	Certificate Holder Authorization Template (CHAT)
	84	01	00	Reference of domain parameters

R-APDU		
SW	90 00	Normal operation

7.2 Command Get Nonce

The chip randomly generates a nonce s and encrypts it with the key K_π

Nonce decrypted (s)	`0000  FA 5B 7E 3E 49 75 3A 0D B9 17 8B 7B 9B D8 98 C8  .[~>Iu:....{....`
Nonce encrypted (z)	`0000  9A BB 88 64 CA 0F F1 55 1E 62 0D 1E F4 E1 35 10  ...d...U.b....5.`

The encrypted nonce is queried by the terminal:

T→C	`0000  10 86 00 00 02 7C 00 00                          .....|..`
C→T	`0000  7C 12 80 10 9A BB 88 64 CA 0F F1 55 1E 62 0D 1E  |......d...U.b..` `0010  F4 E1 35 10 90 00                                  ..5.`

C-APDU				
CLA	`10`		Plain, Command Chaining	
INS	`86`		General Authenticate	
P1/P2	`00 00`		Keys and protocol implicitly known	
L_c	`02`		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	`7C`	`00`	–	-
L_e	`00`			Expected maximal byte length of the response data field

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***
	`7C`	`12`		Dynamic Authentication Data
	`80`	`10`	`9A BB 88 64 CA 0F F1 55 1E 62 0D 1E F4 E1 35 10`	Encrypted Nonce
SW	`90 00`		Normal operation	

7.3 Command Map Nonce

The nonce is mapped to an ephemeral group generator via generic mapping. The required randomly chosen ephemeral keys are also collected in the next table.

PCD Private Key $\widetilde{SK}_{PCD}$	0000 24 C3 C0 E0 A3 28 0E CB 94 33 45 D9 DC 2A 7B 72 $....(...3E..*{r 0010 53 9F DA 6F FD F9 9A B7 B6 CD DD D1 BE 42 5A F3 S..o.........BZ. 0020 D0 2C 4E D0 CD D7 3E BB 4B 2E DF 8C 07 FB 3A 35 .,N...>.K.....:5 0030 90 3F 72 B8 4F 37 71 F4 EB FB 49 52 0D 61 A8 F7 .?r.O7q...IR.a.. 0040 C7 FB 8C 9E 2A BC 24 BF 4F F9 D8 DD F3 81 A1 93 ....*.$.O....... 0050 80 C8 5B 62 3A B0 2A CB F6 D2 20 F5 12 BF 40 65 ..[b:.*... ...@e 0060 83 22 AD 20 9A C0 BF 9E 6F 8D B6 02 D5 19 7D 25 ." .....o.....}% 0070 2B F6 D1 48 51 0C A1 B7 40 AF 0F 99 F3 3C A5 F1 +..HQ...@....<..
PCD Public Key $\widetilde{PK}_{PCD}$	0000 23 FB 37 49 EA 03 0D 2A 25 B2 78 D2 A5 62 04 7A #.7I...*%.x..b.z 0010 DE 3F 01 B7 4F 17 A1 54 02 CB 73 52 CA 7D 2B 3E .?..O..T..sR.}+> 0020 B7 1C 34 3D B1 3D 1D EB CE 9A 36 66 DB CF C9 20 ..4=.=....6f... 0030 B4 91 74 A6 02 CB 47 96 5C AA 73 DC 70 24 89 A4 ..t...G.\.s.p$.. 0040 4D 41 DB 91 4D E9 61 3D C5 E9 8C 94 16 05 51 C0 MA..M.a=......Q. 0050 DF 86 27 4B 93 59 BC 04 90 D0 1B 03 AD 54 02 2D ..'K.Y.......T.- 0060 CB 4F 57 FA D6 32 24 97 D7 A1 E2 8D 46 71 0F 46 .OW..2$.....Fq.F 0070 1A FE 71 0F BB BC 5F 8B A1 66 F4 31 19 75 EC 6C ..q..._..f.1.u.l
PICC Private Key $\widetilde{SK}_{PICC}$	0000 4E C0 25 E4 0C 6D 10 B2 AA F6 FC AC 98 C4 24 4F N.%..m........$O 0010 57 48 1A 49 61 F3 AD C3 72 A9 5E 40 E0 CC 35 55 WH.Ia...r.^@..5U 0020 F7 3C CF C6 5E 9D B9 56 DD 61 B1 43 E0 C7 DC 51 .<..^..V.a.C...Q 0030 9E 7D D8 ED D8 E3 E4 6A 09 4C F2 26 4F D1 93 D0 .}.....j.L.&O... 0040 BC 4B C0 5C DE 6C A4 43 19 C2 43 9F D0 4A 46 44 .K.\.l.C..C..JFD 0050 3C 8D 04 94 48 7F 6F 2F E9 AC 8B E9 B9 EE 16 A3 <...H.o/........ 0060 D2 42 66 8C BA 4F FD 42 EE AC 36 50 9E 16 B4 D1 .Bf..O.B..6P.... 0070 E6 E8 EE 00 25 FF 82 44 B1 90 F5 7D 44 1E C3 28 ....%..D...}D..(
PICC Public Key $\widetilde{PK}_{PICC}$	0000 78 87 9F 57 22 5A A8 08 0D 52 ED 0F C8 90 A4 B2 x..W"Z...R...... 0010 53 36 F6 99 AA 89 A2 D3 A1 89 65 4A F7 07 29 E6 S6........eJ..). 0020 23 EA 57 38 B2 63 81 E4 DA 19 E0 04 70 6F AC E7 #.W8.c......po.. 0030 B2 35 C2 DB F2 F3 87 48 31 2F 3C 98 C2 DD 48 82 .5.....H1/<...H. 0040 A4 19 47 B3 24 AA 12 59 AC 22 57 9D B9 3F 70 85 ..G.$..Y."W..?p. 0050 65 5A F3 08 89 DB B8 45 D9 E6 78 3F E4 2C 9F 24 eZ.....E..x?.,.$ 0060 49 40 03 06 25 4C 8A E8 EE 9D D8 12 A8 04 C0 B6 I@..%L.......... 0070 6E 8C AF C1 4F 84 D8 25 89 50 A9 1B 44 12 6E E6 n...O..%.P..D.n.
Shared Secret H	0010 5B AB EB EF 5B 74 E5 BA 94 B5 C0 63 FD A1 5F 1F [...[t.....c.._. 0020 1C DE 94 87 3E E0 A5 D3 A2 FC AB 49 F2 58 D0 7F ....>......I.X.. 0030 54 4F 13 CB 66 65 8C 3A FE E9 E7 27 38 9B E3 F6 TO..fe.:...'8... 0040 CB BB D3 21 28 A8 C2 1D D6 EE A3 CF 70 91 CD DF ...!(.......p... 0050 B0 8B 8D 00 7D 40 31 8D CC A4 FF BF 51 20 87 90 ....}@1.....Q .. 0060 FB 4B D1 11 E5 A9 68 ED 6B 6F 08 B2 6C A8 7C 41 .K....h.ko..l.|A 0070 0B 3C E0 C3 10 CE 10 4E AB D1 66 29 AA 48 62 0C .<.....N..f).Hb. 0080 12 79 27 0C B0 75 0C 0D 37 C5 7F FF E3 02 AE 7F .y'..u..7.......
Mapped generator $\tilde{G}$	0000 7C 9C BF E9 8F 9F BD DA 8D 14 35 06 FA 7D 93 06 |.........5..}.. 0010 F4 CB 17 E3 C7 17 07 AF F5 E1 C1 A1 23 70 24 96 ....#p$. 0020 84 D6 4E E3 7A F4 4B 8D BD 9D 45 BF 60 23 91 9C ..N.z.K...E.`#.. 0030 BA A0 27 AB 97 AC C7 71 66 6C 8E 98 FF 48 33 01 ..'....qfl...H3. 0040 BF A4 87 2D ED E9 03 4E DF AC B7 08 14 16 6B 7F ...-...N......k.

```
0050  36 06 76 82 9B 82 6B EA 57 29 1B 5A D6 9F BC 84  6.v...k.W).Z....
0060  EF 1E 77 90 32 A3 05 80 3F 74 34 17 93 E8 69 74  ..w.2...?t4...it
0070  2D 40 13 25 B3 7E E8 56 5F FC DE E6 18 34 2D C5  -@.%.~.V_....4-.
```

The following APDUs are exchanged by terminal and chip to map the nonce.

T→C

```
0000  10 86 00 00 86 7C 81 83 81 81 80 23 FB 37 49 EA  .....|.....#.7I.
0010  03 0D 2A 25 B2 78 D2 A5 62 04 7A DE 3F 01 B7 4F  ..*%.x..b.z.?..O
0020  17 A1 54 02 CB 73 52 CA 7D 2B 3E B7 1C 34 3D B1  ..T..sR.}+>..4=.
0030  3D 1D EB CE 9A 36 66 DB CF C9 20 B4 91 74 A6 02  =....6f... ..t..
0040  CB 47 96 5C AA 73 DC 70 24 89 A4 4D 41 DB 91 4D  .G.\.s.p$..MA..M
0050  E9 61 3D C5 E9 8C 94 16 05 51 C0 DF 86 27 4B 93  .a=......Q...'K.
0060  59 BC 04 90 D0 1B 03 AD 54 02 2D CB 4F 57 FA D6  Y.......T.-.OW..
0070  32 24 97 D7 A1 E2 8D 46 71 0F 46 1A FE 71 0F BB  2$.....Fq.F..q..
0080  BC 5F 8B A1 66 F4 31 19 75 EC 6C 00              ._..f.1.u.l.
```

C→T

```
0000  7C 81 83 82 81 80 78 87 9F 57 22 5A A8 08 0D 52  |.....x..W"Z...R
0010  ED 0F C8 90 A4 B2 53 36 F6 99 AA 89 A2 D3 A1 89  ......S6........
0020  65 4A F7 07 29 E6 23 EA 57 38 B2 63 81 E4 DA 19  eJ..).#.W8.c....
0030  E0 04 70 6F AC E7 B2 35 C2 DB F2 F3 87 48 31 2F  ..po...5.....H1/
0040  3C 98 C2 DD 48 82 A4 19 47 B3 24 AA 12 59 AC 22  <...H...G.$..Y."
0050  57 9D B9 3F 70 85 65 5A F3 08 89 DB B8 45 D9 E6  W..?p.eZ.....E..
0060  78 3F E4 2C 9F 24 49 40 03 06 25 4C 8A E8 EE 9D  x?.,.$I@..%L....
0070  D8 12 A8 04 C0 B6 6E 8C AF C1 4F 84 D8 25 89 50  ......n...O..%.P
0080  A9 1B 44 12 6E E6 90 00                          ..D.n...
```

C-APDU				
CLA	10		Plain, Command Chaining	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	86		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	81 83	–	Dynamic Authentication Data
	81	81 80		Mapping Data
			23 FB 37 49 EA 03 0D 2A 25 B2 78 D2 … … BC 5F 8B A1 66 F4 31 19 75 EC 6C	
L_e	00			Expected maximal byte length of the response data field

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	81 83		Dynamic Authentication Data
	82	81 80		Mapping data
			ED 0F C8 90 A4 B2 53 36 F6 99 AA 89 … … 4F 84 D8 25 89 50 A9 1B 44 12 6E E6	
SW	90 00		Normal operation	

7.4 Command Perform Key Agreement

In the third step chip and terminal perform an anonymous DH key agreement using the new domain parameters determined by the ephemeral group generator $\tilde{G}$ of the previous step.

PCD Private Key (SK_{PCD})	0000 4B D0 E5 47 40 F9 A0 28 E6 A5 15 BF DA F9 67 84 K..G@..(.....g. 0010 8C 4F 5F 5F FF 65 AA 09 15 94 7F FD 1A 0D F2 FA .O__.e.......... 0020 69 81 27 1B C9 05 F3 55 14 57 B7 E0 3A C3 B8 06 i.'....U.W..:... 0030 6D E4 AA 40 6C 11 71 FB 43 DD 93 9C 4B A1 61 75 m..@l.q.C...K.au 0040 10 3B A3 DE E1 64 19 AA 24 81 18 F9 0C C3 6A 3D .;...d..$.....j= 0050 6F 4C 37 36 52 E0 C3 CC E7 F0 F1 D0 C5 42 5B 36 oL76R........B[6 0060 00 F0 F0 D6 A6 7F 00 4C 8B BA 33 F2 B4 73 3C 72 ....L..3..s<r 0070 52 44 5C 1D FC 4F 11 07 20 3F 71 D2 EF B2 81 61 RD\..O.. ?q....a
PCD Public Key (PK_{PCD})	0000 00 90 7D 89 E2 D4 25 A1 78 AA 81 AF 4A 77 74 EC ..}...%.x...Jwt. 0010 8E 38 8C 11 5C AE 67 03 1E 85 EE CE 52 0B D9 11 .8..\.g.....R... 0020 55 1B 9A E4 D0 43 69 F2 9A 02 62 6C 86 FB C6 74 U....Ci...bl...t 0030 7C C7 BC 35 26 45 B6 16 1A 2A 42 D4 4E DA 80 A0 |..5&E...*B.N... 0040 8F A8 D6 1B 76 D3 A1 54 AD 8A 5A 51 78 6B 0B C0 ....v..T..ZQxk.. 0050 71 47 05 78 71 A9 22 21 2C 5F 67 F4 31 73 17 22 qG.xq."!,_g.1s." 0060 36 B7 74 7D 16 71 E6 D6 92 A3 C7 D4 0A 0C 3C 5C 6.t}.q........<\ 0070 E3 97 54 5D 01 5C 17 5E B5 13 05 51 ED BC 2E E5 ..T].\.^...Q.... 0080 D4 .
PICC Private Key (SK_{PICC})	0000 02 0F 01 8C 72 84 B0 47 FA 77 21 A3 37 EF B7 AC ....r..G.w!.7... 0010 B1 44 0B B3 0C 52 52 BD 41 C9 7C 30 C9 94 BB 78 .D...RR.A.|0...x 0020 E9 F0 C5 B3 27 44 D8 40 17 D2 1F FA 68 78 39 6A ....'D.@....hx9j 0030 64 69 CA 28 3E F5 C0 00 DA F7 D2 61 A3 9A B8 86 di.(>......a.... 0040 0E D4 61 0A B5 34 33 90 89 7A AB 5A 77 87 E4 FA ..a..43..z.Zw... 0050 EF A0 64 9C 6A 94 FD F8 2D 99 1E 8E 3F C3 32 F5 ..d.j...-...?.2. 0060 14 27 29 E7 04 0A 3F 7D 5A 4D 3C D7 5C BE E1 F0 .')...?}ZM<.\... 0070 43 C1 CA D2 DD 48 4F EB 4E D2 2B 59 7D 36 68 8E C....HO.N.+Y}6h.

PICC Public Key (PK_{PICC})	0000 07 56 93 D9 AE 94 18 77 57 3E 63 4B 6E 64 4F 8E .V.....wW>cKndO. 0010 60 AF 17 A0 07 6B 8B 12 3D 92 01 07 4D 36 15 2B `....k..=...M6.+ 0020 D8 B3 A2 13 F5 38 20 C4 2A DC 79 AB 5D 0A EE C3 .....8 .*.y.]... 0030 AE FB 91 39 4D A4 76 BD 97 B9 B1 4D 0A 65 C1 FC ...9M.v....M.e.. 0040 71 A0 E0 19 CB 08 AF 55 E1 F7 29 00 5F BA 7E 3F q......U..)._.~? 0050 A5 DC 41 89 92 38 A2 50 76 7A 6D 46 DB 97 40 64 ..A..8.PvzmF..@d 0060 38 6C D4 56 74 35 85 F8 E5 D9 0C C8 B4 00 4B 1F 8l.Vt5.....K. 0070 6D 86 6C 79 CE 05 84 E4 96 87 FF 61 BC 29 AE A1 m.ly.....a.)..
Shared Secret K	0000 6B AB C7 B3 A7 2B CD 7E A3 85 E4 C6 2D B2 62 5B k....+.~....-.b[0010 D8 61 3B 24 14 9E 14 6A 62 93 11 C4 CA 66 98 E3 .a;$...jb....f.. 0020 8B 83 4B 6A 9E 9C D7 18 4B A8 83 4A FF 50 43 D4 ..Kj....K..J.PC. 0030 36 95 0C 4C 1E 78 32 36 7C 10 CB 8C 31 4D 40 E5 6..L.x26|...1M@. 0040 99 0B 0D F7 01 3E 64 B4 54 9E 22 70 92 3D 06 F0 .....>d.T."p.=.. 0050 8C FF 6B D3 E9 77 DD E6 AB E4 C3 1D 55 C0 FA 2E ..k..w......U... 0060 46 5E 55 3E 77 BD F7 5E 31 93 D3 83 4F C2 6E 8E F^U>w..^1...O.n. 0070 B1 EE 2F A1 E4 FC 97 C1 8C 3F 6C FF FE 26 07 FD ../......?l..&..

The key agreement is performed as following.

T→C	0000 10 86 00 00 86 7C 81 83 83 81 80 90 7D 89 E2 D4 .....|.....}... 0010 25 A1 78 AA 81 AF 4A 77 74 EC 8E 38 8C 11 5C AE %.x...Jwt..8..\. 0020 67 03 1E 85 EE CE 52 0B D9 11 55 1B 9A E4 D0 43 g.....R...U....C 0030 69 F2 9A 02 62 6C 86 FB C6 74 7C C7 BC 35 26 45 i...bl...t|..5&E 0040 B6 16 1A 2A 42 D4 4E DA 80 A0 8F A8 D6 1B 76 D3 ...*B.N.......v. 0050 A1 54 AD 8A 5A 51 78 6B 0B C0 71 47 05 78 71 A9 .T..ZQxk..qG.xq. 0060 22 21 2C 5F 67 F4 31 73 17 22 36 B7 74 7D 16 71 "!,_g.1s."6.t}.q 0070 E6 D6 92 A3 C7 D4 0A 0C 3C 5C E3 97 54 5D 01 5C ....<\..T].\ 0080 17 5E B5 13 05 51 ED BC 2E E5 D4 00 .^...Q......
C→T	0000 7C 81 83 84 81 80 07 56 93 D9 AE 94 18 77 57 3E |......V.....wW> 0010 63 4B 6E 64 4F 8E 60 AF 17 A0 07 6B 8B 12 3D 92 cKndO.`....k..=. 0020 01 07 4D 36 15 2B D8 B3 A2 13 F5 38 20 C4 2A DC ..M6.+.....8 .*. 0030 79 AB 5D 0A EE C3 AE FB 91 39 4D A4 76 BD 97 B9 y.]......9M.v... 0040 B1 4D 0A 65 C1 FC 71 A0 E0 19 CB 08 AF 55 E1 F7 .M.e..q......U.. 0050 29 00 5F BA 7E 3F A5 DC 41 89 92 38 A2 50 76 7A)._.~?..A..8.Pvz 0060 6D 46 DB 97 40 64 38 6C D4 56 74 35 85 F8 E5 D9 mF..@d8l.Vt5.... 0070 0C C8 B4 00 4B 1F 6D 86 6C 79 CE 05 84 E4 96 87 ....K.m.ly...... 0080 FF 61 BC 29 AE A1 90 00 .a.)..

C-APDU		
CLA	10	Plain, Command Chaining
INS	86	General Authenticate
P1/P2	00 00	Keys and protocol implicitly known

L_c	86		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	81 83	-	Dynamic Authentication Data
	83	81 80		Terminal's Ephemeral Public Key
			90 7D 89 E2 D4 25 A1 78 AA 81 AF 4A 77 … … 17 5E B5 13 05 51 ED BC 2E E5 D4	
L_e	00			Expected maximal byte length of the response data field

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	81 83		Dynamic Authentication Data
	84	81 80		Chip's Ephemeral Public Key
			07 56 93 D9 AE 94 18 77 57 3E 63 4B … … CE 05 84 E4 96 87 FF 61 BC 29 AE A1	
SW	90 00		Normal operation	

By means of the KDF specified in [TR-03110] the AES 128 session keys are derived from the shared secret as following.

K_{Enc}	0000 2F 7F 46 AD CC 9E 7E 52 1B 45 D1 92 FA FA 91 26 /.F...~R.E.....&
K_{Mac}	0000 80 5A 1D 27 D4 5A 51 16 F7 3C 54 46 94 62 B7 D8 .Z.'.ZQ..<TF.b..

7.5 Command Mutual Authentication

The authentication token is constructed by OID and public key on both sides, PICC and PCD.

Construction of input data for Authentication Token T_{PCD}

Tag	***Length***	***Value***	***ASN1.Type***	***Comment***
7F 49	81 8F		PUBLIC KEY	Input data for PCD

				Authentication Token
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER	PACE with DH, generic mapping and AES 128 session keys
84	81 80		UNSIGNED INTEGER	Chip's ephemeral public key
		07 56 93 D9 AE 94 18 77 57 3E 63 4B … … CE 05 84 E4 96 87 FF 61 BC 29 AE A1		

Construction of input data for Authentication Token T_{PICC}

Tag	*Length*	*Value*	*ASN1.Type*	*Comment*
7F 49	81 8F		CONTRUCTED TLV	Input data for PICC Authentication Token
06	0A	04 00 7F 00 07 02 02 04 01 02	OBJECT IDENTIFIER	PACE with DH, generic mapping and AES 128 session keys
84	81 80		UNSIGNED INTEGER	Terminal's ephemeral public key
		90 7D 89 E2 D4 25 A1 78 AA 81 AF 4A 77 … … 5C 17 5E B5 13 05 51 ED BC 2E E5 D4		

Computed Authentication Tokens

T_{PICC}	0000 91 7F 37 B5 C0 E6 D8 D1 ..7.....
T_{PCD}	0000 B4 6D D9 BD 4D 98 38 1F .m..M.8.

Finally these tokens are exchanged and verified.

T→C	0000 00 86 00 00 0C 7C 0A 85 08 B4 6D D9 BD 4D 98 38 .....|....m..M.8 0010 1F 00 ..
C→T	0000 7C 1B 86 08 91 7F 37 B5 C0 E6 D8 D1 87 0F 44 45 |.....7.......DE 0010 54 45 53 54 43 56 43 41 30 30 30 30 33 TESTCVCA00003

C-APDU				
CLA	00		Plain	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	0C		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	0A	–	Dynamic Authentication Data
	85	08	B4 6D D9 BD 4D 98 38 1F	Terminal's Authentication Token MAC
L_e	00			Expected maximal byte length of the response data field

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	1B		Dynamic Authentication Data
	86	08	91 7F 37 B5 C0 E6 D8 D1	Chip's Authentication Token MAC
	87	0F	44 45 54 45 53 54 43 56 43 41 30 30 30 30 33	Certification Authority Reference (CAR)
SW	90 00		Normal operation	

With this successfully exchange and comparison a secure channel based on PACE has been established.

8. Terminal Authentication Example (DH/RSA)

Terminal Authentication enables the chip to verify that the terminal is entitled to access sensitive data.

8.1 Command MSE: Set DST

The command MSE:Set DST is used to send the CAR from the terminal to the chip. The CAR is delivered by PACE before (see 7.5).

CAR	0000 44 45 41 54 43 56 43 41 30 30 30 30 33

The terminal sends a certificate chain to the chip. Until this point the communication is encrypted by Secure Messaging with the keys derived during PACE. The chain starts with a certificate verifiable with the CVCA public key stored on the chip as following.

T→C plain	0000 00 22 81 B6 11 83 0F 44 45 54 45 53 54 43 56 43 ."....DETESTCVC 0010 41 30 30 30 30 33 A00003
T→C coded	0000 0C 22 81 B6 2D 87 21 01 B3 7B B5 7D A1 DB 37 D1 ."..-.!..{.}..7. 0010 C4 96 04 91 7B D6 99 E6 1D 6A 30 74 E6 9E 40 67 ....{....j0t..@g 0020 A1 B3 99 03 88 23 36 33 8E 08 F3 65 26 DE 03 A3 .....#63...e&... 0030 1A 19 00 ...
C→T coded	0000 99 02 90 00 8E 08 EB FF 08 D3 B2 0A 04 14 .....
C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	22		Manage Security Environment	
P1/P2	81 B6		Set Digital Signature Template for verification	
L_c	0F		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	83	0F	44 45 54 45 53 54 43 56 43 41 30 30 30 30 33	Reference of a public key, CAR

R-APDU		
SW	90 00	Normal operation

8.2 Command PSO: Verify Certificate

The DV certificate is send to the chip by the terminal as following.

T→C plain

```
0000  00 2A 00 BE 00 01 6C 7F 4E 81 E4 5F 29 01 00 42  .*....l.N.._)..B
0010  0F 44 45 54 45 53 54 43 56 43 41 30 30 30 30 33  .DETESTCVCA00003
0020  7F 49 81 94 06 0A 04 00 7F 00 07 02 02 02 01 01  .I..............
0030  81 81 80 A0 8C 4D 11 D6 99 F4 25 B0 E7 43 BB A4  .....M....%..C..
0040  F2 19 6E 05 BC 9E F2 4F 53 A6 74 42 90 E6 55 6E  ..n....OS.tB..Un
0050  83 E9 05 77 A9 30 EC 31 4A 4F 9F 03 33 A0 A0 19  ...w.0.1JO..3...
0060  93 11 0E C6 34 86 DF 60 7F D7 B3 04 74 79 B0 EC  ....4..`....ty..
0070  09 04 AC F8 B6 26 5C D0 AB C3 53 8F 4D 72 39 5D  .....&\...S.Mr9]
0080  D5 F1 E7 A1 08 18 A7 FA A0 1D 25 FF 25 BC 6B F1  ..........%.%.k.
0090  9C E8 6A 20 82 33 C5 43 7F F9 90 FE 94 D1 C2 5D  ..j .3.C.......]
00A0  59 BE DB 6A E7 9E 4A 76 DE 22 79 FC D6 A5 A3 D6  Y..j..Jv."y.....
00B0  6F F5 F9 82 03 01 00 01 5F 20 0D 44 45 54 45 53  o......._ .DETES
00C0  54 44 56 44 45 30 31 39 7F 4C 12 06 09 04 00 7F  TDVDE019.L......
00D0  00 07 03 01 02 02 53 05 80 1F FF FF 10 5F 25 06  ......S......_%.
00E0  01 00 00 03 02 04 5F 24 06 01 00 00 04 02 04 5F  ......_$........_
00F0  37 81 80 6B 95 0F 1F A8 FE F8 61 EE A7 57 65 C2  7..k......a..We.
0100  80 5D 79 BB 5D 0D 60 87 8E 93 0A 8C 17 D3 F9 2D  .]y.].`........-
0110  CC 2B E9 54 7D 31 E4 12 6B 75 10 C3 59 27 E8 24  .+.T}1..ku..Y'.$
0120  BD 0C 64 DC 33 96 F5 39 2A AC F6 F6 49 9F 1D 88  ..d.3..9*...I...
0130  CA FA D9 4C A6 16 24 B6 63 7C 75 1B D0 35 FC 08  ...L..$.c|u..5..
0140  4B B8 9F 50 A9 00 EC C1 80 71 25 8B 31 6B DF 3A  K..P.....q%.1k.:
0150  F9 D6 10 92 A1 50 05 64 29 E0 2D 1A 70 DF C1 1E  .....P.d).-.p...
0160  77 D0 FB BA 00 CB 70 0A 63 20 98 05 96 8D BD 17  w.....p.c ......
0170  D3 6E 75                                        .nu
```

T→C coded

```
0000  0C 2A 00 BE 00 01 7F 87 82 01 71 01 49 98 87 ED  .*........q.I...
0010  98 77 65 40 A6 AE FC EA 4E 0F 58 E7 AB CB 3A 2D  .we@....N.X...:-
0020  0A C0 BC 22 46 87 24 3E B9 A0 63 EF 7E 37 09 70  ...."F.$>..c.~7.p
0030  10 16 BA ED FA 70 21 E0 C7 25 39 1E F0 76 B5 A3  .....p!..%9..v..
0040  75 AC BE 08 F5 8D 64 FC 6E B3 EE 9E FC B3 A1 59  u.....d.n......Y
0050  E3 FF 92 40 A9 30 03 C4 5A 65 D2 CB 3A BB 4A BD  ...@.0..Ze..:.J.
0060  18 CF A8 9A A1 7A A5 AA A3 68 E8 EE 36 67 E5 31  .....z...h..6g.1
0070  AB A9 78 0C 67 C1 39 0F FD 78 D5 ED 21 A4 AA 3B  ..x.g.9..x..!..;
0080  74 38 30 89 60 CC 58 06 84 59 C1 2C 00 46 A2 F9  t80.`.X..Y.,.F..
0090  2C AA 51 17 55 B3 57 E2 BB E0 10 F3 AA C2 0D C6  ,.Q.U.W.........
00A0  F2 FF 16 ED 88 9E E2 4A 30 95 C7 62 35 A2 37 F8  .......J0..b5.7.
00B0  A3 8B C5 2D EA B4 91 2F 8E 7D F1 EA 66 73 6C 6E  ...-.../.}..fsln
00C0  B8 89 98 EE 10 65 93 2F 01 94 AC 46 66 46 49 A2  .....e./...FfFI.
00D0  66 35 36 6F D0 3D 86 C6 40 1E 68 94 72 3F 36 92  f56o.=..@.h.r?6.
00E0  83 A5 F8 9E 0C FB 57 CA CF D4 32 88 6F 52 C4 FB  ......W...2.oR..
00F0  75 E5 9C 99 0E 96 FC 52 16 8F FD 20 E9 EA 15 04  u......R... ....
0100  30 FE 48 F2 FA 92 86 28 69 E6 30 EB 93 DC BD B8  0.H....(i.0.....
0110  A5 9F 44 27 44 55 11 F2 43 A3 47 6C 6E 66 87 4F  ..D'DU..C.Glnf.O
0120  2B A8 BF 9F 53 25 8C 0A 50 35 0F 70 A9 8F 3E FE  +...S%..P5.p..>.
0130  4E 47 4E 78 1D 9F E4 16 08 2E F6 73 C6 05 B4 A6  NGNx.......s....
0140  8D 2F 95 E0 48 0E 2E 4A 38 7A E6 5F 1D E1 5C 57  ./..H..J8z._..\W
0150  BC AA DC 4C 60 22 00 36 B7 05 71 00 01 78 C8 FE  ...L`".6..q..x..
```

	0160 93 2F E4 E7 54 DA D1 20 F7 93 F0 B7 D3 51 CD E5 ./..T.. .....Q.. 0170 15 B9 05 FC C8 B4 7A C1 98 ED 34 5E 8E 08 8E 15 ......z...4^.... 0180 06 3B 49 30 87 38 00 00 .;I0.8..
C→T coded	0000 99 02 90 00 8E 08 40 AF BE 48 2A 54 DC 94 ......@..H*T..
C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	2A		Perform Security Operation	
P1/P2	00 BE		Verify self-descriptive certificate	
L_c	00 01 6C		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7F 4E	81 E4	5F 29 01 00 42 0F 44 45 54 45 53 54 … … 03 02 04 5F 24 06 01 00 00 04 02 04	Certificate Body
	5F 37	81 80	6B 95 0F 1F A8 FE F8 61 EE A7 57 65 … … 0A 63 20 98 05 96 8D BD 17 D3 6E 75	Signature

R-APDU		
SW	90 00	Normal operation

8.3 Command MSE: Set DST

The following CAR of the DV certificate is used by the command MSE:Set DST.

CAR	0000 44 45 54 45 53 54 44 56 44 45 30 31 39

The reference of the public key (CAR) is send from the terminal to the chip as following.

T→C plain	0000 00 22 81 B6 0F 83 0D 44 45 54 45 53 54 44 56 44 ."".....DETESTDVD 0010 45 30 31 39 E019
T→C coded	0000 0C 22 81 B6 1D 87 11 01 6A B8 1B 7D 96 08 24 93 ."......j..}..$. 0010 AF 87 D2 C4 2F B2 8C 85 8E 08 DE CB F7 59 13 BC ..../........Y.. 0020 1A 76 00 .v.
C→T coded	0000 99 02 90 00 8E 08 C5 29 A8 ED 4B DC B9 96 ....)..K...
C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	22		Manage Security Environment	
P1/P2	81 B6		Set Digital Signature Template for verification	
L_c	0F		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	83	0D	44 45 54 45 53 54 44 56 44 45 30 31 39	Reference of a public key, CAR

R-APDU		
SW	90 00	Normal operation

8.4 Command PSO: Verify Certificate

The AT certificate is send to the chip by the terminal as following.

T→C plain	0000 00 2A 00 BE 00 01 6A 7F 4E 81 E2 5F 29 01 00 42 .*....j.N.._)..B 0010 0D 44 45 54 45 53 54 44 56 44 45 30 31 39 7F 49 .DETESTDVDE019.I 0020 81 94 06 0A 04 00 7F 00 07 02 02 02 01 01 81 81 .... 0030 80 9F 7E F6 8E 15 3D B4 FD 10 84 DD ED BE AE 84 ..~...=......... 0040 2C 55 6D 41 9F CB 5E F6 21 AA 37 51 F0 FC 0C FD ,UmA..^.!.7Q.... 0050 71 4F C0 E7 68 86 6B 3F 44 E2 72 5A F0 35 1A 97 qO..h.k?D.rZ.5.. 0060 ED B1 BA 88 DF DD 9B 4D 81 D4 08 FE 07 63 34 6A ....M.....c4j 0070 77 2C F6 46 16 46 5C 8F D9 71 B7 75 D2 E1 34 26 w,.F.F\..q.u..4& 0080 C5 BC 11 89 47 95 C5 AD 2C 3E 42 68 37 F3 A1 01 ....G...,>Bh7... 0090 9F E9 51 24 EA 5D 43 3E 90 6D 79 93 49 63 21 EF ..Q$.]C>.my.Ic!.

	00A0 CB DB C3 2D 93 C0 68 0B 45 F3 B8 F6 4A 5D AF CF ...-..h.E...J].. 00B0 B9 82 03 01 00 01 5F 20 0D 44 45 54 45 53 54 41 ....._ .DETESTA 00C0 54 44 45 30 31 39 7F 4C 12 06 09 04 00 7F 00 07 TDE019.L........ 00D0 03 01 02 02 53 05 00 00 00 01 10 5F 25 06 01 00 ....S....._%... 00E0 00 03 02 04 5F 24 06 01 00 00 04 02 04 5F 37 81 ...._$......._7. 00F0 80 8C B1 61 26 A1 FD BB 82 48 C8 8B DB 1F B1 19 ...a&....H...... 0100 9C 3F 25 38 56 FE 10 83 5F 7B FF 62 A3 0B D2 81 .?%8V..._{.b.... 0110 B8 A1 F0 FE 03 81 A5 B0 A4 26 51 F7 7D F7 21 52 ....&Q.}.!R 0120 21 F0 ED E4 88 E6 89 EA 45 CE E2 0B 19 C7 B1 D1 !.......E....... 0130 ED B6 AC 21 F3 40 88 81 9F 6F D5 DC 33 31 09 E1 ...!.@...o..31.. 0140 5A 15 DF F6 85 A2 B6 9D 17 D5 E2 3D AF E3 63 A8 Z..........=..c. 0150 E7 63 31 CC 25 B9 13 FB 6E D8 30 EB 45 7A D0 A6 .c1.%...n.0.Ez.. 0160 73 96 A1 90 CA E3 9C C6 C2 E4 67 1E 60 52 D3 C2 s.........g.`R.. 0170 2D -
T→C coded	0000 0C 2A 00 BE 00 01 7F 87 82 01 71 01 16 52 C1 F3 .*........q..R.. 0010 1A 4C E5 A7 E6 A5 B7 9D D4 18 E7 27 DA 11 6A FA .L.........'..j. 0020 3F 23 A7 7D 6C 9B 45 FB BD 1B FC E3 94 0B A5 D4 ?#.}l.E......... 0030 41 E4 50 A2 32 C8 85 B4 42 18 90 50 3E B6 AB E5 A.P.2...B..P>... 0040 4A EC B7 F8 A0 33 E2 D7 65 8B 83 AD 7A F5 A4 E6 J....3..e...z... 0050 A6 44 BE A1 A0 CE 8D 3D 4D E4 34 F2 E3 58 91 24 .D.....=M.4..X.$ 0060 BB 1C 3A F1 1C D1 8D 3F 32 75 A5 71 C9 61 AD 57 ..:....?2u.q.a.W 0070 ED 6F D6 F6 3E BD A9 95 E1 38 31 E6 4B 3C 09 63 .o..>....81.K<.c 0080 7F 5C 22 57 D1 AC 0D 7D D7 87 0D BD 65 44 70 52 .\"W...}....eDpR 0090 AC 90 50 2C 60 01 C0 75 69 F1 3C 5B CF D7 09 72 ..P,`..ui.<[...r 00A0 E7 A4 F8 19 4D 43 51 D0 4E 94 AF 0C 0B 14 5B 8C ....MCQ.N.....[. 00B0 AE 62 9E FC 4D 7E 92 48 89 A1 9E 6A 01 1F DA 27 .b..M~.H...j...' 00C0 CE AA ED 7E 2E E6 4C 96 53 E4 92 1C EE 4C 2E EB ...~..L.S....L.. 00D0 45 C3 59 90 50 CC 5D 57 1D 6C 90 E0 65 FD 34 DC E.Y.P.]W.l..e.4. 00E0 6D 9E A6 83 08 E1 7E D2 1F 4C E8 DB 24 D8 15 59 m.....~..L..$..Y 00F0 3F 73 39 B2 61 18 6B 75 98 9C 5B F2 C6 78 9D 1F ?s9.a.ku..[..x.. 0100 B6 AA 4B BB FA 3F D2 31 84 ED B8 2A 86 77 34 5C ..K..?.1...*.w4\ 0110 4B C3 B8 F6 2F BE 91 1E 5D 0D 47 0E 06 16 17 31 K.../...].G....1 0120 14 88 6C 92 31 6D D7 65 92 1C 67 EC 94 30 DD 55 ..l.1m.e..g..0.U 0130 50 A8 D0 EC 22 5E 2E 36 64 39 E4 24 E2 5D E0 F4 P..."^.6d9.$.].. 0140 9A 9B 9C 00 79 2F AE EF EA 32 56 51 70 64 BC E4 ....y/...2VQpd.. 0150 6C 23 44 05 B0 A6 52 E0 DD 09 A5 16 31 A7 B6 12 l#D...R.....1... 0160 05 61 5A F5 7A A3 42 5F C6 87 4A AB D4 E1 9B 2E .aZ.z.B_..J..... 0170 2E A2 21 BB 30 96 AF 66 86 28 C4 81 8E 08 EF 7E ..!.0..f.(.....~ 0180 FA 58 DA 6E D9 DD 00 00 .X.n....
C→T coded	0000 99 02 90 00 8E 08 B9 87 F8 19 0C DE 76 4D ....vM
C→T plain	0000 90 00

C-APDU		
CLA	00 / 0C	Plain, SM
INS	2A	Perform Security Operation

P1/P2	00 BE		Verify self-descriptive certificate	
L_c	00 01 6A		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7F 4E	81 E2	5F 29 01 00 42 0D 44 45 54 45 53 54 44 … … 03 02 04 5F 24 06 01 00 00 04 02 04	Certificate Body
	5F 37	81 80	8C B1 61 26 A1 FD BB 82 48 C8 8B DB … … E3 9C C6 C2 E4 67 1E 60 52 D3 C2 2D	Signature

R-APDU		
SW	90 00	Normal operation

8.5 Command MSE: Set AT

Extract the following relevant information from EF.CardAccess. In EF.CardAccess there are two key references for CA defined: 01 and 02. Both use 1024-bit MODP Group with 160-bit Prime Order Subgroup (00).

The terminal generates an ephemeral Diffie-Hellman key pair and sends the compressed ephemeral public key to the chip.

D_{PICC}	00
DH Ephemeral public key $\widetilde{PK}_{PCD}$	0000 A2 83 09 47 A6 FC AA CD E2 FC B8 8B 29 AB 38 E0 ...G........).8. 0010 7C 34 53 AB C4 BC B4 66 08 7E 11 C7 9F 32 A1 9E |4S....f.~...2.. 0020 6E F2 2B E1 08 F8 DD 18 FE 82 49 C9 60 95 15 11 n.+.......I.`... 0030 20 0D C9 85 AA 3E C0 CC AD 59 A5 F9 BB CC 33 EE ....>...Y....3. 0040 5F 15 77 E2 03 30 B4 DD 10 EB 06 B7 40 27 7C 97 _.w..0......@'|. 0050 A1 89 18 0E DE 52 BE E9 D4 29 F1 0F B7 7F 18 0F .....R...)..... 0060 05 D6 A9 9C 49 9C B5 E1 EC EE B8 E9 22 84 F6 6E ....I.......".n 0070 A9 84 79 67 4C E7 3F 53 C5 67 A0 3B 0D 29 78 33 ..ygL.?S.g.;.)x3
DH Ephemeral private key $\widetilde{SK}_{PCD}$	0000 00 A2 CF FD 06 C3 4A FD 62 2E EE 0F C3 1F 09 3F ......J.b......? 0010 DF DA 60 9C 67 12 1C AC F0 A8 F5 22 91 DE 68 53 ..`.g......"..hS 0020 BB 5C 93 CF 76 70 57 75 EC F4 08 A7 43 02 61 3B .\..vpWu....C.a; 0030 EE CB 38 14 47 D3 64 94 C9 E1 89 51 EC 17 25 2D ..8.G.d....Q..%- 0040 D2 A8 07 AA E0 9F A4 DC 30 18 33 39 01 3D 9C 91 ....0.39.=.. 0050 91 30 3C AC EE 3C 91 E9 26 A3 6D 01 4A 5C FA 94 .0<..<..&.m.J\.. 0060 95 0C AD B3 7B 53 4F 32 A9 BF 76 B3 79 80 97 93 ....{SO2..v.y... 0070 04 C5 66 38 71 BD 74 6E B9 E9 5A 47 CA 47 1B 4E ..f8q.tn..ZG.G.N

	0080 DE .
OID for TA	0.4.0.127.0.7.2.2.2.1.1
CHR	44 45 54 45 53 54 41 54 44 45 30 31 39

T→C plain	0000 00 22 81 A4 31 80 0A 04 00 7F 00 07 02 02 02 01 ."..1..... 0010 01 83 0D 44 45 54 45 53 54 41 54 44 45 30 31 39 ...DETESTATDE019 0020 91 14 7D F3 91 B1 78 B9 F8 F3 2B E6 C6 5A 3D BD ..}...x...+..Z=. 0030 92 F1 99 2B 9A 91 ...+..
T→C coded	0000 0C 22 81 A4 4D 87 41 01 82 F2 48 5E 89 27 74 D1 ."..M.A...H^.'t. 0010 39 69 E3 7A FB CF A4 D8 26 B9 6A 1C 72 22 2B A1 9i.z....&.j.r"+. 0020 B4 54 07 44 4B 6F 43 2A 3C A8 5F D9 0A 0D A8 47 .T.DKoC*<._....G 0030 B3 FC A5 58 3C DA 69 02 F6 70 CA DC BB 50 3D 8F ...X<.i..p...P=. 0040 AB 99 4C BC 20 BD C8 60 8E 08 B8 1B 6A 48 79 36 ..L. ..`....jHy6 0050 C6 45 00 .E.
C→T coded	0000 99 02 90 00 8E 08 4A 6E 55 2C 49 55 41 B4 ......JnU,IUA.
C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	22		Manage Security Environment	
P1/P2	81 A4		Terminal Authentication: Set Authentication Template for external authentication	
L_c	3D		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	80	0A	04 00 7F 00 07 02 02 02 01 01	Cryptograhic mechanism reference, OID
	83	0D	44 45 54 45 53 54 41 54 44 45 30 31 39	Reference of public key
	91	20	7D F3 91 B1 78 B9 F8 F3 2B E6 C6 5A 3D BD 92 F1 99 2B 9A 91	Ephemeral public key

R-APDU		
SW	90 00	Normal operation

8.6 Command Get Challenge

The chip is randomly chosing a r_{PICC} and this r_{PICC} is queried by the terminal.

r_{PICC}	FC 21 0C 17 4A 80 1D 46

T→C plain	0000 00 84 00 00 08
T→C coded	0000 0C 84 00 00 0D 97 01 08 8E 08 75 C3 F0 E1 9F 69 .....u....i 0010 82 77 00 .w.
C→T coded	0000 87 11 01 B8 17 44 2F B9 0F A6 8F 8C 9A 84 66 3F .....D/.....f? 0010 EE 72 CC 99 02 90 00 8E 08 0C 75 7A 99 98 DC 8C .r.....uz.... 0020 FE .
C→T plain	0000 FC 21 0C 17 4A 80 1D 46 .!..J..F

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	84		Get Challenge	
P1/P2	00 00		-	
L_e	08			8 byte length of the response expected

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***
			FC 21 0C 17 4A 80 1D 46	8 bytes of randomness
SW	90 00		Normal operation	

8.7 Command External Authenticate

The data to be signed is constructed of the key, the challenge and the hash. The resulting signature is used in the command EXTERNAL AUTHENTICATE. The defined algorithm here is RSA v1.5 with SHA-1.

Key (SK_{PCD})	0000 F4 87 4C 8A 06 8E 57 E7 32 0B 4B B7 13 68 59 CB ..L...W.2.K..hY. 0010 E3 AC 42 C9 ..B.
Challenge (r_{PICC})	0000 FC 21 0C 17 4A 80 1D 46 .!..J..F
Hash (ID_{PICC})	0000 7D F3 91 B1 78 B9 F8 F3 2B E6 C6 5A 3D BD 92 F1 }...x...+..Z=... 0010 99 2B 9A 91 .+..
Data to be signed	0000 F4 87 4C 8A 06 8E 57 E7 32 0B 4B B7 13 68 59 CB ..L...W.2.K..hY. 0010 E3 AC 42 C9 FC 21 0C 17 4A 80 1D 46 7D F3 91 B1 ..B..!..J..F}... 0020 78 B9 F8 F3 2B E6 C6 5A 3D BD 92 F1 99 2B 9A 91 x...+..Z=....+..

Signature (S_{PCD})	0000 37 C7 36 0C 55 57 9D E2 8A 41 DF 8A 1D 17 03 2C 7.6.UW...A....., 0010 4B 9F 90 DF 7F 64 6D F3 3F 77 EF 97 6A E4 C4 5C K....dm.?w..j..\ 0020 DB A3 77 63 99 64 8C 75 50 43 79 0F 0F 19 BF C1 ..wc.d.uPCy..... 0030 46 D0 53 B7 70 36 CA 9B 24 BF B4 B7 93 4F AC 04 F.S.p6..$....O.. 0040 26 71 E2 3B E6 E3 CA 2B 24 6C E2 06 6C 1F 05 50 &q.;...+$l..l..P 0050 38 34 18 19 2F 06 D6 AD 6C 0A CB 1E 70 BD EA D6 84../...l...p... 0060 0E A1 0B 31 E0 74 F4 9E 5E 8A EB 54 E6 F4 F8 3C ...1.t..^..T...< 0070 E9 98 95 79 53 F9 7F 87 00 58 01 3D 0E 74 5D 0A ...yS....X.=.t].

T→C plain	0000 00 82 00 00 80 37 C7 36 0C 55 57 9D E2 8A 41 DF .....7.6.UW...A. 0010 8A 1D 17 03 2C 4B 9F 90 DF 7F 64 6D F3 3F 77 EF ....,K....dm.?w. 0020 97 6A E4 C4 5C DB A3 77 63 99 64 8C 75 50 43 79 .j..\..wc.d.uPCy 0030 0F 0F 19 BF C1 46 D0 53 B7 70 36 CA 9B 24 BF B4 .....F.S.p6..$.. 0040 B7 93 4F AC 04 26 71 E2 3B E6 E3 CA 2B 24 6C E2 ..O..&q.;...+$l. 0050 06 6C 1F 05 50 38 34 18 19 2F 06 D6 AD 6C 0A CB .l..P84../...l.. 0060 1E 70 BD EA D6 0E A1 0B 31 E0 74 F4 9E 5E 8A EB .p......1.t..^.. 0070 54 E6 F4 F8 3C E9 98 95 79 53 F9 7F 87 00 58 01 T...<...yS....X. 0080 3D 0E 74 5D 0A =.t].
T→C coded	0000 0C 82 00 00 9E 87 81 91 01 58 7A 26 7C C4 61 BA ....Xz&|.a. 0010 73 BE 78 E3 F3 FB 07 A9 34 58 02 98 09 E6 B5 08 s.x.....4X...... 0020 5B 21 73 ED 84 F9 65 A4 C8 7E 3C CC 6C F8 C4 7A [!s...e..~<.l..z 0030 73 E9 7D 0C 11 2B A3 D1 24 F7 62 AD FB 67 94 F0 s.}..+..$.b..g.. 0040 BD D9 AA 38 EC 86 53 2B F8 3D 3E B8 AD 08 D2 06 ...8..S+.=>..... 0050 D6 B5 B1 B3 FA B7 95 2F 77 BE A4 29 B4 31 EA D5 ..../w..).1.. 0060 CD 12 6F 35 57 E6 F9 93 83 70 C9 53 F1 C1 CA 34 ..o5W....p.S...4 0070 DD 72 7A 64 18 E8 17 F3 37 99 32 A4 CB DA FA 80 .rzd....7.2..... 0080 F7 3F 8C 5D 25 90 82 88 54 B0 14 50 1C 4A 59 F6 .?.]%...T..P.JY. 0090 6A D2 3B A4 FE 00 D8 1B 0E 8E 08 74 A2 9F B8 49 j.;........t...I 00A0 B0 03 05 00 ....

C→T coded	0000 99 02 90 00 8E 08 85 1F AF F2 E1 5F 54 BA ...._T.
C→T plain	0000 90 00

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	82		External Authenticate	
P1/P2	00 00		Keys and algorithms implicitly known	
L_c	80		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
			37 C7 36 0C 55 57 9D E2 8A 41 DF 8A 1D … … 79 53 F9 7F 87 00 58 01 3D 0E 74 5D 0A	Signature generated by terminal

R-APDU		
SW	90 00	Normal operation

If the last command EXTERNAL AUTHENTICATE performs successfully the Terminal Authentication is established.

9. Chip Authentication Example (DH/RSA)

In this chapter the protocol Chip Authentication is described. Chip Authentication establishes Secure Messaging between a chip and a terminal based on a static key pair stored on the chip. Chip Authentication enables the terminal to verify that the chip is genuine. At first the file EF.CardSecurity must be read by the terminal. This file is defined as followed:

```
SEQUENCE SIZE( 2092 )
  OBJECT IDENTIFIER = { 1 2 840 113549 1 7 2 }
  A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 2077 )
    SEQUENCE SIZE( 2073 )
      INTEGER SIZE( 1 )
        0000  03                                                .
      SET SIZE( 15 )
        SEQUENCE SIZE( 13 )
          OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
          NULL SIZE( 0 )
      SEQUENCE SIZE( 402 )
        OBJECT IDENTIFIER = { 0 4 0 127 0 7 3 2 1 }
        A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 388 )
          OCTET-STRING SIZE( 384 )
            0000  31 82 01 7C 30 0D 06 08 04 00 7F 00 07 02 02 02  1..|0...........
            0010  02 01 02 30 12 06 0A 04 00 7F 00 07 02 02 03 01  ...0............
            0020  02 02 01 02 02 01 01 30 12 06 0A 04 00 7F 00 07  .......0........
            0030  02 02 04 01 02 02 01 02 02 01 00 30 1C 06 09 04  ...........0....
            0040  00 7F 00 07 02 02 03 01 30 0C 06 07 04 00 7F 00  ........0.......
            0050  07 01 02 02 01 00 02 01 01 30 2F 06 08 04 00 7F  .........0/.....
            0060  00 07 02 02 06 16 23 68 74 74 70 73 3A 2F 2F 77  ......#https://w
            0070  77 77 2E 68 6A 70 2D 63 6F 6E 73 75 6C 74 69 6E  ww.hjp-consultin
            0080  67 2E 63 6F 6D 2F 68 6F 6D 65 30 17 06 0A 04 00  g.com/home0.....
            0090  7F 00 07 02 02 05 01 03 30 09 02 01 01 02 01 01  ........0.......
            00A0  01 01 00 30 17 06 0A 04 00 7F 00 07 02 02 05 01  ...0............
            00B0  03 30 09 02 01 01 02 01 02 01 01 FF 30 19 06 09  .0..........0...
            00C0  04 00 7F 00 07 02 02 05 01 30 0C 06 07 04 00 7F  .........0......
            00D0  00 07 01 02 02 01 00 30 81 A6 06 09 04 00 7F 00  .......0........
            00E0  07 02 02 01 01 30 81 95 30 0C 06 07 04 00 7F 00  .....0..0.......
            00F0  07 01 02 02 01 00 03 81 84 00 02 81 80 1B 33 45  ..............3E
            0100  F8 DC 04 34 1B F8 B2 C9 7F 65 2F A6 80 E5 D4 FA  ...4.....e/.....
            0110  4C 14 6A E4 B8 39 43 1A 64 4A 79 BC 36 8C 48 22  L.j..9C.dJy.6.H"
            0120  C8 9C D0 18 A5 7F 95 36 44 BE DA 67 9C 5B 53 29  .......6D..g.[S)
            0130  02 32 0E 83 E1 3B 80 DE EF 8C 18 AF 3E 7D 49 3A  .2...;......>}I:
            0140  E3 F8 81 96 10 1B 9F 78 EA FE 4B 30 25 EF 8B FF  .......x..K0%...
            0150  91 6B 2F C0 2D 76 2D 08 38 DE A2 9C 09 B4 85 59  .k/.-v-.8......Y
            0160  1C 2F 47 F8 7C 71 F5 30 BB 35 8F 56 AF 64 59 D8  ./G.|q.0.5.V.dY.
            0170  6D BF 85 EA F9 ED BD 96 2C D3 64 F7 B8 02 01 01  m.......,.d.....
      A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 1122 )
        SEQUENCE SIZE( 1118 )
          SEQUENCE SIZE( 658 )
            A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 3 )
              INTEGER SIZE( 1 )
                0000  02                                            .
            INTEGER SIZE( 3 )
              0000  01 63 26                                       .c&
            SEQUENCE SIZE( 65 )
              OBJECT IDENTIFIER = { 1 2 840 113549 1 1 10 }
              SEQUENCE SIZE( 52 )
```

```
    A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 15 )
      SEQUENCE SIZE( 13 )
        OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
        NULL SIZE( 0 )
    A1 [ CONTEXT 1 ] IMPLICIT SEQUENCE SIZE( 28 )
      SEQUENCE SIZE( 26 )
        OBJECT IDENTIFIER = { 1 2 840 113549 1 1 8 }
        SEQUENCE SIZE( 13 )
          OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
          NULL SIZE( 0 )
    A2 [ CONTEXT 2 ] IMPLICIT SEQUENCE SIZE( 3 )
      INTEGER SIZE( 1 )
        0000  20
SEQUENCE SIZE( 83 )
  SET SIZE( 11 )
    SEQUENCE SIZE( 9 )
      OBJECT IDENTIFIER = { 2 5 4 6 }
      PRINTABLE-STRING SIZE( 2 )
        0000  44 45                                             DE
  SET SIZE( 23 )
    SEQUENCE SIZE( 21 )
      OBJECT IDENTIFIER = { 2 5 4 10 }
      UTF8-STRING SIZE( 14 )
        0000  48 4A 50 20 43 6F 6E 73 75 6C 74 69 6E 67         HJP Consulting
  SET SIZE( 23 )
    SEQUENCE SIZE( 21 )
      OBJECT IDENTIFIER = { 2 5 4 11 }
      UTF8-STRING SIZE( 14 )
        0000  43 6F 75 6E 74 72 79 20 53 69 67 6E 65 72         Country Signer
  SET SIZE( 18 )
    SEQUENCE SIZE( 16 )
      OBJECT IDENTIFIER = { 2 5 4 3 }
      UTF8-STRING SIZE( 9 )
        0000  48 4A 50 20 50 42 20 43 53                        HJP PB CS
SEQUENCE SIZE( 30 )
  UTC SIZE( 13 )
    0000  30 39 30 39 31 38 30 37 35 39 35 33 5A           090918075953Z
  UTC SIZE( 13 )
    0000  31 30 30 39 31 33 30 37 35 39 35 33 5A           100913075953Z
SEQUENCE SIZE( 84 )
  SET SIZE( 11 )
    SEQUENCE SIZE( 9 )
      OBJECT IDENTIFIER = { 2 5 4 6 }
      PRINTABLE-STRING SIZE( 2 )
        0000  44 45                                             DE
  SET SIZE( 23 )
    SEQUENCE SIZE( 21 )
      OBJECT IDENTIFIER = { 2 5 4 10 }
      UTF8-STRING SIZE( 14 )
        0000  48 4A 50 20 43 6F 6E 73 75 6C 74 69 6E 67         HJP Consulting
  SET SIZE( 24 )
    SEQUENCE SIZE( 22 )
      OBJECT IDENTIFIER = { 2 5 4 11 }
      UTF8-STRING SIZE( 15 )
        0000  44 6F 63 75 6D 65 6E 74 20 53 69 67 6E 65 72     Document Signer
  SET SIZE( 18 )
    SEQUENCE SIZE( 16 )
      OBJECT IDENTIFIER = { 2 5 4 3 }
```

```
        UTF8-STRING SIZE( 9 )
          0000  48 4A 50 20 50 42 20 44 53                        HJP PB DS
    SEQUENCE SIZE( 290 )
      SEQUENCE SIZE( 13 )
        OBJECT IDENTIFIER = { 1 2 840 113549 1 1 1 }
        NULL SIZE( 0 )
      BIT-STRING SIZE( 271 )
        0000  00 30 82 01 0A 02 82 01 01 00 B6 C5 A8 EE 57 30  .0............W0
        0010  76 79 E3 64 E3 F7 E7 76 EA 64 07 4E 9A 72 F6 B3  vy.d...v.d.N.r..
        0020  76 C2 D2 31 89 63 1C 10 BA 65 EA 34 6F EF 70 3B  v..1.c...e.4o.p;
        0030  52 EF 75 93 D4 96 E1 50 0F 71 64 D0 38 E9 A8 80  R.u....P.qd.8...
        0040  D0 6E 90 FC F9 6F AD 5B 60 68 B3 42 CC A8 24 77  .n...o.[`h.B..$w
        0050  0B AD F1 42 9E BB DB 97 88 0A AE A4 31 14 62 CA  ...B........1.b.
        0060  CE 40 AA F2 24 78 35 AB C2 59 1E 18 80 AD D9 FD  .@..$x5..Y......
        0070  35 F2 C0 E4 3C C6 FE B9 1B 0F 13 7C C4 2A D8 34  5...<......|.*.4
        0080  73 24 93 FD 63 F7 8F C7 DA 75 CD B4 A1 BD 4C 7D  s$..c....u....L}
        0090  E1 E0 4A C1 B4 BD 4C 62 C4 6F 8D 83 EE 6B F1 AC  ..J...Lb.o...k..
        00A0  24 05 D5 A1 73 77 6A 58 96 0A 79 B1 B5 B9 0B 79  $...swjX..y....y
        00B0  7A 4A 7A 19 84 57 C7 A0 2A 72 A2 FF 9A 32 7E 55  zJz..W..*r...2~U
        00C0  88 19 67 42 C5 7C 8B 9D 5E E6 4B 8A 46 00 3B C5  ..gB.|..^.K.F.;.
        00D0  6D 24 93 C0 A6 58 82 37 94 AB 23 14 BC F9 79 C5  m$...X.7..#...y.
        00E0  EE DF 32 7C 6C 11 2E 9E DD 86 C6 E4 19 F9 AD 35  ..2|l..........5
        00F0  A9 46 56 FD E7 ED 89 6A F5 C3 46 43 5A B3 D7 BE  .FV....j..FCZ...
        0100  C0 F8 B9 02 56 A3 10 50 B3 97 02 03 01 00 01     ....V..P.......
    A3 [ CONTEXT 3 ] IMPLICIT SEQUENCE SIZE( 82 )
      SEQUENCE SIZE( 80 )
        SEQUENCE SIZE( 31 )
          OBJECT IDENTIFIER = { 2 5 29 35 }
          OCTET-STRING SIZE( 24 )
            0000  30 16 80 14 0D FD 5C 02 88 BF EC E0 B0 7A 5D 40  0.....\......z]@
            0010  FF 80 AC 8A 91 74 3A 9B                        .....t:.
        SEQUENCE SIZE( 29 )
          OBJECT IDENTIFIER = { 2 5 29 14 }
          OCTET-STRING SIZE( 22 )
            0000  04 14 91 93 F4 F0 AA 4A CA C0 D3 A1 B6 AC 83 B2  .......J........
            0010  4F 6F DC 8F F2 1B                              Oo....
        SEQUENCE SIZE( 14 )
          OBJECT IDENTIFIER = { 2 5 29 15 }
          BOOLEAN SIZE( 1 )
            0000  FF                                             .
          OCTET-STRING SIZE( 4 )
            0000  03 02 07 80                                    ....
  SEQUENCE SIZE( 65 )
    OBJECT IDENTIFIER = { 1 2 840 113549 1 1 10 }
    SEQUENCE SIZE( 52 )
      A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 15 )
        SEQUENCE SIZE( 13 )
          OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
          NULL SIZE( 0 )
      A1 [ CONTEXT 1 ] IMPLICIT SEQUENCE SIZE( 28 )
        SEQUENCE SIZE( 26 )
          OBJECT IDENTIFIER = { 1 2 840 113549 1 1 8 }
          SEQUENCE SIZE( 13 )
            OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
            NULL SIZE( 0 )
      A2 [ CONTEXT 2 ] IMPLICIT SEQUENCE SIZE( 3 )
        INTEGER SIZE( 1 )
          0000  20
```

```
        BIT-STRING SIZE( 385 )
          0000  00 A3 AF EC 3B C5 D3 66 E6 61 19 4A CA 8D FC 39  ....;..f.a.J...9
          0010  06 76 06 1D 6E 52 30 18 CA 13 93 0D 79 40 E6 CE  .v..nR0.....y@..
          0020  77 86 1D 18 F6 5F 3C EF 8C BF 44 E8 7D 59 AA FA  w...._<...D.}Y..
          0030  6F 29 EC 57 FB 19 DB 12 30 F0 F2 FC 1B F6 0D 1D  o).W....0.......
          0040  03 96 33
3C 89 A9 2B F2 31 3C 43 60 BA B2 18 DE  ..3<..+.1<C`....
          0050  57 71 3F 39 0C A5 BB B6 99 CD 1A 1E 27 3C 61 8B  Wq?9........'<a.
          0060  25 A7 EE DA B5 F0 BA B0 30 65 AA 74 9D 51 32 60  %.......0e.t.Q2`
          0070  BE 86 7E B0 11 29 1D CF 4A DC 83 33 F7 78 4F DD  ..~..)..J..3.xO.
          0080  E8 17 2F 46 C4 F7 90 42 15 FD C9 8F 5C DE 49 16  ../F...B....\.I.
          0090  F0 3E 24 9C D3 94 07 62 D2 F8 E9 2F 23 17 16 A6  .>$....b.../#...
          00A0  BF 74 2F ED C2 62 7E 62 F0 46 95 6D B9 7B AA D2  .t/..b~b.F.m.{..
          00B0  5C 04 62 47 54 D4 AF 3E 1A 7E C4 72 07 CC 08 BD  \.bGT..>.~.r....
          00C0  15 4E 83 9A 43 55 D0 1F 16 DA 2C C1 61 77 A9 14  .N..CU....,.aw..
          00D0  D4 42 87 E6 52 25 64 D0 00 53 9E C9 6A 2B 0E 1E  .B..R%d..S..j+..
          00E0  6E BB 89 63 81 86 8B 5A FE 0A 0F D3 C3 62 F4 19  n..c...Z.....b..
          00F0  AF FD FF 01 6A 71 17 0A C8 B3 78 A6 E3 99 5D 82  ....jq....x...].
          0100  EE 45 95 0E EB B4 C9 BB F6 31 13 24 82 A5 03 C3  .E.......1.$....
          0110  10 26 B4 C2 CD 94 26 E6 66 3D E4 C4 3E FE 54 01  .&....&.f=..>.T.
          0120  F4 D3 BA 76 E5 4F 66 3B 28 32 3E A3 33 1E 96 A7  ...v.Of;(2>.3...
          0130  08 12 F9 43 15 D6 08 A9 E8 CE 1B F0 2B 6E CF 07  ...C........+n..
          0140  01 5D 40 F4 73 DF E1 6F 5C 12 14 60 81 C4 4C 14  .]@.s..o\..`..L.
          0150  8D AB 09 83 50 46 57 A5 3C CA 16 BD 54 5D 5A D5  ....PFW.<...T]Z.
          0160  9A 21 AA 91 9E 7F 9B B7 B3 50 01 AB EF 61 E7 D5  .!.......P...a..
          0170  6E 21 C7 F1 13 73 42 55 71 A7 91 45 D4 46 2E B2  n!...sBUq..E.F..
          0180  6B                                               k
      SET SIZE( 517 )
        SEQUENCE SIZE( 513 )
          INTEGER SIZE( 1 )
            0000  01                                            .
          SEQUENCE SIZE( 90 )
            SEQUENCE SIZE( 83 )
              SET SIZE( 11 )
                SEQUENCE SIZE( 9 )
                  OBJECT IDENTIFIER = { 2 5 4 6 }
                  PRINTABLE-STRING SIZE( 2 )
                    0000  44 45                                     DE
              SET SIZE( 23 )
                SEQUENCE SIZE( 21 )
                  OBJECT IDENTIFIER = { 2 5 4 10 }
                  UTF8-STRING SIZE( 14 )
                    0000  48 4A 50 20 43 6F 6E 73 75 6C 74 69 6E 67     HJP Consulting
              SET SIZE( 23 )
                SEQUENCE SIZE( 21 )
                  OBJECT IDENTIFIER = { 2 5 4 11 }
                  UTF8-STRING SIZE( 14 )
                    0000  43 6F 75 6E 74 72 79 20 53 69 67 6E 65 72     Country Signer
              SET SIZE( 18 )
                SEQUENCE SIZE( 16 )
                  OBJECT IDENTIFIER = { 2 5 4 3 }
                  UTF8-STRING SIZE( 9 )
                    0000  48 4A 50 20 50 42 20 43 53                  HJP PB CS
            INTEGER SIZE( 3 )
              0000  01 63 26                                      .c&
          SEQUENCE SIZE( 13 )
            OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
```

```
  NULL SIZE( 0 )
A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 74 )
  SEQUENCE SIZE( 23 )
    OBJECT IDENTIFIER = { 1 2 840 113549 1 9 3 }
    SET SIZE( 10 )
      OBJECT IDENTIFIER = { 0 4 0 127 0 7 3 2 1 }
  SEQUENCE SIZE( 47 )
    OBJECT IDENTIFIER = { 1 2 840 113549 1 9 4 }
    SET SIZE( 34 )
      OCTET-STRING SIZE( 32 )
        0000  5F 65 34 5D 29 A8 5A 01 BB 38 AE A4 EB D6 C9 8E  _e4]).Z..8......
        0010  7E CE 6F 9F 0F F4 6A F2 FD D0 7B DC 18 BA 6F 38  ~.o...j...{...o8
SEQUENCE SIZE( 65 )
  OBJECT IDENTIFIER = { 1 2 840 113549 1 1 10 }
  SEQUENCE SIZE( 52 )
    A0 [ CONTEXT 0 ] IMPLICIT SEQUENCE SIZE( 15 )
      SEQUENCE SIZE( 13 )
        OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
        NULL SIZE( 0 )
    A1 [ CONTEXT 1 ] IMPLICIT SEQUENCE SIZE( 28 )
      SEQUENCE SIZE( 26 )
        OBJECT IDENTIFIER = { 1 2 840 113549 1 1 8 }
        SEQUENCE SIZE( 13 )
          OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 }
          NULL SIZE( 0 )
    A2 [ CONTEXT 2 ] IMPLICIT SEQUENCE SIZE( 3 )
      INTEGER SIZE( 1 )
        0000  20
OCTET-STRING SIZE( 256 )
  0000  3B CE 96 95 4D 09 8B D4 C6 CC D6 9D D2 EB 73 DD  ;...M.........s.
  0010  58 85 A4 12 F5 9F 48 93 B4 C1 6F 4F 15 2C 5A 7F  X.....H...oO.,Z.
  0020  62 08 24 DA 91 85 FC 23 6F 3B 72 01 8F 77 59 AD  b.$....#o;r..wY.
  0030  BD D1 66 C1 16 AB 5D 4D E5 4C 89 43 68 0A D9 77  ..f...]M.L.Ch..w
  0040  4D 4B 31 02 8D 6E 3F A4 11 73 5B ED 1E 73 E9 9F  MK1..n?..s[..s..
  0050  9C 5A 25 5B B0 3E F6 94 59 B4 B3 BB A9 58 D3 0D  .Z%[.>..Y....X..
  0060  0F F5 C9 FE 0A 0F CB 09 6F 8D 41 CA B1 D8 FB 0E  ........o.A.....
  0070  A6 15 3F 01 E2 A4 2B 7F E6 B2 30 4D 96 27 E7 30  ..?...+...0M.'.0
  0080  C6 3F 9B CB AB 0A 44 5D E9 DC DA E1 F8 E9 C2 76  .?....D].......v
  0090  35 41 0F 49 C8 EB 45 FA B2 5F 55 C0 5A 78 58 82  5A.I..E.._U.ZxX.
  00A0  03 44 25 46 96 16 FC B7 86 EC BD 7C 92 93 0F 2E  .D%F.......|....
  00B0  2D AE A9 8E F8 55 73 23 98 78 51 3E 4F 9A CD 89  -....Us#.xQ>O...
  00C0  75 31 F5 5E 3E 15 8D 61 81 5B 48 75 D1 D7 6E 0E  u1.^>..a.[Hu..n.
  00D0  E6 38 0D 57 6C F5 CF 8F 2F 0A 8E EC B6 CB 51 34  .8.Wl.../.....Q4
  00E0  AA 89 44 1A 4B 87 58 91 AE 22 81 1B 90 49 45 F8  ..D.K.X.."...IE.
  00F0  4C 53 FC 0E 9B A6 42 93 33 1F 31 5D A9 68 D8 B8  LS....B.3.1].h..
```

The relevant information for CA are:

Public Key (PK_{PICC})	0000 1B 33 45 F8 DC 04 34 1B F8 B2 C9 7F 65 2F A6 80 .3E...4.....e/.. 0010 E5 D4 FA 4C 14 6A E4 B8 39 43 1A 64 4A 79 BC 36 ...L.j..9C.dJy.6 0020 8C 48 22 C8 9C D0 18 A5 7F 95 36 44 BE DA 67 9C .H".....6D..g. 0030 5B 53 29 02 32 0E 83 E1 3B 80 DE EF 8C 18 AF 3E [S).2...;......> 0040 7D 49 3A E3 F8 81 96 10 1B 9F 78 EA FE 4B 30 25 }I:.....x..K0% 0050 EF 8B FF 91 6B 2F C0 2D 76 2D 08 38 DE A2 9C 09 ....k/.-v-.8.... 0060 B4 85 59 1C 2F 47 F8 7C 71 F5 30 BB 35 8F 56 AF ..Y./G.|q.0.5.V.

	0070 64 59 D8 6D BF 85 EA F9 ED BD 96 2C D3 64 F7 B8 dY.m.......,.d..
CA OID	0.4.0.127.0.7.2.2.3.1.2
ECDH Shared Secret (K)	0000 2A 4F C2 D1 14 90 DF 47 73 DD FA 6F F7 05 55 7C *O.....Gs..o..U| 0010 51 F4 AD 45 33 E8 D8 A6 6A 30 01 BF DD 27 1D B8 Q..E3...j0...'.. 0020 7B E3 C1 CA C2 2A 05 E8 AF 1A 06 6D D0 29 8E 75 {....*.....m.).u 0030 DB 92 8A AF DF 00 EB 4B FB 1B D1 2F 37 23 13 C1 ....K.../7#.. 0040 CA 64 90 56 51 73 05 63 85 15 D5 A4 FB E0 AC 59 .d.VQs.c.......Y 0050 BD C8 0E 8C 5A 5F 46 25 4D 23 19 16 EA 77 F8 0A ....Z_F%M#...w.. 0060 C5 8E 6B 63 A2 61 98 EE 43 87 F1 09 81 E8 E4 6F ..kc.a..C......o 0070 FB A2 37 90 C8 1E 67 93 63 C5 89 58 7D 30 BB B3 ..7...g.c..X}0..

9.1 Command MSE: Set AT

In the first step the following information extracted from EF.ChipSecurity are important.

CA OID	0.4.0.127.0.7.2.2.3.1.2
Key Refference	01

In the first step of Chip Authentication the terminal sends its OID for CA and the reference of the private key to the chip with the command MSE:Set AT as following.

T→C plain	0000 00 22 41 A4 0F 80 0A 04 00 7F 00 07 02 02 03 01 ."A..... 0010 02 84 01 01 ....
T→C coded	0000 0C 22 41 A4 1D 87 11 01 1A 47 A5 72 4B 07 3B 39 ."A......G.rK.;9 0010 10 09 B7 D2 73 2D 57 CA 8E 08 38 38 BC 02 6D FD ....s-W...88..m. 0020 F6 F5 00 ...
C→T coded	0000 99 02 90 00 8E 08 D1 AB B4 56 52 77 A2 B1 .....VRw..
C→T plain	0000 90 00

C-APDU		
CLA	00 / 0C	Plain, SM
INS	22	Manage Security Environment
P1/P2	41 A4	Chip Authentication: Set Authentication Template for internal authentication

L_c	0F		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	80	0A	04 00 7F 00 07 02 02 03 01 02	Cryptograhic mechanism reference, OID
	84	01	01	Reference of private key

R-APDU		
SW	90 00	Normal operation

9.2 Command General Authenticate

The terminal send the ephemeral public key $\widetilde{PK}_{PCD}$ to the chip.

$\widetilde{PK}_{PCD}$	
	0000 A2 83 09 47 A6 FC AA CD E2 FC B8 8B 29 AB 38 E0 ...G........).8. 0010 7C 34 53 AB C4 BC B4 66 08 7E 11 C7 9F 32 A1 9E |4S....f.~...2.. 0020 6E F2 2B E1 08 F8 DD 18 FE 82 49 C9 60 95 15 11 n.+.......I.`... 0030 20 0D C9 85 AA 3E C0 CC AD 59 A5 F9 BB CC 33 EE ....>...Y....3. 0040 5F 15 77 E2 03 30 B4 DD 10 EB 06 B7 40 27 7C 97 _.w..0......@'|. 0050 A1 89 18 0E DE 52 BE E9 D4 29 F1 0F B7 7F 18 0F .....R...)..... 0060 05 D6 A9 9C 49 9C B5 E1 EC EE B8 E9 22 84 F6 6E ....I.......".."n 0070 A9 84 79 67 4C E7 3F 53 C5 67 A0 3B 0D 29 78 33 ..ygL.?S.g.;.)x3

The command is performed as following.

T→C plain	0000 00 86 00 00 86 7C 81 83 80 81 80 A2 83 09 47 A6 .....|........G. 0010 FC AA CD E2 FC B8 8B 29 AB 38 E0 7C 34 53 AB C4 ....).8.|4S.. 0020 BC B4 66 08 7E 11 C7 9F 32 A1 9E 6E F2 2B E1 08 ..f.~...2..n.+.. 0030 F8 DD 18 FE 82 49 C9 60 95 15 11 20 0D C9 85 AA .....I.`... .... 0040 3E C0 CC AD 59 A5 F9 BB CC 33 EE 5F 15 77 E2 03 >...Y....3._.w.. 0050 30 B4 DD 10 EB 06 B7 40 27 7C 97 A1 89 18 0E DE 0......@'|...... 0060 52 BE E9 D4 29 F1 0F B7 7F 18 0F 05 D6 A9 9C 49 R...).........I 0070 9C B5 E1 EC EE B8 E9 22 84 F6 6E A9 84 79 67 4C ....".."n..ygL 0080 E7 3F 53 C5 67 A0 3B 0D 29 78 33 00 .?S.g.;.)x3.
T→C coded	0000 0C 86 00 00 A1 87 81 91 01 31 44 28 FE A3 29 FB ....1D(..). 0010 63 C0 A8 22 31 88 10 69 DC 16 91 87 76 14 E0 76 c.."1..i....v..v 0020 66 D1 DD 21 77 90 8E 33 D8 D7 A3 02 DE 4D 88 E1 f..!w..3.....M.. 0030 6E 43 00 A7 DB 12 2D D3 9E 76 D7 34 DD 59 ED 35 nC....-..v.4.Y.5 0040 3A 65 0D E8 16 30 F8 81 9A 35 18 8C 60 E6 68 EB :e...0...5..`.h. 0050 B0 C2 0D DA C8 54 AD 00 26 82 2C 11 56 E5 18 7A .....T..&.,.V..z 0060 CF B4 4C 57 E5 23 C0 D9 08 FD 0B 4A B6 E0 0D 7B ..LW.#.....J...{ 0070 0F 06 34 BB 9A 39 81 C7 11 F2 D4 69 49 BB 3C 18 ..4..9.....iI.<. 0080 E1 C4 ED F2 87 9C 14 67 F8 D8 F7 80 8E 2B 28 E8 ....g.....+(. 0090 D7 31 23 31 9B C3 9A 30 30 97 01 00 8E 08 77 48 .1#1...00.....wH 00A0 54 B1 08 05 0B 6E 00 T....n.
C→T	0000 87 21 01 8C 99 94 3A 83 72 C1 80 59 95 3E 00 92 .!....:.r..Y.>.. 0010 DE 2E 59 08 05 6D C4 CB AB E8 97 8B 55 EF 6F 24 ..Y..m......U.o$

coded	0020 79 88 AB 99 02 90 00 8E 08 B5 57 32 B9 7B 35 4E y.........W2.{5N 0030 51 Q
C→T plain	0000 7C 14 81 08 1A 1A C1 AB 04 D9 69 65 82 08 75 68 |.........ie..uh 0010 91 58 0F 70 16 4D .X.p.M

C-APDU				
CLA	00 / 0C		Plain, SM	
INS	86		General Authenticate	
P1/P2	00 00		Keys and protocol implicitly known	
L_c	86		Length of data field	
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	81 83		Dynamic Authentication Data
	80	81 80	A2 83 09 47 A6 FC AA CD E2 FC B8 8B 29 … … 67 4C E7 3F 53 C5 67 A0 3B 0D 29 78 33	Ephemeral public key of terminal
L_e	00			Expected maximal byte length of the response data field

R-APDU				
Data	***Tag***	***Length***	***Value***	***Comment***
	7C	14		Dynamic Authentication Data
	81	08	1A 1A C1 AB 04 D9 69 65	r_{PICC}
	82	08	75 68 91 58 0F 70 16 4D	T_{PICC}
SW	90 00		Normal operation	

Both the terminal and the chip calculate the shared secret K.

PICC:

SK_{PICC}	0000 00 D0 E5 A9 5E CA 54 1D EF 4F E9 2B 9F F9 92 0D ....^.T..O.+.... 0010 49 A4 54 C2 97 I.T..

$\widetilde{PK}_{PCD}$	0000 A2 83 09 47 A6 FC AA CD E2 FC B8 8B 29 AB 38 E0 ...G........).8. 0010 7C 34 53 AB C4 BC B4 66 08 7E 11 C7 9F 32 A1 9E |4S....f.~...2.. 0020 6E F2 2B E1 08 F8 DD 18 FE 82 49 C9 60 95 15 11 n.+.......I.`... 0030 20 0D C9 85 AA 3E C0 CC AD 59 A5 F9 BB CC 33 EE ....>...Y....3. 0040 5F 15 77 E2 03 30 B4 DD 10 EB 06 B7 40 27 7C 97 _.w..0......@'|. 0050 A1 89 18 0E DE 52 BE E9 D4 29 F1 0F B7 7F 18 0F .....R...)..... 0060 05 D6 A9 9C 49 9C B5 E1 EC EE B8 E9 22 84 F6 6E ....I.......".n 0070 A9 84 79 67 4C E7 3F 53 C5 67 A0 3B 0D 29 78 33 ..ygL.?S.g.;.)x3
D_{PICC}	00
Shared Secret K	0000 2A 4F C2 D1 14 90 DF 47 73 DD FA 6F F7 05 55 7C *O.....Gs..o..U| 0010 51 F4 AD 45 33 E8 D8 A6 6A 30 01 BF DD 27 1D B8 Q..E3...j0...'.. 0020 7B E3 C1 CA C2 2A 05 E8 AF 1A 06 6D D0 29 8E 75 {....*.....m.).u 0030 DB 92 8A AF DF 00 EB 4B FB 1B D1 2F 37 23 13 C1 ....K.../7#.. 0040 CA 64 90 56 51 73 05 63 85 15 D5 A4 FB E0 AC 59 .d.VQs.c.......Y 0050 BD C8 0E 8C 5A 5F 46 25 4D 23 19 16 EA 77 F8 0A ....Z_F%M#...w.. 0060 C5 8E 6B 63 A2 61 98 EE 43 87 F1 09 81 E8 E4 6F ..kc.a..C......o 0070 FB A2 37 90 C8 1E 67 93 63 C5 89 58 7D 30 BB B3 ..7...g.c..X}0.. 0080 1A 1A C1 AB 04 D9 69 65 ......ie

PCD:

$\widetilde{SK}_{PCD}$	0000 00 A2 CF FD 06 C3 4A FD 62 2E EE 0F C3 1F 09 3F ......J.b......? 0010 DF DA 60 9C 67 12 1C AC F0 A8 F5 22 91 DE 68 53 ..`.g......".hS 0020 BB 5C 93 CF 76 70 57 75 EC F4 08 A7 43 02 61 3B .\..vpWu....C.a; 0030 EE CB 38 14 47 D3 64 94 C9 E1 89 51 EC 17 25 2D ..8.G.d....Q..%- 0040 D2 A8 07 AA E0 9F A4 DC 30 18 33 39 01 3D 9C 91 ....0.39.=.. 0050 91 30 3C AC EE 3C 91 E9 26 A3 6D 01 4A 5C FA 94 .0<..<..&.m.J\.. 0060 95 0C AD B3 7B 53 4F 32 A9 BF 76 B3 79 80 97 93 ....{SO2..v.y... 0070 04 C5 66 38 71 BD 74 6E B9 E9 5A 47 CA 47 1B 4E ..f8q.tn..ZG.G.N 0080 DE .
PK_{PICC}	0000 1B 33 45 F8 DC 04 34 1B F8 B2 C9 7F 65 2F A6 80 .3E...4.....e/.. 0010 E5 D4 FA 4C 14 6A E4 B8 39 43 1A 64 4A 79 BC 36 ...L.j..9C.dJy.6 0020 8C 48 22 C8 9C D0 18 A5 7F 95 36 44 BE DA 67 9C .H".......6D..g. 0030 5B 53 29 02 32 0E 83 E1 3B 80 DE EF 8C 18 AF 3E [S).2...;......> 0040 7D 49 3A E3 F8 81 96 10 1B 9F 78 EA FE 4B 30 25 }I:.......x..K0% 0050 EF 8B FF 91 6B 2F C0 2D 76 2D 08 38 DE A2 9C 09 ....k/.-v-.8.... 0060 B4 85 59 1C 2F 47 F8 7C 71 F5 30 BB 35 8F 56 AF ..Y./G.|q.0.5.V. 0070 64 59 D8 6D BF 85 EA F9 ED BD 96 2C D3 64 F7 B8 dY.m.......,.d..
D_{PICC}	00
Shared Secret K	0000 2A 4F C2 D1 14 90 DF 47 73 DD FA 6F F7 05 55 7C *O.....Gs..o..U| 0010 51 F4 AD 45 33 E8 D8 A6 6A 30 01 BF DD 27 1D B8 Q..E3...j0...'.. 0020 7B E3 C1 CA C2 2A 05 E8 AF 1A 06 6D D0 29 8E 75 {....*.....m.).u 0030 DB 92 8A AF DF 00 EB 4B FB 1B D1 2F 37 23 13 C1 ....K.../7#.. 0040 CA 64 90 56 51 73 05 63 85 15 D5 A4 FB E0 AC 59 .d.VQs.c.......Y 0050 BD C8 0E 8C 5A 5F 46 25 4D 23 19 16 EA 77 F8 0A ....Z_F%M#...w.. 0060 C5 8E 6B 63 A2 61 98 EE 43 87 F1 09 81 E8 E4 6F ..kc.a..C......o 0070 FB A2 37 90 C8 1E 67 93 63 C5 89 58 7D 30 BB B3 ..7...g.c..X}0.. 0080 1A 1A C1 AB 04 D9 69 65 ......ie

Input data for Authentication Token:

OID	0000 04 00 7F 00 07 02 02 03 01 02 ....
$\widetilde{PK}_{PCD}$	0000 A2 83 09 47 A6 FC AA CD E2 FC B8 8B 29 AB 38 E0 ...G........).8. 0010 7C 34 53 AB C4 BC B4 66 08 7E 11 C7 9F 32 A1 9E |4S....f.~...2.. 0020 6E F2 2B E1 08 F8 DD 18 FE 82 49 C9 60 95 15 11 n.+.......I.`... 0030 20 0D C9 85 AA 3E C0 CC AD 59 A5 F9 BB CC 33 EE ....>...Y....3. 0040 5F 15 77 E2 03 30 B4 DD 10 EB 06 B7 40 27 7C 97 _.w..0......@'|. 0050 A1 89 18 0E DE 52 BE E9 D4 29 F1 0F B7 7F 18 0F .....R...)..... 0060 05 D6 A9 9C 49 9C B5 E1 EC EE B8 E9 22 84 F6 6E ....I.......".n 0070 A9 84 79 67 4C E7 3F 53 C5 67 A0 3B 0D 29 78 33 ..ygL.?S.g.;.)x3
Complete input data for Token	0000 7F 49 81 8F 06 0A 04 00 7F 00 07 02 02 03 01 02 .I.............. 0010 84 81 80 A2 83 09 47 A6 FC AA CD E2 FC B8 8B 29 ......G........) 0020 AB 38 E0 7C 34 53 AB C4 BC B4 66 08 7E 11 C7 9F .8.|4S....f.~... 0030 32 A1 9E 6E F2 2B E1 08 F8 DD 18 FE 82 49 C9 60 2..n.+.......I.` 0040 95 15 11 20 0D C9 85 AA 3E C0 CC AD 59 A5 F9 BB ... .>...Y... 0050 CC 33 EE 5F 15 77 E2 03 30 B4 DD 10 EB 06 B7 40 .3._.w..0......@ 0060 27 7C 97 A1 89 18 0E DE 52 BE E9 D4 29 F1 0F B7 '|......R...)... 0070 7F 18 0F 05 D6 A9 9C 49 9C B5 E1 EC EE B8 E9 22 ....I........" 0080 84 F6 6E A9 84 79 67 4C E7 3F 53 C5 67 A0 3B 0D ..n..ygL.?S.g.;. 0090 29 78 33)x3
T_{PCD}	75 68 91 58 0F 70 16 4D

The authentication token T_{PCD} computed by the terminal is equal to the authentication T_{PICC} returned by the PICC in the previous command above. This means Chip Authentication has performed successfully.

The new session keys (AES 128) are derived from the shared secret by means of KDF specified in [TR-03110].

K_{Enc}	0000 E8 13 D0 9D F6 9F FC C6 37 63 C5 37 F8 28 98 5C ....7c.7.(.\
K_{Mac}	0000 06 67 21 F3 EB EA 78 7B 4F 1C 6D CA 43 1E C2 29 .g!...x{O.m.C..)

With an established Chip Authentication and the new session keys the data of the chip application can be read.

Annex

Revision history

Version	*Date*	*Alteration*	*Author*
V1.0	30.11.2010	Release of first final version	BSI
V1.01	24.01.2011	Minor corrections and clarifications	BSI
V1.02	03.08.2011	Minor corrections and clarifications	BSI

References

TR-03110: BSI: TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.0.5

Doc9303: IACO: ICAO Doc9303 Part I Volume I, Sixth Edition, ICAO 2006

TR-03105: BSI: TR-03105 Conformity Tests for Official Electronic ID Documents

RFC5114: M. Lepinski, S. Kent, RFC 5114: Additional Diffie-Hellman Groups with IETF Standards, 2008