Tabelle 1

	DESFire DES authentification D40 (legacy mode)																					
01 start the authentification, send 0x0A command to PICC	90	0A	00	00	01	01	00															
02 PICC send the (encrypted) random rndB value	EB	05	33	B4	BC	89	AF	CF	91	AF												
Note: 0x91 AF means more data has to follow, strip off																						
encrypted rndB	EB	05	33	B4	BC	89	AF	CF														
03 run 'setKeyVersion' with keyVersion 0																						
Value of the DES key that is used for authentication	D1	00	23	45	67	89	AB	CD														
Value of the DES key after 'setKeyVersion' with key version 0	D0	00	22	44	66	88	AA	CC														
04 triple the key for a TDES key (24 bytes)	D0	00	22	44	66	88	AA	CC	D0	00	22	..	66	88	AA	CC		(total 24 bytes)				
05 decrypt the encrypted rndB with key from step 04	C4	A3	46	8F	B0	D8	7E	74														
Use an iv0 = 8 bytes of 0x00																						
note: this is rndB (secret from PICC)																						
06 rotate all bytes from rndB to the left	A3	46	8F	B0	D8	7E	74	C4														
07 generate our rndA value (8 bytes random data)	45	CC	39	92	87	13	E1	C0														
08 concatenate rndA with left rotated rndB (step 06)	45	CC	39	92	87	13	E1	C0	A3	46	8F	B0	D8	7E	74	C4						

09 copy the encrypted rndB value (step 02) to iv1	EB	05	33	B4	BC	89	AF	CF													
10 encrypt the value from step 08 (rndA || rndB left rotated) using TripleDES.decrypt in SEND mode	Steps are not shown here, see separate sheet																				
encryption result (encrypted rndA || rndB left rotated)	88	E1	99	B0	2D	A8	33	67	55	72	08	D9	62	AE	4B	4F					
step 11 send the encrypted data to the PICC using the 0xAF command (more data)	90	AF	00	00	10	88	E1	99	B0	2D	A8	33	..	4B	4F	00		(total 22 bytes)			
step 12 the PICC responds with the encrypted rndA	6C	CC	27	D2	13	52	C5	EE	91	00											
note 1: 0x91 00 means success, strip off																					
note 2: the received value is left rotated encrypted rndA																					
left rotated encrypted rndA	6C	CC	27	D2	13	52	C5	EE													
13 decrypt the left rotated encrypted rndA with key from step 04	CC	39	92	87	13	E1	C0	45													
use an iv0 = 8 bytes of 0x00																					
14 rotate decrypted left rotated rndA to RIGHT	45	CC	39	92	87	13	E1	C0													
note: the result is the received rndA																					
15 compare self generated rndA with rndA received from PICC																					
self generated rndA (step 07)	45	CC	39	92	87	13	E1	C0													
received rndA (step 14)	45	CC	39	92	87	13	E1	C0													

Result of comparing	both values are equals = SUCCESS																						
16 generate the DES Session key from rndA and rndB																							
rndA	45	CC	39	92	87	13	E1	C0															
rndB	C4	A3	46	8F	B0	D8	7E	74															
take the first 4 bytes of rndA	45	CC	39	92																			
take the first 4 bytes of rndB	C4	A3	46	8F																			
concatenate rndA (first 4 bytes) || rndB (first 4 bytes)	45	CC	39	92	C4	A3	46	8F															
DES session key (8 bytes)	45	CC	39	92	C4	A3	46	8F															