Signature Application, Short Specification

ACOS Bank Card

Document:	CardSpec ACOS Short.doc
Version:	1.12
Author:	F. Brandl
Date:	18.04.05

Table of Content

Document History

Version	Author	Date	Changes
Version 1.12	BRA	18.04.2005	• short document version derived from full card spec

1. About this document

1.1. Terms and Abbreviations

AC	Access condition
AID	Application identifier
AR	Algorithm reference
ATR	Answer to reset
CH_ID	Certificate holder ID (identifier eines öffentlichen RSA-Keys)
CHV	Card holder verification information (PIN)
CRDO	Control reference data object
CT	Confidentiality template
DF	Dedicated file
DO	Data object
DST	Digital signature template
EF	Elementary file
FID	File-ID
KID	Key identifier (Eindeutige Nummer eines Keys)
LSB	Least significant byte
MF	Master file
MSB	Most significant byte
MSE	Manage security environment (Kartenkommando)
OID	Object identifier
PIN	Personal identification number
PUK	Personal unblocking key
PSO	Perform security operation (Kartenkommando)
RC	Retry counter (Fehlbedienungszähler)
SE	Security environment
SW	Status word
UC	Usage counter (Verwendungszähler)

1.2. Notation

xxx	Decimal
‘xxx’	Hexadecimal
„xxx“	ASCII
xxx°	Binary

DES(k, m)	DES encryption of message m using key k
DES^{-1}(k, m)	DES decryption of message m using key k
3DES(k, m)	Triple DES encryption of message m using key k
$3DES^{-1}$(k, m)	Triple decryption of message m using key k
3DESMAC(k, m)	Triple DES MAC calculation over message m using key k
SHA(m)	Hash calculation using SHA-1 over message m

1.3. Reference Documents

[COHEN]	Cohen, D.: "On Holy Wars and a Plea for Peace", IETF IEN137 bzw. Computer, IEEE, October 1981
[DIN 66291-4]	DIN: DIN V 66291-1 Chipkarten mit Digitaler Signatur-Anwendung / Funktion nach SigG und SigV - Teil 4: Basic Security Services
[ISO7816-3]	ISO/IEC: Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols
[ISO7816-4]	ISO/IEC: Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange
[ISO7816-6]	ISO/IEC: Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements
[ISO7816-8]	ISO/IEC: Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 8: Security related interindustry commands; Final Committee Draft
[PKCS1]	RSA Laboratories: PKCS #1: RSA Encryption Standard; Version 1.5
[ACOS-CMD]	AustriaCard: Commands for ACOS EMV-A03
[ACOS-EVAL-AG]	AustriaCard: Evaluation of the ACOS EMV-A03, Administrator Guidance
[IFCP]	A-Trust Digital Signature: Interface Description for Card Production

2. Introduction

This specification describes the signature card used for the TrustSign signature product.

The card itself is made up of the following components:

Component	Description
Application ‚a-sign Premium'	The A-Trust specific application ‚a-sign Premium' includes the card file structure and the file contents.
Operating System	The card uses the smartcard operating system 'ACOS EMV-A03' supplied by AustriaCard GmbH.
Chip Hardware	The card uses the Smart Card Controller P5CC036 supplied by Philips Semiconductors.

2.1. Application 'a-sign Premium'

The A-Trust specific application ‚a-sign Premium' includes the card file structure and the file contents as described in chapter ‚4. File Structure and Data':

- application ID (AID) values
- file ID (FID) values
- file types and sizes
- file access conditions
- data structure within files
- parameters of cryptographic keys, PINs and PUKs (key sizes, key identifier values, key usages)

2.2. Operating System

The card operating system supplies the

- commands as described in documents [ACOS-CMD].
- the algorithms and mechanisms described in document [ACOS-CMD]).

2.3. Chip Hardware

The chip hardware also supplies (together with the Operating System) the algorithms and mechanisms, like

- cryptographic functions, implemented in a cryptographic co-processor,
- on-board key generation
- physical protection of sensitive data (keys, PINs, PUKs)

3. Card Commands

The card obviously uses standard SPK card commands as described in [ACOS-CMD].

3.1. Command Sequences

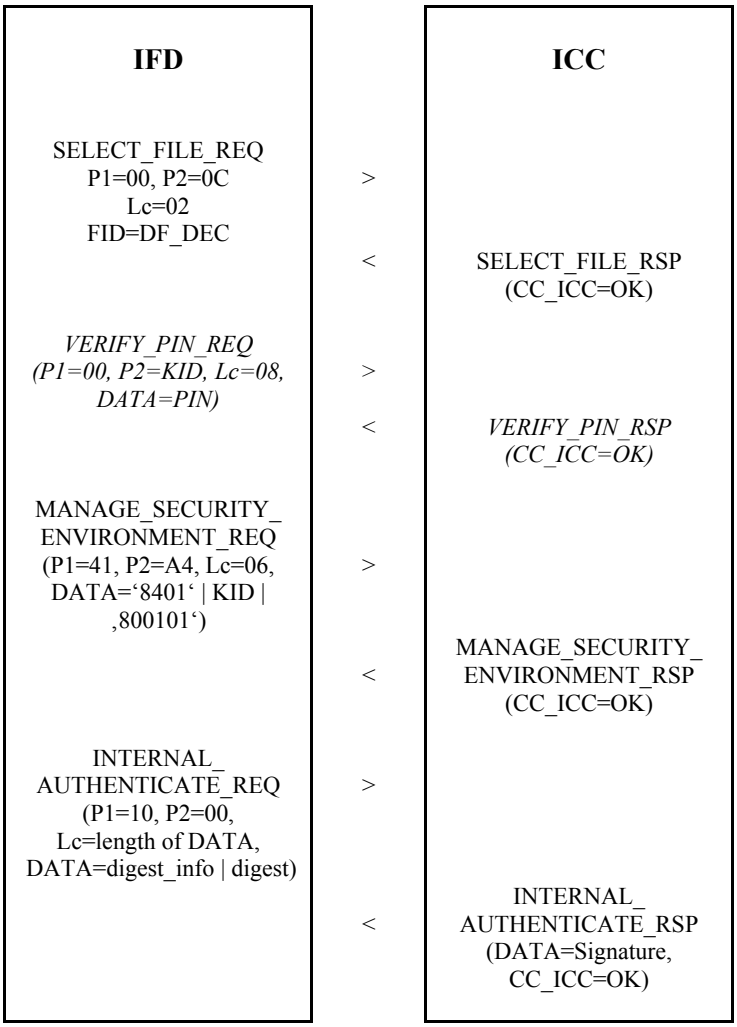
3.1.1. Signature using SK_CH_SIG

Secure signature is done using the secret key part of the signature key pair K_CH_SIG.

IFD		ICC
SELECT_FILE_REQ P1=00, P2=0C Lc=02 FID=DF_SIG	>	
	<	SELECT_FILE_RSP (CC_ICC=OK)
VERIFY_PIN_REQ (P1=00, P2=KID, Lc=08, DATA=PIN)	>	
	<	VERIFY_PIN_RSP (CC_ICC=OK)
MANAGE_SECURITY_ ENVIRONMENT_REQ (P1=81, P2=B6, Lc=06, DATA='8401' | KID | ,800114')	>	
	<	MANAGE_SECURITY_ ENVIRONMENT_RSP (CC_ICC=OK)
PUT_HASH_REQ (P1=90, P2=81, Lc=14, DATA=Hash)	>	
	<	PUT_HASH_RSP (CC_ICC=OK)
COMPUTE_ SIGNATURE_REQ (P1=9E, P2=9A, Lc=00)	>	
	<	COMPUTE_ SIGNATURE_RSP (DATA=Signature, CC_ICC=OK)

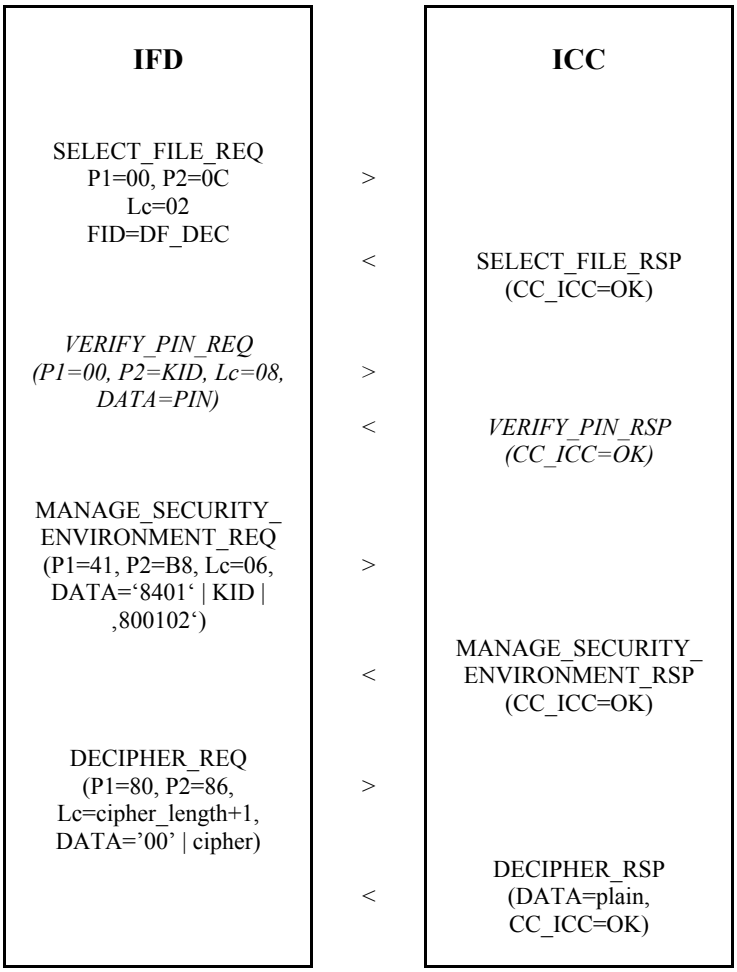
3.1.2. Client/Server Authentication using SK_CH_EKEY

Client/Server Authentication (e.g. for SSL) or simple signature is done using the secret key part of the encryption key pair K_CH_EKEY.



3.1.3. Data Decryption using SK_CH_EKEY

Decryption is done using the secret key part of the encryption key pair K_CH_EKEY.



4. File Structure and Data

4.1. ATR

Note that the cards share the ATR with other bank cards without signature applications on them. Applications therefore have to verify the presence of the signatute AID's.

4.1.1. Historical Characters

'455041xxxxxxxxxxxxxxxxyyyyyyyy', where 'xxxx' = EPA card number CARD_NR
in ASCII: „EPA....."

or

'4D4341xxxxxxxxxxxxxxxxyyyyyyyy', where 'xxxx' = EPA card number CARD_NR
in ASCII: „MCA....."

4.1.2. Complete ATR

'3BBF11008131FE45455041xxxxxxxxxxxxxxxxyyyyyyyyzz'

or

'3BBF11008131FE454D4341xxxxxxxxxxxxxxxxyyyyyyyyzz'

4.2. Short FIDs

Short FIDs (SID's) are explicitly defined. Each EF within a DF may be selected using the defined Short FID (as described in the following chapters).

4.3. Access Conditions

The following abbreviations are used:

ALW	always
AUT	external authentication using the specified key required
NEV	never
PIN	presentation of the specified PIN required
SMA	only using Secure Messaging in Authentic or Combined Mode
SMC	only using Secure Messaging in Combined Mode

AC's not listed are „NEV" by default.

4.4. Keys

4.4.1. Notation

- keys named KD.xxx are double length DES keys which are used in Triple DES mode (EDE).
- keys named SK.xxx are secret RSA or ECC keys (private keys).
- keys named PK.xxx are public RSA or ECC keys (public keys).

All length specifications are in bit. Please note the following:

- for 3DES keys, the length is specified as 112 bit. For storage in the card, 128 bit are needed because of the parity bits.
- for secret RSA keys, the length specification applies to the modulus only. The storage is done exclusively in CRT format as described below.
- for public RSA keys, both the modulus length / exponent length are specified.

4.4.2. Data Storage

Keys are stored in 2 different types of files:

- *Internal Secret Files* (ISF) contain 3DES- and secret RSA or ECC keys as well as PINs and PUKs. ISFs cannot be read and may only be written using the commands WRITE KEY and GENERATE PUBLIC KEY PAIR.
- *Elementary Files* (EF) contain public RSA or ECC keys. IPFs are structured like transparent files and therefore may be read and written using the commands READ BINARY and UPDATE BINARY. Furthermore the command READ PUBLIC KEY can be used, and the command GENERATE PUBLIC KEY PAIR may also be used to store a public key in the EF.

The storage of keys (structure, ...) is described in the document [ACOS-CMD].

4.4.3. Storage of RSA Keys

Secret RSA keys are exclusively stored in CRT format using the following components:

	Component Length in bit for Modulus Length of	
Component	1024 bit	2048 bit
P	512	1024
Q	512	1024
1/e mod (p-1)	512	1024
1/e mod (q-1)	512	1024
1/p mod q	512	1024

4.5. Master File (MF)

FID: ‘3F 00’

The Master File does not contain any Signature Application specific data and therefore is outside the scope of this document.

4.6. Dedicated File DF_SIG

AID: 'A0 00 00 01 18 45 43'
FID: 'DF 70'

4.6.1. ISF_SIG

FID: -
Content: secret keys (PIN, PUK, 3DES, ECC)
Structure: ISF
Size: -
Access Conditions:
Read: NEV
Write: SMC

Key	L (Bits)	KID	Written by	Description
PIN.SIG	64	81	- (selected by cardholder)	PIN for Signature generation (6 digits ASCII leftbound, padded to the right with '00') **RC = 10**
PUK.SIG	64	83	A-Trust	PUK for PIN.SIG (16 digits BCD coded) **UC = 3** **RC = 3**
SK.CH.SIGN	192	88	AustriaCard [1]	ECC secret cardholder signature key

The key SK.CH.SIGN may only be used after successful verification of PIN.SIG. Verification of PIN.SIG thereby enables SK.CH.SIG to be used **one time only**.

[1] generated in card

4.6.2. EF_PK_CH_SIG

FID: ’B0 01’
SID: ’01’
Content: public signature key PK.CH.SIG
Structure: transparent
Size:
Access Conditions:
Read: SMA
Write: NEV (generated by card)

4.6.3. EF_C_CH_DS

FID: ’C0 02’
Content: X.509 certificate for key PK.CH.SIGN
Structure: transparent
Size: 2000
Access Conditions:
Read: ALW
Write: SMA

4.7. Dedicated File DF_DEC

AID: 'A0 00 00 01 18 45 4E'
FID: 'DF 71'

4.7.1. ISF_DEC

FID: -
Content: secret keys (PIN, PUK, 3DES, RSA)
Structure: ISF
Size: -
Access Conditions:
Read: NEV
Write: SMC

Key	L (Bits)	KID	Written by	Description
PIN.DEC	64	81	A-Trust	PIN for decryption and user authentication (4 digits ASCII leftbound, padded to the right with '00') **RC = 10**
PUK.DEC	64	82	A-Trust	PUK for PIN.DEC (16 digits BCD coded) **UC = 3** **RC = 3**
PIN.INF	64	83	A-Trust	PIN for infobox access (4 digits ASCII leftbound, padded to the right with '00') **RC = 10**
PUK.INF	64	84	A-Trust	PUK for PIN.INF (16 digits BCD coded) **UC = 3** **RC = 3**
SK.CH.EKEY	2048 [2]	88	A-Trust	RSA secret cardholder decryption key

The key SK.CH.EKEY may only be used after successful verification of PIN.DEC. Verification of PIN.DEC thereby enables SK.CH.EKEY to be used **an unlimited number of times**.

[2] actual key size may be lower

4.7.2. EF_CIN_CSN

FID: ’D0 01’
SID: ’06’
Content: Cardholder Identification Number (12 hex digits) followed by Card Sequence Number (4 hex digits)
Structure: transparent
Size: 8 bytes (16 hex digits)
Access Conditions:
Read: ALW
Write: SMA

4.7.3. EF_PK_CH_EKEY

FID: ’B0 01’
SID: ’01’
Content: public encryption key PK.CH.EKEY
Structure: transparent
Size:
Access Conditions:
Read: ALW
Write: SMA

4.7.4. EF_C_CH_EKEY

FID: ’C0 01’
SID: ’11’
Content: X.509 certificate for key PK.CH.EKEY
Structure: transparent
Size: 2000
Access Conditions:
Read: ALW
Write: SMA, PIN (PIN.DEC)

4.7.5. EF_INFOBOX

FID: ’C0 02’
SID: ’12’
Content: RFU
Structure: transparent
Size: 1500
Access Conditions:
Read: SMA, PIN (PIN.INF)
Write: SMA, PIN (PIN.INF)