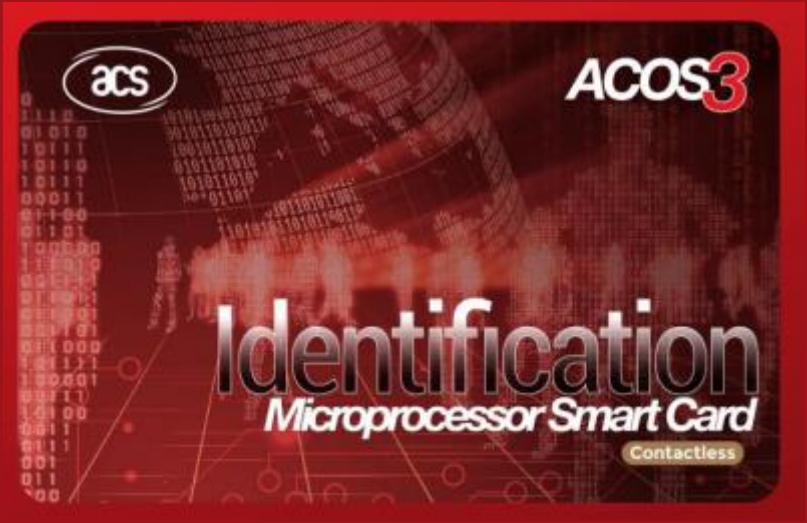


ACOS3

User Manual • Uživatelský manuál • Užívateľský manuál • Használati utasítás • Benutzerhandbuch

Dear customer,

Thank you for purchasing our product. Please read the following instructions carefully before first use and keep this user manual for future reference. Pay particular attention to the safety instructions. If you have any questions or comments about the device, please contact the customer line.

✉ www.alza.co.uk/kontakt

✆ +44 (0)203 514 4411

Importer Alza.cz a.s., Jankovcova 1522/53, Holešovice, 170 00 Prague 7, www.alza.cz

Introduction

The purpose of this document is to describe in detail the features and functions of the ACOS3 Contactless Card, a versatile smart card operating system developed by Advanced Card Systems Ltd.

History of Modifications for ACOS3 Contactless

Nov 2010 ACOS3 Combi Revision 1.17

- Contact and contactless dual interface ACOS3 version
- 8 Kilobyte user storage capacity
- Backward compatible expect ATR/ATS and its customization

June 2014 ACOS3 Combi Revision 1.25

- Modified ATS for quicker response during tearing

Technical Specifications

The following are the features and technical of the ACOS3 Contactless card:

Electrical

- Operating Voltage: 5V DC +/-10% (Class A) and 3V DC +/- 10% (Class B)
- Maximum Supply Current: < 10mA
- ESD Protection: ≤4KV

Environmental

- Operating Temperature: -20°C to 85°C
- Storage Temperature: -40°C to 100°

Communication Protocols

- T=CL with baud up to 848kbps

Memory

- Capacity: 8KB
- EEPROM endurance: 500,00 erase/write cycles
- Data Retention: 20 Years

Cryptographic Capabilities

- DES/3DES: 56/112-bits

Random Number Generation

- FIPS 140-2 compliant RNG

File Security

- Five secret codes + Issuer Code
- PIN code
- Key pair for mutual authentication
- Session key based on random numbers
- Secure Messaging function for confidential and authenticated data transfers
- Support for highly secured e-Purse for payment applications

Compliance to Standards

- Compliance to ISO 14443 (Type A) Parts 1,2,3,4

Answer to Select (ATS)

After receiving a Request for Answer to Select (RATS) from the card reader, the card transmits and Answer to Select (ATS) in compliance with ISO 14443 Part 4.

The following data transmitted in the ATS:

TL	T0	TA_1	TB_1	TC_1	3 Historical Bytes
08h	78h	33h	B5h	02h	

The three (3) bytes string transmitted in the historical bytes is composed as follow:

T1	T2	T3
41h	01h	25h

Card Management

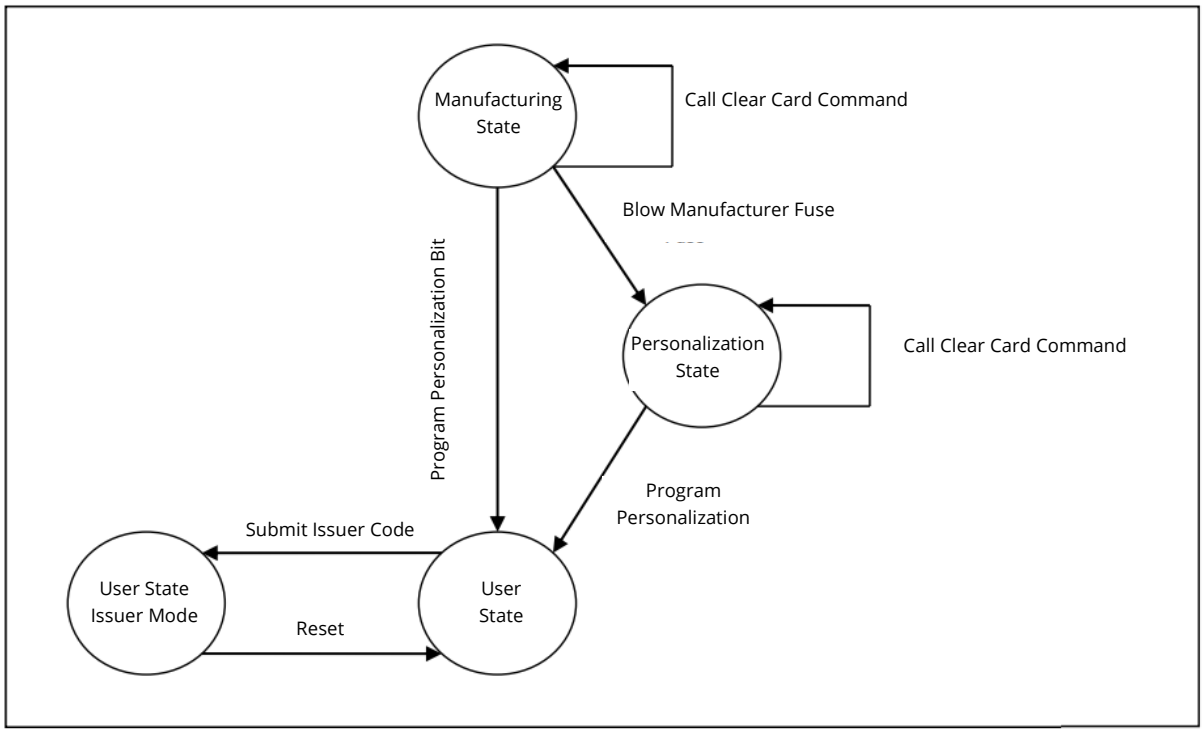
This selection outlines the card level features and management functions.

Card Life Cycle States

During the whole life cycle of the chip-card, three phases and two different operating modes can be distinguished:

- Manufacturing State
- Personalization State
- User State
- User State – Issuer Mode

The card is at any moment in one of these four states. The following diagram shows the possible transitions between the four states:



The actual chip life cycle state is determined by the card operating system immediately after a reset. The life cycle state does not change during the operation of the card. CLEAR CARD command can be issued in the personalization state and manufacture state to clear the card of all data expect the manufacturer data and IC code. However, this command cannot be used to User State.

Manufacturing State

The Manufacturing State is effective from the moment of chip manufacturing until an associated fuse (i.e., certain bit in the EEPROM), the Manufacturer Fuse, has been programmed.

The IC is presented to the card in plain, without encryption.

All command are available in manufacturer state. In addition, the Manufacturer File (FF01h) can only be written in this state.

The manufacturer file contains two records, 8 bytes each, associated to manufacturing state. In this file, it contains the Manufacturer Fuse. After programming the Manufacturer Fuse, the card enters the personalization state and the manufacturer file is on read-only. Data unique to each card and common card data can be programmed, such as, card manufacturer identification, card serial number, etc. The card does not interpret the data.

In this state, the card's data and keys can erased by calling the CLEAR CARD command. This command will physically erase the EEPROM memory expect for the IC code and manufacturer file.

Once the manufacturer fuse has been blown the manufacturing state will be terminated, thus there is no possibility of resetting the card back into the manufacturing state.

Personalization State

Personalization State is effective from the moment of termination of the manufacturing state until an associated bit in the EEPROM, the so-called Personalization Bit, has been programmed.

In this state, the card's data and keys can be erased by calling the CLEAR CARD command. This command will physically erase EEPROM memory expect from the IC code and manufacturer file. Re-personalization of the card is possible.

In the Personalization State, any write access to Internal Data Files, as well as the read access to the Security File is only possible after the presentation of the correct IC code. The card manufacturer writes the IC code in the Manufacturing State.

The IC is presented to the card in plain, without encryption. The Authentication Process should not be executed prior to programming the correct keys in the Personalization State.

Once the Personalization Bit has been programmed and the Personalization State has this been terminated, there is no possibility of resetting the card back into the personalization state.

User State

User State designates the normal operating mode of the card. There are two types of User States – the User State and the User State – Issuer Mode. The User State is effective from the moment of termination of the personalization state. Most card holder operation should occur in this state.

A submission of the Issuer Code changes the operation mode to Issuer Mode. This privileged mode allows access to certain memory areas, which are otherwise not accessible.

Answer To Select

After receiving the Request for Answer To Select (RATS), the card transmits an Answer to Select (ATS) in compliance with ISO 14443 Part 4

Customizing the ATS

Due to the difference in the firmware architecture of the AOCS3 Contactless and ACOS3 Contact, the ATS of the ACOS3 Contactless can only be modified at the ACS production facilities. Please contact your ACS representatives during ordering for custom TA1 and Historical bytes values.

Customized ATS TA1 Value

The contactless protocol currently has TA1 = 33h as its bit rate capability. This means the card supports 106, 212, 424 kpbs for both directions from PICC to PCD and vice versa. This is stated in ISO 14443 part 4. Section 5.4.4. The ACOS3 Contactless card can support up to 848 kbps by setting TA1 value to 77h.

The solution provider should ensure that the baud rate works with all their existing contactless smart card readers (PCDs) before a volume order of ACOS3 Contactless cards. Please contact your ACS representatives for more information.

Customized ATS for Microsoft Windows Usage

For Windows 7 and above operating systems: Windows automatically attempts to download the smart card's minidriver whenever a smart card is presented to the smart card reader. Since ACOS3 is not intended to conform to Windows default usage, a smart card minidriver is not necessary. However, if the ACOS3 is presented info a system running Windows 7 or later, the operating system may search online for the driver ma give a warning that the "device driver was not successfully installed" for the smart card. There are two ways to solve this issue:

1. Disable smart card plug and play and certificate propagation in Windows.
2. Change the ATS so Windows will recognize the ACOS3 Contactless card to use ACS's Unified Null Driver.

For the first solution, please follow instructions in this Microsoft support link to disable smart card plug and play. This may have be done for every computer that will be used in this system. http://support.microsoft.com/kb/976832 .

For the second solution, ACS has developed a Unified Null driver for ACOS line of smart cards. The Unified Null driver will satisfy the Windows requirement to have a minidriver for the card, hence the warning from Windows every time the card is inserted will no longer appear. The Unified Null Driver can be downloaded automatically from Windows Update if Automatic Updated are turned ON.

In order for Windows to recognize the ACOS3 Contactless card and use the Unified Null Driver, the ATS must be customized, which needs to be done by ACS. Please contact your ACS representative regarding such request.

In the case of the ACOS3 Contactless card, the ATS value will be:

ATS: 08 78 XX B5 02 33 4e 44h

The XX is the value of TA1. The TA1 value can be set to the baud rate that the smart card reader used can support.

EEPROM Memory Management

The user EEPROM memory area provided by the card chip is fully usable for user data storage. There is an additional EEPROM area that stores internal card configuration data.

- The User Data Memory stores the data of the card under the control of the application.
- The internal card configuration data is used by the card operating system to manage card functionalities.

Data Files

Access to both the Internal Data Memory area and the User Data Memory area is possible within the scopes of data files and data records. Data files in the Internal Data Memory area referred to as Internal Data Files. Data files in the User Data Memory are called User Data Files.

Data files are the smallest entity to which individual security attributes can be assigned to control the read and write access to the data stored in the EEPROM.

Data files are of either record type or transparent type.

Data File Access Control

Two security attributes are assigned to each Data File: the Read Security Attribute and the Write Security Attribute. Security attributes define the security conditions that must be fulfilled to allow the respective operation:

- The **Read Security Attribute** controls the read access to the data in a file through the READ RECORD/BINARY command. If the security condition specified in the Read Security Attribute is not fulfilled., the card will reject a READ command to that file.
- The **Write Security Attribute** controls the write access to the data in a file through the WRITE RECORD/BINARY command. If the security condition specified in the Write Security Attribute is not fulfilled, the card will reject a WRITE command to that file.

The Read Security Attribute and the Write Security Attribute for each data file specify which Application Code, if any, were submitted correctly to the card to allow the respective operation, and whether the Issuer Code and/or the PIN code must have been submitted.

A logical OR function applies to the specified Application Codes, AC x, i.e., if more than one Application Code is specified in a security attribute, the security condition is fulfilled if any one of the specified Application Codes has been correctly submitted.

A logical AND function applies to the PIN and the IC code, i.e., if PIN and/or IC are specified in a security attribute, the PIN and/or IC code(s) must have been submitted in addition to the specified Application Codes(s).

Internal Data Files

With exception of the Account Data Structure, which has associated a special set of commands, the memory areas of the Internal Data Memory are processed as data files.

The attributes of the Internal Data Files are defined in the card operating system and cannot be changed. However, the security attributes depend on the card life cycle state.

User Data Files

User Data Files are allocated in the Personalization State of the card life cycle. There are two types of User Data Files, Record and Binary files. Record files are specified by number of records and fixed record length. Binary files are specified by a file size and accessed via offsetting into the file.

The data stored in a User Data File can be read though the READ RECORD/BINARY command and update through the WRITE RECORD/BINARY command when the security conditions associated to the data file are fulfilled.

User Data Files are defined by writing the corresponding File Definition Blocks in the records of the User File Management File during the Personalization State. It is not possible to change the number of records of a file once any of the User Data Files has been used. User will be able to access these data as long as it's within the capacity of the card.

Data File Access

The process of data file access is identical for Internal Data Files and for User Data Files.

Account Data Structure

The Account Data Structure – Account, for short – is dedicated for the use in applications in which a numeric value representing some amount must be securely processed. The Account is stores in the Account File.

In the User State of the cad life cycle, the data in the Account cannot be manipulated by WRITE instructions like the data in User Data Files. A set of dedicated instructions is available for the processing of the Account, i.e. for adding value to and subtracting value from the balance in the Account and for reading the current balance.

Different access conditions can be specified for adding to, subtracting from and reading the Account.

Critical Account operations, for example, CREDIT, are carried out under strict security control conditions.

Security Features

The following security mechanisms are provided by the ACOS3 card operating system:

- DES/3DES and MAC Calculation
- Mutual Authentication and Session Key Generation
- Secret Codes
- Secure Messaging for Data Files
- Secure Account Transaction Processing
- Anti-tearing Mechanism

DES refers to the DEA algorithm for data encryption and decryption as specified in the standard ANSI X3.93. MAC refers to the algorithm for generation of cryptographic checksums (DEA in Cipher Block Chaining mode) as specified in the standard ANSI X3.99.

Mutual Authentication is a process in which bot the card and the Card Accepting Device verify that the respective counterpart is genuine. The Session Key is result of the successful execution of the Mutual Authentication. It is used for data encryption and decryption during a "session". A session is defined as the time between the successful execution of a Mutual Authentication procedure and a reset of the card or the execution of another START SESSION command.

Secret Codes and the PIN code are used to selectively enable access to data stored in the card and to features and functions provided by the card, for example, the READ and WRITE commands.

Secure messaging ensures data transmitted between the card and terminal/server is secured and not susceptible to eavesdropping, replay attack and unauthorized modifications. This is achieved by signing the command and response with a MAC and encrypting command and response data.

The Account Transaction Processing provides mechanism for the secure and auditable manipulation of data in the Account Data Structure, in particular, the balance value.

DES and MAC Calculation

All keys used in DES/3DES and MAC calculation are 8/16 bytes long depending on Single/Triple DES selection in Option Register. The least significant bit of each byte of the key is not used in the calculation and is not interpreted by the card operating.

Mutual Authentication and Session Key Generation

The Mutual Authentication is based on the exchange and mutual verification of secret keys between the Card and the Card Accepting Device. The key exchange is performed in a secure way by use of random numbers and DES/3DES data encryption.

The session key is the final result of the Mutual Authentication process, and it is based on the random numbers of both card and terminal.

The successful completion of the Mutual Authentication is recorded in the card. The resulting Session Key K_S is used for all data encryption and decryption during the same session.

The card maintains and error counter CNT K_T count and limit the number of consecutive unsuccessful executions of the AUTHENTICATE command.

The Card Random Number RND_C is derived in a complex non-predictable mathematical process from the Random Number Seed stored in the Security File. The Random Number Seed is internally updated by the Operating System after each START TRANSACTION command.

Secret Codes

Secret codes stored in the card are used to restrict the access to data stored in user data files and to certain commands provided by the card. Secret codes must be presented to the card to be able to read data from or write to user data files and execute certain privileged card commands.

Secure Messaging

ACOS3 Version 1.07 and above support Secure Messaging (SM) for data files. Secure messaging ensures data transmitted between the card and terminal/server is secured and not susceptible to eavesdropping, replay attack and unauthorized modifications. User data file can be specified that secure messaging is required for READ/WRITE RECORD/BINARY commands. Almost all the other commands can also use secure messaging initiated by the terminal.

The SM employed in ACOS3 both encrypts and signs the data transmitting into and out of the card.

Account Transaction Processing

Associated to the Account are four keys:

- The Credit Key K_{CR}
- The Debit Key K_D
- The Certify Key K_{CF}
- The Revoke Debit Key K_{RD}

The keys are stored in the Account Security File.

The keys are used in the calculation and verification of MAC cryptographic checksums on commands and data exchanged between the card and the Card Accepting Device in the Account processing.

Anti-tearing Mechanism

Anti-tearing mechanism help protects card data and security in the event that the card is suddenly powered down or pulled out during a card operation.

When writing user data into the card, ACOS3's anti-tearing mechanism ensures the operation is performed atomically. That is, data is either completely written or the target writing area is left at its previous state before the write operation. The account data files is protected similarly when performing CREDIT/DEBIT/REVOKE DEBIT commands.

Life Supports Application

These products are not designed for use in life support appliances, devices or systems where malfunction of these products can reasonably be expected to result in personal injury. ACS customer using or selling these products for use in such applications do so on their own risk and agree to fully indemnify ACS for any damages resulting from such improper use or sale.

Contac Information

For additional information please visit http://www.acs.com.hk

For sale inquiry please send e-mail to info@acs.com.hk

Warranty Conditions

A new product purchased in the Alza.cz sales network is guaranteed for 2 years. If you need repair or other services during the warranty period, contact the product seller directly, you must provide the original proof of purchase with the date of purchase.

The following are considered to be a conflict with the warranty conditions, for which the claimed claim may not be recognized:

- Using the product for any purpose other than that for which the product is intended or failing to follow the instructions for maintenance, operation, and service of the product.
- Damage to the product by a natural disaster, the intervention of an unauthorized person or mechanically through the fault of the buyer (e.g., during transport, cleaning by inappropriate means, etc.).
- Natural wear and aging of consumables or components during use (such as batteries, etc.).
- Exposure to adverse external influences, such as sunlight and other radiation or electromagnetic fields, fluid intrusion, object intrusion, mains overvoltage, electrostatic discharge voltage (including lightning), faulty supply or input voltage and inappropriate polarity of this voltage, chemical processes such as used power supplies, etc.
- If anyone has made modifications, modifications, alterations to the design or adaptation to change or extend the functions of the product compared to the purchased design or use of non-original components.

Vážený zákazníku,

Děkujeme vám za zakoupení našeho produktu. Před prvním použitím si prosím pečlivě přečtěte následující pokyny a uschovejte si tento návod k použití pro budoucí použití. Zvláštní pozornost věnujte bezpečnostním pokynům. Pokud máte k přístroji jakékoli dotazy nebo připomínky, obraťte se na zákaznickou linku.

✉ www.alza.cz/kontakt

✆ +420 255 340 111

Dovozce Alza.cz a.s., Jankovcova 1522/53, Holešovice, 170 00 Praha 7, www.alza.cz

Úvod

Účelem tohoto dokumentu je podrobně popsat vlastnosti a funkce bezkontaktní karty ACOS3, univerzálního operačního systému pro čipové karty vyvinutého společností Advanced Card Systems Ltd.

Historie úprav pro bezkontaktní systém ACOS3

listopad 2010 ACOS3 Combi Revize 1.17

- Kontaktní a bezkontaktní duální rozhraní verze ACOS3
- 8 kilobajtů uživatelské paměti
- Zpětná kompatibilita s ATR/ATS a jeho přizpůsobení

červen 2014 ACOS3 Combi Revize 1.25

- Upravený systém ATS pro rychlejší odezvu při vytržení

Technické specifikace

Následují technické vlastnosti bezkontaktní karty ACOS3:

Elektrické

- Provozní napětí: 5V DC +/-10% (třída A) a 3V DC +/- 10% (třída B)
- Maximální napájecí proud: < 10mA
- Ochrana před ESD: ≤4KV

Životní prostředí

- Provozní teplota: -20 °C až 85 °C
- Teplota skladování: -40 °C až 100 °C

Komunikační protokoly

- T=CL s přenosovou rychlostí až 848 kb/s

Paměť

- Kapacita: 8KB
- Výdrž paměti EEPROM: 500 000 cyklů mazání/zápisu
- Uchovávání dat: 20 let

Kryptografické schopnosti

- DES/3DES: 56/112 bitů

Generování náhodných čísel

- RNG v souladu se standardem FIPS 140-2

Zabezpečení souborů

- Pět tajných kódů + kód vydavatele
- PIN kód
- Pár klíčů pro vzájemné ověřování
- Klíč relace založený na náhodných číslech
- Funkce Secure Messaging pro důvěrné a ověřené přenosy dat
- Podpora vysoce zabezpečené elektronické peněženky pro platební aplikace

Dodržování norem

- Shoda s normou ISO 14443 (typ A), části 1,2,3,4

Answer to Select (ATS)

Po přijetí požadavku Request Answer to Select (RATS) ze čtečky karet karta vysílá Answer to Select (ATS) v souladu s normou ISO 14443, část 4.

Následující údaje přenášené v systému ATS:

TL	T0	TA_1	TB_1	TC_1	3 historické bity
08h	78h	33h	B5h	02h	

Řetězec tří (3) bajtů přenášený v historických bajtech je složen takto:

T1	T2	T3
41h	01h	25h

Správa karet

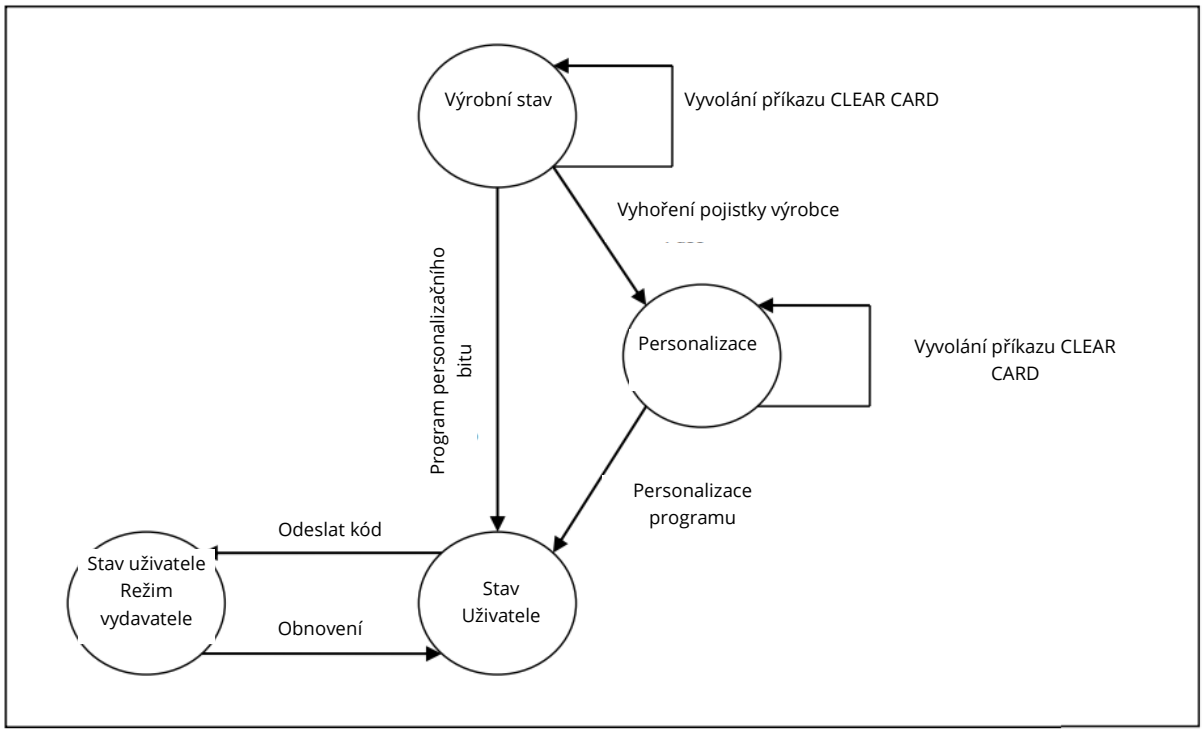
Tento výběr popisuje funkce na úrovni karty a funkce správy.

Stavy životního cyklu karty

Během celého životního cyklu čipové karty lze rozlišit tři fáze a dva různé provozní režimy:

- Výrobní stav
- Stav personalizace
- Stav uživatele
- Stav uživatele - režim vydavatele

Karta se v každém okamžiku nachází v jednom z těchto čtyř stavů. Následující schéma ukazuje možné přechody mezi těmito čtyřmi stavy:



Skutečný stav životního cyklu čipu určuje operační systém karty bezprostředně po resetu. Během provozu karty se stav životního cyklu nemění. Příkaz CLEAR CARD lze vydat ve stavu personalizace a ve stavu výroby, aby se z karty vymazala všechna data kromě údajů výrobce a kódu IC. Tento příkaz však nelze použít do uživatelského stavu.

Výrobní stav

Výrobní stav je platný od okamžiku výroby čipu, dokud není naprogramována přidružená pojistka (tj. určitý bit v paměti EEPROM), Pojistka výrobce.

IC je na kartě prezentován v prosté podobě bez šifrování.

Všechny příkazy jsou k dispozici ve stavu výrobce. Kromě toho lze soubor výrobce (FF01h) zapsat pouze v tomto stavu.

Soubor výrobce obsahuje dva záznamy, každý o 8 bajtech, přiřazené ke stavu výroby. V tomto souboru je obsažena pojistka výrobce. Po naprogramování pojistky výrobce přejde karta do stavu personalizace a soubor výrobce je v režimu pouze pro čtení. Lze naprogramovat údaje jedinečné pro každou kartu a běžné údaje o kartě, například identifikaci výrobce karty, sériové číslo karty atd. Karta tyto údaje neinterpretuje.

V tomto stavu lze data a klíče karty vymazat vyvoláním příkazu CLEAR CARD. Tímto příkazem se fyzicky vymaže paměť EEPROM s výjimkou kódu IC a souboru výrobce.

Jakmile dojde k vyhoření pojistky výrobce, výrobní stav se ukončí, a proto není možné kartu vrátit zpět do výrobního stavu.

Stav personalizace

Stav personalizace je účinný od okamžiku ukončení výrobního stavu, dokud není naprogramován přidružený bit v paměti EEPROM, tzv. personalizační bit.

V tomto stavu lze data a klíče karty vymazat vyvoláním příkazu CLEAR CARD. Tímto příkazem se fyzicky vymaže paměť EEPROM očekávaná od kódu IC a souboru výrobce. Opětovná personalizace karty je možná.

Ve stavu personalizace je jakýkoli přístup k zápisu do interních datových souborů i přístup ke čtení bezpečnostního souboru možný pouze po předložení správného kódu IC. Výrobce karty zapisuje IC kód ve stavu výroby.

IC je na kartě prezentován v prosté podobě bez šifrování. Proces autentizace by neměl být proveden před naprogramováním správných klíčů ve stavu personalizace.

Po naprogramování personalizačního bitu a ukončení stavu personalizace není možné kartu vrátit zpět do stavu personalizace.

Stav uživatele

Uživatelský stav označuje běžný provozní režim karty. Existují dva typy uživatelských stavů - uživatelský stav a uživatelský stav - režim vydavatele. Uživatelský stav je účinný od okamžiku ukončení stavu personalizace. Většina operací držitele karty by měla probíhat v tomto stavu.

Zadání kódu emitenta změní provozní režim na režim emitenta. Tento privilegovaný režim umožňuje přístup k určitým oblastem paměti, které jinak nejsou přístupné.

Answer to Select

Po přijetí požadavku Request Answer to Select (RATS) vysílá karta Answer to Select (ATS) v souladu s normou ISO 14443 část 4.

Přizpůsobení systému ATS

Vzhledem k rozdílům v architektuře firmwaru AOCS3 Contactless a ACOS3 Contact lze ATS ACOS3 Contactless upravovat pouze ve výrobních závodech ACS. Ohledně vlastních hodnot TA1 a historických bajtů se při objednávání obraťte na zástupce společnosti ACS.

Přizpůsobená hodnota ATS TA1

Bezkontaktní protokol má v současné době nastavenou přenosovou rychlost TA1 = 33h. To znamená, že karta podporuje 106, 212, 424 kpbs pro oba směry z PICC do PCD a naopak. To je uvedeno v části 4 normy ISO 14443. Oddíl 5.4.4. Bezkontaktní karta ACOS3 může podporovat až 848 kb/s nastavením hodnoty TA1 na 77h.

Poskytovatel řešení by se měl před hromadnou objednávkou bezkontaktních karet ACOS3 ujistit, že přenosová rychlost funguje se všemi jeho stávajícími čtečkami bezkontaktních čipových karet (PCD). Pro více informací se obraťte na zástupce společnosti ACS.

Přizpůsobená ATS pro používání systému Microsoft Windows

Pro operační systémy Windows 7 a vyšší: Systém Windows se automaticky pokusí stáhnout minidriver čipové karty, kdykoli je čipová karta přiložena ke čtečce čipových karet. Vzhledem k tomu, že ACOS3 není určen k tomu, aby vyhovoval výchozímu použití systému Windows, není minidriver čipové karty nutný. Pokud je však ACOS3 předložen info systému se systémem Windows 7 nebo novějším, může operační systém vyhledat ovladač online ma vydat varování, že "ovladač zařízení nebyl úspěšně nainstalován" pro čipovou kartu. Tento problém lze vyřešit dvěma způsoby:

1. Zakázat plug and play čipových karet a šíření certifikátů v systému Windows.
2. Změňte ATS tak, aby systém Windows rozpoznal bezkontaktní kartu ACOS3 a použil jednotný nulový ovladač ACS.

V případě prvního řešení postupujte podle pokynů uvedených v tomto odkazu podpory společnosti Microsoft a zakažte funkci plug and play u čipových karet. To může být nutné provést pro každý počítač, který bude v tomto systému použit.
http://support.microsoft.com/kb/976832 .

Pro druhé řešení vyvinula společnost ACS ovladač Unified Null pro řadu čipových karet ACOS. Ovladač Unified Null splní požadavek systému Windows na minidriver pro kartu, a proto se již nebude objevovat varování systému Windows při každém vložení karty. Ovladač Unified Null Driver lze automaticky stáhnout ze služby Windows Update, pokud je zapnuta funkce Automatické aktualizace.

Aby systém Windows rozpoznal bezkontaktní kartu ACOS3 a používal jednotný nulový ovladač, musí být systém ATS upraven, což musí provést společnost ACS. S tímto požadavkem se obraťte na svého zástupce společnosti ACS.

V případě bezkontaktní karty ACOS3 bude hodnota ATS:

ATS: 08 78 XX B5 02 33 4e 44h

XX je hodnota TA1. Hodnotu TA1 lze nastavit na přenosovou rychlost, kterou podporuje použitá čtečka čipových karet.

Správa paměti EEPROM

Uživatelská paměť EEPROM, kterou poskytuje čip karty, je plně využitelná pro ukládání uživatelských dat. K dispozici je další oblast EEPROM, do které se ukládají interní konfigurační data karty.

- Paměť uživatelských dat uchovává data karty pod kontrolou aplikace.
- Interní konfigurační data karty používá operační systém karty ke správě funkcí karty.

Datové soubory

Přístup do oblasti interní datové paměti i do oblasti uživatelské datové paměti je možný v rámci datových souborů a datových záznamů. Datové soubory v oblasti interní datové paměti se označují jako interní datové soubory. Datové soubory v oblasti uživatelské datové paměti se nazývají uživatelské datové soubory.

Datové soubory jsou nejmenší entitou, které lze přiřadit jednotlivé bezpečnostní atributy pro řízení přístupu ke čtení a zápisu dat uložených v paměti EEPROM.

Datové soubory jsou buď typu záznam, nebo transparentní.

Řízení přístupu k datovým souborům

Každému datovému souboru jsou přiřazeny dva atributy zabezpečení: atribut zabezpečení čtení a atribut zabezpečení zápisu. Bezpečnostní atributy definují bezpečnostní podmínky, které musí být splněny, aby byla povolena příslušná operace:

- **Atribut zabezpečení čtení** řídí přístup ke čtení dat v souboru prostřednictvím příkazu READ RECORD/BINARY. Pokud není splněna bezpečnostní podmínka zadaná v atributu Read Security, karta příkaz READ k tomuto souboru odmítne.
- **Atribut zabezpečení zápisu** řídí přístup k datům v souboru prostřednictvím příkazu WRITE RECORD/BINARY. Pokud není splněna bezpečnostní podmínka zadaná v atributu zabezpečení zápisu, karta příkaz WRITE do daného souboru odmítne.

Bezpečnostní atribut pro čtení a bezpečnostní atribut pro zápis každého datového souboru určují, který kód aplikace byl případně na kartě správně zadán, aby bylo možné provést příslušnou operaci, a zda musel být zadán kód vydavatele a/nebo kód PIN.

Pro zadané kódy žádostí platí funkce logického OR, AC x, tj. pokud je v bezpečnostním atributu uveden více než jeden kód žádosti, je bezpečnostní podmínka splněna, pokud byl správně předložen některý ze zadaných kódů žádosti.

Na kód PIN a kód IC se vztahuje logická funkce AND, tj. pokud je v bezpečnostním atributu uveden kód PIN a/nebo IC, musí být kromě uvedených kódů aplikace předložen i kód PIN a/nebo IC.

Interní datové soubory

S výjimkou datové struktury účtu, která má přidruženou zvláštní sadu příkazů, se paměťové oblasti interní datové paměti zpracovávají jako datové soubory.

Atributy interních datových souborů jsou definovány v operačním systému karty a nelze je měnit. Bezpečnostní atributy však závisí na stavu životního cyklu karty.

Soubory uživatelských dat

Soubory uživatelských dat se přidělují ve stavu personalizace životního cyklu karty. Existují dva typy uživatelských datových souborů, záznamové a binární soubory. Záznamové soubory jsou specifikovány počtem záznamů a pevnou délkou záznamu. Binární soubory jsou specifikovány velikostí souboru a jsou přístupné prostřednictvím odsazení do souboru.

Data uložená v uživatelském datovém souboru lze číst příkazem READ RECORD/BINARY a aktualizovat příkazem WRITE RECORD/BINARY, pokud jsou splněny bezpečnostní podmínky přiřazené datovému souboru.

Uživatelské datové soubory se definují zápisem odpovídajících bloků definice souborů do záznamů souboru správy uživatelských souborů během stavu personalizace. Po použití některého z uživatelských datových souborů není možné měnit počet záznamů souboru. Uživatel bude mít k těmto datům přístup, pokud to bude v rámci kapacity karty.

Přístup k datovým souborům

Proces přístupu k datovým souborům je stejný pro interní datové soubory i pro uživatelské datové soubory.

Struktura dat účtu

Datová struktura Účet - zkráceně Účet - je určena pro použití v aplikacích, ve kterých je třeba bezpečně zpracovat číselnou hodnotu představující určitou částku. Účet je uložen v souboru Účet.

V uživatelském stavu životního cyklu karty nelze s daty v účtu manipulovat pomocí příkazů WRITE jako s daty v uživatelských datových souborech. Pro zpracování Účtu, tj. pro přičítání hodnot k zůstatku na Účtu a odečítání hodnot od něj a pro čtení aktuálního zůstatku, je k dispozici sada specializovaných instrukcí.

Pro přičítání, odečítání a čtení účtu lze zadat různé podmínky přístupu.

Kritické operace na účtu, například CREDIT, se provádějí za přísných bezpečnostních kontrolních podmínek.

Bezpečnostní prvky

Operační systém karty ACOS3 poskytuje následující bezpečnostní mechanismy:

- Výpočet DES/3DES a MAC
- Vzájemné ověřování a generování klíčů relací
- Tajné kódy
- Zabezpečené zasílání zpráv pro datové soubory
- Bezpečné zpracování transakcí na účtu
- Mechanismus proti roztržení

DES označuje algoritmus DEA pro šifrování a dešifrování dat podle normy ANSI X3.93. MAC označuje algoritmus pro generování kryptografických kontrolních součtů (DEA v režimu Cipher Block Chaining), jak je specifikováno v normě ANSI X3.99.

Vzájemné ověřování je proces, při kterém bot karta a zařízení akceptující kartu ověřují, zda je příslušný protějšek pravý. Výsledkem úspěšného provedení vzájemného ověření je klíč relace. Používá se k šifrování a dešifrování dat během "relace". Relace je definována jako doba mezi úspěšným provedením postupu vzájemného ověřování a resetem karty nebo provedením jiného příkazu START SESSION.

Tajné kódy a kód PIN slouží k selektivnímu přístupu k datům uloženým na kartě a k funkcím a vlastnostem karty, například k příkazům READ a WRITE.

Zabezpečený přenos zpráv zajišťuje, že data přenášená mezi kartou a terminálem/serverem jsou zabezpečená a nejsou náchylná k odposlechu, opakovanému útoku a neoprávněným úpravám. Toho je dosaženo podepsáním příkazu a odpovědi pomocí MAC a zašifrováním dat příkazu a odpovědi.

Zpracování transakcí na účtu poskytuje mechanismus pro bezpečnou a kontrolovatelnou manipulaci s údaji ve struktuře údajů o účtu, zejména s hodnotou zůstatku.

Výpočet DES a MAC

Všechny klíče používané při výpočtu DES/3DES a MAC mají délku 8/16 bajtů v závislosti na volbě Single/Triple DES v Option Register. Nejméně významný bit každého bajtu klíče se při výpočtu nepoužívá a obsluha karty jej neinterpretuje.

Vzájemné ověřování a generování klíčů relací

Vzájemné ověřování je založeno na výměně a vzájemném ověřování tajných klíčů mezi kartou a zařízením přijímajícím kartu. Výměna klíčů se provádí bezpečným způsobem pomocí náhodných čísel a šifrování dat DES/3DES.

Klíč relace je konečným výsledkem procesu vzájemného ověřování a je založen na náhodných číslech karty i terminálu.

Úspěšné dokončení vzájemného ověřování je zaznamenáno na kartě. Výsledný klíč relace K_S se používá pro všechna šifrování a dešifrování dat během téže relace.

Karta udržuje a počítadlo chyb CNT K_T počítá a omezuje počet po sobě jdoucích neúspěšných provedení příkazu AUTHENTICATE.

Náhodné číslo karty RND_C je odvozeno složitým nepředvídatelným matematickým procesem z náhodného čísla Seed uloženého v bezpečnostním souboru. Náhodné číslo Seed je interně aktualizováno operačním systémem po každém příkazu START TRANSACTION.

Tajné kódy

Tajné kódy uložené na kartě slouží k omezení přístupu k datům uloženým v uživatelských datových souborech a k určitým příkazům poskytovaným kartou. Aby bylo možné číst data z uživatelských datových souborů nebo do nich zapisovat a provádět určité privilegované příkazy karty, je třeba kartě předložit tajné kódy.

Zabezpečené zasílání zpráv

ACOS3 verze 1.07 a vyšší podporuje Secure Messaging (SM) pro datové soubory. Zabezpečené zasílání zpráv zajišťuje, že data přenášená mezi kartou a terminálem/serverem jsou zabezpečena a nejsou náchylná k odposlechu, opakovanému útoku a neoprávněným úpravám. U uživatelského datového souboru lze určit, že pro příkazy READ/WRITE RECORD/BINARY je vyžadováno bezpečné zasílání zpráv. Téměř všechny ostatní příkazy mohou rovněž používat zabezpečené zasílání zpráv iniciované terminálem.

Systém SM použitý v systému ACOS3 šifruje a podepisuje data přenášená do karty a z karty.

Zpracování transakcí na účtu

K účtu jsou přiřazeny čtyři klíče:

- Kreditní klíč K_{CR}
- Debetní klíč K_D
- Certifikační klíč K_{CF}
- Klíč Revoke Debit K_{RD}

Klíče jsou uloženy v souboru zabezpečení účtu.

Klíče se používají při výpočtu a ověřování kryptografických kontrolních součtů MAC na příkazech a datech vyměňovaných mezi kartou a zařízením přijímajícím karty při zpracování účtu.

Mechanismus proti vytržení

Mechanismus proti vytržení pomáhá chránit data a zabezpečení karty v případě, že dojde k náhlému vypnutí nebo vytažení karty během operace s kartou.

Při zápisu uživatelských dat na kartu zajišťuje mechanismus ACOS3 proti vytržení, že operace probíhá atomicky. To znamená, že data jsou buď zcela zapsána, nebo je cílová oblast zápisu ponechána v předchozím stavu před operací zápisu. Podobně jsou chráněny soubory s údaji o účtu při provádění příkazů CREDIT/DEBIT/REVOKE DEBIT.

Aplikace Life Supports

Tyto výrobky nejsou určeny pro použití v přístrojích, zařízeních nebo systémech pro podporu života, kde lze důvodně očekávat, že porucha těchto výrobků může mít za následek zranění osob. Zákazník společnosti ACS, který používá nebo prodává tyto výrobky pro použití v takových aplikacích, tak činí na vlastní riziko a souhlasí s tím, že plně odškodní společnost ACS za jakékoli škody vzniklé v důsledku takového nesprávného použití nebo prodeje.

Informace o společnosti Contac

Další informace naleznete na adrese http://www.acs.com.hk

Dotaz na prodej zašlete na e-mailovou adresu info@acs.com.hk.

Záruční podmínky

Na nový výrobek zakoupený v prodejní síti Alza.cz se vztahuje záruka 2 roky. V případě potřeby opravy nebo jiného servisu v záruční době se obraťte přímo na prodejce výrobku, je nutné předložit originální doklad o koupi s datem nákupu.

Za rozpor se záručními podmínkami, pro který nelze reklamaci uznat, se považují následující skutečnosti:

- Používání výrobku k jinému účelu, než pro který je výrobek určen, nebo nedodržování pokynů pro údržbu, provoz a servis výrobku.
- Poškození výrobku živelnou pohromou, zásahem neoprávněné osoby nebo mechanicky vinou kupujícího (např. při přepravě, čištění nevhodnými prostředky apod.).
- přirozené opotřebení a stárnutí spotřebního materiálu nebo součástí během používání (např. baterií atd.).
- Působení nepříznivých vnějších vlivů, jako je sluneční záření a jiné záření nebo elektromagnetické pole, vniknutí kapaliny, vniknutí předmětu, přepětí v síti, elektrostatický výboj (včetně blesku), vadné napájecí nebo vstupní napětí a nevhodná polarita tohoto napětí, chemické procesy, např. použité zdroje atd.

Pokud někdo provedl úpravy, modifikace, změny konstrukce nebo adaptace za účelem změny nebo rozšíření funkcí výrobku oproti zakoupené konstrukci nebo použití neoriginálních součástí.

Vážený zákazník,

ďakujeme vám za zakúpenie nášho výrobku. Pred prvým použitím si pozorne prečítajte nasledujúce pokyny a uschovajte si tento návod na použitie. Venujte osobitnú pozornosť bezpečnostným pokynom. Ak máte akékoľvek otázky alebo pripomienky k prístroju, obráťte sa na linku služieb zákazníkom.

✉ www.alza.sk/kontakt

✆ +421 257 101 800

Dovozca Alza.cz a.s., Jankovcova 1522/53, Holešovice, 170 00 Praha 7, www.alza.cz

Úvod

Účelom tohto dokumentu je podrobne opísať vlastnosti a funkcie bezkontaktnej karty ACOS3, univerzálneho operačného systému pre čipové karty, ktorý vyvinula spoločnosť Advanced Card Systems Ltd.

História úprav bezkontaktného systému ACOS3

November 2010 ACOS3 Combi Revízia 1.17

- Kontaktné a bezkontaktné duálne rozhranie ACOS3
- 8 kilobajtov používateľskej pamäte
- Spätná kompatibilita s ATR/ATS a jej prispôsobenie

jún 2014 ACOS3 Combi Revízia 1.25

- Upravený systém ATS na rýchlejšiu odozvu pri roztrhnutí

Technická špecifikácia

Nasledujú technické vlastnosti bezkontaktnej karty ACOS3:

Elektrické

- Prevádzkové napätie: 5V DC +/-10% (trieda A) a 3V DC +/- 10% (trieda B)
- Maximálny napájací prúd: < 10 mA
- Ochrana pred ESD: ≤4KV

Životné prostredie

- Prevádzková teplota: -20 °C až 85 °C
- Teplota skladovania: -40 °C až 100 °C

Komunikačné protokoly

- T=CL s prenosovou rýchlosťou do 848 kb/s

Pamäť

- Kapacita: 8KB
- Životnosť pamäte EEPROM: 500 000 cyklov vymazania/zápisu
- Uchovávanie údajov: 20 rokov

Kryptografické zručnosti

- DES/3DES: 56/112 bitov

Generovanie náhodných čísel

- RNG v súlade s FIPS 140-2

Zabezpečenie súborov

- Päť tajných kódov + kód emitenta
- PIN kód
- Niekoľko kľúčov pre vzájomné overovanie
- Kľúč relácie založený na náhodných číslach
- Zabezpečené posielanie správ na dôverné a overené prenosy údajov
- Vysoko bezpečná podpora elektronických peňaženiek pre platobné aplikácie

Dodržiavanie noriem

- Súlad s normou ISO 14443 (typ A), časti 1,2,3,4

Odpoveď na Vybrať (ATS)

Po prijatí požiadavky na odpoveď na výber (RATS) z čítačky kariet karta vysiela odpoveď na výber (ATS) v súlade s normou ISO 14443, časť 4.

Nasledujúce údaje prenášané v systéme ATS:

TL	T0	TA_1	TB_1	TC_1	3 historické apartmány
08h	78h	33h	B5h	02h	

Reťazec troch (3) bajtov prenášaných v historických bajtoch sa skladá takto:

T1	T2	T3
41h	01h	25h

Správa kariet

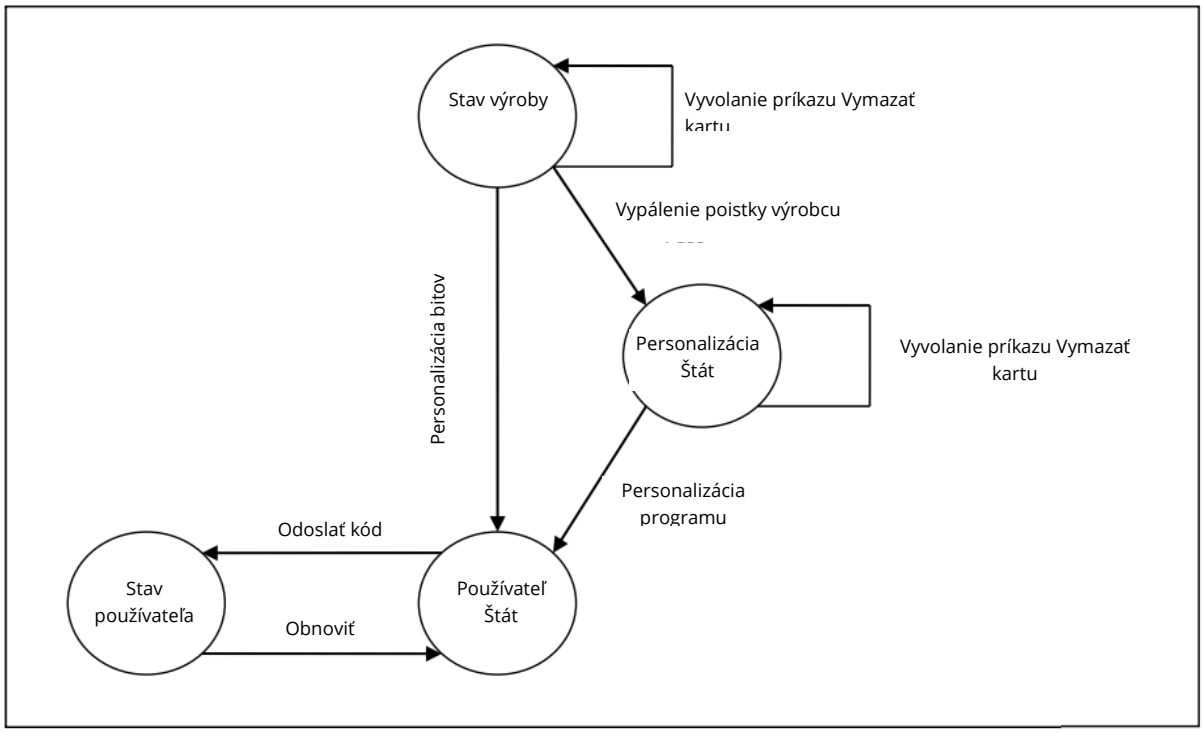
Tento výber popisuje funkcie na úrovni karty a funkcie správy.

Stavy životného cyklu karty

Počas životného cyklu čipovej karty možno rozlíšiť tri fázy a dva rôzne prevádzkové režimy:

- Stav výroby
- Stav personalizácie
- Stav používateľa
- Stav používateľa - režim vydavateľa

Karta je v každom okamihu v jednom z týchto štyroch stavov. Nasledujúci diagram znázorňuje možné prechody medzi týmito štyrmi stavmi:



Skutočný stav životného cyklu čipu určuje operačný systém karty ihneď po resetovaní. Stav životného cyklu sa počas prevádzky karty nemení. Príkaz CLEAR CARD možno vydať v stave personalizácie a v stave výroby na vymazanie všetkých údajov z karty okrem údajov výrobcu a IC kódu. Tento príkaz však nemožno použiť na stav používateľa.

Stav výroby

Výrobný stav je platný od okamihu výroby čipu až do naprogramovania príslušnej poistky (t. j. špecifického bitu v pamäti EEPROM), Manufacturer Fuse.

IC je na karte uvedený v jednoduchej podobe bez šifrovania.

Všetky príkazy sú k dispozícii v stave výrobcu. Okrem toho sa súbor výrobcu (FF01h) môže zapisovať len v tomto stave.

Súbor výrobcu obsahuje dva záznamy, každý o veľkosti 8 bajtov, spojené so stavom výroby. V tomto súbore sa nachádza poistka výrobcu. Keď je naprogramovaná poistka výrobcu, karta prejde do stavu personalizácie a súbor výrobcu je v režime len na čítanie. Možno naprogramovať údaje jedinečné pre každú kartu a bežné údaje o karte, ako je identifikácia výrobcu karty, sériové číslo karty atď. Karta tieto údaje neinterpretuje.

V tomto stave je možné údaje karty a kľúče vymazať príkazom CLEAR CARD. Tento príkaz fyzicky vymaže pamäť EEPROM okrem kódu IC a súboru výrobcu.

Po vyhodení poistky výrobcu je výrobný stav ukončený, a preto sa karta nemôže vrátiť do výrobného stavu.

Stav personalizácie

Stav personalizácie je účinný od okamihu ukončenia výrobného stavu až do naprogramovania príslušného bitu v pamäti EEPROM, ktorý sa nazýva personalizačný bit.

V tomto stave je možné údaje karty a kľúče vymazať príkazom CLEAR CARD. Tento príkaz fyzicky vymaže pamäť EEPROM očakávanú od kódu IC a súboru výrobcu. Kartu je možné opätovne personalizovať.

V stave personalizácie je akýkoľvek prístup k zápisu do interných dátových súborov a prístup k čítaniu bezpečnostného súboru možný len po predložení správneho IC kódu. Výrobca karty zapíše IC kód vo výrobnom stave.

IC je na karte uvedený v jednoduchej podobe bez šifrovania. Proces overovania by sa nemal vykonávať pred naprogramovaním správnych kľúčov v stave personalizácie.

Po naprogramovaní personalizačného bitu a opustení stavu personalizácie sa karta nemôže vrátiť do stavu personalizácie.

Stav používateľa

Používateľský stav označuje normálny prevádzkový režim karty. Existujú dva typy stavov používateľa - stav používateľa a stav používateľa - režim vydavateľa. Stav používateľa je účinný od okamihu ukončenia stavu personalizácie. Väčšina operácií držiteľa karty by sa mala uskutočňovať v tomto štáte.

Zadaním kódu emitenta sa prevádzkový režim zmení na režim emitenta. Tento privilegovaný režim umožňuje prístup do určitých oblastí pamäte, ktoré sú inak neprístupné.

Odpoveď na výber

Po prijatí žiadosti o odpoveď na výber (RATS) karta zašle odpoveď na výber (ATS) v súlade s normou ISO 14443 časť 4.

Prispôsobenie systému ATS

Vzhľadom na rozdiely v architektúre firmvéru medzi AOCS3 Contactless a ACOS3 Contact je možné modifikovať ATS ACOS3 Contactless len vo výrobných zariadeniach ACS. Ak chcete získať vlastné hodnoty TA1 a historické bajty, kontaktujte pri objednávke svojho zástupcu spoločnosti ACS.

Prispôsobená hodnota ATS TA1

Bezkontaktný protokol má v súčasnosti nastavenú prenosovú rýchlosť TA1 = 33h. To znamená, že karta podporuje 106, 212, 424 kpbs pre oba smery z PICC do PCD a naopak. Toto je špecifikované v časti 4 normy ISO 14443. Časť 5.4.4 Bezkontaktná karta ACOS3 môže podporovať rýchlosť až 848 kb/s nastavením TA1 na 77h.
Poskytovateľ riešenia by sa mal pred hromadnou objednávkou bezkontaktných kariet ACOS3 uistiť, že prenosová rýchlosť funguje so všetkými jeho existujúcimi čítačkami bezkontaktných čipových kariet (PCD). Ďalšie informácie vám poskytne zástupca spoločnosti ACS.

ATS prispôsobená na používanie v systéme Microsoft Windows

Pre systém Windows 7 a novší: Systém Windows sa automaticky pokúsi stiahnuť minidriver čipovej karty vždy, keď je k čítačke čipových kariet pripojená čipová karta. Keďže systém ACOS3 nie je navrhnutý na štandardné používanie systému Windows, minidriver čipovej karty nie je potrebný. Ak je však systém ACOS3 prezentovaný v systéme info Windows 7 alebo novšom, operačný systém môže hľadať ovládač online ma vydať upozornenie, že "ovládač zariadenia nebol úspešne nainštalovaný" pre čipovú kartu. Tento problém sa dá vyriešiť dvoma spôsobmi:

1. Zakázanie inteligentných kariet plug and play a distribúcie certifikátov v systéme Windows.
2. Zmeňte systém ATS tak, aby systém Windows rozpoznal bezkontaktnú kartu ACOS3 a používal ovládač ACS s jednou nulou.

V prípade prvého riešenia postupujte podľa pokynov v tomto prepojení podpory spoločnosti Microsoft a vypnite funkciu plug and play na čipových kartách. Toto môže byť potrebné vykonať pre každý počítač, ktorý sa bude v tomto systéme používať. http://support.microsoft.com/kb/976832 .

Pre druhé riešenie vyvinula spoločnosť ACS ovládač Unified Null pre rodinu čipových kariet ACOS. Ovládač Unified Null splní požiadavku systému Windows na miniatúrny ovládač pre kartu, a preto sa pri každom vložení karty už nebude zobrazovať varovanie systému Windows. Zjednotený nulový ovládač sa môže automaticky stiahnuť zo služby Windows Update, ak je povolená funkcia automatickej aktualizácie.

Aby systém Windows rozpoznal bezkontaktnú kartu ACOS3 a používal ovládač s jednou nulou, musí sa upraviť systém ATS, čo musí urobiť spoločnosť ACS. S touto požiadavkou sa obráťte na svojho zástupcu ACS.

V prípade bezkontaktnej karty ACOS3 bude hodnota ATS:

ATS: 08 78 XX B5 02 33 4e 44h

XX je hodnota TA1. Hodnotu TA1 možno nastaviť na prenosovú rýchlosť podporovanú použitou čítačkou čipových kariet.

Správa pamäte EEPROM

Používateľská pamäť EEPROM, ktorú poskytuje čip karty, je plne použiteľná na ukladanie používateľských údajov. V pamäti EEPROM sa nachádza ďalšia oblasť, v ktorej sú uložené interné konfiguračné údaje karty.

- V pamäti používateľských údajov sú uložené údaje karty pod kontrolou aplikácie.
- Interné konfiguračné údaje karty používa operačný systém karty na riadenie funkcií karty.

Dátové súbory

Prístup do internej oblasti dátovej pamäte a oblasti užívateľskej dátovej pamäte je možný v rámci dátových súborov a dátových záznamov. Dátové súbory v internej dátovej pamäti sa označujú ako interné dátové súbory. Dátové súbory v oblasti User Data Memory sa nazývajú User Data Files.

Dátové súbory sú najmenšou entitou, ktorej možno priradiť jednotlivé bezpečnostné atribúty na riadenie prístupu na čítanie a zápis údajov uložených v pamäti EEPROM.

Dátové súbory sú buď typu záznam, alebo transparentné.

Riadenie prístupu k dátovým súborom

Každému dátovému súboru sú priradené dva bezpečnostné atribúty: bezpečnostný atribút čítania a bezpečnostný atribút zápisu. Bezpečnostné atribúty definujú bezpečnostné podmienky, ktoré musia byť splnené, aby bola operácia povolená:

- **Bezpečnostný atribút čítania** riadi prístup k čítaniu údajov v súbore prostredníctvom príkazu READ RECORD/BINARY. Ak nie je splnená bezpečnostná podmienka uvedená v atribúte Read Security, karta odmietne príkaz READ do daného súboru.
- **Bezpečnostný atribút zápisu** riadi prístup k údajom v súbore prostredníctvom príkazu WRITE RECORD/BINARY. Ak nie je splnená bezpečnostná podmienka uvedená v atribúte zabezpečenia zápisu, karta odmietne príkaz WRITE do súboru.

Bezpečnostný atribút čítania a bezpečnostný atribút zápisu každého dátového súboru určuje, ktorý kód aplikácie bol prípadne správne zadaný na karte na vykonanie príslušnej operácie a či bolo potrebné zadať kód vydavateľa a/alebo PIN.

Logická funkcia OR, AC x, sa vzťahuje na zadané kódy žiadostí, t. j. ak je v bezpečnostnom atribúte uvedený viac ako jeden kód žiadosti, bezpečnostná podmienka je splnená, ak bol správne predložený ktorýkoľvek zo zadaných kódov žiadosti.

PIN a IC kód podliehajú logickej funkcii AND, t. j. ak je v bezpečnostnom atribúte uvedený PIN a/alebo IC kód, musí sa okrem uvedených aplikačných kódov predložiť aj PIN a/alebo IC kód.

Interné dátové súbory

S výnimkou štruktúry údajov o účte, ku ktorej je priradená samostatná sada príkazov, sa pamäťové oblasti internej dátovej pamäte spracúvajú ako dátové súbory.

Atribúty interných dátových súborov sú definované v operačnom systéme karty a nemožno ich meniť. Bezpečnostné atribúty však závisia od stavu životného cyklu karty.

Súbory používateľských dát

Súbory s údajmi používateľa sa prideľujú v stave personalizácie životného cyklu karty. Existujú dva typy súborov s používateľskými údajmi, súbory so záznamom a binárne súbory. Súbory záznamov sú špecifikované počtom záznamov a pevnou dĺžkou záznamu. Binárne súbory sú špecifikované veľkosťou súboru a sú prístupné prostredníctvom odsadenia do súboru.

Údaje uložené v súbore používateľských údajov možno čítať príkazom READ RECORD/BINARY a aktualizovať príkazom WRITE RECORD/BINARY, ak sú splnené bezpečnostné podmienky priradené k súboru údajov.

Používateľské dátové súbory sa definujú zápisom príslušných blokov definície súborov do záznamov správy používateľských súborov počas stavu personalizácie. Po použití jedného z užívateľských dátových súborov nemôžete zmeniť počet záznamov v súbore. Používateľ bude mať prístup k týmto údajom, ak sú v rámci kapacity karty.

Prístup k dátovým súborom

Proces prístupu k dátovým súborom je rovnaký pre interné dátové súbory a používateľské dátové súbory.

Štruktúra dát účtu

Dátová štruktúra Účet - skrátene Účet - je určená na použitie v aplikáciách, v ktorých je potrebné bezpečne spracovať číselnú hodnotu predstavujúcu určitú sumu. Účet je uložený v súbore Účet.

V používateľskom stave životného cyklu kade nie je možné manipulovať s údajmi účtu pomocou príkazov WRITE ako s údajmi v súboroch používateľských údajov. Na spracovanie účtu, t. j. na pripočítavanie hodnôt k zostatku účtu a odčítavanie hodnôt od neho a na čítanie aktuálneho zostatku, je k dispozícii súbor špecializovaných pokynov.

Pre pridávanie, odoberanie a čítanie účtu možno určiť rôzne podmienky prístupu.

Kritické transakcie na účte, ako napríklad CREDIT, sa vykonávajú za prísnych podmienok bezpečnostnej kontroly.

Bezpečnostné prvky

Operačný systém karty ACOS3 poskytuje tieto bezpečnostné mechanizmy:

- Výpočet DES/3DES a MAC
- Vzájomné overovanie a generovanie kľúča relácie
- Tajné kódy
- Zabezpečené zasielanie správ pre dátové súbory
- Bezpečné spracovanie transakcií na účte
- Mechanizmus proti roztrhnutiu

DES sa vzťahuje na algoritmus DEA na šifrovanie a dešifrovanie údajov podľa normy ANSI X3.93. MAC označuje algoritmus na generovanie kryptografických kontrolných súčtov (DEA v režime Cipher Block Chaining), ako je špecifikované v norme ANSI X3.99.

Vzájomná autentifikácia je proces, pri ktorom botová karta a zariadenie akceptujúce kartu overujú, či je zodpovedajúci partner pravý. Výsledkom úspešného vzájomného overenia je kľúč relácie. Používa sa na šifrovanie a dešifrovanie údajov počas "relácie". Relácia je definovaná ako čas medzi úspešným vykonaním postupu vzájomného overovania a resetom karty alebo vykonaním ďalšieho príkazu START SESSION.

Tajné kódy a PIN sa používajú na selektívny prístup k údajom uloženým na karte a k funkciám a vlastnostiam karty, ako sú príkazy READ a WRITE.

Zabezpečený prenos správ zabezpečuje, že údaje prenášané medzi kartou a terminálom/serverom sú bezpečné a nie sú náchylné na odpočúvanie, opakované útoky a neoprávnené modifikácie. To sa dosiahne podpísaním príkazu a odpovede pomocou MAC a zašifrovaním údajov príkazu a odpovede.

Spracovanie transakcií na účte poskytuje mechanizmus na bezpečnú a kontrolovateľnú manipuláciu s údajmi v štruktúre údajov účtu, najmä s hodnotou zostatku.

Výpočet DES a MAC

Všetky kľúče použité pri výpočte DES/3DES a MAC majú dĺžku 8/16 bajtov v závislosti od možnosti Single/Triple DES v registri Option Register. Najmenej významný bit každého bajtu kľúča sa pri výpočte nepoužíva a operátor karty ho neinterpretuje.

Vzájomné overovanie a generovanie kľúča relácie

Vzájomné overovanie je založené na výmene a vzájomnom overovaní tajných kľúčov medzi kartou a zariadením, ktoré kartu prijíma. Výmena kľúčov sa vykonáva bezpečným spôsobom s použitím náhodných čísel a šifrovania údajov DES/3DES.

Kľúč relácie je konečným výsledkom procesu vzájomného overovania a je založený na náhodných číslach karty aj terminálu.

Úspešné ukončenie vzájomného overovania sa zaznamená na karte. Výsledný kľúč relácie K_S sa používa na všetky šifrovania a dešifrovania údajov počas tej istej relácie.

Karta udržiava a počítadlo chýb CNT K_T počíta a obmedzuje počet po sebe nasledujúcich neúspešných vykonaní príkazu AUTHENTICATE.

Náhodné číslo karty RND_C sa získava zložitým nepredvídateľným matematickým procesom z náhodného čísla Seed uloženého v bezpečnostnom súbore. Náhodné číslo Seed je interne aktualizované operačným systémom po každom príkaze START TRANSACTION.

Tajné kódy

Tajné kódy uložené na karte sa používajú na obmedzenie prístupu k údajom uloženým v súboroch s údajmi používateľa a k určitým príkazom poskytovaným kartou. Aby bolo možné čítať z používateľských dátových súborov alebo do nich zapisovať a vykonávať určité privilegované príkazy karty, je potrebné predložiť karte tajné kódy.

Zabezpečené zasielanie správ

ACOS3 verzie 1.07 a vyššie podporuje Secure Messaging (SM) pre dátové súbory. Zabezpečený prenos správ zabezpečuje, že údaje prenášané medzi kartou a terminálom/serverom sú bezpečné a nie sú náchylné na odpočúvanie, opakované útoky alebo neoprávnené modifikácie. Pre súbor používateľských údajov možno určiť, že pre príkazy READ/WRITE RECORD/BINARY sa vyžaduje bezpečné zasielanie správ. Takmer všetky ostatné príkazy môžu tiež používať terminálom iniciované bezpečné správy.

Systém SM používaný v systéme ACOS3 šifruje a podpisuje údaje prenášané na kartu a z karty.

Spracovanie transakcií na účte

K účtu sú priradené štyri kľúče:

- Kreditný kľúč K_{CR}
- Debetný kľúč K_D
- Certifikačný kľúč K_{CF}
- Kľúč Revoke Debit K_{RD}

Kľúče sú uložené v súbore zabezpečenia účtu.

Kľúče sa používajú pri výpočte a overovaní kryptografických kontrolných súčtov MAC príkazov a údajov vymieňaných medzi kartou a zariadením prijímajúcim kartu počas spracovania účtu.

Mechanizmus proti roztrhnutiu

Mechanizmus proti vysunutiu pomáha chrániť údaje a bezpečnosť karty v prípade náhleho vypnutia alebo vysunutia karty počas operácie s kartou.

Pri zápise používateľských údajov na kartu zabezpečuje mechanizmus proti roztrhnutiu ACOS3 atómovú operáciu. To znamená, že údaje sa buď úplne zapíšu, alebo sa cieľová oblasť zápisu ponechá v predchádzajúcom stave pred operáciou zápisu. Podobne sú chránené aj súbory s údajmi o účte pri vykonávaní príkazov CREDIT/DEBIT/REVOKE DEBIT.

Aplikácia Life Supports

Tieto výrobky nie sú určené na použitie v prístrojoch, zariadeniach alebo systémoch na podporu života, kde sa dá odôvodnene očakávať, že zlyhanie týchto výrobkov môže mať za následok zranenie osôb. Zákazník spoločnosti ACS, ktorý používa alebo predáva tieto výrobky na použitie v takýchto aplikáciách, tak robí na vlastné riziko a súhlasí s tým, že v plnej miere odškodní spoločnosť ACS za akékoľvek škody vyplývajúce z takéhoto nesprávneho použitia alebo predaja.

Informácie o spoločnosti Contac

Viac informácií nájdete na stránke http://www.acs.com.hk

Otázky týkajúce sa predaja posielajte na adresu info@acs.com.hk.

Záručné podmienky

Na nový výrobok zakúpený v predajnej sieti Alza.sk sa vzťahuje záruka 2 roky. V prípade potreby opravy alebo iného servisu v záručnej dobe sa obráťte priamo na predajcu výrobku, je nutné predložiť originálny doklad o kúpe s dátumom nákupu.

Za rozpor so záručnými podmienkami, pre ktorý nemožno reklamáciu uznať, sa považujú nasledujúce skutočnosti:

- Používanie výrobku na iný účel, než na ktorý je výrobok určený alebo nedodržiavanie pokynov pre údržbu, prevádzku a servis výrobku.
- Poškodenie výrobku živelnou pohromou, zásahom neoprávnenej osoby alebo mechanicky vinou kupujúceho (napr. pri preprave, čistení nevhodnými prostriedkami a pod.).
- Prirodzené opotrebovanie a starnutie spotrebného materiálu alebo súčastí počas používania (napr. batérií atď.).
- Pôsobenie nepriaznivých vonkajších vplyvov, ako je slnečné žiarenie a iné žiarenie alebo elektromagnetické pole, vniknutie kvapaliny, vniknutie predmetu, prepätie v sieti, elektrostatický výboj (vrátane blesku), chybné napájacie alebo vstupné napätie a nevhodná polarita tohto napätia, chemické procesy, napr. použité zdroje atď.

Ak niekto vykonal úpravy, modifikácie, zmeny konštrukcie alebo adaptácie za účelom zmeny alebo rozšírenia funkcií výrobku oproti zakúpenej konštrukcii alebo použitie neoriginálnych súčastí.

Kedves vásárló,

Köszönjük, hogy megvásárolta termékünket. Kérjük, az első használat előtt figyelmesen olvassa el az alábbi utasításokat, és őrizze meg ezt a használati útmutatót a későbbi használatra. Fordítson különös figyelmet a biztonsági utasításokra. Ha bármilyen kérdése vagy észrevétele van a készülékkel kapcsolatban, kérjük, forduljon az ügyfélvonalhoz.

✉ www.alza.hu/kapcsolat

✆ +36-1-701-1111

Importőr Alza.cz a.s., Jankovcova 1522/53, Holešovice, 170 00 Prága 7, www.alza.cz

Bevezetés

E dokumentum célja, hogy részletesen ismertesse az ACOS3 érintésmentes kártya, az Advanced Card Systems Ltd. által kifejlesztett sokoldalú intelligens kártya operációs rendszer jellemzőit és funkcióit.

Az ACOS3 érintésmentes ACOS3 módosításainak története

2010. november ACOS3 Combi 1.17. felülvizsgálat

- Érintkező és érintkező nélküli kettős interfész ACOS3 változat
- 8 Kilobájt felhasználói tárolókapacitás
- Visszafelé kompatibilis az ATR/ATS és annak testreszabhatósága elvárásainak megfelelően

2014. június ACOS3 Combi Revision 1.25

- Módosított ATS a gyorsabb reagálás érdekében.

Műszaki specifikációk

Az alábbiakban az ACOS3 érintésmentes kártya jellemzői és műszaki jellemzői következnek:

Elektromos

- Működési feszültség: 5V DC +/-10% (A osztály) és 3V DC +/- 10% (B osztály)
- Maximális tápáram: < 10mA
- ESD védelem: ≤4KV

Környezetvédelmi

- Működési hőmérséklet: -20°C és 85°C között
- Tárolási hőmérséklet: -40°C és 100° között

Kommunikációs protokollok

- T=CL 848 kbit/s-ig terjedő bauddal

Memória

- Kapacitás: 8KB
- EEPROM tartósság: törlési/írási ciklusok: 500,00
- Adatmegőrzés: 20 év

Kriptográfiai képességek

- DES/3DES: 56/112 bit

Véletlenszám generálás

- FIPS 140-2 szabványnak megfelelő RNG

Fájlbiztonság

- Öt titkos kód + Kibocsátó kódja
- PIN-kód
- Kulcspár a kölcsönös hitelesítéshez
- Munkamenetkulcs véletlen számok alapján
- Biztonságos üzenetküldési funkció a bizalmas és hitelesített adatátvitelhez
- A nagy biztonságú e-Purse támogatása a fizetési alkalmazásokhoz

A szabványoknak való megfelelés

- Megfelelés az ISO 14443 (A típus) 1., 2., 3., 4. részének.

Válasz a kiválasztásra (ATS)

Miután a kártya a kártyaolvasótól megkapta a kiválasztási válaszkérést (RATS), a kártya az ISO 14443 4. részének megfelelően továbbítja a kiválasztási választ (ATS).

Az ATS-ben továbbított következő adatok:

TL	T0	TA_1	TB_1	TC_1	3 történelmi bájtok
08h	78h	33h	B5h	02h	

A történelmi bájtokban továbbított három (3) bájtos karakterlánc a következőképpen épül fel:

T1	T2	T3
41h	01h	25h

Kártyakezelés

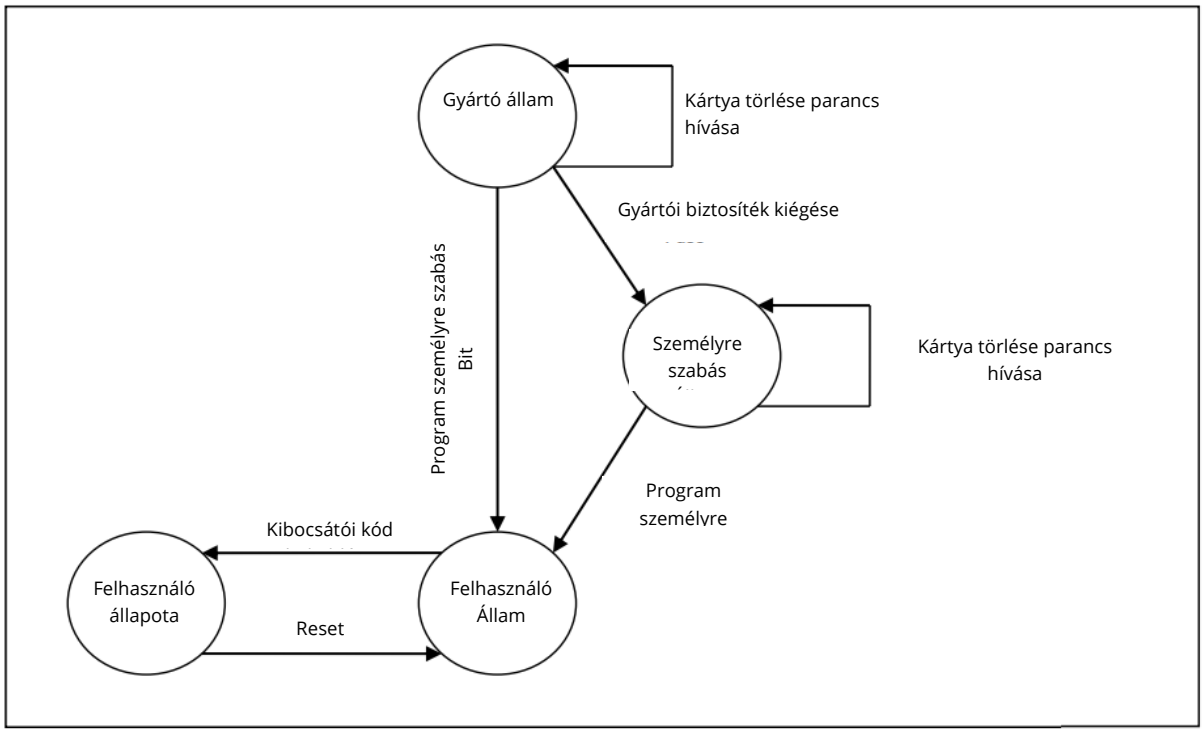
Ez a kiválasztás a kártyaszintű funkciókat és kezelési funkciókat ismerteti.

A kártya életciklusának állapotai

A chipkártya teljes életciklusa során három fázis és két különböző működési mód különböztethető meg:

- Gyártó állam
- Személyre szabás állapota
- Felhasználó állapota
- Felhasználói állapot - Kibocsátó üzemmód

A kártya bármelyik pillanatban e négy állapot valamelyikében van. A következő ábra a négy állapot közötti lehetséges átmeneteket mutatja:



A chip tényleges életciklus-állapotát a kártya operációs rendszere határozza meg közvetlenül a visszaállítás után. Az életciklus állapota a kártya működése során nem változik. A CLEAR CARD parancs a megszemélyesítési és a gyártási állapotban adható ki a kártya minden adatának törléséhez, kivéve a gyártó adatait és az IC-kódot. Ez a parancs azonban nem használható felhasználói állapotba.

Gyártó állam

A Gyártói állapot a chip gyártásának pillanatától addig érvényes, amíg a hozzá tartozó biztosíték (azaz bizonyos bit az EEPROM-ban), a Gyártói biztosíték beprogramozására nem kerül sor.

Az IC-t a kártyán kódolás nélkül, egyszerű formában mutatják be.

Minden parancs elérhető a gyártó állapotában. Ezenkívül a gyártófájl (FF01h) csak ebben az állapotban írható.

A gyártói fájl két, egyenként 8 bájtos rekordot tartalmaz, amelyek a gyártási állapothoz kapcsolódnak. Ebben a fájlban a gyártó biztosítékát tartalmazza. A gyártói biztosíték programozása után a kártya a megszemélyesítési állapotba lép, és a gyártói fájl csak olvasható állapotba kerül. Az egyes kártyákra egyedi és általános kártyaadatok programozhatók, mint például a kártya gyártójának azonosítója, a kártya sorozatszáma stb. A kártya nem értelmezi az adatokat.

Ebben az állapotban a kártya adatai és billentyűi a CLEAR CARD parancs hívásával törölhetők. Ez a parancs fizikailag törli az EEPROM memóriát, kivéve az IC kódot és a gyártó fájlját.

A gyártói biztosíték kialvása után a gyártási állapot megszűnik, így nincs lehetőség a kártya visszaállítására a gyártási állapotba.

Személyre szabás állapota

A személyre szabási állapot a gyártási állapot befejezésének pillanatától addig érvényes, amíg az EEPROM-ban egy kapcsolódó bit, az úgynevezett személyre szabási bit beprogramozására nem kerül sor.

Ebben az állapotban a kártya adatai és billentyűi a CLEAR CARD parancs hívásával törölhetők. Ez a parancs fizikailag törli az EEPROM memóriát az IC kódtól és a gyártó fájljától számítva. A kártya újbóli megszemélyesítése lehetséges.

A megszemélyesítési állapotban a belső adatfájlokhoz való írásbeli hozzáférés, valamint a biztonsági fájlhoz való olvasási hozzáférés csak a megfelelő IC-kód bemutatása után lehetséges. Az IC-kódot a kártya gyártója írja be a gyártási állapotban.

Az IC-t a kártyán kódolás nélkül, egyszerű formában mutatják be. A hitelesítési folyamatot nem szabad végrehajtani a megfelelő kulcsok személyre szabási állapotba történő programozása előtt.

Miután a személyre szabási bitet beprogramozták, és a személyre szabási állapot megszűnt, nincs lehetőség a kártya visszaállítására a személyre szabási állapotba.

Felhasználó állapota

A Felhasználói állapot a kártya normál működési módját jelöli. Kétféle felhasználói állapot létezik: a felhasználói állapot és a felhasználói állapot - kibocsátói üzemmód. A Felhasználói állapot a megszemélyesítési állapot megszűnésének pillanatától hatályos. A kártyabirtokos legtöbb műveletének ebben az állapotban kell történnie.

A Kibocsátói kód megadása a működési módot Kibocsátói módra változtatja. Ez a kiváltságos üzemmód lehetővé teszi a hozzáférést bizonyos, egyébként nem elérhető memóriaterületekhez.

Válasz a kiválasztáshoz

A RATS-kérelem (Request for Answer To Select) fogadása után a kártya az ISO 14443 4. részének megfelelően választási választ (Answer to Select, ATS) küld.

Az ATS testreszabása

Az AOCS3 Contactless és az ACOS3 Contact firmware-architektúrája közötti különbség miatt az ACOS3 Contactless ATS csak az ACS gyártóüzemében módosítható. Kérjük, a megrendelés során vegye fel a kapcsolatot az ACS képviselőivel az egyedi TA1 és a Történelmi bájt értékekért.

Egyedi ATS TA1 érték

Az érintésmentes protokoll bitsebesség-képessége jelenleg TA1 = 33h. Ez azt jelenti, hogy a kártya 106, 212, 424 kpbs-t támogat mindkét irányban a PICC és a PCD között és fordítva. Ezt az ISO 14443 szabvány 4. része tartalmazza. 5.4.4. szakasz. Az ACOS3 érintésmentes kártya a TA1 érték 77h-ra történő beállításával akár 848 kbps sebességet is támogathat.

A megoldásszállítónak az ACOS3 érintésmentes kártyák sorozatos megrendelése előtt meg kell győződnie arról, hogy a baud-sebesség működik az összes meglévő érintésmentes intelligens kártyaolvasójával (PCD). További információért forduljon az ACS képviselőihez.

Testreszabott ATS a Microsoft Windows használatához

Windows 7 és magasabb operációs rendszerekhez: A Windows automatikusan megpróbálja letölteni az intelligens kártya minidrivert, amikor egy intelligens kártyát bemutatnak az intelligens kártyaolvasónak. Mivel az ACOS3 nem a Windows alapértelmezett használatához igazodik, nincs szükség chipkártya-minidriverre. Ha azonban az ACOS3-at egy Windows 7 vagy újabb Windows rendszert futtató rendszerre mutatják be, az operációs rendszer az interneten keresheti az illesztőprogramot, és figyelmeztetést adhat, hogy az "eszközillesztőprogram nem lett sikeresen telepítve" az intelligens kártyához. Ezt a problémát kétféleképpen lehet megoldani:

1. Az intelligens kártya plug and play és a tanúsítványok terjesztésének letiltása a Windowsban.
2. Módosítsa az ATS-t, hogy a Windows felismerje az ACOS3 érintésmentes kártyát, hogy az ACS Unified Null Driver-t használja.

Az első megoldáshoz kövesse a Microsoft támogatási linkjének utasításait az intelligens kártya plug and play letiltásához. Ezt minden olyan számítógépen meg kell tenni, amelyet ebben a rendszerben használni fognak.
http://support.microsoft.com/kb/976832 .

A második megoldáshoz az ACS kifejlesztett egy Unified Null illesztőprogramot az ACOS intelligens kártyákhoz. Az Unified Null illesztőprogram megfelel a Windows azon követelményének, hogy a kártyához minidriverrel kell rendelkeznie, így a Windows minden egyes alkalommal, amikor a kártyát behelyezi, nem jelenik meg többé a figyelmeztetés. Az Unified Null illesztőprogram automatikusan letölthető a Windows Update-ről, ha az Automatikus frissítés be van kapcsolva.

Annak érdekében, hogy a Windows felismerje az ACOS3 érintésmentes kártyát és használja az Unified Null illesztőprogramot, az ATS-t testre kell szabni, amit az ACS-nek kell elvégeznie. Kérjük, vegye fel a kapcsolatot az ACS képviselőjével az ilyen kéréssel kapcsolatban.

Az ACOS3 érintésmentes kártya esetében az ATS értéke a következő:

ATS: 08 78 XX B5 02 33 4e 44h

A XX a TA1 értéke. A TA1 értéket arra a baud-rátaértékre lehet beállítani, amelyet a használt intelligens kártyaolvasó támogat.

EEPROM memória kezelése

A kártyachip által biztosított felhasználói EEPROM memóriaterület teljes mértékben használható a felhasználói adatok tárolására. Van egy további EEPROM terület, amely a kártya belső konfigurációs adatait tárolja.

- A felhasználói adatmemória tárolja a kártya adatait az alkalmazás ellenőrzése alatt.
- A kártya belső konfigurációs adatait a kártya operációs rendszere használja a kártya funkcióinak kezelésére.

Adatfájlok

Az adatfájlok és adatrekordok hatókörén belül mind a belső adatmemória területhez, mind a felhasználói adatmemória területhez való hozzáférés lehetséges. A Belső adatmemória területen található adatfájlokat Belső adatfájloknak nevezzük. A felhasználói adatmemória területén lévő adatfájlokat felhasználói adatfájloknak nevezzük.
Az adatfájlok a legkisebb egység, amelyhez egyedi biztonsági attribútumok rendelhetők az EEPROM-ban tárolt adatokhoz való olvasási és írási hozzáférés ellenőrzésére.
Az adatfájlok rekord típusúak vagy átlátszó típusúak.

Adatfájlok hozzáférésének ellenőrzése

Minden egyes adatfájlhoz két biztonsági attribútum van hozzárendelve: az Olvasás biztonsági attribútum és az Írás biztonsági attribútum. A biztonsági attribútumok határozzák meg azokat a biztonsági feltételeket, amelyeknek teljesülniük kell az adott művelet engedélyezéséhez:

- Az **Olvasás biztonsági attribútum a** READ RECORD/BINARY parancson keresztül szabályozza a fájlban lévő adatokhoz való olvasási hozzáférést. Ha az Olvasás biztonsági attribútumban meghatározott biztonsági feltétel nem teljesül, a kártya elutasítja az adott fájlra vonatkozó READ parancsot.
- Az **Írásbiztonsági attribútum a** WRITE RECORD/BINARY parancson keresztül szabályozza a fájlban lévő adatokhoz való írási hozzáférést. Ha a Write Security Attribute attribútumban meghatározott biztonsági feltétel nem teljesül, a kártya elutasítja az adott fájlra vonatkozó WRITE parancsot.

Az egyes adatfájlok biztonsági olvasási és írási attribútuma meghatározza, hogy az adott művelet engedélyezéséhez melyik alkalmazási kódot - ha van ilyen - adták meg helyesen a kártyán, és hogy a kibocsátó kódját és/vagy a PIN-kódot be kellett-e adni.

A logikai VAGY függvény a megadott alkalmazási kódokra (AC x) vonatkozik, azaz ha egynél több alkalmazási kód van megadva egy biztonsági attribútumban, a biztonsági feltétel akkor teljesül, ha a megadott alkalmazási kódok bármelyikét helyesen adták meg.

A PIN-kódra és az IC-kódra logikai ÉS függvény vonatkozik, azaz ha a PIN és/vagy IC kódot egy biztonsági attribútumban megadták, akkor a PIN és/vagy IC kód(ok)nak a megadott alkalmazási kód(ok)on kívül a PIN és/vagy IC kód(ok)nak is szerepelnie kell.

Belső adatfájlok

A számla adatszerkezet kivételével, amelyhez egy speciális parancskészlet tartozik, a belső adatmemória memóriaterületei adatfájlokként kerülnek feldolgozásra.

A belső adatfájlok attribútumait a kártya operációs rendszere határozza meg, és azok nem módosíthatók. A biztonsági attribútumok azonban a kártya életciklusának állapotától függnek.

Felhasználói adatfájlok

A felhasználói adatfájlok a kártya életciklusának megszemélyesítési állapotában kerülnek kiosztásra. A felhasználói adatfájloknak két típusa van, a rekord és a bináris fájlok. A rekordfájlokat a rekordok száma és a rögzített rekordhossz határozza meg. A bináris fájlokat a fájlméret határozza meg, és a fájlba való belépés a fájlba történő eltolással történik.

A felhasználói adatfájlban tárolt adatok a READ RECORD/BINARY paranccsal olvashatók, és a WRITE RECORD/BINARY paranccsal frissíthetők, ha az adatfájlhoz kapcsolódó biztonsági feltételek teljesülnek.

A felhasználói adatfájlok meghatározása a megfelelő fájldefiníciós blokkok írásával történik a felhasználói fájlkezelő fájl rekordjaiba a megszemélyesítési állapot során. A fájl rekordjainak számát nem lehet megváltoztatni, ha már valamelyik felhasználói adatfájlt használták. A felhasználó mindaddig hozzáférhet ezekhez az adatokhoz, amíg az a kártya kapacitásán belül van.

Adatfájl-hozzáférés

Az adatfájlokhoz való hozzáférés folyamata a belső adatfájlok és a felhasználói adatfájlok esetében azonos.

Számlaadatok szerkezete

A Számla adatszerkezet - röviden Számla - olyan alkalmazásokban való használatra szolgál, amelyekben valamilyen összeget képviselő numerikus értéket kell biztonságosan feldolgozni. A Számla a Számla fájlban tárolódik.

A cad életciklus felhasználói állapotában a fiókban lévő adatokat nem lehet WRITE utasításokkal manipulálni, mint a felhasználói adatfájlok adatait. A Számla feldolgozására, azaz a Számla egyenlegéhez érték hozzáadására és abból érték kivonására, valamint az aktuális egyenleg leolvasására egy sor külön utasítás áll rendelkezésre.

Különböző hozzáférési feltételek adhatók meg a számlához való hozzáadáshoz, a számlából való kivonáshoz és az olvasáshoz.

A kritikus számlaműveleteket, például a CREDIT-et, szigorú biztonsági ellenőrzési feltételek mellett végzik.

Biztonsági jellemzők

Az ACOS3 kártya operációs rendszere a következő biztonsági mechanizmusokat biztosítja:

- DES/3DES és MAC-számítás
- Kölcsönös hitelesítés és munkamenetkulcs-generálás
- Titkos kódok
- Biztonságos üzenetküldés az adatfájlokhoz
- Biztonságos számlatranzakciók feldolgozása
- Szakadásgátló mechanizmus

A DES az ANSI X3.93 szabványban meghatározott, az adatok titkosítására és visszafejtésére szolgáló DEA algoritmusra utal. A MAC az ANSI X3.99 szabványban meghatározott, kriptográfiai ellenőrző összegek létrehozására szolgáló algoritmusra utal (DEA a Cipher Block Chaining módban).

A kölcsönös hitelesítés olyan folyamat, amelynek során a kártya és a kártyaelfogadó eszköz egyaránt ellenőrzi, hogy a másik fél valódi. A munkamenetkulcs a kölcsönös hitelesítés sikeres végrehajtásának eredménye. Ezt használják az adatok titkosítására és visszafejtésére a "munkamenet" során. A munkamenet a kölcsönös hitelesítési eljárás sikeres végrehajtása és a kártya visszaállítása vagy egy másik START SESSION parancs végrehajtása közötti idő.

A titkos kódok és a PIN-kód a kártyán tárolt adatokhoz és a kártya által biztosított funkciókhoz, például a READ és WRITE parancsokhoz való hozzáférés szelektív engedélyezésére szolgálnak.

A biztonságos üzenetküldés biztosítja, hogy a kártya és a terminál/kiszolgáló között továbbított adatok biztonságban legyenek, és ne legyenek kitéve lehallgatásnak, visszajátszási támadásnak és jogosulatlan módosításoknak. Ez a parancs és a válasz MAC aláírásával, valamint a parancs- és válaszadatok titkosításával érhető el.

A számlatranzakciók feldolgozása mechanizmust biztosít a számlaadatstruktúrában lévő adatok, különösen az egyenlegérték biztonságos és ellenőrizhető manipulációjához.

DES és MAC számítás

A DES/3DES és a MAC számításhoz használt összes kulcs 8/16 bájt hosszú, az Option Registerben lévő Single/Triple DES választástól függően. A kulcs minden egyes bájtjának legalacsonyabb értékű bitjét nem használják fel a számítás során, és a kártya működése nem értelmezi.

Kölcsönös hitelesítés és munkamenetkulcs-generálás

A kölcsönös hitelesítés a kártya és a kártyaelfogadó eszköz közötti titkos kulcsok cseréjén és kölcsönös ellenőrzésén alapul. A kulcscsere biztonságos módon, véletlen számok és DES/3DES adattitkosítás alkalmazásával történik.

A munkamenetkulcs a kölcsönös hitelesítési folyamat végeredménye, amely a kártya és a terminál véletlenszerű számain alapul.

A kölcsönös hitelesítés sikeres befejezését a kártya rögzíti. Az így kapott K_S munkamenetkulcsot használják az összes adattitkosításhoz és -dekódoláshoz ugyanazon munkamenet során.

A kártya fenntartja a CNT K_T hibaszámlálót és korlátozza az AUTHENTICATE parancs egymást követő sikertelen végrehajtásainak számát.

A kártya RND_C véletlenszámát egy összetett, nem megjósolható matematikai folyamat során a biztonsági fájlban tárolt véletlenszám-vetőmagból származtatják. A véletlenszámmagot az operációs rendszer minden START TRANSACTION parancs után belsőleg frissíti.

Titkos kódok

A kártyán tárolt titkos kódok a felhasználói adatfájlokban tárolt adatokhoz és a kártya által biztosított bizonyos parancsokhoz való hozzáférés korlátozására szolgálnak. A titkos kódokat be kell mutatni a kártyának ahhoz, hogy adatokat lehessen olvasni a felhasználói adatfájlokból, illetve írni a felhasználói adatfájlokba, valamint bizonyos kiváltságos kártyaparancsokat lehessen végrehajtani.

Biztonságos üzenetküldés

Az ACOS3 1.07-es és magasabb verziója támogatja a biztonságos üzenetküldést (SM) az adatfájlok számára. A biztonságos üzenetküldés biztosítja, hogy a kártya és a terminál/kiszolgáló között továbbított adatok biztonságban legyenek, és ne legyenek kitéve lehallgatásnak, visszajátszási támadásnak és jogosulatlan módosításoknak. A felhasználói adatfájlban megadható, hogy a READ/WRITE RECORD/BINARY parancsokhoz biztonságos üzenetküldésre van szükség. Szinte az összes többi parancs is használhatja a terminál által kezdeményezett biztonságos üzenetküldést.

Az ACOS3-ban alkalmazott SM titkosítja és aláírja a kártyára érkező és onnan távozó adatokat.

Számlatranzakciók feldolgozása

A fiókhoz négy kulcs tartozik:

- A hitelkulcs K_{CR}
- A terhelési kulcs K_D
- A Certify Key K_{CF}
- A terhelés visszavonása kulcs K_{RD}

A kulcsok a fiókbiztonsági fájlban vannak tárolva.

A kulcsokat a kártya és a kártyaelfogadó eszköz között a számlafeldolgozás során kicserélt parancsok és adatok MAC kriptográfiai ellenőrző összegének kiszámítására és ellenőrzésére használják.

Szakadásgátló mechanizmus

A szakadásgátló mechanizmus segít megvédeni a kártya adatait és a biztonságot abban az esetben, ha a kártyát hirtelen kikapcsolják vagy kihúzzák a kártya működése közben.

A felhasználói adatok kártyára írása során az ACOS3 szakadásgátló mechanizmusa biztosítja, hogy a művelet atomi módon történjen. Azaz az adatok vagy teljesen kiíródnak, vagy az írási célterületet az írási művelet előtti állapotában hagyják. A számla adatfájlok hasonlóan védettek a CREDIT/DEBIT/REVOKE DEBIT parancsok végrehajtásakor.

Alkalmazás támogatás

Ezeket a termékeket nem olyan életfenntartó készülékekben, eszközökben vagy rendszerekben való használatra tervezték, ahol a termékek meghibásodása ésszerűen várhatóan személyi sérülést okozhat. Az ACS ügyfelei, akik ezeket a termékeket ilyen alkalmazásokban való felhasználásra használják vagy értékesítik, ezt saját felelősségükre teszik, és vállalják, hogy teljes mértékben kártalanítják az ACS-t az ilyen nem megfelelő használatból vagy értékesítésből eredő károkért.

Contac információ

További információkért kérjük, látogasson el a http://www.acs.com.hk weboldalra.

Az eladási érdeklődéshez kérjük, küldjön e-mailt a info@acs.com.hk címre.

Jótállási feltételek

Az Alza.cz értékesítési hálózatában vásárolt új termékre 2 év garancia vonatkozik. Ha a garanciális időszak alatt javításra vagy egyéb szolgáltatásra van szüksége, forduljon közvetlenül a termék eladójához, a vásárlás dátumával ellátott eredeti vásárlási bizonylatot kell bemutatnia.

Az alábbiak a jótállási feltételekkel való ellentétnek minősülnek, amelyek miatt az igényelt követelés nem ismerhető el:

- A terméknek a termék rendeltetésétől eltérő célra történő használata, vagy a termék karbantartására, üzemeltetésére és szervizelésére vonatkozó utasítások be nem tartása.
- A termék természeti katasztrófa, illetéktelen személy beavatkozása vagy a vevő hibájából bekövetkezett mechanikai sérülés (pl. szállítás, nem megfelelő eszközökkel történő tisztítás stb. során).
- A fogyóeszközök vagy alkatrészek természetes elhasználódása és öregedése a használat során (pl. akkumulátorok stb.).
- Káros külső hatásoknak való kitettség, például napfény és egyéb sugárzás vagy elektromágneses mezők, folyadék behatolása, tárgyak behatolása, hálózati túlfeszültség, elektrosztatikus kisülési feszültség (beleértve a villámlást), hibás táp- vagy bemeneti feszültség és e feszültség nem megfelelő polaritása, kémiai folyamatok, például használt tápegységek stb.

Ha valaki a termék funkcióinak megváltoztatása vagy bővítése érdekében a megvásárolt konstrukcióhoz képest módosításokat, átalakításokat, változtatásokat végzett a konstrukción vagy adaptációt végzett, vagy nem eredeti alkatrészeket használt.

Sehr geehrter Kunde,

vielen Dank für den Kauf unseres Produkts. Bitte lesen Sie die folgenden Anweisungen vor dem ersten Gebrauch sorgfältig durch und bewahren Sie diese Bedienungsanleitung zum späteren Nachschlagen auf. Beachten Sie insbesondere die Sicherheitshinweise. Wenn Sie Fragen oder Kommentare zum Gerät haben, wenden Sie sich bitte an den Kundenservice.

✉ www.alza.de/kontakt

✆ 0800 181 45 44

✉ www.alza.at/kontakt

✆ +43 720 815 999

Lieferant Alza.cz a.s., Jankovcova 1522/53, Holešovice, 170 00 Prag 7, www.alza.cz

Einführung

In diesem Dokument werden die Merkmale und Funktionen der ACOS3 Contactless Card, eines vielseitigen Chipkarten-Betriebssystems, das von Advanced Card Systems Ltd. entwickelt wurde, im Detail beschrieben.

Geschichte der Modifikationen für ACOS3 Contactless

Nov 2010 ACOS3 Combi Revision 1.17

- Kontakt- und kontaktlose Doppelschnittstelle ACOS3 Version
- 8 Kilobyte Benutzerspeicherkapazität
- Abwärtskompatibel mit ATR/ATS und dessen Anpassung

Juni 2014 ACOS3 Combi Revision 1.25

- Modifiziertes ATS für schnelleres Ansprechen beim Aufreißen

Technische Daten

Nachfolgend finden Sie die Merkmale und technischen Eigenschaften der ACOS3 Contactless Karte:

Elektrisch

- Betriebsspannung: 5V DC +/-10% (Klasse A) und 3V DC +/- 10% (Klasse B)
- Maximaler Versorgungsstrom: < 10mA
- ESD-Schutz: ≤4KV

Rahmenbedingung

- Betriebstemperatur: -20°C bis 85°C
- Lagertemperatur: -40°C bis 100°C

Kommunikationsprotokolle

- T=CL mit Baud bis zu 848kbps

Speicher

- Kapazität: 8KB
- EEPROM-Ausdauer: 500.00 Schreib-/Löschzyklen
- Datenaufbewahrung: 20 Jahre

Kryptographische Fähigkeiten

- DES/3DES: 56/112-Bit

Erzeugung von Zufallszahlen

- FIPS 140-2-konformer RNG

Datei-Sicherheit

- Fünf Geheimcodes + Ausstellerkode
- PIN-Code
- Schlüsselpaar für die gegenseitige Authentifizierung
- Sitzungsschlüssel auf Basis von Zufallszahlen
- Secure Messaging-Funktion für vertrauliche und authentifizierte Datenübertragungen
- Unterstützung für hochsichere e-Purse für Zahlungsanwendungen

Einhaltung von Normen

- Übereinstimmung mit ISO 14443 (Typ A) Teile 1,2,3,4

Antwort an Select (ATS)

Nach dem Empfang einer RATS-Anfrage (Request for Answer to Select) vom Kartenleser sendet die Karte eine ATS-Antwort (Answer to Select) gemäß ISO 14443 Teil 4.

Die folgenden Daten werden im ATS übertragen:

TL	T0	TA_1	TB_1	TC_1	3 Historische Bytes
08h	78h	33h	B5h	02h	

Die drei (3) Bytes lange Zeichenkette, die in den historischen Bytes übertragen wird, setzt sich wie folgt zusammen:

T1	T2	T3
41h	01h	25h

Kartenmanagement

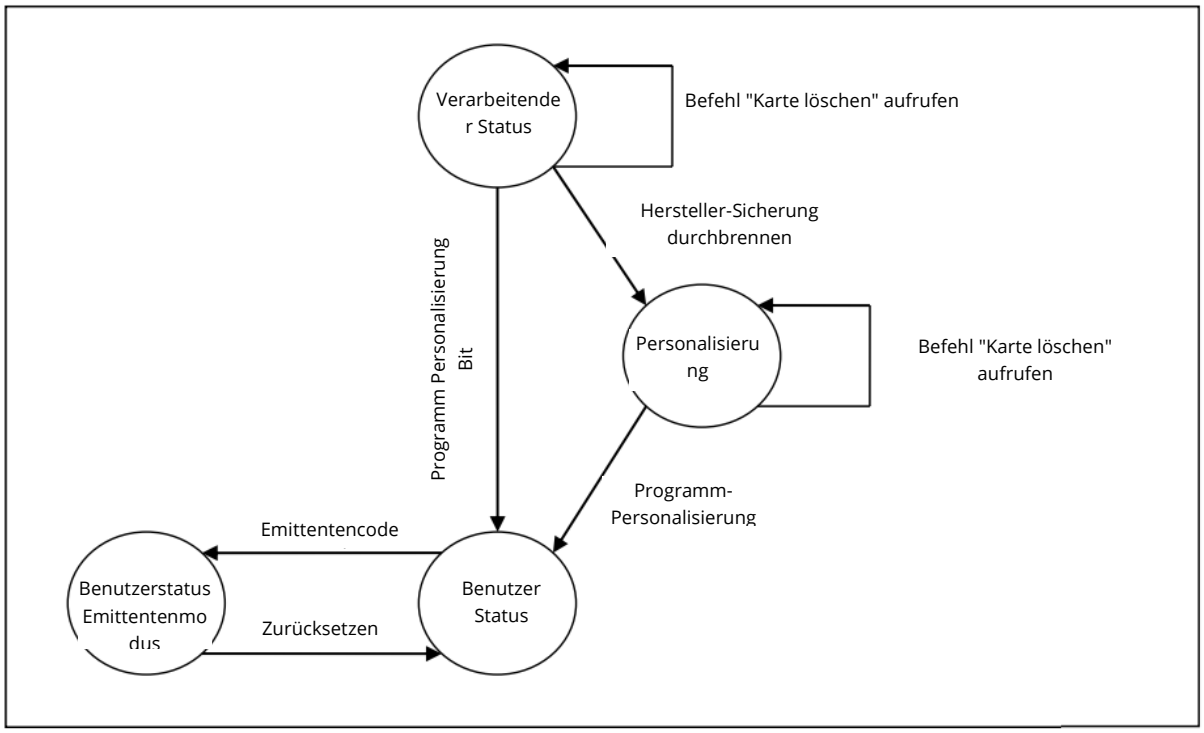
In dieser Auswahl werden die Merkmale und Verwaltungsfunktionen der Kartenebene beschrieben.

Zustände im Lebenszyklus der Karte

Während des gesamten Lebenszyklus der Chipkarte lassen sich drei Phasen und zwei verschiedene Betriebsarten unterscheiden:

- Verarbeitender Status
- Personalisierungsstatus
- Anwenderstatus
- Benutzerstatus - Ausstellermodus

Die Karte befindet sich zu jedem Zeitpunkt in einem dieser vier Zustände. Das folgende Diagramm zeigt die möglichen Übergänge zwischen den vier Zuständen:



Der tatsächliche Lebenszykluszustand des Chips wird vom Betriebssystem der Karte unmittelbar nach einem Reset bestimmt. Während des Betriebs der Karte ändert sich der Lebenszyklusstatus nicht. Der Befehl CLEAR CARD kann im Personalisierungsstatus und im Herstellungsstatus erteilt werden, um die Karte von allen Daten außer den Herstellerdaten und dem IC-Code zu löschen. Dieser Befehl kann jedoch nicht im Benutzerzustand verwendet werden.

Verarbeitender Status

Der Fertigungsstatus gilt ab dem Zeitpunkt der Chipherstellung, bis eine zugehörige Sicherung (d. h. ein bestimmtes Bit im EEPROM), die Hersteller Sicherung, programmiert wurde.

Der IC wird der Karte unverschlüsselt vorgelegt.

Alle Befehle sind im Herstellerstatus verfügbar. Darüber hinaus kann die Herstellerdatei (FF01h) nur in diesem Zustand geschrieben werden.

Die Herstellerdatei enthält zwei Datensätze zu je 8 Byte, die dem Herstellungszustand zugeordnet sind. In dieser Datei ist die Hersteller-Sicherung enthalten. Nach der Programmierung der Herstellersicherung geht die Karte in den Personalisierungsstatus über und die Herstellerdatei ist schreibgeschützt. Es können kartenspezifische Daten und allgemeine Kartendaten programmiert werden, z. B. die Kartenherstelleridentifikation, die Kartenseriennummer usw. Die Karte interpretiert diese Daten nicht.

In diesem Zustand können die Daten und Schlüssel der Karte durch den Aufruf des Befehls CLEAR CARD gelöscht werden. Mit diesem Befehl wird der EEPROM-Speicher mit Ausnahme des IC-Codes und der Herstellerdatei physisch gelöscht.

Wenn die Herstellersicherung durchgebrannt ist, wird der Herstellungszustand beendet, so dass es keine Möglichkeit gibt, die Karte wieder in den Herstellungszustand zurückzusetzen.

Personalisierungsstatus

Der Personalisierungszustand ist ab dem Zeitpunkt der Beendigung des Fertigungszustandes wirksam, bis ein zugehöriges Bit im EEPROM, das sogenannte Personalisierungsbit, programmiert wurde.

In diesem Zustand können die Daten und Tasten der Karte mit dem Befehl CLEAR CARD gelöscht werden. Dieser Befehl löscht den EEPROM-Speicher physisch, abgesehen vom IC-Code und der Herstellerdatei. Eine erneute Personalisierung der Karte ist möglich.

Im Personalisierungsstatus ist ein Schreibzugriff auf interne Datendateien sowie ein Lesezugriff auf die Sicherheitsdatei nur nach Vorlage des korrekten IC-Codes möglich. Der Kartenhersteller schreibt den IC-Code in den Herstellungsstatus.

Der IC wird der Karte in unverschlüsselter Form präsentiert. Der Authentifizierungsprozess sollte nicht vor der Programmierung der richtigen Schlüssel im Personalisierungsstatus ausgeführt werden.

Nach der Programmierung des Personalisierungsbits und der Beendigung des Personalisierungsstatus gibt es keine Möglichkeit, die Karte wieder in den Personalisierungsstatus zurückzusetzen.

Anwenderstatus

Der Benutzerstatus bezeichnet den normalen Betriebsmodus der Karte. Es gibt zwei Arten von Benutzerzuständen - den Benutzerzustand und den Benutzerzustand - Ausgabemodus. Der Benutzerstatus ist ab dem Zeitpunkt der Beendigung des Personalisierungsstatus wirksam. Die meisten Vorgänge des Karteninhabers sollten in diesem Zustand erfolgen.

Durch Eingabe des Issuer Codes wird der Betriebsmodus in den Issuer Mode geändert. Dieser privilegierte Modus erlaubt den Zugriff auf bestimmte Speicherbereiche, die sonst nicht zugänglich sind.

Antwort zum Auswählen

Nach dem Empfang der RATS-Anfrage (Request for Answer To Select) sendet die Karte eine ATS-Antwort (Answer to Select) in Übereinstimmung mit ISO 14443 Teil 4

Anpassen des ATS

Aufgrund der Unterschiede in der Firmware-Architektur des AOCS3 Contactless und des ACOS3 Contact kann das ATS des ACOS3 Contactless nur in den ACS-Produktionsstätten geändert werden. Bitte wenden Sie sich bei der Bestellung an Ihre ACS-Vertretung, um kundenspezifische TA1- und historische Byte-Werte zu erhalten.

Maßgeschneiderter ATS TA1-Wert

Das kontaktlose Protokoll hat derzeit TA1 = 33h als Bitratenfähigkeit. Das bedeutet, dass die Karte 106, 212, 424 kpbs für beide Richtungen von PICC zu PCD und umgekehrt unterstützt. Dies ist in ISO 14443 Teil 4 festgelegt. Abschnitt 5.4.4. Die ACOS3-Kontaktloskarte kann bis zu 848 kpbs unterstützen, indem der TA1-Wert auf 77h gesetzt wird.

Der Lösungsanbieter sollte sich vor einer Großbestellung von ACOS3 Contactless-Karten vergewissern, dass die Baudrate mit allen seinen vorhandenen kontaktlosen Chipkartenlesern (PCDs) funktioniert. Bitte kontaktieren Sie Ihren ACS-Vertreter für weitere Informationen.

Angepasstes ATS für die Verwendung von Microsoft Windows

Für Windows 7 und höhere Betriebssysteme: Windows versucht automatisch, den Minidriver der Smartcard herunterzuladen, sobald eine Smartcard in den Smartcard-Leser eingeführt wird. Da ACOS3 nicht für die standardmäßige Verwendung von Windows vorgesehen ist, ist ein Smartcard-Minidriver nicht erforderlich. Wenn der ACOS3 jedoch an ein System mit Windows 7 oder höher angeschlossen wird, sucht das Betriebssystem möglicherweise online nach dem Treiber und gibt eine Warnung aus, dass der Gerätetreiber für die Chipkarte nicht erfolgreich installiert wurde". Es gibt zwei Möglichkeiten, dieses Problem zu lösen:

1. Deaktivieren Sie Smartcard-Plug-and-Play und Zertifikatsübertragung in Windows.
2. Ändern Sie das ATS, damit Windows die ACOS3 Contactless-Karte erkennt und den Unified Null Driver von ACS verwendet.

Für die erste Lösung folgen Sie bitte den Anweisungen in diesem Microsoft-Support-Link, um Smartcard-Plug & Play zu deaktivieren. Dies muss möglicherweise für jeden Computer, der in diesem System verwendet wird, durchgeführt werden. http://support.microsoft.com/kb/976832.

Für die zweite Lösung hat ACS einen Unified-Null-Treiber für die ACOS-Smartcards entwickelt. Der Unified Null-Treiber erfüllt die Windows-Anforderung, einen Minitreiber für die Karte zu haben, so dass die Warnung von Windows bei jedem Einstecken der Karte nicht mehr erscheint. Der Unified Null-Treiber kann automatisch von Windows Update heruntergeladen werden, wenn die automatische Aktualisierung aktiviert ist.

Damit Windows die ACOS3 Kontaktloskarte erkennt und den Unified Null Driver verwendet, muss das ATS angepasst werden, was von ACS durchgeführt werden muss. Bitte wenden Sie sich diesbezüglich an Ihren ACS-Vertreter.

Im Falle der ACOS3 Contactless-Karte lautet der ATS-Wert:

ATS: 08 78 XX B5 02 33 4e 44h

Die XX ist der Wert von TA1. Der TA1-Wert kann auf die Baudrate eingestellt werden, die der verwendete Chipkartenleser unterstützt.

EEPROM-Speicherverwaltung

Der vom Kartenchip bereitgestellte Benutzer-EEPROM-Speicherbereich ist vollständig für die Speicherung von Benutzerdaten nutzbar. Es gibt einen zusätzlichen EEPROM-Bereich, in dem interne Kartenkonfigurationsdaten gespeichert werden.

- Der Benutzerdatenspeicher speichert die Daten der Karte unter der Kontrolle der Anwendung.
- Die internen Kartenkonfigurationsdaten werden vom Kartenbetriebssystem zur Verwaltung der Kartenfunktionen verwendet.

Daten-Dateien

Im Rahmen von Datendateien und Datensätzen ist der Zugriff sowohl auf den internen Datenspeicher als auch auf den Benutzerdatenspeicher möglich. Datendateien im Bereich des internen Datenspeichers werden als interne Datendateien bezeichnet. Datendateien im Benutzerdatenspeicher werden als Benutzerdatendateien bezeichnet. Datendateien sind die kleinste Einheit, der einzelne Sicherheitsattribute zugewiesen werden können, um den Lese- und Schreibzugriff auf die im EEPROM gespeicherten Daten zu kontrollieren.
Datendateien sind entweder vom Typ Datensatz oder vom Typ transparent.

Zugriffskontrolle für Datendateien

Jeder Datendatei werden zwei Sicherheitsattribute zugewiesen: das Sicherheitsattribut Lesen und das Sicherheitsattribut Schreiben. Die Sicherheitsattribute definieren die Sicherheitsbedingungen, die erfüllt sein müssen, um die jeweilige Operation zu ermöglichen:

- Das **Sicherheitsattribut Lesen** steuert den Lesezugriff auf die Daten in einer Datei über den Befehl READ RECORD/BINARY. Wenn die im Sicherheitsattribut "Lesen" angegebene Sicherheitsbedingung nicht erfüllt ist, weist die Karte einen READ-Befehl für diese Datei zurück.
- Das **Sicherheitsattribut Schreiben** steuert den Schreibzugriff auf die Daten in einer Datei über den Befehl WRITE RECORD/BINARY. Wenn die im Attribut "Schreibsicherheit" angegebene Sicherheitsbedingung nicht erfüllt ist, weist die Karte einen WRITE-Befehl für diese Datei zurück.

Das Sicherheitsattribut "Lesen" und das Sicherheitsattribut "Schreiben" für jede Datendatei geben an, welcher Anwendungscode, falls vorhanden, korrekt an die Karte übermittelt wurde, um den jeweiligen Vorgang zu ermöglichen, und ob der Ausstellerkode und/oder der PIN-Code übermittelt werden müssen.

Für die angegebenen Anwendungscodes AC x gilt eine logische ODER-Funktion, d. h. wenn in einem Sicherheitsattribut mehr als ein Anwendungscode angegeben ist, ist die Sicherheitsbedingung erfüllt, wenn einer der angegebenen Anwendungscodes korrekt übermittelt wurde.

Für den PIN- und den IC-Code gilt eine logische UND-Funktion, d. h. wenn PIN und/oder IC in einem Sicherheitsattribut angegeben sind, müssen der/die PIN- und/oder IC-Code(s) zusätzlich zu dem/den angegebenen Anwendungscode(s) übermittelt worden sein.

Interne Datendateien

Mit Ausnahme der Kontodatenstruktur, der ein spezieller Befehlssatz zugeordnet ist, werden die Speicherbereiche des internen Datenspeichers als Dateien verarbeitet.

Die Attribute der internen Datendateien sind im Betriebssystem der Karte definiert und können nicht geändert werden. Die Sicherheitsattribute hängen jedoch vom Zustand des Lebenszyklus der Karte ab.

Benutzerdaten-Dateien

Benutzerdatendateien werden im Personalisierungsstatus des Kartenlebenszyklus zugewiesen. Es gibt zwei Arten von Benutzerdatendateien, Datensatz- und Binärdateien. Datensatzdateien sind durch die Anzahl der Datensätze und eine feste Datensatzlänge spezifiziert. Binärdateien werden durch eine Dateigröße spezifiziert und der Zugriff erfolgt durch Offset in der Datei.

Die in einer Benutzerdatendatei gespeicherten Daten können durch den Befehl READ RECORD/BINARY gelesen und durch den Befehl WRITE RECORD/BINARY aktualisiert werden, wenn die mit der Datendatei verbundenen Sicherheitsbedingungen erfüllt sind.

Benutzerdatendateien werden definiert, indem die entsprechenden Dateidefinitionsblöcke in die Datensätze der Benutzerdateiverwaltungsdatei während des Personalisierungsstatus geschrieben werden. Es ist nicht möglich, die Anzahl der Datensätze einer Datei zu ändern, sobald eine der Benutzerdatendateien verwendet wurde. Der Benutzer kann auf diese Daten so lange zugreifen, wie die Kapazität der Karte ausreicht.

Zugriff auf Datendateien

Der Prozess des Zugriffs auf Datendateien ist für interne Datendateien und für Benutzerdatendateien identisch.

Struktur der Kontodaten

Die Datenstruktur Konto - kurz Konto - ist für den Einsatz in Anwendungen vorgesehen, in denen ein numerischer Wert, der einen Betrag repräsentiert, sicher verarbeitet werden muss. Das Konto wird in der Kontodatei gespeichert.

Im Benutzerzustand des cad-Lebenszyklus können die Daten im Konto nicht wie die Daten in Benutzerdatendateien durch WRITE-Befehle manipuliert werden. Für die Bearbeitung des Kontos, d. h. für das Hinzufügen und Abziehen von Werten zum bzw. vom Saldo des Kontos und für das Ablesen des aktuellen Saldos, steht ein Satz spezieller Anweisungen zur Verfügung.

Für das Addieren, Subtrahieren und Lesen des Kontos können unterschiedliche Zugriffsbedingungen festgelegt werden.

Kritische Kontobewegungen, wie zum Beispiel CREDIT, werden unter strengen Sicherheitskontrollen durchgeführt.

Sicherheitsmerkmale

Die folgenden Sicherheitsmechanismen werden vom ACOS3 Kartenbetriebssystem bereitgestellt:

- DES/3DES und MAC-Berechnung
- Gegenseitige Authentifizierung und Sitzungsschlüsselgenerierung
- Geheime Codes
- Sicheres Messaging für Datendateien
- Sichere Verarbeitung von Kontotransaktionen
- Anti-Verschleiß-Mechanismus

DES bezieht sich auf den DEA-Algorithmus zur Ver- und Entschlüsselung von Daten, wie in der Norm ANSI X3.93 beschrieben. MAC bezieht sich auf den in der Norm ANSI X3.99 spezifizierten Algorithmus zur Generierung von kryptografischen Prüfsummen (DEA im Cipher Block Chaining-Modus).

Die gegenseitige Authentifizierung ist ein Prozess, bei dem sowohl die Karte als auch das Kartenakzeptanzgerät die Echtheit des jeweiligen Gegenübers überprüfen. Der Sitzungsschlüssel ist das Ergebnis der erfolgreichen Durchführung der gegenseitigen Authentifizierung. Er wird für die Ver- und Entschlüsselung von Daten während einer "Sitzung" verwendet. Eine Sitzung ist definiert als die Zeit zwischen der erfolgreichen Ausführung eines Verfahrens zur gegenseitigen Authentifizierung und einem Reset der Karte oder der Ausführung eines anderen START SESSION-Befehls.

Geheimcodes und der PIN-Code werden verwendet, um selektiv den Zugriff auf die auf der Karte gespeicherten Daten und auf die von der Karte bereitgestellten Merkmale und Funktionen zu ermöglichen, z. B. die Befehle READ und WRITE.

Secure Messaging gewährleistet, dass die zwischen der Karte und dem Terminal/Server übertragenen Daten sicher sind und nicht abgehört, wiedergegeben oder unbefugt verändert werden können. Dies wird durch die Signierung von Befehl und Antwort mit einem MAC und die Verschlüsselung von Befehls- und Antwortdaten erreicht.

Die Kontotransaktionsverarbeitung bietet einen Mechanismus für die sichere und prüfbare Manipulation von Daten in der Kontodatenstruktur, insbesondere des Saldowerts.

DES- und MAC-Berechnung

Alle in der DES/3DES- und MAC-Berechnung verwendeten Schlüssel sind 8/16 Byte lang, je nach Auswahl von Single/Triple DES im Optionsregister. Das niedrigstwertige Bit jedes Bytes des Schlüssels wird bei der Berechnung nicht verwendet und vom Kartenbetrieb nicht interpretiert.

Gegenseitige Authentifizierung und Sitzungsschlüsselgenerierung

Die gegenseitige Authentifizierung basiert auf dem Austausch und der gegenseitigen Überprüfung von geheimen Schlüsseln zwischen der Karte und dem Kartenakzeptanzgerät. Der Schlüsselaustausch erfolgt auf sichere Weise durch die Verwendung von Zufallszahlen und DES/3DES-Datenverschlüsselung.

Der Sitzungsschlüssel ist das Endergebnis des Prozesses der gegenseitigen Authentifizierung und basiert auf den Zufallszahlen von Karte und Terminal.

Der erfolgreiche Abschluss der gegenseitigen Authentifizierung wird auf der Karte gespeichert. Der daraus resultierende Sitzungsschlüssel K_S wird für alle Datenverschlüsselungen und -entschlüsselungen während derselben Sitzung verwendet.

Die Karte unterhält einen Fehlerzähler CNT K_T , der die Anzahl der aufeinanderfolgenden erfolglosen Ausführungen des Befehls AUTHENTICATE zählt und begrenzt.

Die Kartenzufallszahl RND_C wird in einem komplexen, nicht vorhersehbaren mathematischen Prozess aus der in der Sicherheitsdatei gespeicherten Zufallszahl Seed abgeleitet. Der Zufallszahlensatz wird intern vom Betriebssystem nach jedem START TRANSACTION-Befehl aktualisiert.

Geheime Codes

Auf der Karte gespeicherte Geheimcodes werden verwendet, um den Zugriff auf in Benutzerdatendateien gespeicherte Daten und auf bestimmte von der Karte bereitgestellte Befehle zu beschränken. Die Geheimcodes müssen der Karte vorgelegt werden, um Daten aus Benutzerdatendateien zu lesen oder in diese zu schreiben und bestimmte privilegierte Kartenbefehle ausführen zu können.

Sicheres Messaging

ACOS3 Version 1.07 und höher unterstützen Secure Messaging (SM) für Datendateien. Secure Messaging stellt sicher, dass die zwischen der Karte und dem Terminal/Server übertragenen Daten gesichert und nicht anfällig für Abhören, Wiederholungsangriffe und unbefugte Änderungen sind. In der Benutzerdatendatei kann festgelegt werden, dass Secure Messaging für die Befehle READ/WRITE RECORD/BINARY erforderlich ist. Fast alle anderen Befehle können auch vom Terminal initiierte sichere Nachrichtenübermittlung verwenden.

Das in ACOS3 eingesetzte SM verschlüsselt und signiert die Daten, die auf die Karte ein- und von ihr ausgehen.

Verarbeitung von Kontotransaktionen

Mit dem Konto sind vier Schlüssel verbunden:

- Der Kreditschlüssel K_{CR}
- Der Debit Key K_D
- Der Zertifizierungsschlüssel K_{CF}
- Der Widerruf des Lastschriftschlüssels K_{RD}

Die Schlüssel werden in der Kontosicherheitsdatei gespeichert.

Die Schlüssel werden für die Berechnung und Überprüfung der kryptografischen MAC-Prüfsummen von Befehlen und Daten verwendet, die zwischen der Karte und dem Kartenakzeptanzgerät bei der Kontobearbeitung ausgetauscht werden.

Anti-Verschleiß-Mechanismus

Der Anti-Tearing-Mechanismus schützt die Kartendaten und die Sicherheit, falls die Karte plötzlich ausgeschaltet oder während eines Kartenvorgangs herausgezogen wird.

Beim Schreiben von Nutzdaten auf die Karte stellt der Anti-Tearing-Mechanismus von ACOS3 sicher, dass der Vorgang atomar durchgeführt wird. Das heißt, die Daten werden entweder vollständig geschrieben oder der Zielschreibbereich wird in seinem vorherigen Zustand vor dem Schreibvorgang belassen. Die Kontodatendateien sind in ähnlicher Weise geschützt, wenn CREDIT/DEBIT/REVOKE DEBIT-Befehle ausgeführt werden.

Lebenserhaltungssystem-Anwendung

Diese Produkte sind nicht für den Einsatz in lebenserhaltenden Geräten, Vorrichtungen oder Systemen vorgesehen, bei denen eine Fehlfunktion dieser Produkte nach vernünftigem Ermessen zu Personenschäden führen kann. Kunden von ACS, die diese Produkte für solche Anwendungen verwenden oder verkaufen, tun dies auf eigenes Risiko und erklären sich damit einverstanden, ACS für alle Schäden, die aus einer solchen unsachgemäßen Verwendung oder einem solchen Verkauf resultieren, vollständig zu entschädigen.

Contac Informationen

Für weitere Informationen besuchen Sie bitte http://www.acs.com.hk

Für Verkaufsanfragen senden Sie bitte eine E-Mail an info@acs.com.hk

Garantiebedingungen

Auf ein neues Produkt, das im Vertriebsnetz von Alza gekauft wurde, wird eine Garantie von 2 Jahren gewährt. Wenn Sie während der Garantiezeit eine Reparatur oder andere Dienstleistungen benötigen, wenden Sie sich direkt an den Produktverkäufer. Sie müssen den Originalkaufbeleg mit dem Kaufdatum vorlegen.

Als Widerspruch zu den Garantiebedingungen, für die der geltend gemachte Anspruch nicht anerkannt werden kann, gelten:

- Verwendung des Produkts für einen anderen Zweck als den, für den das Produkt bestimmt ist, oder Nichtbeachtung der Anweisungen für Wartung, Betrieb und Service des Produkts.
- Beschädigung des Produkts durch Naturkatastrophe, Eingriff einer unbefugten Person oder mechanisch durch Verschulden des Käufers (z.B. beim Transport, Reinigung mit unsachgemäßen Mitteln usw.).
- Natürlicher Verschleiß und Alterung von Verbrauchsmaterialien oder Komponenten während des Gebrauchs (wie Batterien usw.).
- Exposition gegenüber nachteiligen äußeren Einflüssen wie Sonnenlicht und anderen Strahlungen oder elektromagnetischen Feldern, Eindringen von Flüssigkeiten, Eindringen von Gegenständen, Netzüberspannung, elektrostatische Entladungsspannung (einschließlich Blitzschlag), fehlerhafte Versorgungs- oder Eingangsspannung und falsche Polarität dieser Spannung, chemische Prozesse wie verwendet Netzteile usw.
- Wenn jemand Änderungen, Modifikationen, Konstruktionsänderungen oder Anpassungen vorgenommen hat, um die Funktionen des Produkts gegenüber der gekauften Konstruktion zu ändern oder zu erweitern oder nicht originale Komponenten zu verwenden.