INSO
16386-2
1st.Edition
Jun.2013

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۶۳۸۶ـ۲
چاپ اول
تیر ۱۳۹۲

کارت‌های شناسایی ـ واسط‌های برنامه نویسی کارت دارای مدار مجتمع ـ قسمت ۲ : واسط عمومی کارت

Identification cards –Integrated circuit card programming interface Part 2 : Generic card interface

ICS:35.240.15

به نام خدا

آشنایی باسازمان ملی استاندارد ایران

مؤسسهٔاستاندارد و تحقیقات صنعتی ایران به موجب بندیک مادهٔ۳ قانون اصلاح قوانین ومقررات مؤسسهٔ استانداردو تحقیقات صنعتی ایران،مصوب بهمن ماه۱۳۷۱تنها مرجع رسمی کشوراست که وظیفه تعیین،تدوین ونشر استانداردهای ملی (رسمی) ایران رابه عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد درحوزه های مختلف درکمیسیون های فنی مرکب ازکارشناسان سازمان ،صاحبنظران مراکز و مؤسسات علمی،پژوهشی،تولیدی واقتصادی آگاه ومرتبط انجام میشود وکوششی همگام با مصالح ملی وباتوجه به شرایط تولیدی، فناوری وتجاری است که از مشارکت آگاهانه ومنصفانهٔ صاحبان حق و نفع ، شامل تولیدکنندگان ، مصرف‌کنندگان، صادرکنندگان و واردکنندگان،مراکز علمی وتخصصی ،نهادها ، سازمان های دولتی و غیر دولتی حاصل میشود.پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذینفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها درکمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر میشود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند وذیصلاح نیز با رعایت ضوابط تعیین شده تهیه میکنند درکمیتهٔ ملی طرح و بررسی و در صورت تصویب ،به عنوان استاندارد ملی ایران چاپ و منتشر میشود .بدین ترتیب، استانداردهایی ملی تلقی میشوندکه براساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استان دارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استانداردایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1]،کمیسیون بین المللی الکتروتکنیک (IEC)[2]وسازمان بین المللی اندازه شناسی قانونی(OIML)[3] است و به عنوان تنها رابط[4]کمیسیون کدکس غذایی (CAC)[5]درکشورفعالیت می کند. درتدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی ونیازمندی های خاص کشور ،ازآخرین پیشرفت های علمی،فنی وصنعتی جهان و استانداردهای بین المللی بهره‌گیری می‌شود .

سازمان ملی استانداردایران میتواند با رعایت موازین پیش بینی شده در قانون ، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی ، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی ،اجرای بعضی ازاستانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و /یا اقلا م وارداتی ، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور،اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید .همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره،آموزش،بازرسی،ممیزی و صدورگواهی سیستم های مدیریت کیفیت ومدیریت زیست محیطی،آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش،سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی میکند و در صورت احراز شرایط لازم،گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند.ترویج دستگاه بین المللی یکاها ،کالیبراسیون (واسنجی)وسایل سنجش،تعیین عیار فلزات گران بها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (OrganisationInternationale de MetrologieLegale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

" کارت‌های شناسایی ـ واسط‌های برنامه نویسی کارت دارای مدار مجتمع ـ قسمت ۲ :واسط عمومی کارت"

رئیس:	**سمت و/ یا نمایندگی**
تهرانی طریقت، محمدابراهیم (کارشناسی ارشد مدیریت فناوری اطلاعات)	مشاور ریاست سازمان ثبت احوال و قائم مقام مجری طرح کارت ملی هوشمند
دبیر:	
داوری تبریزی، بیژن (لیسانس مهندسی صنایع)	مدیر عامل شرکت مهندسی و بهبود کیفیت شریف
اعضاء: (اسامی به ترتیب حروف الفبا)	
بداغی، امیرحسین (کارشناسی ارشد مهندسی الکترونیک)	کارشناس سازمان فناوری اطلاعات
جمیل‌پناه، ناصر (کارشناسی ارشد مدیریت)	کارشناس سازمان فناوری اطلاعات
جهان‌شاه، فرناد (کارشناسی مهندسی نرم‌افزار)	کارشناس شرکت مهندسی و بهبود کیفیت شریف
سعیدی، عذرا (کارشناسی ارشد مهندسی مخابرات)	کارشناس سازمان فناوری اطلاعات
صفرنیا، فتانه (کارشناسی فیزیک)	نماینده حوزه طرح کارت ملی هوشمند سازمان ثبت احوال

زنده نام، مهدی (کارشناسی فناوری اطلاعات)	کارشناس حوزه طرح کارت ملی هوشمند سازمان ثبت احوال
نوروزی‌زاده، حمیرا (کارشناسی مهندسی صنایع)	کارشناس استاندارد

فهرست مندرجات

پیش گفتار

استاندارد " کارت‌های شناسایی ـ واسط‌های برنامه نویسی کارت دارای مدار مجتمع ـ قسمت ۲ :واسط عمومی کارت" که پیش‌نویس آن در کمیسیون‌های مربوط توسط شرکت مهندسی و بهبود کیفیت شریف تهیه و تدوین شده است و در صدوشصت‌ویکمین اجلاس کمیته ملی استاندارد خدمات مورخ ۹۱/۱۲/۱۹ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 24727-2:2008, Identification cards -- Integrated circuit card programming interfaces -- : Generic card interface Part 2

مقدمه

استانداردهای ملی ایران شماره ۱۶۳۸۶ مجموعه‌ای از واسط‌های برنامه‌نویسی برای برهم‌کنش(تعامل)[۱] بین کارت‌های دارای مدار مجتمع و برنامه‌های کاربردی خارجی است که خدمات عمومی[۲] برای مصارف چند بخشی[۳] را شامل می‌شود. سازمان و عملکرد کارت های دارای مدار مجتمع با استاندارد ISO/IEC 7816-4 مطابقت دارد .

این استاندارد، قسمتی از مجموعه استانداردهای ملی ایران ۱۶۸۳۶ می‌باشد .

1 -Interaction
2-Generic services
3 - Multi-sector use

کارت‌های شناسایی ـ واسط‌های برنامه‌نویسی کارت دارای مدار مجتمع ـ

قسمت ۲ :

واسط عمومی کارت

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین یک واسط[1] عمومی کارت برای کارت‌های مدار مجتمع، می‌باشد. این واسط به صورت زیر ارائه می‌گردد:

- جفت‌های فرمان ـ پاسخ برای تعامل‌پذیری،
- توصیف و تعیین قابلیت کارت و برنامه کاربردی،

این استاندارد مبتنی بر استانداردهای ISO/IEC 7816-4، ISO/IEC 7816-8، ISO/IEC 7816-9 و ISO/IEC 7816-15 است.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد،اصلاحیه ها و تجدید نظرهای بعدی آن مورد نظر ایناستاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲ ـ ۱ استاندارد ملی ایران شماره ۱ ـ ۱۶۳۸۶، کارت‌های شناسایی ـ واسط‌های برنامه‌نویسی کارت دارای مدار مجتمع ـ قسمت ۱ : معماری

2-2 ISO/IEC 7816-4, Identification cards — Integrated circuit cards — Part 4: Organization, security and
commands for interchange

2-3 ISO/IEC 7816-8, Identification cards — Integrated circuit cards — Part 8: Commands for security operations

2-4 ISO/IEC 7816-9, Identification cards — Integrated circuit cards — Part 9: Commands for card management

2-5 ISO/IEC 7816-15, Identification cards — Integrated circuit cards — Part 15: Cryptographic information application

---

1 - Interface

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین شده در استاندارد ملی ایران شماره ۱ـ ۱۶۳۸۶، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

۳-۱

شیء داده

اطلاعات موجود در واسط، متشکل از الحاق فیلد برچسب قواعد کدگذاری شده DER[1] استاندارد ملی ایران ـ ایزو ـ آی ای سی شماره ۸۸۲۵، فیلد طول DER-کدگذاری شده استاندارد ملی ایران ـ ایزو ـ آی ای سی شماره ۸۸۲۵ و یک فیلد مقدار اختیاری است .

۳-۲

فایل

ساختاری برای برنامه کاربردی و یا داده‌های درون کارت، به همان صورت که در هنگام پردازش فرمان‌ها در واسط عمومی کارت دیده می شود.

۳-۳

کد ترجمه

نرم افزار رویه‌ای است که فرمان‌های روی واسط عمومی کارت را به فرمان‌های پیاده‌سازی شده بر روی کارت دارای مدار مجتمع ترجمه می‌نماید.

۴ کوته‌نوشت‌ها

در این استاندارد، علاوه بر کوته‌نوشت‌های تعیین شده در استاندارد ملی ایران شماره ۱ـ ۱۶۳۸۶ کوته‌نوشت‌های زیر نیز به‌کار می‌رود:

ATS answer to select, as defined in ISO/IEC 14443-3	پاسخ به انتخاب، همانگونه که در استاندارد ملی ایران ـ ایزو ـ آی ای سی ۳ ـ ۱۴۴۴۳ تعریف شده است
DF dedicated file	فایل اختصاصی
DO data object	شیء داده
FCP file control parameters	پارامترهای کنترلی فایل
FID file identifier	شناسه فایل
RFU reserved for further use	درنظرگرفته‌شده برای استفاده‌های آتی

1- Distinguished Encoding Rules (DER)-encoded

۵ سازماندهی برای تعامل پذیری

این بند، زیرمجموعه‌ای از ساختار، فرمان‌ها و ساختار داده‌ای تعریف شده در استانداردهای ISO/IEC 7816-4، ISO/IEC 7816-8 و ISO/IEC 7816-9 را مشخص می‌کند.

موارد زیر را نمی‌توان در واسط عمومی کارت مشخص نمود:

- شناسه‌های کوتاه فایل
- کانال‌های منطقی
- فایل‌های با ساختار مستندشده[1]

کارت فیزیکی که به وسیله کد ترجمه به واسط عمومی کارت نگاشت شده است، مجاز است که از یک شناسه کوتاه EF[2]، کانال‌های منطقی و فایل‌های با ساختار مستندشده استفاده کند.

۵-۱ جفت‌های فرمان- پاسخ برای تعامل پذیری

۵-۱-۱ کدگذاری فرمان و پاسخ

درخواست‌های موجود در GCI[3] از لحاظ منطقی معادل فرمان APDU[4]هایی از نوع فرمان هستند که در استانداردهای ISO/IEC 7816-4، ISO/IEC 7816-8 و ISO/IEC 7816-9 مشخص شده‌اند.

تاییدهای موجود در GCI از لحاظ منطقی معادلAPDUهایی از نوع پاسخ هستند که در استانداردهای ISO/IEC 7816-4، ISO/IEC 7816-8 و ISO/IEC 7816-9 مشخص شده‌اند.

برای ارسال مستقیم یک فرمان واسط عمومی کارت به یک پیاده‌سازی از این استاندارد، استفاده از واسط زیر مجاز است:

ExecuteCommand(فرمان توالی-بایت‌ها) توالی-بایت‌ها

این واسط، فرمانی را به پیاده‌سازی این استاندارد ارسال می‌کند و پاسخ پیاده‌سازی آن را به عنوان مقدار خود برمی‌گرداند.

در سایر قسمت‌های استاندارد ملی ایران شماره ۱۶۳۸۶ واسط‌های بیشتری مجاز هستند که تعریف شوند.

۵-۱-۲ بایت کلاس[5]

جدول ۱ مقادیر بایت کلاس را که باید در فرمان‌های روی واسط عمومی کارت استفاده شوند نشان می‌دهد.

---

1 - Record Structure
2 - Elementary File
3 - Generic Card Interface
4 - Application Protocol Data Unit
5 - Class Byte

جدول ۱- مقادیر CLA روی GCI

توضیح	b1	b2	b3	b4	b5	b6	b7	b8
این فرمان، آخرین یا تنها فرمان یک زنجیره است	-	-	-	-	۰	-	-	۰
این فرمان، آخرین فرمان یک زنجیره نیست	-	-	-	-	۱	-	-	۰
این فرمان، برای پیاده‌سازی قسمت ۲ است	۱	۱	۱	۱	۱	۱	۱	۱

این استاندارد باید از زنجیره‌ای کردن فرمان‌ها فقط برای انتقال داده‌های رشته‌ای طولانی‌تر از یک فرمان واحد، پشتیبانی نماید؛ به عنوان مثال، ثابت INS، P1 و P2 در میان تمام فرمان‌های زنجیره.
برای انتقال درخواست‌هایی که در پیاده‌سازی این استاندارد در مورد آنها اقدام شده است، به‌طورکلی بدون انتقال APDUها **به** کارت، باید از CLA='FF' استفاده گردد.

۵-۱-۳ بایت دستورالعمل

جدول ۲ و جدول ۳ مقادیر بایت دستورالعمل را فهرست می‌کند که توصیه می‌شود در فرمان‌های درون GCI استفاده شود زیرا این فرمان‌ها استقلال استاندارد شده پیاده‌سازی‌های این استاندارد و ملی ایران شماره ۳ـ ۱۶۳۸۶را تضمین می‌کند.
یک درخواست GCI با INS که در جدول ۲ وجود نداشته باشد باید بطور مستقیم به کارت ارسال گردد و پاسخ کارت-واسط باید به درخواست‌کننده برگردانده شود.
فرمان‌های دارای بایت‌های دستورالعمل موجود در جدول ۳ باید به وسیله پیاده‌سازی این استاندارد مورد اقدام قرار گیرند و نباید به اسکریپت مترجم[1] محول شوند.

جدول ۲- درخواست‌های GCI که به وسیله اسکریپت مترجم، اداره می‌شوند

نام فرمان	INS	بسته	محدودیت‌ها
SELECT	'A4'	A	SELECT بر اساس شناسه فایل (P1-P2='00-04' یا '00-0C') و SELECT بر اساس نام DF (P1-P2='04-04' یا '04-0C') با بازگشت شیء داده‌ای FCP یا هیچ داده‌ای نباید پشتیبانی شود. (یادآوری را ملاحظه فرمایید)
READ BINARY	'B0'	A	بیت ۸ مربوط به P1 باید به 0 تنظیم شود.
READ BINARY	'B1'	A	P1 و P2 باید به '00' تنظیم شوند.
UPDATE BINARY	'D6'	A	بیت ۸ مربوط به P1 باید به 0 تنظیم شود.
UPDATE BINARY	'D7'	A	P1 و P2 باید به '00' تنظیم شوند.

1 - Translation Script

جدول ۲ (ادامه)

GET DATA	‘CA’ ‘CB’	A	هیچ.
PUT DATA	‘DA’ ‘DB’	A	هنگامی که PUT DATA به شیء داده‌ای اشاره می کند که هم-اکنون وجود دارد، آن شیء داده باید رونویسی شود.
GENERATE ASYMMETRIC KEY PAIR	‘46’ ‘47’	B	خارج از دامنه
VERIFY	‘20’	A	P2 صفر نباشد.
VERIFY	‘21’	A	P2 صفر نباشد.
CHANGE REFERENCE DATA	‘24’	A	هیچ.
GET CHALLENGE	‘84’	A	هیچ.
INTERNAL AUTHENTICATE	‘88’	A	هیچ.
EXTERNAL AUTHENTICATE	‘82’	A	هیچ.
MUTUAL AUTHENTICATE	‘82’	A	هیچ.
GENERAL AUTHENTICATE	‘86’ ‘87’	A	هیچ.
PERFORM SECURITY OPERATION: COMPUTE DIGITAL SIGNATURE	‘2A’	A	P1=’9E’ P2=’9A’ فیلد داده فرمان: - Absent (مقدار hash از طریق PERFORM SECURITY OPERATION:HASH ارائه می‌شود)
PERFORM SECURITY OPERATION: VERIFY DIGITAL SIGNATURE	‘2A’	A	P1=’00’ P2=’A8’ فیلد داده فرمان: - DO ‘9E’
PERFORM SECURITY OPERATION: HASH	‘2A’	A	P1=’90’ P2=’80’ یا ‘9A’ فیلد داده فرمان: ۱) - DO ‘90’ (مقدار hash میانی || مقدار بیت‌های hash شده) || DO ‘80’ (آخرین بلوک متن) یا ۲) – مقدار hash DO ‘90’

جدول ۲(ادامه)

PERFORM SECURITY OPERATION:VERIFY CERTIFICATE	‘2A’	A	P1-‘00’ P2=’AE’ یا ‘BE’ فیلد داده فرمان: - ’7F21‘ DO (گواهی قابل‌تایید کارت)
PERFORM SECURITY OPERATION: ENCIPHER	‘2A’	A	P1=’86’ P2=’80’ فیلد داده فرمان: داده‌ای که قرار است رمزگذاری شود
PERFORM SECURITY OPERATION: DECIPHER	‘2A’	A	P1=’80’ P2=’86’ فیلد داده فرمان: داده‌ای که قرار است رمزگشایی شود (PI || cryptogram)
MANAGE SECURITY ENVIRONMENT	‘22’	A	SET (P1=’x1’) و RESTORE (P1=F3’)
CREATE FILE	‘E0’	B	فقط اشیاء داده FCP موجود در جدول ۹ پشتیبانی می‌شوند. فایل ایجاد شده، فایل جاری می‌شود.
DELETE FILE	‘E4’	B	فقط P1-P2=’00-00’ پشتیبانی می‌شود. پس از حذف فایل، والد فایل حذف شده، فایل اختصاصی انتخاب شده جاری می‌شود.
ACTIVATE FILE	‘44’	B	فقط P1-P2=’00-00’ پشتیبانی می‌شود.
DEACTIVATE FILE	‘04’	B	فقط P1-P2=’00-00’ پشتیبانی می‌شود.
RESET RETRY COUNTER	‘2C’	A	هیچ.
GET RESPONSE	‘C0’	A	فقط P1-P2=’00-00’ پشتیبانی می‌شود. کلمه وضعیت 6985 یعنی هیچ داده‌ای برای بازیابی وجود ندارد

یادآوری ــ در صورتی که SELECT بر اساس نام DF، FCP (P1-P2=’04-04’) را برگرداند، شیء داده FCP برگردانده شده مجاز است که شامل شیء داده‌ای با برچسب ’87‘ باشد که نشان‌دهنده فایل پایه‌ای است که حاوی توصیف قابلیت برنامه-کاربردی کارت می‌باشد.

جدول ۳- مقادیر INS روی GCI که پیاده‌سازی استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶بر روی آنها عمل می‌کند (CLA=’FF’)

نام فرمان	INS	P1 P2	بسته	محدودیت‌ها
COLD RESET	‘00’	‘0000’	A	Lc وجود ندارد، Le=’00’.
WARM RESET	‘00’	‘00FF’	A	
DEACTIVATE CONTACTS	‘00’	‘0100’	A	Lc و Le وجود ندارند
DEACTIVATE CONTACTS AND EJECT	‘00’	‘0200’	A	
SELECT PROCEDURAL ELEMENT	‘A4’	‘0400’	A	Lc در محدوده ۵ تا ۱۶ قرار دارد، Le وجود ندارد. یک فیلد داده‌ای استاندارد باید یک AID حاوی OID یک استاندارد ISO باشد که مطابق با استاندارد ISO/IEC 7816-4 پیاده‌سازی را تعریف می‌کند. فیلد داده اختصاصی پیاده‌سازی باید با ‘FX’ شروع شود.
GET DATA	CA		A	برچسب‌ها باید از کلاس وابسته به زمینه باشند، مگر در حالتی که DOهایی که منتقل می شوند دارای برچسب‌های برنامه کاربردی-کلاس تعریف شده در استانداردهای ISO/IEC 7816 یا استاندارد ملی ایران شماره ۱۶۳۸۶باشند. هنگامی که PUT DATA به یک شیء داده موجود اشاره می-کند، آن شیء داده باید رونویسی شود. برچسب‌های بخصوصی در PUT DATA مجاز هستند که رویه را به وسیله جزء فراخوانده شده، اجرا کنند. اگر بیش از یک پارامتر برای ارسال به رویه وجود داشته باشد، آن پارامترها باید درون یک DO ساخته شده ارسال شوند. مطابق بند ۵-۲، کد وضعیت ‘0000’ نمایانگر اجرای صحیح رویه است.
PUT DATA	DA		A	
LIST READERS	CA	‘7F64’	A	Lc وجود ندارد، Le=’00’ مقدار DO 7F64 را برمی‌گرداند. این مقدار، حاصل الحاق DOهای دربرگیرنده نام reader ها در قالب UTF8 است.

کارت فیزیکی که به وسیله کد ترجمه به واسط عمومی کارت نگاشت شده است، مجاز است که از سایر فرمان-های سازگار با استاندارد ISO/IEC 7816 استفاده نماید.

مقادیر دستورالعمل دریافت شده در GCI، شامل موارد جدول ۲، مجاز هستند که یک جزء رویه‌ای را در یک توصیف قابلیت فعال نمایند. به بند ۶-۳ رجوع کنید.

بسته A برای استفاده عملیاتی ضروری است. بسته‌های A و B برای کاربرد مدیریت کارت ضروری هستند.

تکمیل موفقیت‌آمیز فرمان RESET باید هم پیاده‌سازی استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶و هم کارت را راه‌اندازی مجدد نماید. راه‌اندازی مجدد پیاده‌سازی استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶ باید دربرگیرنده تنظیم CCD و تمام ACDها به مقدار ‘undefined’ باشد.

داده پاسخ درون R-APDU مربوط به RESET C-APDU باید در صورت وجود بایت‌های قدیمی متعلق به کارت ATR، ATS یا پاسخ به ATTRIB باشند. در صورت تکمیل موفقیت‌آمیز، کلمه‌های وضعیت باید ‘0000’ و در غیر اینصورت باید ‘0F00’ باشند.

۵-۱-۴ بایت توصیف‌کننده فایل

جدول ۴ مقادیر بایت توصیف‌کننده فایل را که باید در FCP روی GCI مورد استفاده قرار گیرند نشان می‌دهد. فایل‌های موجود روی GCI قابل اشتراک نیستند.

جدول ۴- مقادیر بایت توصیف‌کننده فایل روی GCI

توضیح	b1	b2	b3	b4	b5	b6	b7	b8
فایل اختصاصی	۰	۰	۰	۱	۱	۱	۰	۰
فایل اولیه در حال کار، ساختار شفاف	۱	۰	۰	۰	۰	۰	۰	۰
فایل اولیه در حال کار، ساختار TLV برای اشیاء داده BER-TLV	۱	۰	۰	۱	۱	۱	۰	۰

۵-۲ وضعیت‌های کارت برای تعامل پذیری

جدول ۵ و جدول ۶ وضعیت‌هایی را که باید در پیاده‌سازی‌های واسط عمومی کارت مورد استفاده قرار گیرند، نشان می‌دهند و رویدادهای گذار وضعیت بین این وضعیت‌ها را توصیف می‌کنند.

جدول ۵- وضعیت‌های کارت و برنامه کاربردی و رویدادهای گذار وضعیت روی GCI

نام وضعیت	همیشه تعریف شده است	نوع تغییر وضعیت	رویداد گذار وضعیت
برنامه کاربردی منتخب جاری	بله	تنظیم شده	SELECT بر اساس نام DF؛ به عنوان مثال شناسه برنامه کاربردی
فایل اختصاصی منتخب جاری	بله	تنظیم شده	SELECT بر اساس شناسه فایل مربوط به یک فایل اختصاصی
		تنظیم شده	CREATE FILE بطوری که فایل اختصاصی جدید، فایل اختصاصی منتخب جاری می‌شود
		تنظیم شده	DELETE FILE (حذف) فایل اختصاصی منتخب جاری به‌طوری که والد فایل اختصاصی حذف شده، فایل اختصاصی جدید می‌شود
فایل اولیه منتخب جاری	خیر	تنظیم شده	SELECT بر اساس شناسه فایل مربوط به یک فایل اولیه
		تنظیم شده	CREATE FILE به‌طوری که فایل اولیه اخیرا ایجاد شده، فایل اولیه منتخب جاری می‌شود
		تنظیم نشده	SELECT بر اساس نام DF
		تنظیم نشده	SELECT بر اساس شناسه فایل مربوط به یک فایل اختصاصی
		تنظیم نشده	DELETE FILE (حذف) فایل اولیه منتخب جاری یا فایل اختصاصی منتخب جاری
		تنظیم نشده	CREATE FILE (ایجاد) فایل اختصاصی

جدول ۶- فایل‌های منتخب جاری پس از اجرای موفقیت‌آمیز فرمان‌ها روی GCI

فرمان	برنامه‌کاربردی/DF جاری	فایل اولیه جاری
SELECT بر اساس نام DF	تغییر به برنامه‌کاربردی/DF مشخص شده	پاک شده و وجود ندارد
SELECT DF بر اساس شناسه فایل	تغییر به DF مشخص شده	پاک شده و وجود ندارد
SELECT EF بر اساس شناسه فایل	بدون تغییر	تغییر به EF مشخص شده
CREATE FILE مربوط به DF	تغییر به DF مشخص شده	پاک شده و وجود ندارد
CREATE FILE مربوط به EF	بدون تغییر	تغییر به EF مشخص شده
DELETE FILE مربوط به DF	در صورت حذف DF منتخب جاری، تغییر به DF والد	در صورت حذف یک DF که اخیرا EF را انتخاب کرده است، پاک شده و وجود ندارد
DELETE FILE مربوط به EF	بدون تغییر	پاک شده و وجود ندارد
بلافاصله پس از فرمان RESET، برنامه‌کاربردی/DF منتخب جاری باید MF یا برنامه‌کاربردی/DF منتخب پیش‌فرض بشود. وضعیت EF منتخب جاری نیز به‌صورت «پاک شده و وجود ندارد» درمی‌آید.		

۵-۳ کلمه‌های[1] وضعیت تعامل‌پذیری

کلمه‌های وضعیتی که باید در واسط عمومی کارت استفاده شوند در جدول ۷ فهرست شده‌اند.

جدول ۷- کلمه‌های وضعیت تعامل‌پذیری

	نماد	مقدار	معنی
عادی	OK	‘9000’	اتمام موفقیت‌آمیز فرمان
	MORE	‘61xx’	اتمام موفقیت‌آمیز فرمان با حداقل xx [2] بایت داده‌های پاسخ اضافی در دسترس
هشدار	EOP-NOCHANGE	‘62xx’	پایان غیرمنتظره پردازش که در این صورت، وضعیت حافظه غیرفرار را نسبت به آنچه که بلافاصله قبل از شروع اجرای فرمان بود، بدون تغییر باقی می‌گذارد.
	EOD	‘6282’	فرا رسیدن پایان داده‌ها
	EOP-RC	‘63Cx’	داده‌های مرجع اشتباه – به تعداد x بار، اقدام مجدد، مجاز است
	EOP-CHANGED	‘63xx’ بجز ‘63Cx’	پایان غیرمنتظره پردازش که در این صورت، وضعیت حافظه غیرفرار را از آنچه که بلافاصله قبل از شروع اجرای فرمان بود، تغییر می‌دهد.
خطای اجرایی	ABORT-NO CHANGE	‘64xx’	پایان پردازش به علت خطا که در این صورت، وضعیت حافظه غیرفرار را نسبت به آنچه که بلافاصله قبل از شروع اجرای فرمان بود، بدون تغییر باقی می‌گذارد.
	ABORT-CHANGED	‘65xx’	پایان پردازش به علت خطا که وضعیت حافظه غیرفرار را از آنچه که بلافاصله قبل از شروع اجرای فرمان بود، تغییر می-دهد.
	ABORT-SECURITY	‘66xx’	پایان پردازش به علت خطای مربوط به یک وضعیت امنیتی که حافظه غیرفرار را در وضعیت تعریف نشده قرار می‌دهد.
خطای بررسی	WRONG LENGTH	‘6700’	طول نادرست
	SECURITY CONDITION	‘6982’	شرط امنیتی برآورده نشده است
	REFERENCE DATA BLOCKED	‘6983’	داده‌های مرجع مسدود شده است
	CONDITION OF USE	‘6985’	شرایط استفاده، برآورده نشده است
	DATA FIELD	‘6A80’	پارامترهای نادرست در فیلد داده‌های فرمان
	FUNCTION NOT SUPPORTED	‘6A81’	تابع، پشتیبانی نشده است؛ به عنوان مثال، کانالهای منطقی اضافی در دسترس نیست
	FILE NOT FOUND	‘6A82’	فایل یا برنامه‌کاربردی پیدا نشد

1 - Words

۲ - xx تعداد کمینه بایت داده‌های پاسخ اضافی در دسترس می‌باشد.

جدول ۷ (ادامه)

	P1-P2	‘6A86’	پارامترهای P1-P2 نادرست هستند
	DATA NOT FOUND	‘6A88’	داده‌های مرجع پیدا نشده است
	BAD INS	‘6D00’	دستورالعمل، پشتیبانی نشده یا نامعتبر است
	BAD CLA	‘6E00’	کد کلاس پشتیبانی نشده است
	UNDEFINED	‘6F00’	عیب‌یابی دقیقی موجود نیست
پاسخ ایجاد شده به وسیله لایه دسترسی عمومی کارت	OK	‘0000’	پردازش موفقیت‌آمیز به وسیله پیاده‌سازی ISO/IEC 24727-2 شامل CCD و اجزاء رویه‌ای ACD
	SIGNATURE INVALID	‘02xx’	امضای اسکریپت ترجمه قابل تایید نیست
	EXCEPTION	‘0080’	داده‌های پاسخ حاوی یک استثنای تعریف شده به وسیله زبان[1] است
	NOT MAPPED	‘0A81’	هیچ ترجمه‌ای به وسیله جزء رویه‌ای ISO/IEC 24727-2 ارائه نشده است
	IFD NOT FOUND	‘0A82’	وسیله واسط در دسترس نیست
	CARD MISSING	‘0A88’	کارت پیدا نشده است
	UNDEFINED	‘0F00’	عیب‌یابی دقیقی موجود نیست

تمام مقادیر SW1 SW2 برگردانده شده به واسط عمومی کارت که SW1 برابر ’6X‘ یا ’9X‘ نیست از پاسخ APDU کارت نشات نمی‌گیرند و ناشی از میان‌افزار ISO/IEC 24727-2 هستند. به ازای X>0، ’0X YZ‘ همان معنی ’6X YZ‘ صادر شده به وسیله کارت را دارد. مقادیری که تا کنون تعریف شده‌اند در جدول ۷ نشان داده شده‌اند. در قسمتهای دیگر این استاندارد، مقادیر بیشتری مجاز هستند که تعریف شوند. در این استاندارد، کلمه-های وضعیت کارت و کلمه‌های وضعیت اجزاء رویه‌ای که در این جدول یافت نمی‌شوند به منظور سهولت، به ترتیب به ’6F00‘ و ’0F00‘ نگاشت شده‌اند.

تمام SW1هایی که با ’0‘,’1‘,’2‘,’3‘,’4‘,’5‘,’7‘,’8‘,’A‘,’B‘,’C‘,’D‘,’E‘ شروع می‌شوند یا در این استاندارد یا در RFU به وسیله ISO/IEC JTC1/SC17 تعریف شده‌اند.

استفاده از تمام SW1هایی که با ’F‘ شروع می‌گردند اختصاصی است.

۵-۴ ساختارهای داده‌ای برای تعامل‌پذیری

ساختارهای داده‌ای برای تعامل‌پذیری باید به صورت فایل‌ها یا اشیاء داده‌ای BER-TLV پیاده‌سازی شوند. این فایل‌ها و اشیاء داده‌ای BER-TLV در استاندارد ISO/IEC 7816-4 تعریف شده‌اند.

اشیاء داده‌ای مجاز هستند که بر روی واسط عمومی کارت با استفاده از فرمان‌های GET DATA و PUT DATA مدیریت شوند. همچنین اشیاء داده‌ای مجاز هستند که در برنامه‌های کاربردی کارت قرار داشته باشند

1- Language-Defined

و به وسیله آن‌ها مدیریت شوند. مشخصات امنیتی اشیاء داده‌ای موجود در یک فایل اولیه با ساختار TLV، در FCP فایل اولیه قرار دارند.

هر برنامه کاربردی کارت باید به وسیله یک شناسه برنامه کاربردی ISO/IEC 7816-4 به صورت جهانی مشخص شود.

جدول‌های ۸ تا ۱۳ الگوها و برچسبهایی را که باید روی واسط عمومی کارت استفاده شوند، توضیح می‌دهند.

سایر قسمت‌های استاندارد ملی ایران شماره ۱۶۳۸۶، مجاز هستند که الگوها و اشیاء داده‌ای بیشتری را شامل شوند.

جدول ۸- اشیاء داده‌ای تعامل‌پذیری برای الگوها

زمینه	کلاس برچسب	توضیح	برچسب	نماد
سراسری	برنامه کاربردی	الگوی پارامتر کنترلی فایل داده‌ای	‘62’	FCP
مدیریت محیط امنیت و اجرای فرمان‌های عملیات امنیت	مربوط به زمینه	الگوی مرجع کنترل برای احراز هویت	‘A4’	AT
		الگوی مرجع کنترل برای کنترل صحت داده‌های[1] رمزنگاری	‘B4’	CCT
		الگوی مرجع کنترل برای امضای دیجیتال	‘B6’	DST
		الگوی مرجع کنترل برای محرمانه نگه داشتن	‘B8’	CT
		الگوی Hash	‘AA’	HT

جدول ۹- اشیاء داده‌ای تعامل‌پذیری در الگوی پارامتر کنترلی فایل (FCP)

توضیح	برچسب	نماد
تعداد بایت‌های داده موجود در فایل بجز اطلاعات ساختاری	‘80’	SIZE
تعداد بایت‌های اختصاص داده شده به EF یا DF شامل اطلاعات ساختاری	‘81’	ALLOC
بایت توصیف‌گر فایل (۱ بایت)	‘82’	FSB
شناسه فایل	‘83’	FID
نام فایل اختصاصی و یا به‌طور کلی یک شناسه برنامه کاربردی	‘84’	DFNAME
شناسه یک EF شامل توسعه‌ای بر اطلاعات کنترلی فایل	‘87’	FID-ACD
الگوی مشخصه امنیتی در قالب توسعه یافته	‘AB’	SEC-EXP
مشخصه امنیتی در قالب فشرده	‘8C’	SEC-COM
الگوی مشخصه امنیتی برای اشیاء داده‌ای	‘A0’	SEC-DO

در جدول ۹، اگر نماد FID-ACD (برچسب ’87‘) وجود داشته باشد، باید شناسانه فایل اولیه‌ای باشد که شامل توصیف قابلیت برنامه کاربردی کارت است

1-Checksum

جدول ۱۰- اشیاء داده‌ای تعامل‌پذیری در الگوی مرجع کنترل احراز هویت (AT)

نماد	برچسب	توضیح
CM-REF	‘80’	مرجع سازوکار رمزنگاشتی
SEC-KEY/PuKR	‘83’	مرجع کلید یک کلید سری یا مرجع کلید عمومی
SES-KEY/PrKR	‘84’	مرجع کلید یک کلید جلسه یا مرجع کلید خصوصی

جدول ۱۱- اشیاء داده‌ای تعامل‌پذیری در الگوی مرجع کنترل صحت داده‌های رمزنگاشتی (CCT)

نماد	برچسب	توضیح
CM-REF	‘80’	مرجع سازوکار رمزنگاشتی
SEC-KEY	‘83’	مرجع کلید یک کلید سری
SES-KEY	‘84’	مرجع کلید یک کلید جلسه

جدول ۱۲- اشیاء داده‌ای تعامل‌پذیری در الگوی مرجع کنترل امضای دیجیتال (DST)

نماد	برچسب	توضیح
CM-REF	‘80’	مرجع سازوکار رمزنگاشتی
PuKR	‘83’	مرجع کلید عمومی
PrKR	‘84’	مرجع کلید خصوصی

جدول ۱۳- اشیاء داده‌ای تعامل‌پذیری در الگوی مرجع کنترل برای محرمانه نگه داشتن (CT)

نماد	برچسب	توضیح
CM-REF	‘80’	مرجع سازوکار رمزنگاشتی
SEC-KEY/PuKR	‘83’	مرجع کلید یک کلید سری یا مرجع کلید عمومی
SES-KEY/PrKR	‘84’	مرجع کلید یک کلید جلسه یا مرجع کلید خصوصی

اشیاء داده‌ای اضافی، بخصوص آن‌هایی که به پیام‌رسانی ایمن مربوط هستند، در سایر قسمت‌های استاندارد ملی ایران شماره ۱۶۳۸۶ نشان داده می‌شوند.

۵-۵ برنامه‌های کاربردی کارت برای تعامل پذیری

۵-۵-۱ برنامه کاربردی کارت آلفا

برنامه کاربردی با شناسه کاربردی ’E8 28 81 C1 17 02‘ باید برنامه کاربردی کارت آلفا باشد. برنامه کاربردی کارت آلفا باید یا روی GCI موجود و قابل انتخاب باشد یا در لایه SAL شبیه‌سازی[1] شود.

برنامه کاربردی کارت آلفا باید اطلاعات مربوط به کارت را بطور مستقل از برنامه کاربردی، همانطور که در استاندارد ISO/IEC 7816-4 تعریف شده، فراهم نماید. این اطلاعات شامل اطلاعات مدیریتی کارت، فایل و برنامه کاربردی کارت می‌باشد.

۵-۵-۲ برنامه کاربردی رمزنگاشتی اطلاعات

برنامه کاربردی رمزنگاشتی اطلاعات در استاندارد ISO/IEC 7816-15 تعریف شده است. اگر پروفایل کلی برنامه کاربردی رمزنگاشتی اطلاعات، مطابق آنچه که در CCD (در زیر) مشخص شده ، وجود داشته باشد آنگاه باید برنامه کاربردی رمزنگاشتی اطلاعات روی GCI قابل انتخاب باشد.

نمونه‌ای از پیاده‌سازی برنامه کاربردی رمزنگاشتی اطلاعات، مربوط به استاندارد ISO/IEC 7816-15 در پیوست ب نشان داده شده است.

۶ توصیف‌های قابلیت

دو نوع توصیف قابلیت وجود دارد، توصیف قابلیت کارت (CCD) و یک توصیف قابلیت برنامه کاربردی (ACD) به ازای هر برنامه کاربردی کارت. هنگامی بازیابی از واسط عمومی کارت، توصیف قابلیت کارت باید تحت برچسب ’7F62‘ بازیابی گردد و توصیف قابلیت برنامه کاربردی باید تحت برچسب ’7F63‘ بازیابی شود.

۶-۱ توصیف قابلیت کارت (CCD)

برنامه کاربردی کارت آلفا باید از بازیابی شیء داده CCD (برچسب ’7F62‘) پشتیبانی نماید.

جدول ۱۴ اشیاء داده‌ای را که مجاز هستند در CCD یافت شوند، فهرست می‌نماید. این اشیاء داده باید برای تمام برنامه‌های کاربردی سازگار با ISO/IEC 24727 روی کارت بکار بروند و مجاز هستند که فهرستی از برنامه-های کاربردی کارت موجود روی کارت و کد رویه‌ای در حال نگاشت بین فرمان‌های درونی کارت و فرمان‌های شرح داده شده در جدول ۲، را شامل شوند.

1 - Emulate

جدول ۱۴- اشیاء داده درون CCD (‘7F62’)

یادآوری	مقدار	الزامی/ اختیاری	توضیح	برچسب	نماد
ارائه شده به وسیله کارت	‘00’	الزامی	پروفایل استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶که این CCD با آن سازگاری دارد	‘80’	PRO
مجاز است که به وسیله پیاده-سازی این استاندارد بر پایه اطلاعاتی از کارت، ساخته شود	الحاق اشیاء داده با برچسب ‘4F’	اختیاری	ترتیب شناسه‌های برنامه کاربردی مربوط به برنامه‌های کاربردی کارت	‘A0’	SAID
مجاز است که به وسیله پیاده-سازی این استاندارد بر پایه اطلاعاتی از کارت، ساخته شود	اشیاء داده به صورت تعریف شده در جدول ۱۶	اختیاری	الگوی توصیف جزء رویه‌ای (۶-۳ را ملاحظه فرمایید)	‘A1’	LANG
		اختیاری	URL مربوط به کدی که ترجمه را انجام می‌دهد	‘5F50’	LANG-URL
اگر بیت i به ۱ تنظیم شود نشان‌دهنده آن است که پروفایل i وجود دارد. بیت صفر نشان-دهنده وجود پروفایل در پیوست الف است. بقیه بیت‌ها RFU هستند.	رشته بیتی	اختیاری	پروفایل CIA حاضر روی واسط عمومی کارت	‘81’	CIA-PROFILES
اگر بیت i به ۱ تنظیم شود نشان‌دهنده آن است که پروفایل باید به وسیله پیاده‌سازی این استاندارد ایجاد شود، بیت صفر نشان‌دهنده وجود پروفایل در پیوست الف است. بقیه بیت‌ها RFU هستند.	رشته بیتی	اختیاری	پروفایل CIA حاضر روی واسط عمومی کارت	‘82’	CIA-PROFILES-AUTOMATIC
زیرساخت کلید امضای دیجیتال، خارج از دامنه است	شیء داده بلوک امضای دیجیتال	اختیاری	اطلاعات امضای دیجیتال برای جزء رویه‌ای	‘5F3D’	DIGITAL-SIGNATURE-ON-CODE
به وسیله کارت فراهم شده. اگر وجود داشته باشد، کارت از واسط استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶پشتیبانی می‌کند.	‘00’	اختیاری	پروفایل واسط استاندارد ملی ایران شماره ۳ـ ۱۶۳۸۶	‘83’	IF-PROFILE

این استاندارد، پروفایل برنامه کاربردی اطلاعات رمزنگاشتی‌شده، ISO/IEC 7816-15، را تعریف می‌کند. در این پروفایل، داده‌های برنامه کاربردی اطلاعات رمزنگاشتی‌شده باید یا در برنامه کاربردی کارت آلفا یا در برنامه کاربردی اطلاعات رمزنگاشتی‌شده، یافت شوند. برای تعریف یک پروفایل، پیوست الف را ملاحظه فرمایید.

۶-۲ توصیف قابلیت برنامه کاربردی (ACD)

هر برنامه کاربردی، از جمله برنامه کاربردی کارت آلفا مجاز است که به وسیله یک شیء داده ACD ('7F63') توصیف شود.

جدول ۱۵ اشیاء داده‌ای که مجاز هستند در یک ACD یافت شوند را فهرست می‌نماید. این اشیاء داده‌ای حاوی اطلاعاتی درباره برنامه کاربردی کارت مربوطه هستند.

جدول ۱۵- اشیاء داده در توصیف قابلیت برنامه کاربردی ('7F63')

یادآوری	مقدار	الزامی/ اختیاری	توضیح	برچسب	نماد
به وسیله برنامه کاربردی کارت یا پیاده‌سازی استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶ فراهم می‌شود	اشیاء داده به صورت تعریف شده در جدول ۱۶	اختیاری	الگوی توصیف جزء رویه‌ای (۶-۳ را ملاحظه فرمایید)	'A1'	LANG
		اختیاری	URL مربوط به کدی که ترجمه را انجام می‌دهد	'5F50'	LANG-URL
	فیلد مقدار شیء داده، الحاق مقدار CIAinfo کدگذاری شده-DER به دنبال مقادیر ISO/IEC 7816-15 CIOChoice کدگذاری شده-DER است همانگونه که در پیوست پ شرح داده شده	اختیاری	توصیف خدمات پشتیبانی شده به وسیله برنامه کاربردی کارت	'7F66'	SERVICE-DESCRIPTION
	مقدار URL محل منبع حاوی الحاق مقادیر ISO/IEC 7816-15 CIOChoice کدگذاری شده-DER است همانگونه که در پیوست پ شرح داده شده	اختیاری		'7F67'	SERVICE-DESCRIPTION-LOCATION
زیرساخت کلید امضای دیجیتال، خارج از دامنه است	شیء داده بلوک امضای دیجیتال	اختیاری	اطلاعات امضای دیجیتال برای جزء رویه‌ای	'5F3D'	DIGITAL-SIGNATURE-ON-CODE

۶-۳ اجزاء رویه‌ای

یک جزء رویه‌ای در یک توصیف قابلیت باید کد ترجمه‌ای برای پردازش هر درخواست GCI متعلق به جدول ۲ و هر تایید برنامه کاربردی کارت مربوطه مطابق با تابع TranslationCode شرح داده شده در زیر باشد. اجزاء

رویه‌ای درون CCD یا درون یک ACD یا روی خود کارت قرار دارند یا با استفاده از یک URL به آنها ارجاع داده می‌شود.

الگوی توصیف جزء رویه‌ای مشخص شده در جدول ۱۶، فناوری توصیف رویه‌ای مورد استفاده در CCD یا یک ACD را شرح می‌دهد و برای انجام ترجمه‌ها بین درخواست‌ها/ تاییدهای GCI و فرمان‌ها/ پاسخ‌های APDU واسط کارت، کد اجرایی درون این فناوری توصیف رویه‌ای را در بر می‌گیرد یا به آن اشاره می‌کند.

جدول ۱۶- اشیاء داده در الگوی توصیف جزء رویه‌ای ('A1')

مقدار	الزامی/ اختیاری	توضیح	برچسب	نماد
{iso(1) standard(0) iso20060(20060)}	اختیاری	شناسه شیء استاندارد یا مشخصه بیانگر زبان رویه‌ای.	'06'	LANG-OID
نشانه‌های خاص LANG-OID	اختیاری	کد ترجمه	'81'	LANG-CODE

هنگامی که جزء رویه‌ای (برچسب 'A1') در یک توصیف قابلیت، حاوی یک شیء داده برای یک URL (برچسب '5F50') باشد و آن URL به یک سند که بطور مناسب به عنوان یک توصیف قابلیت قالب‌بندی شده است، اشاره کند (جدول ۱۴ و جدول ۱۵ را ملاحظه فرمایید)، آنگاه جزء رویه‌ای در توصیف قابلیت باید به جزء رویه‌ای بازیابی شده از سند مورد اشاره، اضافه شود.

۶-۳-۱ مدل محاسباتی اجزاء رویه‌ای

یک جزء رویه‌ای در یک توصیف قابلیت باید یک کد ترجمه در نظر گرفته شده برای پردازش آرگومان‌های منتقل شده به وسیله تابع TranslationCode باشد. اجزاء رویه‌ای می‌توانند به وسیله یک فرمان SELECT بطور صریح انتخاب شوند (جدول ۳ را ملاحظه فرمایید)، بخصوص اگر آن‌ها انتقال APDUها را به کارت، محول نکنند. از وقوع تعاملات با کارت جلوگیری نمی‌شود.

سایر امکانات این مدل برای اسکریپت‌های بازیابی شده از کارت بکار می‌روند. آنها برای کد دریافت شده از دنیای خارج، استفاده نمی‌شوند.

یک جزء رویه‌ای در یک توصیف قابلیت باید یک تابع با یک آرگومان منطقی و یک آرگومان آرایه بایت باشد.

زمانی که جزء رویه‌ای برای تبدیل یک APDU فرمان GCI به یک یا چند APDU فرمان واسط کارت، اجرا می‌شود، آرگومان منطقی باید به TRUE تنظیم شود.

هنگامی که جزء رویه‌ای برای تبدیل یک APDU پاسخ کارت به یک تایید GCI، اجرا می‌شود، آرگومان منطقی باید به FALSE تنظیم شود.

به محض ورود، اگر آرگومان منطقی وارد شده به جزء رویه‌ای TRUE باشد، آرگومان دیگر، آرایه اکتت[1]، باید حاوی اکتت‌های تشکیل‌دهنده APDU فرمان GCI باشد.
به محض ورود، اگر آرگومان منطقی وارد شده به جزء رویه‌ای FALSE باشد، آرگومان آرایه باید حاوی اکتت‌های تشکیل‌دهنده تایید باشد.
به محض خروج، جزء رویه‌ای برای برگرداندن آرگومان آرایه بایت تبدیل شده، به پیاده‌سازی قسمت ۳، باید آرگومان منطقی را به TRUE تنظیم نماید. جزء رویه‌ای برای ارسال ارایه بایت تبدیل شده، به کارت، باید آرگومان منطقی را به FALSE تنظیم کند.
امضای نقطه ورود به کد ترجمه باید به صورت زیر باشد:
TranslationCode(Boolean b IN/OUT, Array c IN/OUT)

۶-۳-۲ به‌کارگیری اجزاء رویه‌ای

برای یافتن جزء رویه‌ای در ACD آن به منظور اداره کردن یک درخواست GCI یا APDU پاسخ واسط کارت، ACD مربوط به برنامه کاربردی کارت انتخاب شده فعلی و CCD، باید به همین ترتیب مورد استفاده قرار گیرند.
اگر برنامه کاربردی انتخاب شده فعلی، یک جزء رویه‌ای فراهم کند، آنگاه هر درخواست GCI یا APDU پاسخ واسط کارت باید به این جزء رویه‌ای داده شود.
اگر برنامه کاربردی انتخاب شده فعلی، یک جزء رویه‌ای فراهم نکند و CCD یک جزء رویه‌ای فراهم نماید، آنگاه هر درخواست GCI یا APDU پاسخ واسط کارت باید به این جزء رویه‌ای داده شود.
اگر یک درخواست GCI روی GCI دریافت شود که برای آن هیچ جزء رویه‌ای درون CCD یا ACD برنامه کاربردی انتخاب شده فعلی، وجود ندارد، آنگاه درخواست باید به کارت فرستاده شود و پاسخ واسط کارت باید به موجودیتی که درخواست GCI را ایجاد نموده، برگردانده شود.

۶-۴ تعیین مقدار توصیف قابلیت

۶-۴-۱ قاعده کلی

اگر مقدار توصیف قابلیت در حال حاضر در میان‌افزار این استاندارد موجود نباشد، آنگاه این مقدار باید به وسیله بازیابی اشیاء داده مطابق رویه مشروح زیر، تعیین شود.

۶-۴-۲ تعیین مقدار CCD

تعیین مقدار CCD باید از خدمات کارت مستقل از برنامه کاربردی تعریف شده به وسیله ISO/IEC 7816-4 استفاده کند.

1-Octet

مقدار CCD مجاز است که به صورت زیر، بلافاصله بعد از راه‌اندازی مجدد کارت، تعیین شود. اگر اجزای داده بین صنعتی ‘داده‌های دستیابی اولیه’ در بایتهای قدیمی ATR، ATS یا پاسخ به ATTRIB وجود داشته باشند، شیء داده ‘7F62’ مجاز است که با استفاده از رشته داده اولیه، تعیین شود.

در غیر این صورت، CCD باید با استفاده از یکی از رویه‌های زیر تعیین گردد. ترتیبی که رویه‌های تعریف شده زیر، باید طبق آن اجرا شوند، تعریف نشده است. اگر تمام این رویه‌ها در تعیین یک CCD ناموفق باشند، کارت با این استاندارد، سازگار نیست.

- خواندن EF.ATR، در حالی که شیء داده ‘7F62’ ممکن است وجود داشته باشد؛
- یک فرمان GET DATA به همراه
  - INS=’CA’; P1-P2=’7F62’ و Le=’00’ یا
  - INS=’CB’; P1-P2=’3FFF’ و فیلد داده فرمان حاوی ‘5C027F62’ باشد

  که مجاز است در فیلد داده پاسخ، CCD را برگرداند؛
- به وسیله انتخاب کردن برنامه کاربردی کارت آلفا با استفاده از AID ‘E8 28 81 C1 17 02’ به دنبال یک فرمان GET DATA، همانگونه که قبلا شرح داده شد.

اگر فهرست برنامه‌های کاربردی، با استفاده از رویه‌های فوق تعیین نشد، آنگاه برای تعیین فهرست برنامه‌های کاربردی کارت، باید EF.DIR خوانده شود.

۶-۴-۳ تعیین مقدار یک ACD

بلافاصله پس از اینکه با استفاده از یکی از رویه‌های زیر، برنامه کاربردی کارت انتخاب شد، تعیین مقدار یک ACD مجاز است که انجام شود:

- خواندن یک فایل که در پاسخ به فرمان SELECT تحت برچسب ‘87’، به آن ارجاع شده است؛
- یک فرمان GET DATA به همراه
  - P1-P2=’7F63’ و Le=’00’ یا
  - P1-P2=’3FFF’ و فیلد داده فرمان حاوی ‘5C027F63’ باشد

  که در فیلد داده پاسخ، ACD را برمی‌گرداند.

پیوست الف
(اطلاعاتی)
پروفایل برنامه کاربردی اطلاعات رمزنگاشتی شده روی واسط عمومی کارت

الف-۱ پروفایل A

وجود یک برنامه کاربردی اطلاعات رمزنگاشتی‌شده ISO/IEC 7816-15 مطابق با این پروفایل به وسیله تنظیم کردن بیت ۱ اولین بایت فیلد مقدار شیء داده CIA-PROFILES در جدول ۱۴، به مقدار ۱ مشخص شده است.

الف-۱-۱ EF.CIAInfo

EF.CIAInfo الزامی است. شناسه فایل EF.CIAInfo برابر ’5032‘ می‌باشد.

الف-۱-۲ EF.OD

EF.OD الزامی است. شناسه فایل EF.OD برابر ’5031‘ می‌باشد.EF.OD نباید شامل اجزاء trustedPublicKeys، trustedCertificate، یا usefulCertificates باشد.

الف-۱-۳ EF.PrKD

EF.PrKD مجاز است که وجود داشته باشد. محدودیت‌های زیر به هر شیء کلید خصوصی ارجاع شده در EF.PrKD اعمال می‌شوند:

- اجزاء CommonKeyAttributes.startDate و CommonKeyAttributes.endDate مجاز هستند که وجود داشته باشند اما بهتر است که مقادیر آنها به وسیله برنامه کاربردی سرویس گیرنده مطابق با استاندارد ملی ایران شماره ۱۶۳۸۶نادیده گرفته شوند.
- اجزاء CommonKeyAttributes.accessFlags، CommonKeyAttributes.keyReference و CommonKeyAttributes.algReference بهتر است که وجود داشته باشند.
- جزء CommonPrivateKeyAttributes.generalName مجاز است که وجود داشته باشد.

الف-۱-۴ EF.PuKD

EF.PuKD مجاز است که وجود داشته باشد. محدودیت‌های زیر به هر شیء کلید عمومی ارجاع شده در EF.PuKD اعمال می‌شوند:

- برای CommonObjectAttributes، هر جزء کنار جزء **برچسب**، بهتر است که به وسیله برنامه کاربردی سرویس گیرنده مطابق با استاندارد ملی ایران شماره ۱۶۳۸۶ نادیده گرفته شوند.
- جزء CommonKeyAttributes.algReference بهتر است که وجود داشته باشند.
- اجزاء CommonKeyAttributes.accessFlags، CommonKeyAttributes.startDate و CommonKeyAttributes.endDate مجاز هستند که وجود داشته باشند.
- اجزاء CommonPublicKeyAttributes.trustedUsage و CommonPublicKeyAttributes.generalName مجاز هستند که وجود داشته باشند.

الف-۱-۵ EF.SKD

EF.SKD مجاز است که وجود داشته باشد. محدودیت‌های زیر به هر شیء کلید رمز ارجاع شده در یک EF.SKD اعمال می‌شوند:
- جزء CommonKeyAttributes.algReference بهتر است که وجود داشته باشند.
- اجزاء CommonKeyAttributes.accessFlags، CommonKeyAttributes.startDate و CommonKeyAttributes.endDate مجاز هستند که وجود داشته باشند.
- جزء CommonSecretKeyAttributes.keyLen بهتر است که وجود داشته باشد.

الف-۱-۶ EF.CD

EF.CD مجاز است که وجود داشته باشد. محدودیتهای زیر به هر شیء گواهی ارجاع شده در یک EF.CD اعمال می‌شوند:
- اجزاءCommonCertificateAttributes.certHash و CommonCertificateAttributes.validity مجاز هستند که وجود داشته باشند.
- توصیه می‌شود که گزینه **غیرمستقیم** ObjectValue برای تمام انواع گواهی، استفاده شود.

الف-۱-۷ EF.AOD

EF.AOD مجاز است که وجود داشته باشد. محدودیتهای زیر به هر شیء احراز هویت ارجاع شده در یک EF.AOD اعمال می‌شوند:
- اجزاء CommonObjectAttributes.flags و CommonObjectAttributes.userConsent مجاز هستند که وجود داشته باشند.
- برای اشیاء کلمه عبور، توصیه می‌شود که جزء PasswordAttributes.path وجود داشته باشد.

الف-۱-۸ EF.DCOD

EF.DCOD مجاز است که وجود داشته باشد. محدودیتهای زیر به هر شیء محتوی داده‌های ارجاع شده در یک EF.DCOD اعمال می‌شوند:

- جزء CommonObjectAttributes.userConsent مجاز است که وجود داشته باشد.
- توصیه می‌شود که فقط گزینه opaqueDO به عنوان یک مقدار DataContainerObjectChoice واقع شود.
- توصیه می‌شود که گزینه **غیرمستقیم** ObjectValue برای تمام مقادیر OpaqueDOAttributes، استفاده شود.

پیوست ب

(اطلاعاتی)

نمونه‌هایی از پروفایل A

ب ـ ۱ ـ ویژگی eSign K

ـ این مثال از پروفایل A، برنامه کاربردی امضای مطابق با CWA 14890 (مشخصه eSign K)را شرح می‌دهد.
ـ این برنامه کاربردی از دو محیط امنیتی استفاده می‌نماید. SE#1 در یک محیط مورد اطمینان استفاده می‌شود
ـ که تحت کنترل صاحب کارت است. در SE#1 فرمان‌ها بدون پیام‌رسانی ایمن اعمال می‌شوند. SE#2 در یک
ـ محیط غیر قابل اطمینان استفاده می‌شود بطوری که یک احراز هویت دستگاه با برقراری کلید جلسه برای
ـ پیام‌رسانی ایمن، مورد نیاز است.
ـ صاحب کارت برای تایید اینکه یک کانال مورد اطمینان، برقرار شده است، از Display Message (DM)
ـ استفاده می‌نماید. DM می‌تواند پس از احراز موفقیت‌آمیز هویت دستگاه، فقط با پیام‌رسانی ایمن،
ـ خوانده شود.

```
ESignK-SignatureApplication
DEFINITIONS IMPLICIT TAGS ::= BEGIN
IMPORTS
CIAInfo, CIOChoice, AuthenticationObjectChoice,
PrivateKeyChoice, PublicKeyChoice,
CertificateChoice, DataContainerObjectChoice
FROM
CryptographicInformationFramework;
```

تعریف فایل‌های فهرست ISO 7816-15

```
EFODF ::= SEQUENCE OF CIOChoice
EFAODF ::= SET OF AuthenticationObjectChoice
EFPrKDF ::= SEQUENCE OF PrivateKeyChoice
EFPuKDF ::= SEQUENCE OF PublicKeyChoice
EFCDF ::= SEQUENCE OF CertificateChoice
EFDCODF ::= SEQUENCE OF DataContainerObjectChoice
-- EF.CIAInfo
eSignK-EFCIAInfo CIAInfo ::=
{ version v2,
profileIndication {"CWA 14890"},
serialNumber ''H,
label "Signature Application",
cardflags { authRequired, prnGeneration },
seInfo
{ { se 1,
 AID مربوط به  برنامه کاربردی aid 'A000000167455349474E'H }, -- eSignK
{ se 2,
 AID مربوط به  برنامه کاربردی aid 'A000000167455349474E'H } }, -- eSignK
supportedAlgorithms
{
-- الگوریتم‌های درهم‌سازی[1]
```

1 - Hash

-- AlgID: 0x10, SHA-1

مرجع یکتا{ reference 1, --

CKM_SHA_1 = 0x220سازوکار نوعalgorithm 544, -- PKCS#11

نوع پارامترها NULLاستparameters NULL: NULL, -- و مقدار

supportedOperations {hash},
objId {1 3 14 3 2 26 },

برابر است با 0x10، CWA 14890-1 و جدول ۱۳-۱ را ملاحظه فرمایید algRef 16

},

الگوریتم‌های امضای دیجیتال --

AlgID: 0x11، RSA با DSI مطابق با ISO/IEC 9796-2 با عدد تصادفی و SHA-1--

مرجع یکتا، ارجاع متقابل از PrKDF -- { reference 2,

الگوریتم در PKCS#11 تعریف نشده است، -- algorithm 2147483648

فروشنده 0x80000000 را تعریف کرده است --

نوع پارامترها NULL و مقدارNULL است -- parameters NULL: NULL,

supportedOperations {compute-signature},
objId {1 3 36 3 4 3 2 1},

برابر است با 0x11، CWA 14890-1 و جدول ۱۳-۱ را ملاحظه فرمایید -- algRef 17

},

AlgID: 0x12، RSA با DSI مطابق با PKCS#1 و SHA-1--

مرجع یکتا، ارجاع متقابل ازPrKDF -- { reference 3,

CKM_SHA_1_RSA_PKCS سازوکار نوع PKCS#11 -- algorithm 6,

نوع پارامترها NULL و مقدارNULL است -- parameters NULL: NULL,

supportedOperations {compute-signature},
objId {1 2 840 113549 1 1 5},

برابر است با 0x12، CWA 14890-1 و جدول ۱۳-۱ را ملاحظه فرمایید -- algRef 18

},

الگوریتم احراز هویت دستگاه --

AlgID: 0x17، پروتکل انتقال کلید تعریف شده در CWA 14890-1 --

{
reference 4,

الگوریتم درPKCS#11 تعریف نشده است، -- algorithm 2147483649 ,

فروشنده 0x80000001 را تعریف کرده است --

نوع پارامترها NULL و مقدارNULL است -- parameters NULL: NULL,

supportedOperations {compute-signature, verify-signature},

پروتکل انتقال کلید CWA 14890-1 را ملاحظه فرمایید -- objId {1 3 36 7 2 1 1},

برابر است با 0x17، CWA 14890-1 و جدول ۱۳-۲ را ملاحظه فرمایید -- algRef 23

},

تایید امضای گواهی متغیر کارت (CV) --

مرجع یکتا، ارجاع متقابل ازPuKDF -- { reference 5,

الگوریتم درPKCS#11 تعریف نشده است، -- algorithm 2147483650,

فروشنده 0x80000002 را تعریف کرده است --

نوع پارامترها NULL و مقدارNULL است -- parameters NULL: NULL,

supportedOperations {verify-signature},
objId {1 3 36 3 4 3 2 1},

algRef استفاده نشده است (کلید و الگوریتم به وسیله مقام مرجع گواهی CAR--

انتخاب می‌شوند که در گواهی قابل تایید کارت CV ارائه می‌شوند --

}
}
}

-- EF.ODF

eSignK-EFODF EFODF ::=
{
authObjects : path : { efidOrPath '4003'H },
privateKeys : path : {efidOrPath '4001'H},
publicKeys : path : {efidOrPath '4002'H },
certificates : path : {efidOrPath '4005'H },
dataContainerObjects : path : { efidOrPath '4006'H }
}

-- EF.AODF

eSignK-EFAODF EFAODF ::=
{

-- PIN.CH.AUT

pwd :
{
commonObjectAttributes
{ label "global password",

ارجاع متقابل به PUK.CH.AUT -- authId '03'H,

SE#2 فرمان VERIFY و CHANGE REFERENCE DATA باید به همراه پیام‌رسانی ایمن اعمال شوند--

در

کلیدهای جلسه مربوطه به وسیله یک احراز هویت دستگاه، برقرار می‌شوند--

ـ برای SE#1 هیچ شرایط امنیتی اعمال نمی‌شود، یعنی این فرمان‌ها همیشه می‌توانند

--اجرا شوند (بدون پیام‌رسانی ایمن)

accessControlRules
{
{ accessMode { execute },
securityCondition authReference:
{
authMethod { secureMessaging, extAuthentication },
seIdentifier 2
}
}
}
},
classAttributes
{ authId '01'H },
typeAttributes

```
{ pwdFlags { initialized},
pwdType ascii-numeric,
 minLength 4,                                   برحسب نویسه --
   storedLength 0,                              برحسب بایت، لت‌گذاری[1] لازم  نیست--
   maxLength 8,                                 برحسب نویسه --
   pwdReference 1,                              شناسه کلید 0x01 --
به دلیل اینکه PIN.CH.AUT یک کلمه عبور سراسری است، به مسیر احتیاجی نیست --
}
},
-- PIN.CH.DS
pwd :
{
commonObjectAttributes
{ label "Signature password",
--همان قوانین کنترل دستیابی بکار رفته در کلمه عبور سراسری، اعمال می‌شوند
accessControlRules
{
{ accessMode { execute },
securityCondition authReference:
{
authMethod { secureMessaging, extAuthentication },
seIdentifier 2
}
}
}
},
classAttributes
{ authId '02'H },
typeAttributes
{ pwdFlags { local, unblock-disabled, initialized },
--هیچ کد راه‌اندازی مجددی پشتیبانی نمی‌شود
pwdType ascii-numeric,
 minLength 6,                                   برحسب نویسه --
storedLength 0,                                 برحسب بایت، لت‌گذاری لازم نیست --
 maxLength 8,                                   برحسب نویسه --
pwdReference 129,                               شناسه کلید 0x81 --
path { efidOrPath '3F 00 3F 01'H }
مسیر  DF.ESIGN  که باید قبل از فرمان VERIFY انتخاب شود--
(کلمه عبور محلی) --
}
},
-- PUK.CH.AUT
pwd :
{
commonObjectAttributes
{ label "resetting code for the global password",
```

1-Padding

-- باید به همراه RESET RETRY COUNTER فرمان SE#2 در
--پیام‌رسانی ایمن مورد استفاده قرار گیرد. کلیدهای جلسه مربوطه به وسیله
--دستگاه احراز هویت برقرار می‌شوند.
-- هیچ شرایط امنیتی اعمال نمی‌شود، یعنی این فرمان همیشه می‌تواند SE#1 برای
--اجرا شوند (بدون پیام‌رسانی ایمن)

```
accessControlRules
{
{ accessMode { execute },
securityCondition authReference:
{
authMethod { secureMessaging, extAuthentication },
seIdentifier 2
}
}
}
},
```

-- PIN.CH.AUT برای ارجاع متقابل از

```
classAttributes
{ authId '03'H },
typeAttributes
{ pwdFlags { local, initialized, unblockingPassword },
pwdType ascii-numeric,
minLength 8,
```

-- برحسب نویسه

```
storedLength 0,
```

-- برحسب بایت، لت‌گذاری لازم نیست

```
}
}
}
```

-- EF.PrKDF

```
eSignK-EFPrKDF EFPrKDF ::=
{
```

-- SK.CH.DS

```
privateRSAKey :
{
commonObjectAttributes
{ label "Signature Key",
flags { private },
authId '02'H,
```

-- PIN.CH.DS ارجاع متقابل به

```
userConsent 1,
```

PSO: COMPUTE DIGITAL SIGNATURE ، یک احراز هویت کاربر به وسیله کلمه عبور امضای PIN.CH.DS لازم است --
در SE#1 قبل از هر فرمان
در SE#2 فرمان PSO باید به همراه پیام‌رسانی ایمن اعمال شود.--
--کلیدهای جلسه مربوطه به وسیله یک دستگاه احراز هویت، برقرار می‌شوند
بعلاوه، پیش از هر استفاده از فرمان PSO یک تایید کاربر به وسیله PIN.CH.DS ضروری است --

```
accessControlRules
{
{ accessMode { execute },
securityCondition or:
```

ارجاع متقابل به PIN.CH.DS --

```
{ and: { authId: '02'H,
authReference: { authMethod { userAuthentication },
seIdentifier 1
}
},
```

ارجاع متقابل به PIN.CH.AUT --

```
and: { authId: '01'H,
authReference: { authMethod { secureMessaging,
extAuthentication,
userAuthentication },
seIdentifier 2
}
}
}
}
}
},
classAttributes
```

باید همان iD را با گواهی به اشتراک بگذارد--

```
{ iD '01'H,
usage { sign , signRecover, nonRepudiation},
native TRUE,
accessFlags { sensitive,
alwaysSensitive,
neverExtractable,
cardGenerated },
```

KID 0x84 درون کارت --

```
keyReference 132
algReference
{
2, -- RSA ISO با SHA1
3 -- RSA PKCS#1 با SHA1
}
},
typeAttributes
{
value indirect : path : {efidOrPath "H},
modulusLength 1024
}
},
```

-- SK.ICC.AUT

کلید خصوصی ICC مورد استفاده برای احراز هویت دستگاه و برقراری کلید جلسه. --

این کلید در پروتکل انتقال کلید مشخص شده در CWA 14890-1 مورد استفاده قرار می‌گیرد.--

```
privateRSAKey :
{
commonObjectAttributes
{ label "SK.ICC.AUT",
flags { private },
},
```

باید همان iD را با گواهی قابل تایید کارت C_CV.ICC.AUT (CV) به اشتراک بگذارد --

```
classAttributes
{ iD '02'H,
usage { decipher, signRecover },
native TRUE,
accessFlags { sensitive,
alwaysSensitive,
```

```
neverExtractable },
keyReference 17,
```
KID 0x11 درون کارت --

```
algReference
{
 4
}
},
typeAttributes
{ value indirect : path : {efidOrPath "H },
modulusLength 1024
}
}
}
```
احراز هویت دستگاه، پروتکل انتقال کلید --

```
-- EF_PuKDF
eSignK-EFPuKDF EFPuKDF ::=
{
-- PK.RCA.CS-AUT
```
کلید عمومی Root CA که به عنوان تکیه‌گاه امنیتی در ICC ذخیره می‌شود.--

این کلید برای تایید گواهی CV در زمینه دستگاه احراز هویت، استفاده می‌شود.--

```
publicRSAKey :
{
commonObjectAttributes
{ label "PK.RCA.CS-AUT"},
classAttributes
{ iD '03'H,
usage { verifyRecover },
native TRUE,
```
مرجع نگهدارنده گواهی (CHR) به عنوان مرجع کلید استفاده می‌شود --

CWA 14890-1، فصل ۱۴ را ملاحظه فرمایید --

```
keyReference 1122334455667788,
algReference
{
5
}
},
typeAttributes
{ value indirect : path : { efidOrPath "H },
modulusLength 1024
}
}
}
```
الگوریتم برای تایید گواهی CV --

```
-- EF.CDF
eSignK-EFCDF EFCDF ::=
{
-- C_X509.CH.DS
```
--گواهی صاحب کارت برای خدمت امضای دیجیتال

```
x509Certificate :
{
commonObjectAttributes
{ label "certificate for signature service" },
```
--باید همان شناسه را با کلید خصوصی به اشتراک بگذارد

```
classAttributes
{ iD '01'H,
```

```
authority FALSE },
```

مسیر EF.C.X509_1.CH.DS جایی که گواهی، ذخیره می‌شود --

```
typeAttributes
{ value indirect : path : {efidOrPath '3F 00 3F 01 C0 00'H } }
},
```

-- C_X509.CA.CS-DS

گواهی CA که صادر کننده C_X509.CH.DS است --

```
x509Certificate :
{
commonObjectAttributes
{ label "CA certificate for signature service"},
classAttributes
{ iD '01'H,
authority TRUE },
```

مسیر EF.C_X509.CA.CS جایی که گواهی، ذخیره می‌شود --

```
typeAttributes
{ value indirect : path : {efidOrPath '3F 00 3F 01 C6 08'H} }
},
```

-- C_CV.ICC.AUT

گواهی قابل تایید کارت ICC مورد استفاده در خدمت احراز هویت دستگاه --

```
cvCertificate :
{
commonObjectAttributes
{ label "C_CV.ICC.AUT" },
```

باید همان شناسه را با کلید خصوصی به اشتراک بگذارد --

```
classAttributes
{ iD '02'H,
authority FALSE },
```

مسیر EF.C_CV.ICC.AUT جایی که گواهی، ذخیره می‌شود --

```
typeAttributes
{ value indirect : path : {efidOrPath '3F 00 2F 03'H} }
}
}
```

-- EF_DCODF

```
eSignK-EFDCODF EFDCODF ::=
{
```

-- Display Message

سازوکار Display Message برای اطمینان از برقراری یک کانال مورد اعتماد بین دستگاه واسط و ICC --

--به وسیله صاحب کارت مورد استفاده قرار می‌گیرد،

.CWA 14890-1 را ملاحظه فرمایید --

```
opaqueDO :
{
commonObjectAttributes
{ label "Display Message",
flags {private, modifiable},
accessControlRules
{
{ accessMode { update },
securityCondition or:
```

ارجاع متقابل به PIN.CH.AUT --

```
{ and: { authId: '01'H,
authReference: { authMethod { userAuthentication },
```

```
seIdentifier 1
}
},
and: { authId: '01'H ,
```

ارجاع متقابل به PIN.CH.AUT --

```
authReference: { authMethod { secureMessaging,
extAuthentication,
userAuthentication },
seIdentifier 2
}
}
}
},
{ accessMode { read },
securityCondition authReference:
{ authMethod {secureMessaging,extAuthentication },
seIdentifier 2
}
}
}
},
```

applicationName یا applicationOID باید وجود داشته باشند --

```
classAttributes
{ applicationName "A000000167455349474E" },
```

AID مربوط به برنامه کاربردی eSignK --

مسیر EF که حاوی Display Message است --

```
typeAttributes
indirect : path : {efidOrPath '3F 00 3F 01 D0 00'H }
}
}
END
```

پیوست پ

(الزامی)

برنامه کاربردی اطلاعات رمزنگاشتی‌شده برای توصیف خدمت برنامه کاربردی کارت

یک برنامه کاربردی اطلاعات رمزنگاشتی‌شده ISO/IEC 7816-15 کدگذاری‌شده -DER از طریق یک شیء داده‌ها با برچسب ’7F66‘ یا ’7F67‘ در توصیف قابلیت برنامه کاربردی کارت با هر برنامه کاربردی کارت مرتبط است، که خدمات ارائه شده به وسیله برنامه کاربردی کارت را توصیف می‌نماید. این اطلاعات برای ترجمه درخواستهای واسط برنامه کاربردی استاندارد ملی ایران شماره ۳ـ ۱۶۳۸۶به فرمان‌های واسط عمومی کارت استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶، به وسیله یک پیاده‌سازی استاندارد ملی ایران شماره ۳ـ ۱۶۳۸۶ مورد استفاده قرار می‌گیرد.

فیلد مقدار شیء داده ’7F66‘ (یا داده‌های ارجاع‌شده با URL درون شیء داده ’7F67‘) باید حاوی یک CardApplicationServiceDescriptionValue کدگذاری‌شده-DER باشد.

CardApplicationServiceDescriptionValue یک مقدار ISO/IEC 7816-15 CIAInfo می‌باشد که باید پس از آن صفر یا بیشتر مقدار ISO/IEC 7816-15 CIOChoice قرار گیرد که هر یک، اشیاء انتخاب PathOrObjects را کدگذاری می‌کند.

```
::= SEQUENCE { CardApplicationServiceDescription
ciaInfo CIAInfo,
cioChoice SEQUENCE OF CIOChoice
}
```

مقدار اولیه CIAInfo کدگذاری‌شده-DER، الگوریتم‌های رمزنگاشتی، پروتکل‌های احراز هویت و محیط‌های امنیتی پشتیبانی شده به وسیله برنامه کاربردی کارت را توصیف می‌نماید.

ترتیب مقادیر CIOChoice کدگذاری‌شده-DER زیر، شامل یک مدخل CIOChoice برای هر مجوعه داده استاندارد ملی ایران شماره ۱۶۳۸۶در برنامه کاربردی کارت، یک مدخل CIOChoice به ازای هر هویت متمایزکننده استاندارد ملی ایران شماره ۱۶۳۸۶درون برنامه کاربردی کارت و یک مدخل CIOChoice برای هر خدمت استاندارد ملی ایران شماره ـ۱۶۳۸۶در برنامه کاربردی کارت، می‌باشد.

هر مجموعه داده استاندارد ملی ایران شماره ۱۶۳۸۶ در یک برنامه کاربردی کارت استاندارد ملی ایران شماره ۱۶۳۸۶، به وسیله یک عنصر جزء ISO/IEC 7816-15 dataContainerObjects نمایندگی می‌شود.

هر هویت متمایزکننده استاندارد ملی ایران شماره ۱۶۳۸۶در یک برنامه کاربردی کارت استاندارد ملی ایران شماره ۱۶۳۸۶، به وسیله عناصر جزء ISO/IEC 7816-15 authObjects, privateKeys, یا secretKeys publicKeys, trustedPublicKeys نمایندگی می‌شود.

هر خدمت استاندارد ملی ایران شماره ۱۶۳۸۶ در یک برنامه کاربردی کارت استاندارد ملی ایران شماره ۱۶۳۸۶، به وسیله یک عنصر dataContainerObjects ISO/IEC 7816-15 نمایندگی می‌شود.
الحاق مقادیر کدگذاری‌شده-DER CIOChoice تشکیل دهنده توصیف خدمت یک برنامه کاربردی کارت استاندارد ملی ایران شماره ۱۶۳۸۶مجاز است که شامل مقادیر اضافی ISO/IEC 7816-15 CIOChoice مانند اجزای privateKeys، publicKeys، secretKeys و certificates باشد که با استفاده از خصوصیت authId به هویت‌های متمایزکننده، مرتبط هستند. هر یک از خصوصیات مشخص شده به وسیله ISO/IEC 7816-15 مجاز هستند که در این مقادیر CIOChoice اضافی وجود داشته باشند.

الگوریتم‌های رمزنگاشتی و پروتکل‌های احراز هویت
مقدار CIAInfo که در ابتدا قرار دارد، الگوریتم‌های رمزنگاشتی پیاده‌سازی شده به وسیله برنامه کاربردی کارت، بخصوص الگوریتم‌های رمزنگاشتی مورد استفاده در پروتکل‌های احراز هویت را تشریح می‌نماید.
جزء الزامی version، به ویرایشی از ISO/IEC 7816-15 که توصیف خدمت با آن مطابقت دارد، تنظیم می‌گردد.
جزء الزامی cardflags، خصوصیات برنامه کاربردی کارت را به ازای ISO/IEC 7816-15 بیان می‌کند.
اجزاء لیست SEQUENCE OF AlgorithmInfo، الگوریتم‌های رمزنگاشتی پشتیبانی شده به وسیله برنامه کاربردی کارت را توصیف می‌نمایند. با استفاده از فیلد reference به یک الگوریتم خاص، ارجاع شده است. توصیف یک الگوریتم باید شامل شناسه شیء (objId) الگوریتم و مرجع الگوریتم (algRef) الگوریتم درون برنامه کاربردی کارت باشد.
مجموعه داده‌های استاندارد ملی ایران شماره ۱۶۳۸۶و ساختارهای داده‌ها برای تعامل‌پذیری
هر مجموعه داده در یک برنامه کاربردی کارت استاندارد ملی ایران شماره ۱۶۳۸۶به وسیله یک جزء استاندارد ملی ایران ۱۶۳۸۶dataContainerObjects که ترتیبی از اشیاء اطلاعاتی محتوی داده‌ها است، در توصیف خدمت برنامه کاربردی کارت، نمایندگی می‌شود. اولین شیء اطلاعاتی محتوی داده‌ها، مجموعه داده را توصیف می‌کند و هر شیء اطلاعاتی محتوی داده‌های بعدی، یک ساختار داده‌های تکی را برای تعامل‌پذیری درون مجموعه داده توصیف می‌نماید.
خصوصیت ISO/IEC 7816-15 label در خصوصیات شیء مشترک اولین شیء اطلاعاتی محتوی داده‌های ISO/IEC 7816-15 در ترتیبی از اشیاء محتوی داده‌های تشکیل دهنده یک مجموعه داده استاندارد ملی ایران ۱۶۳۸۶، نام مجموعه داده می‌باشد.
خصوصیت accessControlRules ISO/IEC 7816-15 مربوط به اولین شیء اطلاعاتی محتوی داده‌های ISO/IEC 7816-15 در ترتیب اشیاء اطلاعاتی محتوی داده‌هایی که یک مجموع داده استاندارد ملی ایران شماره ۱۶۳۸۶را تشکیل می‌دهند، لیست کنترل دستیابی استاندارد ملی ایران شماره ۱۶۳۸۶ برای مجموعه داده و در نتیجه برای تمام ساختارهای داده‌ای تعامل‌پذیری (DSIهای) درون مجموعه داده را با استفاده از حالت دستیابی مطابق با آنچه در جدول پ-۴ زیر توضیح داده شده است، پیاده‌سازی می‌کند.

هر شیء اطلاعاتی محتوی داده‌های ISO/IEC 7816-15 بعدی در ترتیب اشیاء اطلاعاتی محتوی داده‌هایی که یک ISO/IEC 24727 Data Set را تشکیل می‌دهند، نمایانگر یک ساختار داده‌های ISO/IEC 24727 برای تعامل‌پذیری درون ISO/IEC 24727 Data Set است.

خصوصیت label ISO/IEC 7816-15 در خصوصیات شیء مشترک اشیاء اطلاعاتی محتوی داده‌های ISO/IEC 7816-15 که نشاندهنده یک ساختار داده‌های استاندارد ملی ایران ۱۶۳۸۶برای تعامل‌پذیری است، نام ساختار داده‌ها برای تعامل‌پذیری می‌باشد.

CHOICE **غیرمستقیم** باید برای ObjectValue مربوط به typeAttributes شیء اطلاعاتی محتوی داده‌های ISO/IEC 7816-15 که نمایانگر یک DSI است، نشان داده شود. مسیر شرح داده شده زیر، باید انطباق نام DSI با نمونه واقعی DSI روی واسط عمومی کارت باشد. بنابراین، مسیر، شامل محل DSI درون برنامه کاربردی کارت، آفست اولین بایت DSI در این محل، و طول داده‌های درون DSI بر حسب بایت، می‌باشد.

جدول پ-۱ -کدگذاری ISO/IEC 7816-15 مربوط به یک Data Set

Data-Set	خصوصیت	توضیح
Common Object Attributes	label	نام data-set
	accessControlRules	لیست کنترل دستیابی data-set؛ به عبارت دیگر برای تمام DSIهای درون data-set
Common Data Container Object Attributes	<unused>	یا applicationName یا applicationOID باید وجود داشته باشند و نباید مقدار NULL داشته باشند. این مقدار باید نادیده گرفته شود.
Data Object Attributes	<unused>	ObjectValue باید با CHOICE مستقیم مقدار NULL وجود داشته باشد و باید نادیده گرفته شود.
DSI		
Common Object Attributes	Label	نام DSI
Common Data Container Object Attributes	<unused>	یا applicationName یا applicationOID باید وجود داشته باشند و نباید مقدار NULL داشته باشند. این مقدار باید نادیده گرفته شود.
Data Object Attributes	Iso7816DO.realative.path	مسیر DSI در برنامه کاربردی کارت، آفست اولین بایت داده‌ها در این محل، و طول داده‌ها بر حسب بایت

هویت‌های متمایزکننده استاندارد ملی ایران ۱۶۳۸۶

هر هویت متمایزکننده در یک برنامه کاربردی کارت استاندارد ملی ایران ۱۶۳۸۶به وسیله یک جزء ISO/IEC 7816-15 authObjects که دقیقا دربرگیرنده یک شیء اطلاعاتی احراز هویت است، در توصیف خدمت برنامه کاربردی کارت، نشان داده می‌شود. این اشیاء اطلاعاتی احراز هویت، تمام هویت‌های متمایزکننده شناخته‌شده به وسیله برنامه کاربردی کارت، نه فقط هویت‌های متمایزکننده متعلق به متغیرهای وضعیت احراز هویت واقع در قوانین دستیابی، را توصیف می‌کند.

خصوصیت ISO/IEC 7816-15 label در خصوصیات شیء مشترک مربوط به شیء اطلاعاتی احراز هویت ISO/IEC 7816-15 که یک هویت متمایزکننده استاندارد ملی ایران ۱۶۳۸۶را توصیف می‌نماید، نام هویت متمایزکننده است.

خصوصیت ISO/IEC 7816-15 accessControlRules مربوط به هر شیء اطلاعاتی احراز هویت، با استفاده از بایت حالت دستیابی مطابق با جدول ۱ زیر، لیست کنترل دستیابی استاندارد ملی ایران ۱۶۳۸۶ را برای هویت متمایزکننده، پیاده‌سازی می‌نماید.

خصوصیت ISO/IEC 7816-15 authId در خصوصیات شیء مشترک مربوط به شیء اطلاعاتی احراز هویت ISO/IEC 7816-15، که یک هویت متمایزکننده استاندارد ملی ایران ۱۶۳۸۶را توصیف می‌نماید، اختیاری است. اگر وجود داشته باشد، حاوی مقدار یافت شده در فیلد reference مربوط به یک مدخل در لیست supportedAlgorithms در ciaInfo است با این معنی که این الگوریتم برای احراز هویت هویت متمایزکننده استفاده شده است.

خصوصیت ISO/IEC 7816-15 authId در خصوصیات شیء احراز هویت مشترک مربوط به شیء اطلاعاتی احراز هویت ISO/IEC 7816-15، که یک هویت متمایزکننده استاندارد ملی ایران ۱۶۳۸۶را توصیف می‌نماید، یک شناسه منحصر بفرد هویت متمایزکننده درون توصیف خدمت است. این خصوصیت برای ارجاع متقابل خصوصیات سایر اشیاء اطلاعاتی به این Differential-Attribute استفاده شده است.

خصوصیت ISO/IEC 7816-15 authReference در خصوصیات شیء احراز هویت مشترک مربوط به شیء اطلاعاتی احراز هویت ISO/IEC 7816-15، که یک هویت متمایزکننده استاندارد ملی ایران ۱۶۳۸۶را توصیف می‌نماید، یک ارجاع کلید است که برای اشاره به هویت متمایزکننده درون محیطهای امنیتی و قوانین دستیابی استفاده می‌شود.

اگر خصوصیت مسیر در خصوصیات ویژه نوع، مربوط به شیء اطلاعاتی احراز هویت، وجود داشته باشد، به علامت‌گذار مربوط به هویت متمایزکننده، ارجاع خواهد داد.

جدول پ-۲ -کدگذاری ISO/IEC 7816-15 مربوط به یک هویت متمایزکننده

هویت متمایزکننده	خصوصیت	توضیح
Common Object Attributes	label	نام هویت متمایزکننده
	accessControl Rules	لیست کنترل دستیابی برای هویت متمایزکننده
	authId	مقدار فیلد مرجع در یک عضو لیست supportedAlgorithms در ciaInfo
Common Authentication Object Attributes	authId	شناسه منحصر بفرد هویت متمایزکننده درون برنامه کاربردی کارت
	authReference	مرجع کلید هویت متمایزکننده
Auth Object Attributes	<any>	توصیف پارامترهای احراز هویت مورد استفاده برای احراز هویت مربوط به هویت متمایزکننده

خدمات و اعمال برنامه کاربردی کارت ISO/IEC 24727

هر خدمت برنامه کاربردی کارت در یک برنامه کاربردی کارت استاندارد ملی ایران ۱۶۳۸۶ در توصیف خدمت برنامه کاربردی کارت، به وسیله یک جزء ISO/IEC 7816-15 dataContainerObjects که حاوی ترتیب اشیاء اطلاعاتی محتوی داده‌ها است، نشان داده می‌شود. اولین شیء اطلاعاتی محتوی داده‌ها، خدمت را توصیف می-کند. اشیاء اطلاعاتی محتوی داده‌های بعدی، اختیاری هستند و در صورت وجود، هر کدام یک عمل درون خدمت را توصیف می‌نمایند.

خصوصیت ISO/IEC 7816-15 label در خصوصیات شیء مشترک مربوط به اولین شیء اطلاعاتی محتوی داده-های ISO/IEC 7816-15 در ترتیب اشیاء اطلاعاتی محتوی داده‌ها، نام خدمت برنامه کاربردی کارت می‌باشد.

خصوصیت ISO/IEC 7816-15 accessControlRules در خصوصیات شیء مشترک مربوط به اولین شیء اطلاعاتی محتوی داده‌های ISO/IEC 7816-15 در ترتیب اشیاء اطلاعاتی محتوی داده‌های تشکیل دهنده یک خدمت استاندارد ملی ایران ۱۶۳۸۶، لیست کنترل دستیابی استاندارد ملی ایران ۱۶۳۸۶ برای خدمت با استفاده از نگاشتهای مشروح در جدول پ-۴ زیر را نشان می‌دهد.

خصوصیت ISO/IEC 7816-15 iD در خصوصیات شیء محتوی داده‌های مشترک مربوط به اولین شیء اطلاعاتی محتوی داده‌های ISO/IEC 7816-15 در ترتیب اشیاء اطلاعاتی محتوی داده‌های تشکیل دهنده یک خدمت استاندارد ملی ایران ۱۶۳۸۶، شامل یک توصیف آزاد از خدمت است.

هر شیء اطلاعاتی محتوی داده‌های ISO/IEC 7816-15 بعدی در ترتیب اشیاء اطلاعاتی محتوی داده‌های تشکیل دهنده یک خدمت استاندارد ملی ایران ۱۶۳۸۶، یک عمل استاندارد ملی ایران ۱۶۳۸۶ در خدمت استاندارد ملی ایران ۱۶۳۸۶شرح داده شده به وسیله اولین شیء اطلاعاتی محتوی داده‌ها را توصیف می‌نماید.

خصوصیت ISO/IEC 7816-15 label در خصوصیات شیء مشترک مربوط به یک شیء اطلاعاتی محتوی داده-های ISO/IEC 7816-15 در توصیف یک عمل، نام آن عمل می‌باشد.

CHOICE **غیرمستقیم** باید برای ObjectValue مربوط به typeAttributes شیء اطلاعاتی محتوی داده‌های نمایانگر یک DSI، نشان داده شود. مسیر توصیف شده باید مسیر کد اجرایی پیاده‌سازی‌کننده آن عمل باشد. در واقع، کد اجرایی مجاز است که یک برنامه کاربردی کامل کارت را محقق سازد؛ به عنوان مثال، کد اجرایی مجاز است که یک پودمان استاندارد ملی ایران ـ ایزو ـ آی ای سی ۲۰۰۶۰، یک کاربرد تحت MULTOS[1] یا یک کاربرد تحت جاوا[2] باشد.

اگر یک خدمت یا یک عمل در یک ISO/IEC 7816-15 dataContainerObject شرح داده نشده باشد، آنگاه توصیه می‌شود که وضعیت دسترسی به آن، به "Never" تنظیم شود.

جدول پ-۳ -کدگذاری ISO/IEC 7816-15 مربوط به یک خدمت

خدمت	خصوصیت	توضیح
Common Object Attributes	label	نام خدمت (به وسیله استاندارد ملی ایران ۳ـ ۱۶۳۸۶)
	accessControlRules	قوانین دستیابی برای اعمال درون خدمت که هدف آنها لیست کنترل دستیابی مربوط به خدمت است
Common Data Container Object Attributes	RFU	یا applicationName یا applicationOID باید وجود داشته باشند و نباید مقدار NULL داشته باشند. این مقدار باید نادیده گرفته شود.
Data Object Attributes	objectValue	ObjectValue به همراه CHOICE غیرمستقیم با ReferenceValue که محل کد اجرایی پیاده‌سازی‌کننده خدمت درون برنامه کاربردی کارت یا NULL است.
Action		
Common Object Attributes	label	نام عمل (به وسیله استاندارد ملی ایران ۳ـ ۱۶۳۸۶)؛ نگاشتهای درون جدول پ-۴ را ملاحظه فرمایید.
	accessControlRules	قوانین دستیابی برای عمل‌هایی در خدمت که هدف آنها برنامه کاربردی کارت است
Common Data Container Object Attributes	RFU	یا applicationName یا applicationOID باید وجود داشته باشند و نباید مقدار NULL داشته باشند. این مقدار باید نادیده گرفته شود.
Data Object Attributes	objectValue	ObjectValue به همراه CHOICE غیرمستقیم با ReferenceValue که محل کد اجرایی پیاده‌سازی‌کننده عمل درون برنامه کاربردی کارت یا NULL است.

1 -MULTOS Cardlet
2 -Java Applet

نگاشت اعمال به بایت‌های حالت دستیابی

جدول پ-۴ -اعمال استاندارد ملی ایران ۳ـ ۱۶۳۸۶تگاشت شده به ISO/IEC 7816-15 CommonObjectAttributes.label

عمل استاندارد ملی ایران ۳ـ ۱۶۳۸۶	CommonObjectAttributes.label (الزامی)
ACLList	“ACL_LIST”
ACLModify	“ACL_MODIFY”
CardApplicationEndSession	“CA_END_SESSION”
CardApplicationStartSession	“CA_START_SESSION”
CardApplicationDisconnect	“CA_DISCONNECT”
CardApplicationConnect	“CA_CONNECT”
CardApplicationCreate	“CA_CREATE”
CardApplicatonDelete	“CA_DELETE”
CardApplicatonServiceCreate	“CA_SERVICE_CREATE”
CardApplicationServiceLoad	“CA_SERVICE_LOAD”
CardApplicationServiceDelete	“CA_SERVICE_DELETE”
CardApplicationList	“CA_LIST”
CardApplicationServiceList	“CA_SERVICE_LIST”
CardApplicationServiceDescribe	“CA_SERVICE_DESCRIBE”
ExecuteAction	“EXECUTE_ACTION”
DataSetCreate	“DS_CREATE”
DataSetDelete	“DS_DELETE”
DataSetSelect	“DS_SELECT”
DataSetList	“DS_LIST”
DSICreate	“DSI_CREATE”
DSIDelete	“DSI_DELETE”
DSIList	“DSI_LIST”
DSIWrite	“DSI_WRITE”
DSIRead	“DSI_READ”
DIDList	“DID_LIST”
DIDCreate	“DID_CREATE”
DIDDelete	“DID_DELETE”
DIDUpdate	“DID_UPDATE”
DIDGet	“DID_GET”
DIDAuthenticate	"DID_AUTHENTICATE"
Encipher	“ENCIPHER”
Decipher	“DECIPHER”
GetRandom	“GET_RANDOM”

جدول پ ـ ۴ (ادامه)

Hash	“HASH”
Sign	“SIGN”
VerifySignature	“VERIFY_SIGNATURE”
VerifyCertificate	“VERIFY_CERTIFICATE

پیوست ت

(اطلاعاتی)

نمونه‌ای از برنامه کاربردی اطلاعات رمزنگاشتی‌شده برای توصیف خدمت برنامه کاربردی کارت

```
{ -- SEQUENCE --
cardInfo { -- SEQUENCE --
version 2,
serialNumber '0102030405060708'H,
manufacturerID '41434d45'H -- "ACME" --,
label '506572736f6e616c204461746120566175c74'H
-- "Personal Data Vault" --,
cardflags '60'H,
supportedAlgorithms { -- SEQUENCE OF --
{ -- SEQUENCE --
reference 1,
algorithm 16,
supportedOperations '02'H,
objId {1 3 14 3 2 26},
algRef 1
},
{ -- SEQUENCE --
reference 2,
algorithm 272,
supportedOperations '0c'H,
objId {1 3 36 3 1 1},
algRef 2
},
{ -- SEQUENCE --
reference 3,
algorithm 544,
supportedOperations '50'H,
objId {1 2 840 113 549 1 1 5},
algRef 18
}
},
issuerId '4b61726d61204c6f6f70'H -- "Karma Loop" --,
holderId '53616c6c7920477265656e'H -- "Sally Green" --,
lastUpdate generalizedTime '313938353131303632313036323 72e335a'H
-- "19851106210627.3Z" --,
preferredLanguage '4573706572616e746f'H -- "Esperanto" --
},
cioChoice { -- SEQUENCE OF --
dataContainerObjects objects { -- SEQUENCE OF --
iso7816DO { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '436c6f7468696e672053697a6573'H -- "Clothing Sizes" --,
accessControlRules { -- SEQUENCE OF --
{ -- SEQUENCE --
accessMode '0000'b –- READ --,
securityCondition authId '01'H
},
{ -- SEQUENCE --
accessMode '0000'b –- WRITE --,
securityCondition authId '03'H
}
}
},
classAttributes { -- SEQUENCE --
```

```
applicationName '00'H
},
typeAttributes indirect path { -- SEQUENCE --
type efidOrPath "H
}
},
iso7816DO { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '4861742053697a65'H -- "Hat Size" --
},
classAttributes { -- SEQUENCE --
applicationName '00'H
},
typeAttributes indirect path { -- SEQUENCE --
type tagRef { -- SEQUENCE --
tag 'c1'H
},
length 4
}
},
iso7816DO { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '536f636b2053697a65'H -- "Sock Size" --
},
classAttributes { -- SEQUENCE --
applicationName '00'H
},
typeAttributes indirect path { -- SEQUENCE --
type tagRef { -- SEQUENCE --
tag 'c1'H
},
index 4,
length 4
}
}
},
authObjects objects { -- SEQUENCE OF --
pwd { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '53616c6c7920477265656e202d2050494e'H
-- "Sally Green - PIN" --,
authId '01'H
},
classAttributes { -- SEQUENCE --
authId '81'H,
authReference 128,
seIdentifier 2
},
typeAttributes { -- SEQUENCE --
pwdFlags '0000 1000'b,
pwdType 0,
minLength 4,
storedLength 4,
maxLength 8,
pwdReference 129,
padChar '00'H,
path { -- SEQUENCE --
type efidOrPath "H
}
}
}
},
authObjects objects { -- SEQUENCE OF --
```

```
pwd { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '53616c6c7920477265656e202d2050554b'H
-- "Sally Green - PUK" --,
authId '01'H
},
classAttributes { -- SEQUENCE --
authId '82'H,
authReference 129,
seIdentifier 2
},
typeAttributes { -- SEQUENCE --
pwdFlags '00101100'b,
pwdType 0,
minLength 8,
storedLength 8,
maxLength 8,
pwdReference 130,
padChar '00'H,
path { -- SEQUENCE --
type efidOrPath "H
}
}
}
},
authObjects objects { -- SEQUENCE OF --
authKey { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '53616c6c7920477265656e202d20536563726574204b6579'H
-- "Sally Green - Secret Key" --,
authId '02'H
},
classAttributes { -- SEQUENCE --
authId '03'H,
authReference 3,
seIdentifier 2
},
typeAttributes { -- SEQUENCE --
derivedKey FALSE,
authKeyId "H
}
}
},
dataContainerObjects objects { -- SEQUENCE OF --
iso7816DO { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '436f6e6e656374696f6e2053657276696365'H
-- "Connection Service" --,
accessControlRules { -- SEQUENCE OF --
{ -- SEQUENCE --
accessMode '0000'b –- ACL_LIST and ACL_MODIFY --,
securityCondition always NULL
}
}
},
classAttributes { -- SEQUENCE --
applicationName '00'H
},
typeAttributes indirect path { -- SEQUENCE --
type efidOrPath "H
}
}
},
```

```
dataContainerObjects objects { -- SEQUENCE OF --
iso7816DO { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '436172642d4170706c69636174696f6e2053657276696365'H
-- "Card-Application Service" --,
accessControlRules { -- SEQUENCE OF --
{ -- SEQUENCE --
accessMode '0000'b –- ACL_LIST --,
securityCondition always NULL
}
}
},
classAttributes { -- SEQUENCE --
applicationName '00'H
},
typeAttributes indirect path { -- SEQUENCE --
type efidOrPath "H
}
}
},
dataContainerObjects objects { -- SEQUENCE OF --
iso7816DO { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '4e616d65642044617461205365727669636 5'H
-- "Named Data Service" --,
accessControlRules { -- SEQUENCE OF --
{ -- SEQUENCE --
accessMode 'c0'H –- ACL_LIST and ACL_MODIFY --,
securityCondition authId '03'H
}
}
},
classAttributes { -- SEQUENCE --
applicationName '00'H
},
typeAttributes indirect path { -- SEQUENCE --
type efidOrPath "H
}
},
iso7816DO { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '4453495f52454144'H -- "DSI_READ" --,
accessControlRules { -- SEQUENCE OF --
{ -- SEQUENCE --
accessMode '0000 0000 0000 0000 0000 0000'b –- DSI_READ --,
securityCondition authId '01'H
}
}
},
classAttributes { -- SEQUENCE --
applicationName '00'H
},
typeAttributes indirect path { -- SEQUENCE --
type efidOrPath "H
}
},
iso7816DO { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '4453495f5752495445'H -- "DSI_WRITE" --,
accessControlRules { -- SEQUENCE OF --
{ -- SEQUENCE --
accessMode '0000 0000 0000 0000 0000 0000'b –- DSI_WRITE --,
securityCondition authId '03'H
```

```
}
}
},
classAttributes { -- SEQUENCE --
applicationName '00'H
},
typeAttributes indirect path { -- SEQUENCE --
type efidOrPath "H -- "" --
}
}
},
secretKeys objects { -- SEQUENCE OF --
genericSecretKey { -- SEQUENCE --
commonObjectAttributes { -- SEQUENCE --
label '534b2d31'H -- "SK-1" --
},
classAttributes { -- SEQUENCE --
iD '77'H,
usage '0000'b,
native TRUE,
accessFlags '1001'b,
keyReference 1
},
subClassAttributes { -- SEQUENCE --
keyLen 64
},
typeAttributes { -- SEQUENCE --
keyType {1 3 36 3 4 3 2 1},
keyAttr '01001101'b
}
}
}
}
}
```

پیوست ث
(اطلاعاتی)
کشف DID

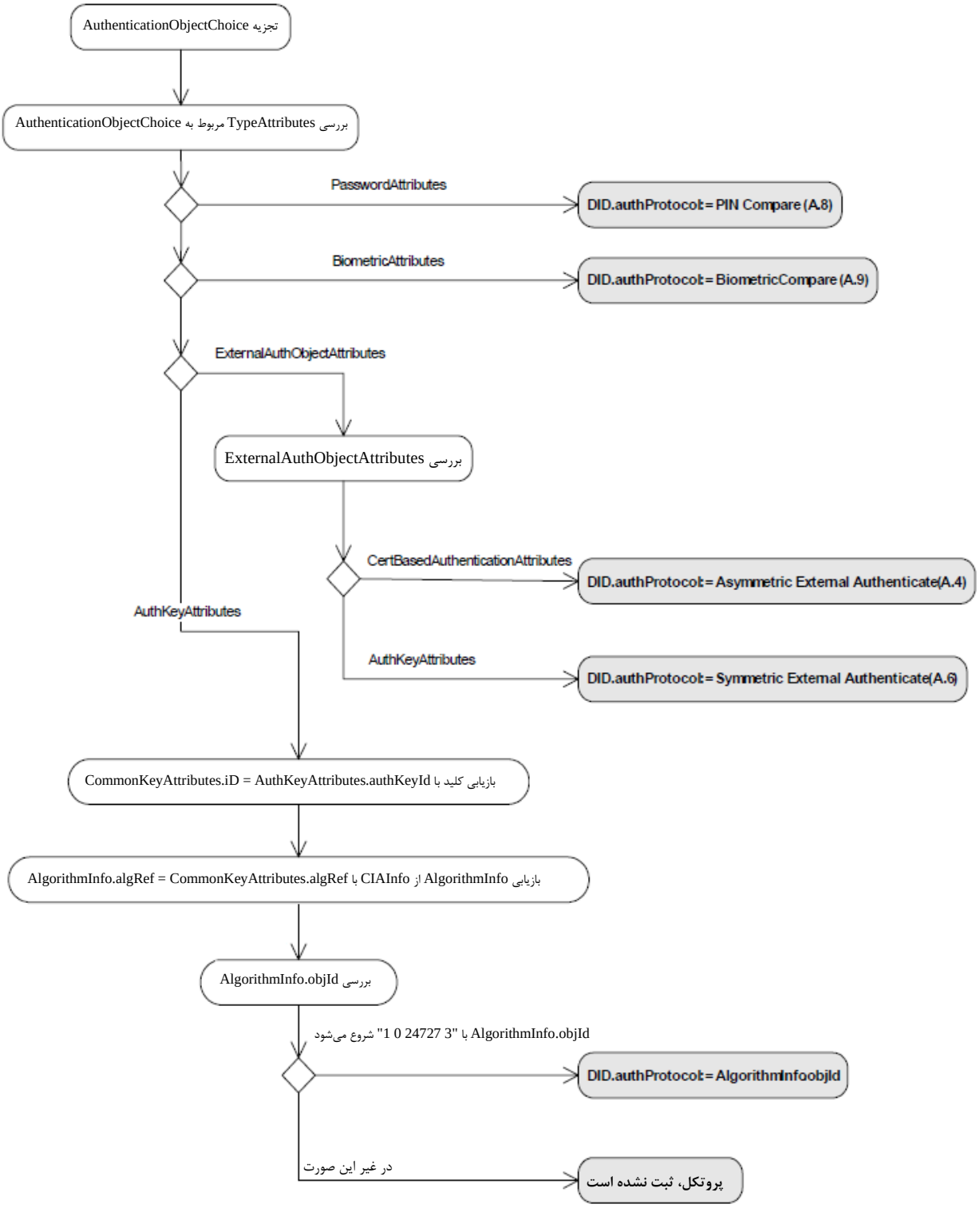
ساختار هویت تفاضلی، به شدت به پروتکل احراز هویت مورد استفاده، بستگی دارد. ساختارهای علامتگذار و تصدیق‌کننده تنها پس از تعیین شدن پروتکل احراز هویت، مشخص می‌شوند. بنابراین، اولین قدم در سازوکار کشف در حالی که توصیف خدمت مربوط به توصیف‌کننده قابلیت برنامه کاربردی تجزیه می‌شود، بازیابی مقدار صحیح برای پروتکل احراز هویت، است.

سازوکار کشف برای مقدار پروتکل احراز هویت، نشان‌داده‌شده در سازوکار، با تجزیه AuthenticationObjectChoice شروع می‌شود. در آغاز، TypeAttributes مربوط به AuthenticationObjectChoice تعیین خواهند شد. اگر TypeAttributes، PasswordAttributes یا BiometricAttributes باشند، نوع پروتکل احراز هویت یا پروتکل PIN Compare یا Biometric Compare خواهند بود.

در صورتی که TypeAttributes، ExternalAuthObjectAttributes باشند، باید بررسی شود که کدام گزینه برای ExternalAuthObjectAttributes انتخاب شده است:

اگر از CertBasedAuthenticationAttributes استفاده شده باشد، این پروتکل، پروتکل احراز هویت خارجی نامتقارن خواهد بود،

در صورتی که AuthKeyAttributes استفاده شده باشند، این پروتکل احراز هویت خارجی متقارن است، مگر آن که به وسیله objId مربوطه، خلاف آن مشخص گردد: AlgorithmInfo متناظر درون ساختار CIAInfo مربوط به برنامه کاربردی مناسب، برای بازیابی objId بکار گرفته می‌شود. اگر مقدار غیر DER-TLV کدگذاری‌شده معادل این objId، با "1 0 24727 3" شروع شود، این مقدار بطور مستقیم برای تعیین مقدار پروتکل احراز هویت، استفاده خواهد شد.



شکل ث-۱ کشف مقدار پروتکل احراز هویت

پیوست ج

(اطلاعاتی)

کتابنامه

[۱] استاندارد ملی ایران ـ ایزو ـ آی ای سی ۳ـ ۹۷۹۶ ،فن آوری اطلاعات - فنون امنیتی – طرح‌های امضای دیجیتال با قابلیت بازیابی پیام - قسمت سوم - سازوکارهای مبتنی بر لگاریتم گسسته

[۲] استاندارد ملی ایران شماره : ۲ـ ۱۶۱۹۶، فناوری اطلاعات ـ فنون امنیتی ـ طرح‌های امضای رقمی(دیجیتال) با بازیابی پیام - قسمت ۲: سازوکارهای مبتنی بر تجزیه اعداد صحیح

[۳] استاندارد ملی ایران ـ ایزو ـ آی ای سی ۱ ـ ۹۷۹۷ ،فناوری اطلاعات -فنون امنیتی -کدهای احراز هویت پیام (MAC) قسمت ۱ - سازو کارهای استفاده از رمز گذاری بلوکی

[۴] استاندارد ملی ایران شماره ۱ ـ ۱۰۸۲۵، فناوری اطلاعات -فنون امنیتی -احراز هویت هستار قسمت ۱ - کلیات

[۵] استاندارد ملی ایران شماره ۲ ـ ۱۰۸۲۵، فناوری اطلاعات -فنون امنیتی -احراز هویت هستارقسمت ۲ - سازوکارهای استفاده کننده از الگوریتم های پوشیده سازی متقارن

[۶] استاندارد ملی ایران شماره ۳ ـ ۱۰۸۲۵، فناوری اطلاعات -فنون امنیتی -احراز هویت هستارقسمت ۲ - سازوکارهای استفاده کننده از الگوریتم های پوشیده سازی متقارن

[۷] استاندارد ملی ایران شماره ۴ ـ ۱۰۸۲۵، فن آوری اطلاعات -فنون امنیتی تشخیص هویت نهاد-قسمت چهارم-مکانیزم های استفاده کننده از یک تابع مقابله رمز نگاری

[۸] استاندارد ملی ایران شماره ۵ ـ ۱۰۸۲۵ ،فناوری اطلاعات – فنون امنیتی– احراز هویت هستار-قسمت ۵ : سازوکارهای استفاده‌کننده از فنون دانش_صفر

[۹] استاندارد ملی ایران شماره ۶ ـ ۱۰۸۲۵، فناوری اطلاعات -فنون امنیتی -احراز هویت هستار قسمت ۶ - سازوکارهای استفاده از انتقال دستی داده ها

[۱۰] استاندارد ملی ایران شماره ۹۶۰۰ ، فن آوری اطلاعات -روش های امنیتی -حالت های عملیاتی یک الگوریتم رمز نگاری قطعه ای N بیتی

[۱۱] استاندارد ملی ایران شماره ۱ـ ۹۵۹۸ ،فن آوری اطلاعات -روش های امنیتی -توابع در هم ساز قسمت اول -کلیات

[۱۲] استاندارد ملی ایران شماره ۳ ـ ۹۵۹۸، فناوری اطلاعات -فنون امنیتی -توابع درهم ساز -قسمت ۳- توابع درهم ساز اختصاصی

[۱۳] استاندارد ملی ایران شماره ۴ـ ۹۵۹۸، فن آوری اطلاعات -روش های امنیتی -توابع در هم ساز قسمت چهارم-توابع درهم ساز با استفاده از محاسبات پیمانه ای

[۱۴] استاندارد ملی ایران شماره ۳ ـ ۱۰۸۲۲، فناوری اطلاعات -فنون امنیتی-مدیریت کلید -قسمت ۳-ساز و کارهای مبتنی بر فنون نامتقارن

[۱۵] استاندارد ملی ایران شماره ۴ ـ۱۰۸۲۲ ، فن آوری اطلاعات -فنون امنیتی -مدیریت کلید-قسمت چهارم -مکانیزم مبتنی بر رازهای ضعیف
[۱۶] استاندارد ملی ایران شماره ۲ ـ۱۶۲۹۰،کارتهای شناسایی -کارت های مدار مجتمع بدون تماس -کارت های مجاورتی -قسمت ۲- توان بسامد رادیویی و واسط سیگنال
[۱۷] استاندارد ملی ایران شماره ۴ ـ۱۶۲۹۰،کارتهای شناسایی -کارت های مدار مجتمع بدون تماس -کارت های مجاورتی -قسمت ۴- پروتکل انتقال
[۱۸] استاندارد ملی ایران شماره ۱ـ ۱۱۴۹۴،فناوری اطلاعات -فنون امنیت امضاهای دیجیتال با پیوست قسمت ۱:کلیات
[۱۹] استاندارد ملی ایران ایزو ـ آی ای سی شماره ۲ ـ ۱۴۸۸۸، فناوری اطلاعات -فنون امنیتی -امضاهای رقمی(دیجیتالی)با پیوست قسمت ۲- سازوکارهای بر پایه عامل بندی صحیح
[۲۰] استاندارد ملی ایران ایزو ـ آی ای سی شماره ۳ـ ۱۴۸۸۸،فناوری اطلاعات -فنون امنیتی -امضاهای رقمی (دیجیتال) با پیوست قسمت ۳- سازوکارهای بر پایه لگاریتم گسسته
[۲۱] استاندارد ملی ایران ۱ ـ ۱۰۸۲۴،فن آوری اطلاعات -فنون امنیتی الگوریتم های رمز نگاری-قسمت اول- کلیات
[۲۲] استاندارد ملی ایران ۳ ـ ۱۰۸۲۴،فناوری اطلاعات -فنون امنیتی -الگوریتم های رمز نگاری-قسمت ۳:رمزهای بلوکی
[۲۳] استاندارد ملی ایران ۴ ـ ۱۰۸۲۴، فن آوری اطلاعات -فنون امنیتی الگوریتم های رمز نگاری-قسمت چهارم-رمز گذاری جریانی
[۲۴] استاندارد ملی ایران ـ ایزو ـ آی ای سی ۲۰۰۶۰، فناوری اطلاعات-معماری پایانه باز (OTA) ماشین مجازی
[۲۵] استاندارد ملی ایران ـ ایزو ـ آی ای سی ۱ ـ ۸۸۲۵، فناوری اطلاعات -قواعد کد بندی نشانه گذاری قاعده ی نحوی انتزاعی یک (ASN.1) ویژگی قواعد کد بندی پایه (BER) قواعد کد بندی متعارف (CER) و قواعد کد بندی متمایز(DER)
[۲۶] استاندارد ملی ایران ـ ایزو ـ آی ای سی ۲ ـ ۸۸۲۵، فناوری اطلاعات -قواعد کد بندی نشانه گذاری قاعده ی نحوی انتزاعی یک(ASN.1) ویژگی قواعد کد بندی فشرده (PER)
[۲۷] استاندارد ملی ایران ـ ایزو ـ آی ای سی۳ـ ۸۸۲۵، فناوری اطلاعات -قواعد کد بندی نشانه گذاری قاعده ی نحوی انتزاعی یک (ASN.1) ویژگی نشانه گذاری کنترل کد بندی(ECN)
[۲۸] استاندارد ملی ایران ـ ایزو ـ آی ای سی ۴ـ ۸۸۲۵، فناوری اطلاعات -قواعد کد بندی نشانه گذاری قاعده ی نحوی انتزاعی یک(ASN.1) قواعد کد بندیXML(XER)
[۲۹] استاندارد ملی ایران ـ ایزو ـ آی ای سی ۵ ـ ۸۸۲۵، فناوری اطلاعات -قواعد کد بندی نشانه گذاری قاعده ی نحوی انتزاعی یک(ASN.1) نگاشت تعازیف نماواره ASN.1 W3C XML

[۳۰] استاندارد ملی ایران ـ ایزو ـ آی ای سی ۶ ـ ۸۸۲۵، فناوری اطلاعات -قواعد کدبندی نشانه‌گذاری قاعده‌ی نحوی انتزاعی شماره یک(ASN.1) ثبت و کاربرد دستور العمل‌های کدبندی قواعد کدبندی بسته یا(PER)
[۳۱] استاندارد ملی ایران شماره ۱ ـ ۱۱۶۸۶،کارت‌های شناسایی –کارت‌های مدار(های) مجتمع غیر تماسی – کارت‌های مجاورتی (دوربرد)قسمت ۱-خصوصیات فیزیکی
[32] ISO/IEC 8825 (all parts), Information technology — ASN.1 encoding rules
[33] ISO/IEC 9979:1999, Information technology — Security techniques — Procedures for the registration of cryptographic algorithms
[34] ISO 9992-2:1998, Financial transaction cards — Messages between the integrated circuit card and the card accepting device — Part 2: Functions, messages (commands and responses), data elements and structures
[35] IETF RFC 1738:1994, Uniform Resource Locators (URL)
[36] IETF RFC 1778:1995, The String Representation of Standard Attribute Syntaxes
[37] IETF RFC 2396:1998, Uniform Resource Identifiers (URI): Generic Syntax
[38] ISO/IEC 9797-2:2011, Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
[39] ISO/IEC 9797-3:2011, Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 3: Mechanisms using a universal hash-function
[40] ISO 10118-2: 2010, Information technology -- Security techniques -- Hash-functions -- Part 2 : Hash-functions using an n-bit block cipher
[41] ISO/IEC 11770-1:2010 , Information technology -- Security techniques -- Key management -- Part 1: Framework
[42] ISO/IEC 11770-2:2008 , Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques
[43] ISO/IEC 11770-5:2011 , Information technology -- Security techniques -- Key management -- Part 5: Group key management
[44] ISO/IEC 14443-1:2008 , Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics
[45] ISO/IEC 14443-3:2011, Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision
[46] ISO/IEC 18033-2:2006 , Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers
[47] ISO/IEC 15693-2:2006 , Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 2: Air interface and initialization
[48] ISO/IEC 15693-3:2009 , Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 3: Anticollision and transmission protocol