INSO
16386-1
1st.Edition
Jun.2013

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

استاندارد ملی ایران
۱ـ۱۶۳۸۶
چاپ اول
تیر ۱۳۹۲

کارت‌های شناسایی ـ واسط‌های برنامه نویسی کارت دارای مدار مجتمع ـ قسمت ۱ :معماری

Identification cards -- Integrated circuit card programming interfaces -- Part 1: Architecture

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 برنامه‌نویسی کارت دارای مدار مجتمع ـ

قسمت ۱ :

معماری"

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

نوروزی زاده، حمیرا
(کارشناسی مهندسی صنایع)

کارشناس استاندارد

فهرست مندرجات

عنوان		صفحه
آشنایی با سازمان ملی استاندارد		ب
کمیسیون فنی تدوین استاندارد		ج
پیش گفتار		و
مقدمه		ز
۱	هدف و دامنه کاربرد	۱
۲	مراجع الزامی	۱
۳	اصطلاحات و تعاریف	۱
۴	کوته‌نوشت‌ها	۵
۵	تعامل‌پذیری	۶
۶	معماری	۶
۷	منطق امنیتی	۱۱
۸	پیوست الف(اطلاعاتی) مثال‌های پیکربندی پیاده‌سازی	۱۲
۹	پیوست ب(اطلاعاتی) کتابنامه	۲۴

پیش گفتار

استاندارد " کارت‌های شناسایی ـ واسط‌های برنامه نویسی کارت دارای مدار مجتمع ـ قسمت **۱** :معماری" 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 24727-1:2007, Identification cards -- Integrated circuit card programming interfaces -- : Architecture Part 1

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[1] برنامه نویسی کارت دارای مدار مجتمع ـ
قسمت ۱ :معماری

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین موارد زیر می‌باشد :

- معماری سامانه و اصول عملکرد
- ساز و کار کشف قابلیت‌ها
- اصول امنیتی

این استاندارد مستقل از فناوری واسط فیزیکی 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 می‌شود. در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آن مورد نظراست.

استفاده از مرجع زیر، برای این استاندارد الزامی است:

2-1 ISO/IEC 7816-4:2005 Identification cards – Integrated circuit cards – Part 4 : Organization ,Security and commands for interchange

۳ اصطلاحات و تعاریف

در این استاندارد، تعاریف و اصطلاحات زیر به کار می‌رود:

۳ – ۱

احراز هویت[2]

فرآیند ارزیابی سطح اعتماد در هویت یا شناسایی است.

۳ – ۲

پروتکل احراز هویت[3]

فرآیند خاص برای احراز هویت است .

1-Interfaces
2- Authentication
3 - Authentication protocol

۳-۳

کارت

کارت دارای مدار مجتمع است .

۴ – ۳

برنامه کاربردی کارت[1]

مجموعه‌ای از کارکردهای کارت دارای مدار مجتمع قابل نشانی‌دهی یکتا که ذخیره‌سازی داده‌ها و ارائـه خـدمات محاسباتی را به یک برنامه کاربردی کارخواه فراهم می‌نماید.

۵ – ۳

برنامه کاربردی کارخواه[2]

نرم‌افزار پردازشی که نیاز به دسترسی به یک یا چند برنامه یا برنامه‌های کاربردی کارت دارد.

۶–۳

عنصر داده[3]

بخشی از اطلاعات موجود در واسط که نشان‌دهنده یک نام، یک شرح از محتوای منطقی، یک قالب و یک کد است.

۷ – ۳

مجموعه داده‌ها[4]

مجموعه‌ای از ساختارهای داده برای تعامل‌پذیری

۸ – ۳

ساختار داده برای تعامل‌پذیری[5]

فایل استاندارد ISO/IEC 7816-4 شناسایی‌شده به وسیله یک شناسه فایل دو بایتی یا یک ISO/IEC 8825 BER-TLV برای شئ داده شناسایی‌شده توسط یک رشـته بـایتی کدبنـدی بـا برچسـب نشـانه‌گـذاری نحـوی انتزاعی(ASN.1)[6] می‌باشد.

1- Card-application
2 - Client-application
3- Data element
4 - Data set
5- Data structure for interoperability
6-Abstract Syntax Notation.1

۳- ۹

هویت متمایزکننده[1]

مجموعه‌ای از اطلاعات که شامل نام، علامت و پروتکل احراز هویت است.

۳- ۱۰

لایه دسترسی عام کارت[2]

مولفه‌هایی که واسط استاندارد ملی ایران شماره ۲ ـ ۱۶۳۸۶ را برای یک لایه دسترسی خدمات فراهم می‌کند.

۳ – ۱۱

شناسایی[3]

مجموعه‌ای از مشخصه‌ها و فرآیندها است که به وسیله آن‌ها یک هستار[4] قابل‌تشخیص یا شناسایی می‌شود.

۳- ۱۲

واسط

نقطه‌ای است که در آن سامانه‌های مستقل و غالباً غیرمرتبط با یکدیگر تلاقی و عمل می‌کنند یا در ارتباط با هم هستند.

۳- ۱۳

تعامل‌پذیری[5]

توانایی برای هر واسط برنامه کاربردی کارت مطابق با استاندارد ملی ایران شماره ۱۶۳۸۶، استفاده شده توسط هر برنامه کاربردی کارخواه مطابق با استاندارد ملی ایران شماره ۱۶۳۸۶ .

---

1 - Differential -identity
2- Generic card access layer
3 - Identification
4 - Entity
5 - Interoperability

۳ -۱۴

علامت[1]

بخشی از اطلاعات در مشخصه هویت که نماینده خصوصیت منحصر به فرد یک هستار می‌باشد.

۳ – ۱۵

میان افزار[2]

نرم‌افزاری که دو برنامه مستقل غیرمرتبط را به هم مرتبط می‌نماید.

۳- ۱۶

خدمت[3]

مجموعه‌ای از کارکردهای پردازشی قابل دسترس در یک واسط.

۳- ۱۷

لایه دسترسی خدمت[4]

مولفه‌هایی که یک واسط برنامه‌نویسی برنامه کاربردی (API) مطابق با استاندارد ملی ایـران شـماره ۳ ـ ۱۶۳۸۶را برای یک برنامه کاربردی کارخواه فراهم می‌نماید.

۴ کوته‌نوشت‌ها

شناسانه برنامه کاربردی	AID application indentifier
توصیف قابلیت برنامه کاربردی	ACD application capability description
واحد داده پروتکل برنامه کاربردی	APDU application protocol data unit
واسط برنامه‌نویسی برنامه کاربردی	API application programming interface

1 - Marker
2- Middleware
3 - Service
4 - Service access layer

BER	basic encoding rules	قواعد کدبندی پایه
CCD	card capability description	توصیف قابلیت کارت
DSI	data structure for interoperability	ساختار داده برای تعامل‌پذیری
GCAL	generic card access layer	لایه دسترسی عمومی کارت
GCI	generic card interface	واسط عمومی کارت
IAS	Identity, authentication, and (digital) signature services	هویت، احراز هویت و خدمات امضای دیجیتال
ICC	integrated circuit card	کارت دارای مدار مجتمع
IFD	interface device	دستگاه واسط
OID	object identifier	شناسه شئ
PKI	public key infrastructure	زیرساخت کلید عمومی
RFU	reserved for future use by ISO/IEC	رزرو شده برای استفاده آتی توسط ISO/IEC
SAL	service access layer	لایه دسترسی به خدمت
TLV	tag-length –value	برچسب ـ طول ـ مقدار
URL	uniform resource locator	مکان‌یاب یکسان منبع

۵ تعامل پذیری

تعامل‌پذیری، توانایی هر واسط برنامه کاربردی کارت مطابق با استاندارد ملی ایران شماره ۱۶۳۸۶است که توسط هر برنامه کاربردی کارخواه در تطابق با استاندارد ملی ایران شماره ۱۶۳۸۶استفاده می‌شود.

استاندارد ملی ایران شماره ۱۶۳۸۶، مجموعه‌ای از واسط‌ها و سازوکارهای کشف، را طوری تعریف می‌کند که پیاده‌سازی‌های مستقل که از لحاظ عملکردی، یکسان هستند به وسیله آزمودن، قابل تائید می‌باشند.

استاندارد ملی ایران شماره ۱۶۳۸۶ واسط‌ها را در دو سطح تعیین می‌نماید.

ـ بین یک برنامه کاربردی کارخواه و واسط خدمت،

ـ بین یک لایه دسترسی خدمت و یک واسط عمومی کارت.

برای هر واسط مشخص‌شده، قسمت‌های مربوط به استاندارد که از نظر کاربردی، توسط آن واسط پشتیبانی می‌شوند، باید تعریف گردند.

استاندارد ملی ایران شماره ۱۶۳۸۶، برای کارت‌های دارای مدار مجتمع با توصیف قابلیت، به صورت مستقیم یا غیرمستقیم به‌کارمی‌رود. توصیف قابلیت در بند ۶ ـ۶ آورده شده است.

واسط خدمت، واسط کارت عمومی و توصیف قابلیت‌ها ممکن است با توجه به توسعه آینده فناوری‌های کارت‌های دارای مدار مجتمع، گسترش یابد.

۶ معماری

۶-۱ کلیات

استاندارد ملی ایران شماره ۱۶۳۸۶کارکرد بین برنامه کاربردی کارخواه بر روی پلاتفرم[۱] میزبان و یک مجموعه لایه‌بندی‌شده از خدمات را تفکیک می‌کند که می‌تواند توسط یک برنامه کاربردی کارخواه استفاده شود. سازمان ارائه دهنده خدمت، واسط خدمت، واسط عمومی کارت، و یک یا چند برنامه کاربردی مستقر بر روی کارت دارای مدار مجتمع را تعریف می‌کند.

۶ ـ۲ خصوصیات معماری

ویژگی‌های پیاده‌سازی واسط خدمت، در بند ۶-۵ ذکر شده است.

ویژگی‌های پیاده‌سازی واسط عمومی کارت، در بند۶-۸ ذکر شده است.

ویژگی‌های پیاده‌سازی واسط اتصال، در بند ۶-۹ ذکر شده است.

ویژگی‌های پیاده‌سازی واسط کانال مورد اعتماد، در بند ۶-۱۰ ذکر شده است.

برنامه‌های کاربردی کارت، مجموعه داده‌ها را مدیریت می‌کند. هر مجموعه داده‌ها، نامگذاری می‌شود و فهرست داده‌های مجموعه نام‌های برنامه کاربردی کارت، برای برنامه کاربردی کارخواه از طریق آگاهی مستقیم یا کشف، قابل‌دسترس است. یک برنامه کاربردی کارخواه، از نام مجموعه داده‌ها وقتی که خدمت، اجرا بر روی مجموعه داده‌ها را درخواست می‌کند، استفاده می‌نماید.

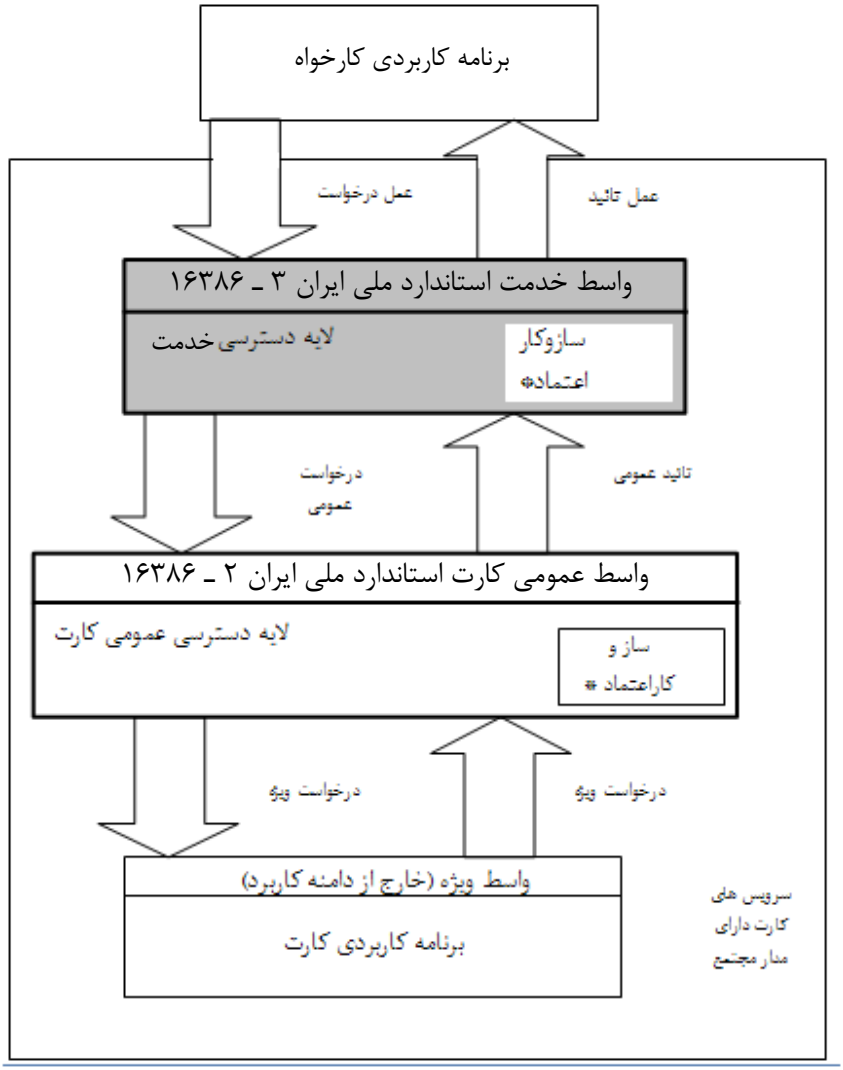
دسترسی به مجموعه داده‌ها از طریق یک فهرست کنترل دسترسی، کنترل شده است. فهرست کنترل دسترسی، شرایط امنیتی را شرح می‌دهد که به منظور انجام اقدام بر روی مجموعه داده‌ها، قابل‌دستیابی است. استاندارد ملی ایران شماره ۳ـ ۱۶۳۸۶جزئیات بیشتر در مورد فهرست‌های کنترل دسترسی، هویت‌ها، و اقدامات را ارائه می‌کند. برنامه‌های کاربردی کارت در کارت‌های دارای مدار مجتمع به عنوان یک برنامه کارت

1- Platform

آلفا و یک یا چند برنامه کاربردی کارت، سازمان‌یافته است. برنامه‌های کاربردی کارت به وسیله AID در واسط خدمت قابل‌انتخاب هستند.

۶ ـ ۳ معماری منطقی

شکل ۱ ارتباط بین نرم‌افزار کارخواه، لایه‌ها و واسط‌های تعریف شده در استاندارد ملی ایران شماره ۱۶۳۸۶، و یک برنامه کاربردی کارت مستقر در ICC را نشان می‌دهد. جریان درخواست‌های مشاهده‌شده از برنامه کاربردی کارخواه به برنامه کاربردی کارت به صورت پیکان جهت‌دار برای درخواست یا تأیید نشان داده شده است. نامگذاری هر یک از پیکان‌ها، بیان‌کننده قابلیتی است که استاندارد پشتیبانی می‌کند. بیان جزئیات قالب واقعی نحو[1] درخواست یا تأیید در این استاندارد آورده نشده است.



شکل ۱ ـ معماری منطقی استاندارد ملی ایران شماره ۱۶۳۸۶

1 - Syntax

کارکرد استاندارد ملی ایران شماره ۱۶۳۸۶می‌تواند در بیش از یک روش، پیاده‌سازی شود.

۶ ـ ۴ استقلال پروتکل

واسط‌های تعیین شده در استاندارد ملی ایران شماره ۱۶۳۸۶، در روشی مستقل از پروتکل‌های مورد نیاز، مشخص شده است تا ارتباط بین برنامه کاربردی کارخواه و برنامه کاربردی کارت را برقرار نماید.

شکل ۱، یک پشته[1] لایه‌ها و واسط‌ها را نشان می‌دهد.

یک پروکسی[2]، پیاده‌سازی واسط عنصر پشته می‌باشد که به پیاده‌سازی عنصر پشته اجازه تقسیم شدن بدهد. برای مثال، برنامه کاربردی کارت در شکل ۱، یک پروکسی برای کارت واقعی است.

برای جزئیات در مورد پیکربندی‌های پیاده‌سازی پشته به پیوست الف رجوع شود.

۶ـ ۵ واسط لایه دسترسی خدمات برنامه کاربردی کارخواه

استاندارد ملی ایران شماره ۳ــ ۱۶۳۸۶شرح مفصلی از واسط خدمت در دسترس برای برنامه کاربردی خدمت‌گیرنده ارائه می‌کند.

یک پیاده‌سازی واسط خدمت

ـ درخواست یک عمل را به یک یا چند درخواست عمومی، ترجمه می‌کند،

ـ یک یا چند تایید عمومی را به یک تایید عمل، ترجمه می‌کند.

واسط خدمت شامل موارد زیر می‌باشد:

ـ اتصال برنامه کاربردی کارخواه به برنامه کاربردی کارت با استفاده از واسط عمومی کارت،

ـ امنیت برنامه کاربردی کارخواه به برنامه کاربردی کارت مطابق با اصول امنیتی،

ـ خدمت رمزنگاشتی[3]،

ـ خدمت مشخصه هویت.

۶ ـ۶ توصیف قابلیت

واسط خدمت و واسط عمومی کارت با شیوه‌ای که کشف توانایی‌های یک یا چند برنامه کاربردی کارت مستقر بر روی یک ICC تسهیل می‌کند، را شرح داده است.

---

1 -Stack
2 -Proxy
3-Cryptographic service

توصیف قابلیت، ساختار اطلاعاتی برای فعال‌سازی این سازوکار کشف، است. جزئیات دو سطح توصیف قابلیت در استاندارد ملی ایران شماره ۱۶۳۸۶آورده شده است.

ـ یک توصیف قابلیت کارت (CCD)، برای کشف یک یا چند برنامه کاربردی کارت مستقر در ICC، استفاده شده است. CCDها در برنامه کاربردی کارت آلفا مستقر می‌شوند. CCD، اطلاعات ترجمه APDU را ارائه می‌کند.

ـ یک توصیف قابلیت کاربردی (ACD)، مجاز است با یک برنامه کاربردی کارت ارائه شود. اگر ACD حضور داشته باشد، برای اطلاع‌رسانی درخواست‌های هویت توانایی اضافی یا تجدیدنظرشده از آنچه در CDD آمده است، استفاده می‌کند.

استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶، جزئیات توصیف توانایی را ارائه می‌کند. هدف از توصیف توانایی، قادر ساختن کشف هر دو جنبه واسط کارت عمومی و واسط خدمت می‌باشد. هر گونه ترجمه جفت فرمان-پاسخ بین واسط کارت عمومی و واسط خدمت می‌تواند با استفاده از توصیف توانایی مشخص گردد.

استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶در آینده، روش‌شناسی توصیف قابلیت مرتبط با اینکه چگونه با استفاده از برنامه‌های کاربردی کارت مستقر بر روی یک ICC اطلاعات سازمان داده شود، محافظت شود، بازیابی شود و به روز شود، را توضیح می‌دهد.

۶ ـ ۷ مدل داده

مدل‌های داده، عناصر داده‌ها و ارتباط داخلی بین آن‌ها را تعیین می‌کند. هر مدل داده، وابسته به یک برنامه کاربردی است. مدل‌های داده، به گونه‌ای در نظر گرفته شده‌اند که به وسیله برنامه‌های کاربردی کارخواه، قابل-کشف باشند.

۶ـ ۸ واسط عمومی کارت

استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶، وسیله‌ای را برای دسترسی به برنامه کاربردی کارت در یک ICC، تعریف می‌کند. جزئیات واسط عمومی کارت در استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶ یک مجموعه ثابت‌شده از توانایی‌ها را توضیح می‌دهد.

یک پیاده‌سازی واسط عمومی کارت :

ـ یک درخواست عمومی را به یک یا چند درخواست خاص ترجمه می‌کند.

ـ یک یا چند تائید خاص را به یک تائید عمومی ترجمه می‌کند.

استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶، کارکرد موجود برای پردازش داده‌ها، مدیریت امنیت و اداره کردن را تعریف می‌کند.

۶ ـ ۹ واسط اتصال

استاندارد آتی ملی ایران شماره ۴ـ ۱۶۳۸۶، توصیف واسط اتصال در دسترس برای اجزاء را به طور مفصل ارائه می‌کند. از پیاده‌سازی واسط اتصال برای تعیین یک ارتباط بین مولفه‌های مجاور در پشته ارتباطی استفاده می-شود.

۶ ـ۱۰ واسط کانال مورد اعتماد

استاندارد آتی ملی ایران شماره ۴ـ ۱۶۳۸۶، جزئیات توصیف واسط کانال مورد اعتماد در دسترس مولفه‌ها را تعیین می‌کند. از پیاده‌سازی واسط کانال مورد اعتماد برای تعیین یک کانال ارتباطی ایمن بین مولفه‌های مجاور در پشته ارتباطی استفاده می‌شود.

۷ منطق امنیتی

استاندارد ملی ایران شماره ۱۶۳۸۶، مفاهیم امنیتی سازوکارهای تعیین شده در بند ۵-۴ در استاندارد ISO/IEC 7816-4:2004 را به‌کارمی‌برد. استاندارد ملی ایران شماره ۱۶۳۸۶حالت‌های خاص پیام‌رسانی ایمن از استاندارد ISO/IEC 7816-4 را حمایت می‌کند.

امنیت در پیاده‌سازی استاندارد I ملی ایران شماره ۱۶۳۸۶بستگی دارد به توانایی نگاشت‌ساز و کارهای معماری امنیتی تعریف شده در استاندارد ISO/IEC 7816-4 بر روی سازوکارهای معماری امنیتی پشتیبانی شده به وسیله ICC.

کشف اطلاعات رمزنگاشتی، می‌تواند در بیشتر از یک شکل، پیاده‌سازی شود مانند:

ـ استفاده از توصیف قابلیت

ـ استفاده از استاندارد ملی ایران شماره ۵ ـ ۸۲۳۲

استاندارد ملی ایران شماره ۳ـ ۱۶۳۸۶، سازوکارهای منطق امنیتی از یک چشم‌انداز برنامه کاربردی کارخواه را شرح می‌دهد.

پیوست الف
(اطلاعاتی)
مثال‌های پیکربندی پیاده‌سازی

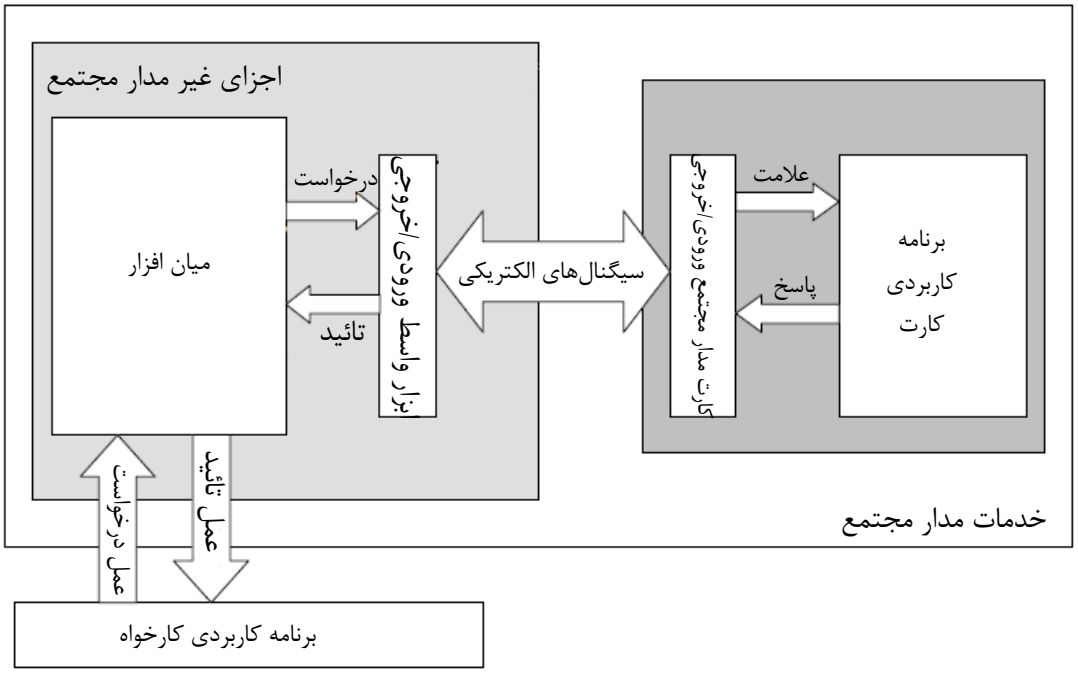
الف ـ ۱ کلیات

بحث در مورد پیکربندی پیش‌بینی‌شده در این پیوست به جزئیات داده شده است. خواننده باید توجه داشته باشد که این پیوست، یک فهرست کامل از پیکربندی نمی‌باشد.

اتصال به یک IFD و سایر جزئیات لایه انتقال، در شکل‌ها بازنمایی شده است اما خارج از دامنه این استاندارد می‌باشند. با توجه بر اینکه قادر به ایجاد ارتباط بین برنامه کاربردی کارت، IFD، یک یا بیشتر لایه‌های استاندارد ملی ایران ۱۶۳۸۶و برنامه کاربردی کارخواه هستند.

خدمات ارائه شده در برنامه کاربردی کارخواه می‌تواند جفت‌های پاسخ-فرمان APDU را به همان منظور که یک درخواست را ایجاد می‌کند و یک تائید دریافت می‌کند، مورد استفاده قرار گیرد. این پیوست، جزئیات ساختاری یا معنایی[1] هر واسط نشان داده شده را توضیح نمی‌دهد.

هر دیاگرام، یک چشم‌انداز معماری فیزیکی یک برنامه کاربردی کارخواه منفرد را مرتبط با یک برنامه کاربردی کارت منفرد نشان داده شده در شکل الف-۱ نشان می‌دهد. توسعه احتمالی تبادلات درخواست/تایید در واسط برنامه کاربردی کارت در این شکل‌ها نشان داده نشده است.



شکل الف ـ ۱ـ معماری فیزیکی

1 - Semantics

شکل ۱در بند ۶ و شکل الف-۱، همان سیستم را با چشم‌اندازهای متفاوت نشان می‌دهد.
شکل ۱، یک دید منطقی از معماری همانگونه که شکل الف-۱ دید فیزیکی را نشان می‌دهد، به نمایش می‌گذارد. نگاشت مولفه بین چشم‌اندازهای فیزیکی و منطقی به پیکربندی پیاده‌سازی منطقی همانگونه که در بندهای بعدی این پیوست خواهد آمد، بستگی دارد.
شرح خلاصه‌ای از معماری فیزیکی نشان داده شده در شکل الف-۱، در زیر می‌آید :

خدمات ICC :
یک پیاده‌سازی که خدمات به برنامه کاربردی کارخواه را فراهم می‌کند و یک ICC را استفاده می‌کند.

ICC :
یک عنصر از خدمات ICC. جزئی که مساوی با ICC فیزیکی است.

اجزاء غیر ICC :
این عنصر، سایر توانایی‌های ایجاد شده توسط خدمات ICC را نشان می‌دهد . این عنصر مکمل ICC است.

سیگنال‌های الکتریکی :
دو بخش عملیاتی اصلی از خدمات ICC، از طریق یک کانال که "سیگنال‌های الکتریکی" نامیده می‌شود، ارتباط برقرار می‌کند.
نوع ویژه سیگنال‌های الکتریکی (مانند (T=0 , T=1) استاندارد ملی ایران ـ ایزو ـ آی ای سی ۳ ـ ۷۸۱۶، USB استاندارد ملی ایران ـ ایزو ـ آی ای سی ۱۲ـ ۷۸۱۶، بدون تماس استاندارد ملی ایران ۱۶۲۹۰) خارج از دامنه استاندارد ملی ایران شماره ۱۶۳۸۶ هستند.

ICC I/O :
این یک جزء از ICC است. مقصود آن انتقال پیام‌های داده شده از طریق کانال "سیگنال‌های الکتریکی" به درخواست‌هایی است که به برنامه کاربردی کارت، فرستاده می‌شوند. علاوه بر این، این جزء، تائیدهای دریافت شده از برنامه کاربردی کارت را به سیگنال الکتریکی انتقال می‌دهد و از طریق کانال "سیگنال‌های الکتریکی" می‌فرستد. ICC I/O خارج از دامنه استاندارد ملی ایران شماره ۱۶۳۸۶ می‌باشد.

: IFD I/O

این کارکرد، حاوی "مولفه‌های غیر ICC "، یک مسئولیت مشابه مانند ICC I/O دارند. IFD I/O خارج از دامنه استاندارد ملی ایران شماره ۱۶۳۸۶ می‌باشد.

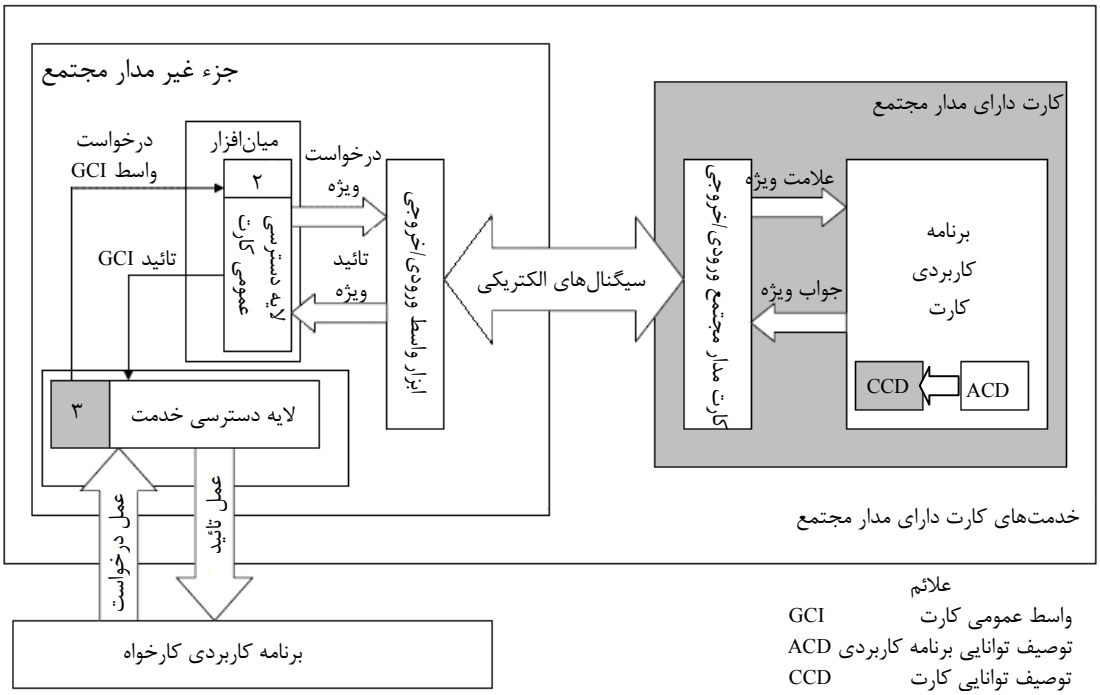
برنامه کاربردی کارت :

در بند ۳ـ ۴ شرح داده شده است.

میان افزار :

در بند ۳ ـ ۱۵شرح داده شده است.

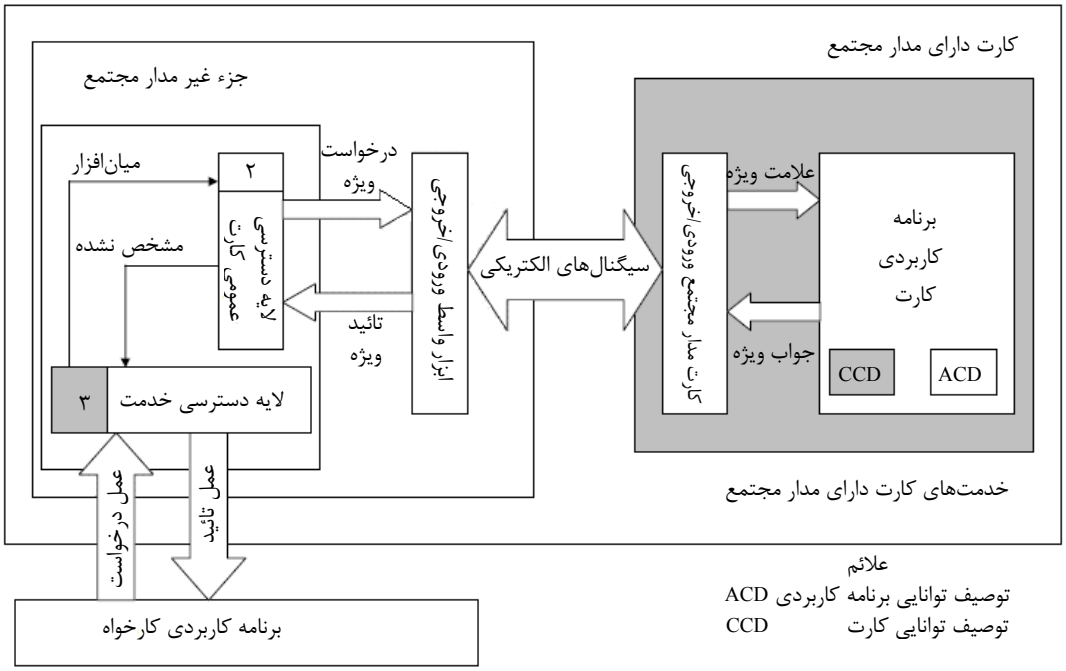
الف ـ ۲ پیکربندی لایه مجزا



شکل الف ـ ۲ ـ پیاده سازی مجزا هر واسط و لایه

این پیکربندی، پیاده‌سازی استانداردهای ملی ایران شماره ۲ـ ۱۶۳۸۶و ۳ ـ ۱۶۳۸۶ را به صورت مولفه‌های متفاوت نشان می‌دهد. این پیکربندی برای الزامات در حال تکامل، پیشنهاد شده است. لایه دسترسی عمومی کارت، که به عنوان یک پروکسی ICC می‌باشد، می‌تواند ترجمه لازم مورد نیاز برای ICC مستقر شده موجود را ارائه کند.

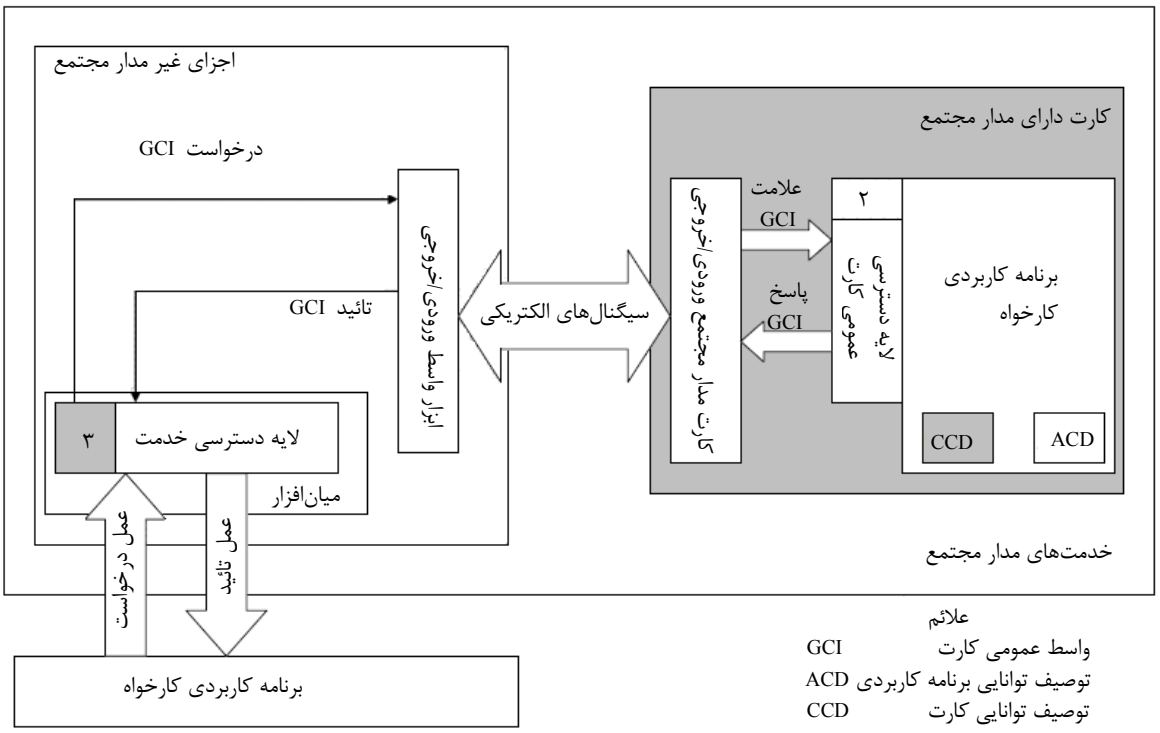
الف ـ۳ پیکربندی ترکیبی



شکل الف ـ۳ ـ پیاده سازی ترکیبی

این تنظیم، واسط خدمت، کشف و هرگونه ترجمه APDU پیاده‌سازی شده به عنوان جزء نرم‌افزاری منفرد را مطرح می‌کند. تعامل بین واسط کارت عمومی استاندارد ملی ایران شماره ۲ـ ۱۶۳۸۶ و لایه دسترسی خدمت استاندارد ملی ایران شماره ۳ـ ۱۶۳۸۶در این مورد مشخص نشده است.

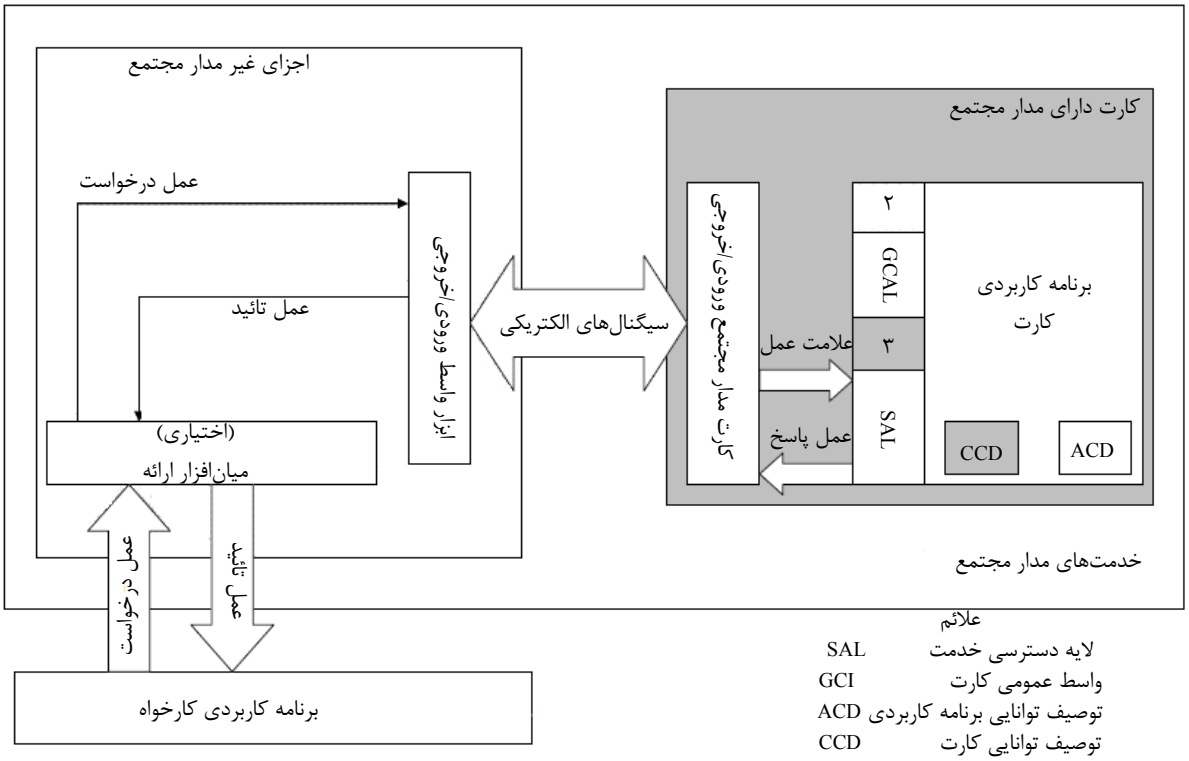
الف ـ ۴ پیکر بندی لایه دسترسی عمومی کارت بر روی ICC



شکل الف ـ۴ ـ لایه دسترسی عمومی کارت پیاده‌سازی شده بر روی ICC

این پیکربندی، واسط عمومی کارت و لایه دسترسی پیاده‌سازی‌شده بر روی ICC را مطرح می‌کند. هیچ ترجمه‌ای از جفت‌های پاسخ-فرمان APDU، پیش‌بینی نشده است.

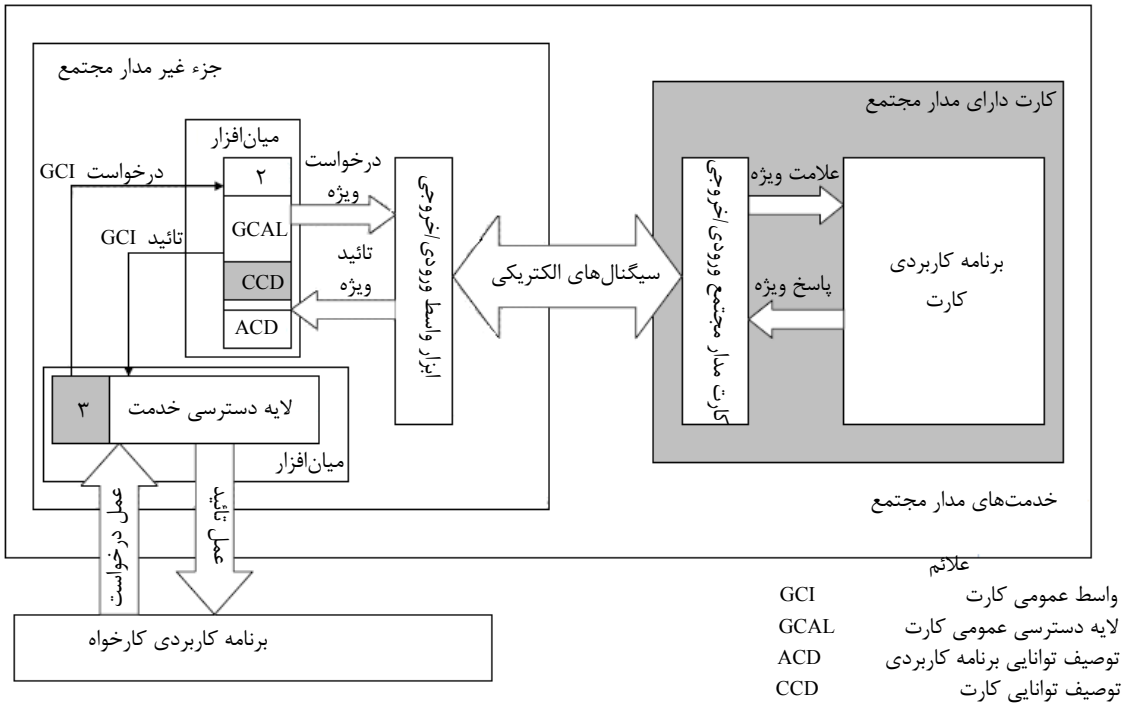
الف-۵ پیاده‌سازی لایه‌های دسترسی عمومی کارت و دسترسی خدمت بر روی ICC



شکل الف ـ۵ ـ لایه‌های دسترسی خدمت و دسترسی عمومی کارت پیاده سازی‌شده بر روی ICC

در این پیکربندی، ISO/IEC 7816-4، روشی برای پوشش جامع عملیات APDUهای استاندارد معین نمی‌کند.

الف-۶ میزبانی اجزاء غیرICC ثابت شده/ قابل‌بارگذاری توصیف قابلیت



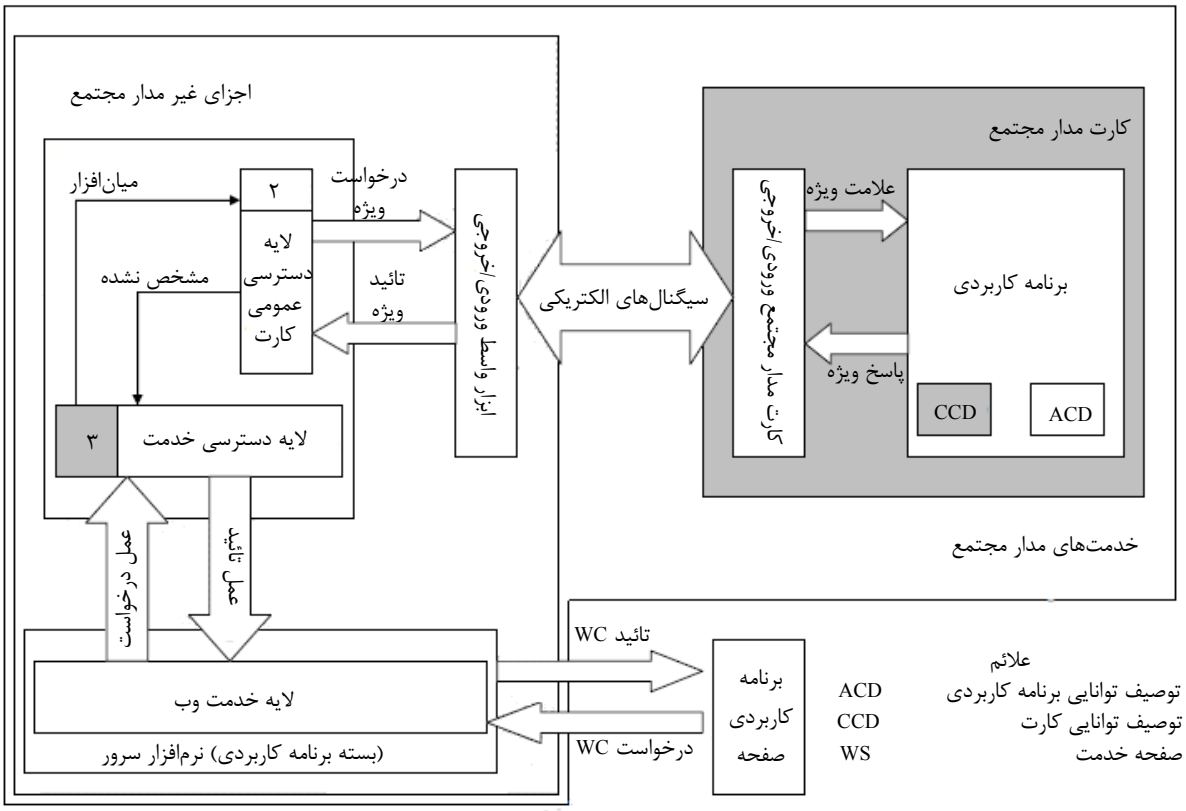
شکل الف ـ۶ ـ پیکربندی ثابت‌شده یا قابل‌بارگذاری

پیکربندی قابل‌بارگذاری، برای جایگذاری یک ICC، که نمی‌تواند توصیف قابلیت بارگذاری را پشتیبانی کند پیشنهاد شده است. CCD و ACD به وسیله میان‌افزار با استفاده از ابزارهای نامشخص ارائه شده‌اند.

پیکربندی ثابت‌شده برای جایگذاری یک ICC که نمی‌تواند توصیف قابلیت بارگذاری را حمایت کند پیشنهاد شده است. علاوه بر این، میان‌افزار، از یک مجموعه شناخته‌شده از پیاده‌سازی‌های ICC پشتیبانی می‌کند. توصیف قابلیت‌ها می‌تواند به طور صریح یا به طور ضمنی در کارکرد میان‌افزار، ارائه شود مانند (یک API قابل بارگذاری)

یادآوری ـ از آنجایی که هیچ وسیله تعامل‌پذیر مشخصی برای پیاده‌سازی قسمت ۲ این مجموعه استانداردها برای کشف CCD/ACD وجود ندارد، این نوع خاص پیکر بندی، ممکن است چالشی برای دستیابی به تعامل‌پذیری ایجاد کند.

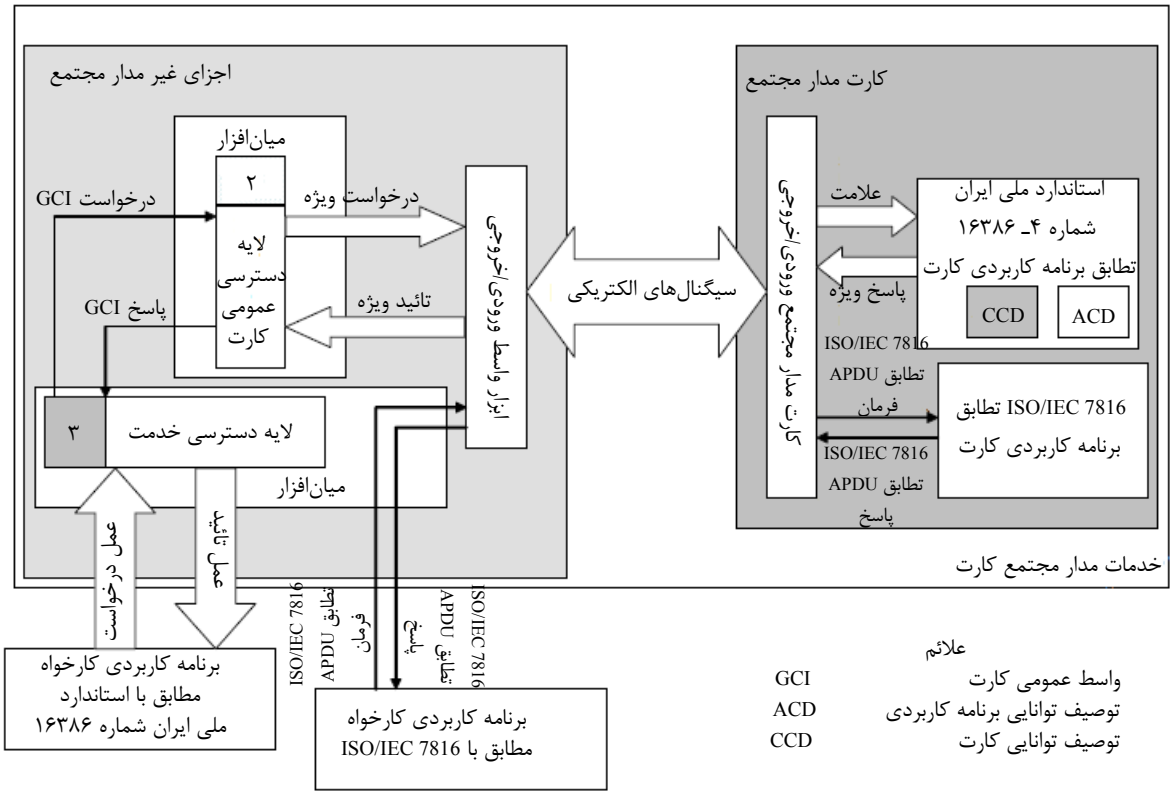
الف-۷ پیکر بندی خدمت وب



شکل الف ـ۷ ـ پیکربندی خدمت وب

این پیکربندی، یک واسط خدمت وب را که می‌تواند به وسیله برنامه‌های کاربردی وب، مورد دستیابی قرار گیرد، را پیشنهاد می‌کند. لایه خدمت وب، می‌تواند به عنوان یک برنامه کاربردی کارخواه محلی ارائه شود که برنامه‌های کاربردی وب را در معرض واسط خدمت استاندارد ملی ایران شماره ۳ــ ۱۶۳۸۶یا واسط اختصاصی (نامشخص) قرار می‌دهد.

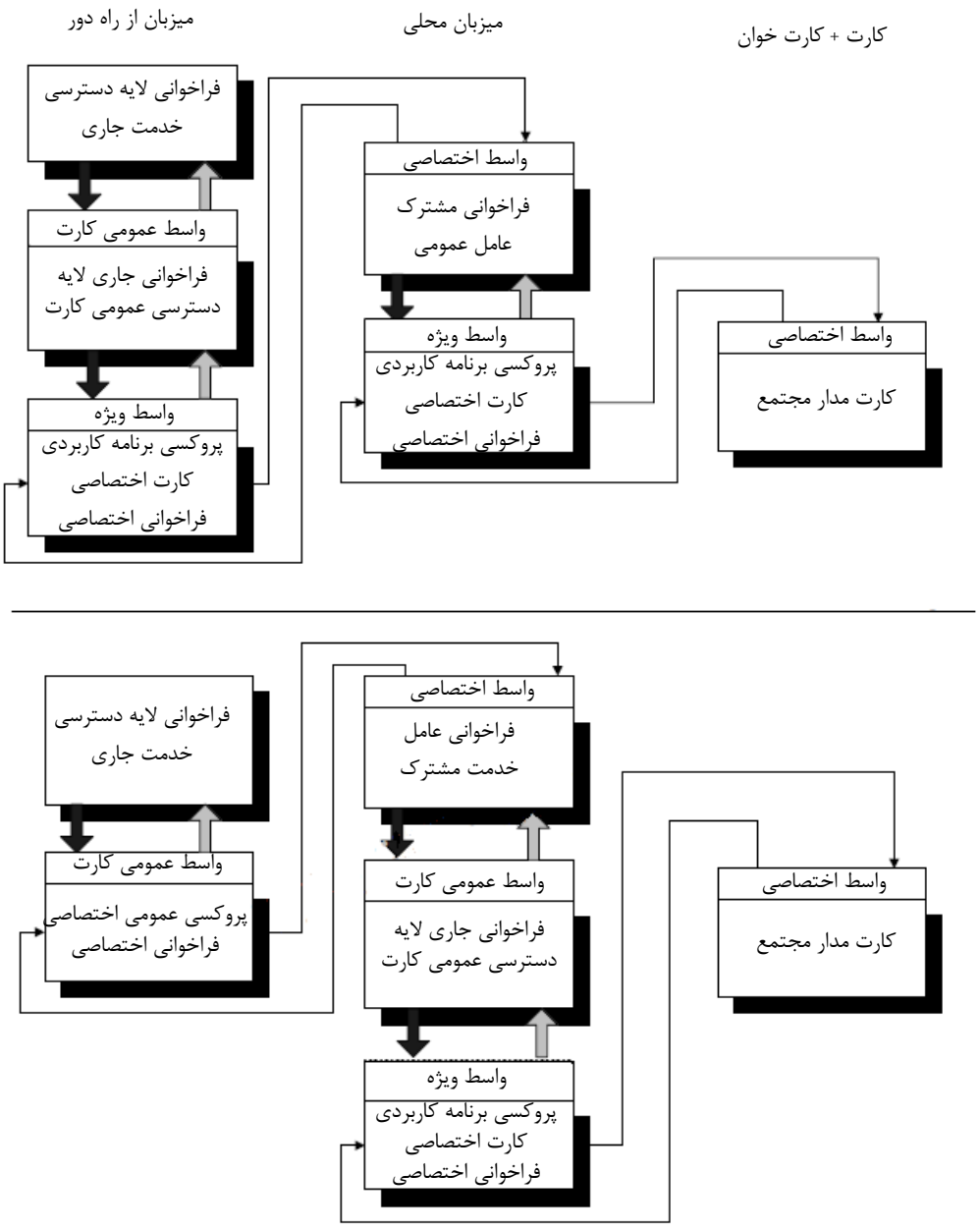
الف-۸ پیکربندی برنامه کاربردی چندتایی



شکل الف ـ ۸ ـ پیکربندی برنامه کاربردی چندتایی

این پیکربندی، حضور همزمان برنامه کاربردی کارت استاندارد ملی ایران شماره ۱۶۳۸۶درون یک ICC را نشان می‌دهد که سایر برنامه‌های کاربردی کارت ISO/IEC 7816-4 را نیز پشتیبانی می‌کند.

الف-۹ پیاده‌سازی توزیع‌شده پشته



شکل الف ـ۹ ـ پیاده‌سازی توزیع‌شده پشته

این دیاگرام‌ها همان ساختار (فراخوانی‌های مشترک، خط انتهای یک کادر) برای دسترسی به API خاص و واسط عمومی کارت (فریم‌های هاشورخورده) را استفاده می‌کند. این روش، اطمینان می‌دهد که لایه‌های درج شده در پشته یا در درسترس از طریق یک پروکسی (به عنوان مثال شبیه‌سازهای[1] کارت، ابزار آزمون انطباق) بر

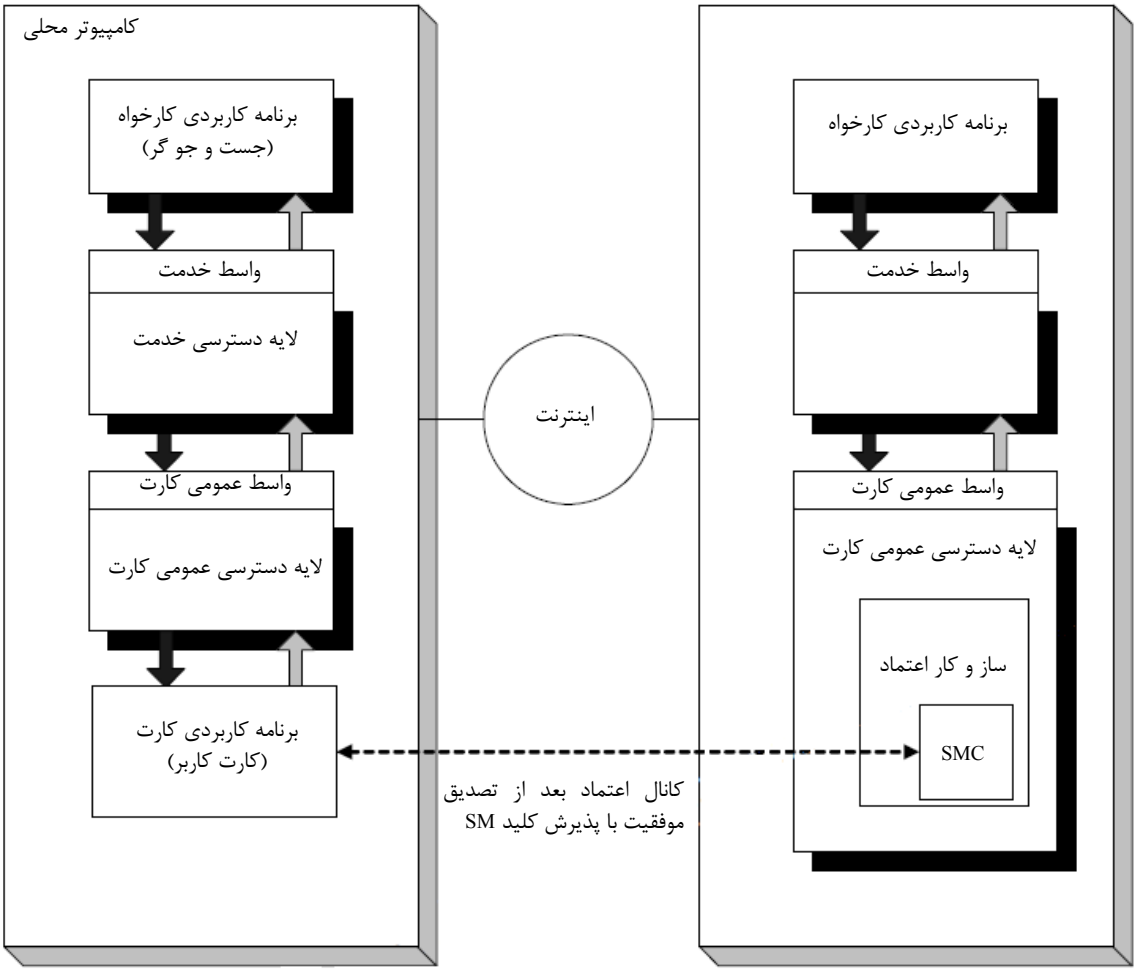
1- Emulators

روی مدول‌های[1] استاندارد تاثیر نمی‌گذارد اگر آن لایه‌ها نیز واسط عمومی کارت را ارائه می‌دهند و از همان فراخوانی‌های مشترک استفاده می‌کنند.

فراخوانی‌های خدمت، " اختصاصی" نامیده می‌شوند، چون به واسط‌های مرتبط با استاندارد دسترسی ندارند. برای مثال، انتقال بین میزبان محلی و میزبان راه دور می‌تواند از سوکت‌های ایمن استفاده کنند.

در اینجا یک عامل[2]، به عنوان استفاده‌کننده از یک جزء پشته، تعریف می‌شود که به جزء پشته‌ای اشاره می‌نماید که در همان ماشین، پیاده‌سازی نشده است.

الف-۱۰ پیاده‌سازی توزیع شده با استفاده از یک سازوکار اعتماد



علائم :

کارت پودمان امنیتی SMC

شکل الف ـ ۱۰ پیاده‌سازی توزیع‌شده با استفاده از یک سازوکار اعتماد

1 - Modules
2- Agent

این پیکربندی، پیشنهاد می‌دهد که یک سازوکار اعتماد چگونه ممکن است پیاده‌سازی شود. لایه دسترسی عمومی کارت سمت خدمت‌دهنده، یک درخواست به واسط عمومی سمت خدمت‌دهنده می‌فرستد تا نشان دهد که نیاز به استفاده از سازوکار اعتماد دارد.

سازوکار اعتماد، با کمک SMC، درخواست ایمن شده‌ای را که قرار است از کانال اعتماد فرستاده شود، تولید می‌کند و تائید ایمن از کانال مورد اعتماد را پردازش می‌کند. هرگونه داده پاسخ، به صورت یک متن آشکار به لایه دسترسی عمومی کارت سمت خدمت‌دهنده، تحویل داده می‌شود.

پیوست ب

(اطلاعاتی)

کتابنامه

[۱] استاندارد ملی ایران شماره ۱ـ ۸۲۳۱ ، کارت‌های شناسایی-شناسایی صادرکنندگان کارت‌ها-قسمت اول: سیستم شماره‌گذاری

[۲] استاندارد ملی ایران ـ ایزو ـ آی ای سی ۳-۷۸۱۶، کارت‌های شناسایی - کارت‌های مدار یکپارچه قسمت ۳- کارت‌های دارای اتصالات - واسط الکتریکی و پروتکل‌های انتقال

[۳] استاندارد ملی ایران ـ ایزو ـ آی ای سی ۱۲ ـ ۷۸۱۶ ،کارت های شناسایی –کارت‌های مدار یکپارچه قسمت ۱۲- کارت‌های دارای اتصالات - واسط الکتریکی USB و رویه‌های عامل

[۴] استاندارد ملی ایران ـ ایزو ـ آی ای سی ۱ـ ۸۸۲۵ ، فناوری اطلاعات -قواعد کدبندی نشانه‌گذاری قاعده‌ی نحوی انتزاعی یک (ASN.1) ویژگی قواعد کدبندی پایه (BER) قواعد کد بندی متعارف (CER) و قواعد کدبندی متمایز(DER)

[۵] 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

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

[۷] 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

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

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

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

[۱۱] استاندارد ملی ایران شماره ۴ ـ ۱۰۸۲۵، فن آوری اطلاعات - فنون امنیتی تشخیص هویت نهاد-قسمت چهارم-مکانیزم‌های استفاده کننده از یک تابع مقابله رمزنگاری

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

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

[۱۴] استاندارد ملی ایران شماره ۹۶۰۰، فن‌آوری اطلاعات –روش‌های امنیتی –حالت‌های عملیاتی یک الگوریتم رمز نگاری قطعه ای N بیتی
[۱۵] استاندارد ملی ایران شماره ۱ـ ۹۵۹۸ ،فن‌آوری اطلاعات –روش‌های امنیتی -توابع در هم ساز قسمت اول -کلیات
[۱۶] استاندارد ملی ایران شماره ۳ ـ ۹۵۹۸، فناوری اطلاعات -فنون امنیتی -توابع درهم‌ساز -قسمت ۳- توابع درهم‌ساز اختصاصی
[۱۷] استاندارد ملی ایران شماره ۴ـ ۹۵۹۸، فن‌آوری اطلاعات –روش‌های امنیتی -توابع در هم ساز قسمت چهارم-توابع درهم ساز با استفاده از محاسبات پیمانه‌ای
[۱۸] استاندارد ملی ایران ایزو ـ آی ای سی ۳ ـ ۱۰۵۳۶،کارت های شناسایی- کارت های مدار(های)یکپارچه بدون تماس -(CICCS)قسمت۳- سیگنال‌های الکترونیکی و رویه‌های باز نشاندن
[۱۹] استاندارد ملی ایران شماره ۱ ـ ۱۱۶۸۴،کارت‌های شناسایی –کارت‌های مدار(های) مجتمع غیر تماسی – کار های جفت‌شدگی قوی- قسمت ۱-خصوصیات فیزیکی
[۲۰] استاندارد ملی ایران شماره ۳ ـ ۱۰۸۲۲، فناوری اطلاعات -فنون امنیتی-مدیریت کلید -قسمت ۳-ساز و کارهای مبتنی بر فنون نامتقارن
[۲۱] استاندارد ملی ایران شماره ۴ ـ۱۰۸۲۲ ، فن‌آوری اطلاعات -فنون امنیتی -مدیریت کلید-قسمت چهارم- مکانیزم مبتنی بر رازهای ضعیف
[۲۲] استاندارد ملی ایران شماره ۲ ـ۱۶۲۹۰،کارت‌های شناسایی –کارت‌های مدار مجتمع بدون تماس –کارت های مجاورتی -قسمت ۲- توان بسامد رادیویی و واسط سیگنال
[۲۳] استاندارد ملی ایران شماره ۴ ـ۱۶۲۹۰،کارت‌های شناسایی –کارت‌های مدار مجتمع بدون تماس –کارت های مجاورتی -قسمت ۴- پروتکل انتقال
[۲۴] استاندارد ملی ایران شماره ۱ـ ۱۱۴۹۴،فناوری اطلاعات -فنون امنیت امضاهای دیجیتال با پیوست قسمت ۱:کلیات
[۲۵] 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 عامل‌بندی صحیح
[۲۶] 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
[۲۷] استاندارد ملی ایران ۱ ـ ۱۰۸۲۴،فن‌آوری اطلاعات -فنون امنیتی الگوریتم‌های رمز نگاری-قسمت اول- کلیات
[۲۸] استاندارد ملی ایران ۳ ـ ۱۰۸۲۴،فناوری اطلاعات -فنون امنیتی –الگوریتم‌های رمز نگاری-قسمت ۳- رمزهای بلوکی

[۲۹] استاندارد ملی ایران ۴ ـ ۱۰۸۲۴، فن‌آوری اطلاعات - فنون امنیتی الگوریتم‌های رمزنگاری-قسمت چهارم-رمزگذاری جریانی
[۳۰] استاندارد ملی ایران شماره ۲ ـ ۱۶۳۸۶، کارت‌های شناسایی ـ واسط‌های برنامه‌نویسی کارت دارای مدار مجتمع ـ قسمت ۲ : واسط عمومی کارت
[۳۱] استاندارد ملی ایران شماره ۳ ـ ۱۶۳۸۶، کارت‌های شناسایی ـ واسط‌های برنامه‌نویسی کارت داری مدار مجتمع ـ قسمت ۳ : واسط برنامه کاربردی
[32] ETSI TS 102 221 , Smart cards , UICC-Terminal interface , Physical and logical characteristics
[33] ETSI TS 102 222, Integrated Circuit Cards(ICC) , Administrative commands for telecommunications
[34] ETSI TS 102 223, Smart cards ,Card Application Toolkit (CAT)
[35] Interoperability Specification for ICCs and Personal Computer System , Version 2.0 PC/SC Workgroup , 2004
[36] ISO 3166-1 , Codes for the representation of names of countries and their subdivisions – Part 1 : Country codes
[37] ISO/IEC 7816-6:2004 , Identification Cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange
[38] ISO/IEC 7816-8:2004 , Identification Cards – Integrated circuit cards – Part 8: Commands for security operations
[39] ISO/IEC 7816-9:2004 , Identification Cards – Integrated circuit cards – Part 9: Commands for card management
[40] ISO/IEC 7816-13:2007, Identification Cards – Integrated circuit cards – Part 13: Commands for application management in a multi-envirinment
[41] ISO/IEC 7816-15:2004 , Identification Cards – Integrated circuit cards – Part 15: Cryptographic information application
[42] ISO/ IEC TR 9577:1999 , Information Technology – Protocol identification in the network layer
[43] ISO/IEC 9797-2:2011, Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
[44] ISO/IEC 9797-3:2011, Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 3: Mechanisms using a universal hash-function
[45] ISO 9992-2, Financial transaction cards- Messages between the integrated circuit card and the card accepting device – Part 2 : Function , messages (commands and responses) , data elements and structures
[46] ISO 10118-2: 2010, Information technology -- Security techniques -- Hash-functions -- Part 2 : Hash-functions using an n-bit block cipher
[47] ISO/IEC 10536-2:1995 , Identification cards -- Contactless integrated circuit(s) cards -- Part 2: Dimensions and location of coupling areas
[48] ISO/IEC 11770-1:2010 , Information technology -- Security techniques -- Key management -- Part 1: Framework
[49] ISO/IEC 11770-2:2008 , Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques
[50] ISO/IEC 11770-5:2011 , Information technology -- Security techniques -- Key management -- Part 5: Group key management

[51] ISO/IEC 14443-1:2008 , Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics
[52] ISO/IEC 14443-3:2011, Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision
[53] ISO/IEC 18033-2:2006 , Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers