INSO
16386-1

1st. Revision
2017

Identical with
ISO/IEC
24727-1:2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران
۱۶۳۸۶-۱
تجدیدنظر اول
۱۳۹۶

کارت‌های شناسایی-
واسط‌های برنامه‌نویسی مدار یکپارچه-
قسمت ۱: معماری

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

ICS: 35.240.15

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri .gov.ir

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها 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 for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«کارت‌های شناسایی– واسط‌های برنامه‌نویسی مدار یکپارچه- قسمت ۱: معماری»

«تجدیدنظر اول»

رئیس:	**سمت و/ یا محل اشتغال:**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات- سیستم‌های اطلاعاتی)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
کیامهر، بیتا (فوق لیسانس مدیریت تکنولوژی)	معاون مدیر کل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
ابوالقاسمی، پیمان (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات - مرکز تحقیقات مخابرات ایران
ارجمند، مهدی (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات - مرکز تحقیقات مخابرات ایران
جوادزاده، غزاله (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات - مرکز تحقیقات مخابرات ایران
جهانیان، علی (دکتری مهندسی کامپیوتر- معماری)	دانشیار- دانشگاه شهید بهشتی
رادمهر، وحید (کارشناسی مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات - مرکز تحقیقات مخابرات ایران
مغانی، مهدی (کارشناسی ارشد ریاضی کاربردی)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران
ناظمی، اسلام (دکتری مهندسی کامپیوتر)	دانشیار- دانشگاه شهید بهشتی

اعضاء : (اسامی به ترتیب حروف الفبا)

	سمت و/ یا محل اشتغال:
نصیری آسایش، حمیدرضا (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی

ویراستار:	**سمت و/ یا محل اشتغال:**
معروف، سینا (لیسانس مهندسی کامپیوتر- سخت‌افزار)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «کارت‌های شناسایی– واسط‌های برنامه‌نویسی مدار یکپارچه- قسمت ۱: معماری» که نخستین بار در سال ۱۳۹۱ بر مبنای پذیرش استانداردهای بین‌المللی به‌عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی شمارهٔ ۵ تدوین و منتشر شد، بر اساس پیشنهادهای دریافتی و بررسی و تایید کمیسیون‌های مربوط برای اولین بار مورد تجدیدنظر قرار گرفت و در پانصد و دوازدهمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۶/۰۳/۰۸ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران شماره ۱-۱۶۳۸۶: سال ۱۳۹۱ است.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 24727-1: 2014, Identification cards — Integrated circuit card programming interfaces — Part 1: Architecture

مقدمه

استاندارد ISO/IEC 24727 مجموعه‌ای از قراردادها و واسط‌های برنامه‌نویسی را که امکان تعاملات بین کارت‌های مدار یکپارچه (ICCs)[1] و برنامه‌های کاربردی مقیم روی بسترهای رایانه‌ای گوناگون را فراهم می‌سازد، مشخص می‌کند. کارت‌های ICCs خدمات عام برای کاربرد چند-بخشی و ترجیحا با هدف پشتیبانی از عملیات شناسایی، اصالت‌سنجی و امضای (IAS) [2] قابل اعتماد، فراهم می‌کند. سازمان‌دهی و بهره‌برداری از ICCs با استاندارد ISO/IEC 7816-4 انطباق دارد.

استاندارد ISO/IEC 24727 از اصول کلیِ الگوی مرجع اتصال متقابل سامانه‌های باز که در استاندارد ISO/IEC 7498-1 | ITU-T Rec. X.200 ارائه شده است، استفاده می‌کند. این اصول پیشنهاد می‌کند که اتصال برنامه‌های کاربردی مکمل روی بسترهای رایانه‌ای گوناگون از طریق رویه‌های خوش تعریف انجام شود که از طریق واسط‌های استاندارد به آن‌ها دسترسی وجود دارد. این رویه‌ها، شامل امکانات نرم‌افزاری و سخت‌افزاری است که به برنامه کاربردی حتی زمانی که این برنامه‌های کاربردی از طریق گذرگاه‌های ارتباطی پیچیده جدا مانده باشند، این امکان را می‌دهد تا با یکدیگر تعامل داشته باشند.

به مجموعه رویه‌هایی که برنامه کاربردی را به برنامه کاربردی دیگری متصل می‌کند، با عنوان پشته‌ی قرارداد[3] اشاره می‌شود. هر مولفه از چنین پشته‌ای از یک واسط و یک لایه تشکیل شده است. لایه از پیاده-سازیِ کارکرد رویه‌ای تشکیل شده است که درخواست‌های رسیده از طریق واسط را می‌پذیرد و پاسخ می-دهد. استاندارد ISO/IEC 24727 واسط‌هایی را مشخص می‌کند که این واسط‌ها تبادل‌پذیر[4] بودنِ پیاده-سازی‌های مستقل لایه را امکان‌پذیر می‌کنند. این موضوع، تعریف پایه‌ای از تعامل‌پذیری را تشکیل می‌دهد: *پیاده‌سازی‌های مستقل* تبادل‌پذیر هستند.

برای دستیابی به تعامل‌پذیری در گستره‌ای از دامنه‌های برنامه کاربردی، ممکن است برخی از آن‌ها قبل از استاندارد ISO/IEC 24727 باشد، نیاز به پرداختن به سازوکارهای گوناگونی درون پیاده‌سازی‌های مربوط است. این سازوکارها شامل: معماری‌های مشترک، معناشناسی مشترک، واسط‌هایی که به صورت رسمی تعریف شده‌اند، قابلیت کشف، توسعه‌پذیری، همسازی با قبل[5] و آزمون انطباق است. بندهای پیرو و دیگر قسمت‌های استاندارد ISO/IEC 24727 به وسایلِ تحقق این سازوکارها می‌پردازد.

1- Integrated Circuit Cards

2- Identification, Authentication and Signature

3- Protocol stack

4- Interchangeable

5- Backward compatibility

کارت‌های شناسایی– واسط‌های برنامه‌نویسی مدار یکپارچه- قسمت ۱: معماری

۱ هدف و دامنه کاربرد

هدف از تدوین این مجموعه استاندارد، تعیین مجموعه‌ای از قراردادها و واسط‌های برنامه‌نویسی است که تعاملات بین کارت‌های مدار یکپارچه (ICCs) و برنامه‌های کاربردی مقیم روی بسترهای رایانه‌ای گوناگون را توانمند می‌سازد. کارت‌های مدار یکپارچه خدماتی عمومی برای استفاده چند-بخشی از طریق برنامه‌های کاربردی فراهم نموده است. سازمان‌دهی و بهره‌برداری از ICCs با استاندارد ISO/IEC 7816-4 انطباق دارد. پیش‌بینی می‌شود که بعضی از دامنه‌های کاربردی برای دستیابی به تعامل‌پذیری از طریق استاندارد ISO/IEC 24727 خواهند بود، حتی اگر برنامه‌های کاربردی این امکانات را از پیش داشته باشند. برای این منظور، وسایل مختلف همسازی با قبل از طریق سازوکارهای مشخص‌شده در استاندارد ISO/IEC 24727 تعیین شده‌اند.

این استاندارد موارد زیر را مشخص می‌کند:

- معماری سامانه و اصول بهره‌برداری،
- وسایلی برای دستیابی به تعامل‌پذیری بین دامنه‌های کاربردی گوناگون،
- مدل‌های مفهومی خدمت و داده که در دامنه‌های کاربردی مربوط گسترده شده‌اند، و
- منطق برای فرایندهای مورد اعتماد فعال تحت این مدل‌ها.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به‌صورت الزامی به آن‌ها ارجاع داده شده است. بدین ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

درصورتی‌که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

2-1 ISO/IEC 7816-4:2015, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات با تعاریف زیر به‌کار می‌رود:

۳-۱

اصالت‌سنجی

authentication

فرایندهای ارزیابی سطح اعتمادِ هویت یا شناسایی است.

۳-۲

قرارداد اصالت‌سنجی

authentication protocol

فرایند خاصِ اصالت‌سنجی است.

۳-۳

کارت

card

کارت مدار یکپارچه است.

۳-۴

برنامه کاربردی-کارت

card-application

مجموعه‌ای از کارکردهای ICC که به صورت یکتا قابل شناسایی هستند و خدمات ذخیره‌سازی و رایانشی داده برای برنامه کاربردی-کارخواه فراهم می‌کند.

۳-۵

برنامه کاربردی-کارخواه

client-application

نرم‌افزارِ پردازش‌گر که نیازمند دسترسی به یک یا تعدادی برنامه کاربردی-کارت است.

۶-۳

عنصر داده‌ای

data element

قلمی از اطلاعات موجود در واسط که برای آن اسم، توصیفی از محتوای منطقی، قالب و کد، مشخص شده است.

(منبع : ISO/IEC 7816-4)

۷-۳

مجموعه داده‌ای

data set

مجموعه‌ای نام‌دار از ساختارهای داده برای تعامل‌پذیری است.

۸-۳

ساختار داده برای تعامل‌پذیری

data structure for interoperability

پرونده‌ی ISO/IEC 7816-4 که توسط شناسانه‌ی دو بایتی پرونده‌ی یا شی داده‌ای ISO/IEC 8825 BER-TLV که از طریق رشته هشت‌تایی که برچسب ASN.1 را کدبندی می‌کند، شناسایی می‌شود.

۹-۳

هویت-تفاوتی

differential-identity

مجموعه اطلاعات که در بردارنده‌ی اسم، نشانگر و قرارداد اصالت‌سنجی است.

۱۰-۳

لایهٔ دسترسی عمومی کارت

generic card access layer

مولفه‌ای که واسط استاندارد ISO/IEC 24727-2 را برای لایهٔ دسترسی کارت فراهم می‌کند.

۳-۱۱

شناسایی

identification

جمیع جنبه‌هایی از مجموعه مشخصه‌ها و فرایندها که از طریق آن، هستار قابل تشخیص و شناخته می‌شود.

۳-۱۲

واسط

interface

نقطه‌ای که سامانه‌های غیروابسته و اغلب نامرتبط، یکدیگر را ملاقات کرده و با یکدیگر در ارتباط و تعامل هستند.

۳-۱۳

تعامل‌پذیری

interoperability

توانایی هر واسط برنامه کاربردی-کارت که مطابق با استاندارد ISO/IEC 24727 است تا از طریق هر برنامه کاربردی-کارخواه مطابق با استاندارد ISO/IEC 24727 استفاده شود.

۳-۱۴

نشانگر

marker

قلمی از اطلاعات درون هویت-تفاوتی که نمایندهٔ مشخصه‌ای منحصر به فرد از هستار است.

۳-۱۵

میان‌افزار

middleware

نرم‌افزاری که دو برنامه کاربردی جداگانه را به هم متصل می‌کند.

۳-۱۶

SAL-lite

مولفه‌ی سبک وزن که زیرمجموعه‌ای از API استاندارد ISO/IEC 24727-3 را برای قابلیت‌کشف ساختارهای داده توسط برنامه کاربردی-کارخواه فراهم می‌کند.

۳-۱۷

خدمت

service

مجموعه‌ای از کارکردهای پردازشیِ دردسترس در واسط است.

۳-۱۸

لایهٔ دسترسی خدمت

service access layer

مولفه ای که واسط API استاندارد ISO/IEC 24727-3 را برای برنامه کاربردی-کارخواه فراهم می‌کند.

۴ کوته‌نوشت‌ها

AID	application identifier	شناسانهٔ برنامه کاربردی
ACD	application capability description	توصیف قابلیت برنامه کاربردی
APDU	application protocol data unit	واحد داده‌ای قرارداد برنامه کاربردی
API	application programming interface	واسط برنامه‌نویسی برنامه کاربردی
BER	basic encoding rules	قواعد پایه کدبندی
CCD	card capability description	توصیف قابلیت کارت
GCAL	generic card access layer	لایهٔ دسترسی عمومی کارت
GCI	generic card interface	واسط کارت عمومی
ICC	integrated circuit card	کارت مدار یکپارچه
IFD	interface device	افزاره واسط
SAL	service access layer	لایهٔ دسترسی خدمت

SAL-lite	service access layer lightweight component	مولفه سبک وزن لایهٔ دسترسی به خدمت
TLV	tag-length-value	برچسب-طول- مقدار

۵ تعامل‌پذیری

تعامل‌پذیری به امکاناتی می‌پردازد که واسط‌های برنامه کاربردی-کارت مطابق با استاندارد ISO/IEC 24727 می‌توانند توسط برنامه کاربردی-کارخواه مطابق با استاندارد ISO/IEC 24727 در دسترس قرار گیرند. استاندارد ISO/IEC 24727 از طریق فرایندهای مختلف به تعامل‌پذیری دست می‌یابد، این فرایندها عبارتند از:

- معماری مشترک
- معناشناسی مشترک
- واسط‌های تعریف شده به صورت رسمی
- قابلیت کشف
- توسعه‌پذیری
- همسازی با قبل، و
- آزمون انطباق

تمامی واسط‌های موجود در استاندارد ISO/IEC 24727 از طریق زبان‌های رسمی مشخص شده‌اند. این امر سبب برقراری بیانی دقیق از گرامر و معناشناسی می‌شود که به واسط‌ها این امکان را می‌دهد تا به صورت مستقل پیاده‌سازی شوند و از طریق قراردادهای متنوع و به شکلی تعامل‌پذیر، انتقال یابند.

همان‌طور که در شکل ۱ نشان داده شده است، به ازای هر واسط مشخص، قسمت‌های مربوط از استاندارد ISO/IEC 24727 باید کارکرد مورد پشتیبانی را تعریف کنند.

استاندارد ISO/IEC 24727 برای ICC کاربرد دارد که این ICC به صورت مستقیم یا غیرمستقیم ارائه کننده‌ی توصیف قابلیت است. توصیف قابلیت در بند ۶-۶ و به صورت دقیق‌تر در استاندارد ISO/IEC 24727-2 تشریح شده است.

در قسمت‌های مختلف استاندارد، به وسایل گسترشِ واسط‌ها و قراردادهای مختلف که در استاندارد ISO/IEC 24727 اشاره شده است، از جمله فناوری مرتبط با ICC، پرداخته شده است.

۶ معماری

۶-۱ عمومی

استاندارد ISO/IEC 24727 کارکرد بین برنامه کاربردی-کارخواه که در بستر میزبان اجرا می‌شود و مجموعه خدمات فراهم شده توسط برنامه کاربردی مقیم در ICC که از طریق برنامه کاربردی-کارخواه استفاده می‌شوند را بخش‌بندی می‌کند. دسترسی به این خدمات از طریق قراردادهایی فراهم شده است که این قراردادها واسط خدمت، واسط کارت عمومی، و یک یا تعداد بیشتری از برنامه‌های کاربردی مقیم در ICC را ارائه می‌کنند.

۶-۲ صفات معمارانه

واسط خدمت، ویژگی‌های بحث‌شده در بند ۶-۵ را که به صورت مفصل در استاندارد ISO/IEC 24727-3 مورد بررسی قرار گرفته‌اند پیاده‌سازی می‌کند.

واسط کارت عمومی، ویژگی‌های بحث‌شده در بند ۶-۸ را که به صورت مفصل در استاندارد ISO/IEC 24727-2 مورد بررسی قرار گرفته‌اند پیاده‌سازی می‌کند.

واسط اتصال، ویژگی‌های بحث‌شده در بند ۶-۹ که به صورت مفصل در استاندارد ISO/IEC 24727-3 و استاندارد ISO/IEC 24727-3 و استاندارد ISO/IEC 24727-6 مورد بررسی قرار گرفته است را پیاده‌سازی می‌کند.

واسط کانال قابل اطمینان ویژگی‌های بحث‌شده در بند ۶-۱۰ را که در استاندارد ISO/IEC 24727-4 به‌دقت به آن‌ها پرداخته شده پیاده‌سازی می‌کند.

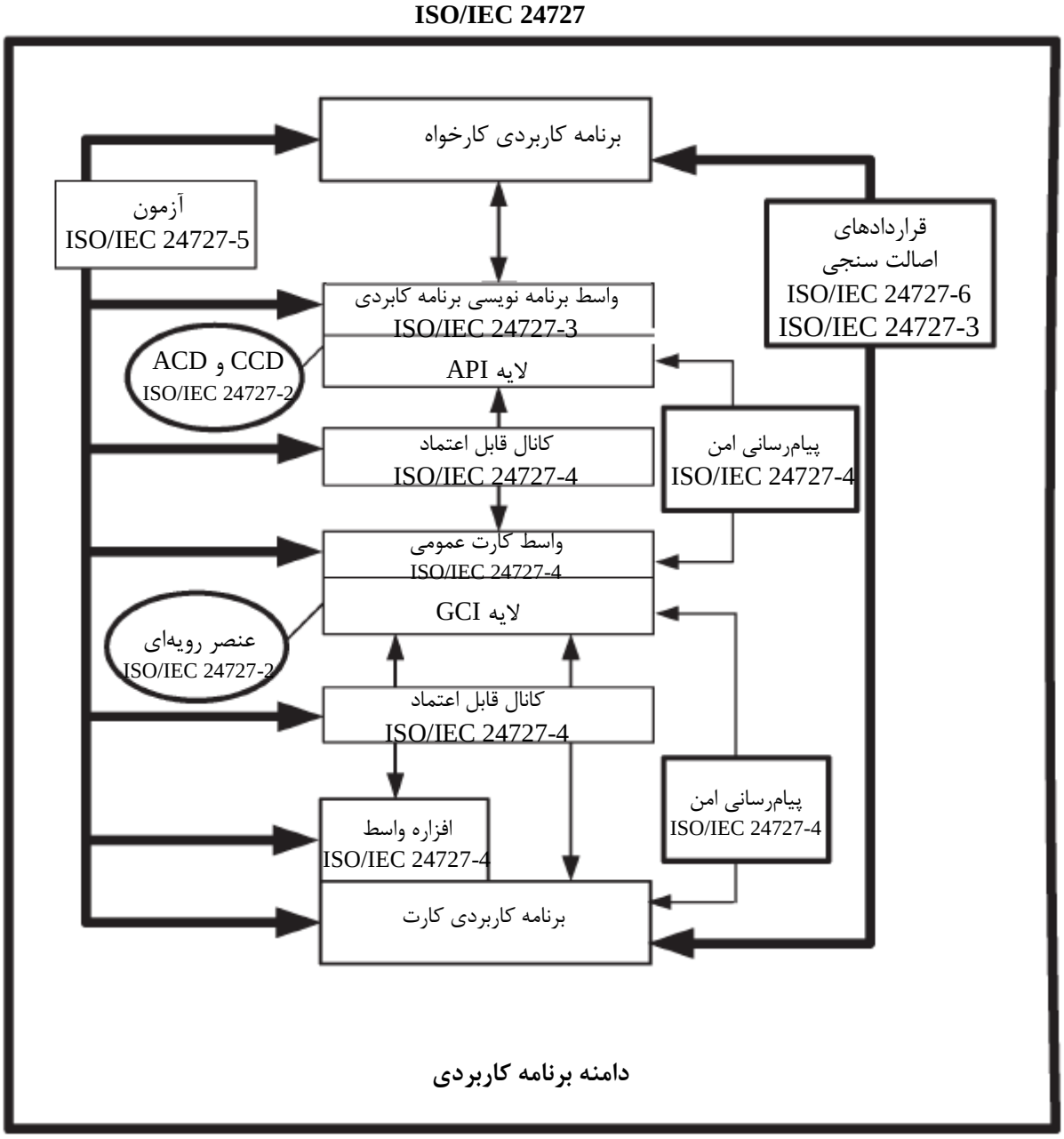
برنامه‌های‌کاربردی کارت، مجموعه‌های داده (شامل ایجاد فضای اسمی واحد برای مجموعه داده‌ها و همه اطلاعات موجود در مجموعه‌های داده) را مدیریت می‌کند. هر مجموعه داده نام‌گذاری شده و فهرست برنامه کاربردی-کارت مربوط به اسامی مجموعه‌ی داده‌ها توسط شناسایی یا کشف مستقیم در دسترس است. برنامه کاربردی-کارخواه هنگامی از اسامی مجموعه داده‌ها استفاده می‌کند که درخواست خدماتی به مجموعه داده‌ها ارسال شده باشد.

دسترسی به مجموعه داده‌ها از طریق فهرست واپایش دسترسی، واپایش می‌شود. فهرست واپایش دسترسی، توصیف کننده‌ی شرایط امنیتی است که باید به منظور انجام فعالیتی برای مجموعه داده‌ها مهیا شود. استاندارد ISO/IEC 24727-3 و ISO/IEC 24727-4 جزئیات بیشتر در مورد فهرست‌ها، شناسایی‌ها و فعالیت‌های واپایش دسترسی فراهم می‌کند.

برنامه‌های کاربردی-کارت، در ICC و از طریق برنامه کاربردی-کارت آلفا و یک یا تعداد بیشتری برنامه‌های کاربردی-کارت، ساماندهی شده‌اند. برنامه‌های کاربردی-کارت را می‌توان توسط AID در واسط خدمات انتخاب کرد.

۳-۶ معماری منطقی

شکل ۱ روابط بین برنامه کاربردی-کارخواه، لایه‌ها و واسط‌های تعریف شده در استاندارد ISO/IEC 24727 و برنامه کاربردی-کارت مقیم در ICC را نمایش می‌دهد. جریان درخواست‌ها از برنامه کاربردی-کارخواه به برنامه کاربردی-کارت به صورت بردارهای مستقیمی نشان شده است که این پیکان بیانگر درخواست یا تایید است. هر پیکان نشان دهنده‌ی کارکردی است که توسط استاندارد پشتیبانی می‌شود. قالب و نحو واقعی درخواست یا تایید در قسمتِ نشان داده شده از استاندارد ISO/IEC 24727 به تفصیل مورد بررسی قرار گرفته است.



شکل ۱- معماری منطقی استاندارد ISO/IEC 24727

کارکرد استاندارد ISO/IEC 24727 را می‌توان به روش‌های مختلفی به همراه انطباق واسط تایید شده از طریق آزمون مشخص شده توسط استاندارد ISO/IEC 24727-5 پیاده‌سازی کرد.

۶-۴ استقلال قرارداد

واسط‌های استاندارد ISO/IEC 24727 از طریق توصیف ASN.1 و همراه با توصیفات XML مشخص می‌شوند. واسط‌ها به گونه‌ای مستقل از قراردادهای مورد نیاز برای برقراری ارتباطات بین برنامه‌های کاربردی

کارخواه و برنامه‌های کاربردی-کارت مشخص شده‌اند.

شکل ۱ پشته‌ای از لایه‌ها و واسط‌های لازم برای اتصال‌دهندگی بین برنامه‌های کاربردی کارخواه و برنامه‌های کاربردی-کارت را نشان می‌دهد.

سازوکار عامل-پیشکار[1] پیاده‌سازیِ واسط یک عنصر پشته‌ای است که این امکان را ایجاد می‌کند تا پیاده‌سازیِ عنصر پشته‌ای، بین پیشکار و عاملی موجود در نقطه‌ای در پشته قرارداد، تقسیم شوند. سازوکار تعامل‌پذیرِ عامل-پیشکار، به توصیف زبان رسمی و سازوکار خوش تعریف قاب‌بندی وابسته است. این امکانات، در استاندارد ISO/IEC 24727-4 مشخص شده‌اند.

پیوست الف، تعدادی از پیکربندی‌های عمومی مفید را نشان می‌دهد. این پیکربندی‌ها، به صورتی دقیق‌تر در استاندارد ISO/IEC 24727-4 در نظر گرفته شده‌اند.

۶-۵ واسط لایه دسترسی خدمات برنامه کاربردی-کارخواه

استاندارد ISO/IEC 24727-3 توصیفی مفصل از واسط خدمت، در دسترس برای برنامه کاربردی-کارخواه، ارائه می‌کند.

پیاده‌سازیِ واسط خدمت موارد زیر را شامل می‌شود:

- درخواستِ کنش را که در معناشناسیِ(معنای) برنامه کاربردی-کارخواه بیان می‌شود به یک یا تعداد بیشتری درخواست‌های عمومی که در معناشناسیِ(معنای) برنامه کاربردی-کارت مقیم در ICC بیان می‌شود، ترجمه می‌کند.
- یک یا تعداد بیشتری از تاییدهای عمومی از برنامه کاربردی-کارت به تاییدِ کنش برای برنامه کاربردی-کارخواه ترجمه می‌کند.

واسط خدمت شامل موارد زیر است:

- اتصال‌دهندگیِ برنامه کاربردی-کارخواه به برنامه کاربردی-کارت با استفاده از واسط کارت عمومی
- امنیت برنامه کاربردی-کارخواه به برنامه کاربردی-کارت مطابق با منطق‌های امنیت
- خدمت رمزنگاشتی
- خدمت هویت-تفاوتی

۶-۶ توصیف قابلیت

واسط خدمت و واسط کارت عمومی به صورتی مشخص شده‌اند که کشف قابلیت‌های یک یا تعداد بیشتری برنامه‌های کاربردی-کارت مقیم در ICC را تسهیل می‌کنند. ساختار اطلاعاتی برای قادر ساختنِ سازوکار

1- Proxy-agent

کشف، **توصیف قابلیت** است.

دو سطح از توصیف قابلیت در استاندارد ISO/IEC 24727 به صورت تفصیلی آورده شده است:

- توصیف قابلیت کارت (CCD) [1] برای کشف یک یا تعداد بیشتری از برنامه‌های کاربردی کارت مقیم در ICC استفاده می‌شود. CCD روی برنامه کاربردی-کارت آلفا واقع است. CCD اطلاعات برگردان APDU را فراهم می‌کند.
- توصیف قابلیت برنامه کاربردی (ACD) [2] ممکن است به همراه برنامه کاربردی-کارت فراهم شود. توصیف ACD در صورت وجود، به منظورِ اطلاع دادن به هستار درخواست‌کننده از قابلیت اضافی یا تجدید نظرشده از چیزی است که در CCD فراهم شده است، استفاده می‌شود.

استاندارد ISO/IEC 24727-2 به جزئیات توصیف قابلیت هردو سطح پرداخته است. هدف توصیف قابلیت این است که امکان کشف را در هر دو واسط کارت عمومی و واسط خدمت فراهم کند. هر جفت انتقال فرمان-پاسخ بین واسط کارت عمومی و واسط خدمت ممکن است با استفاده از توصیف قابلیت مشخص شود.

استاندارد ISO/IEC 24727 به بررسی جزئیات بیشتری از روش‌های توصیف قابلیت که متناسب با چگونگی ساماندهی، محافظت، بازیابی و به‌روزرسانی آن استفاده از برنامه کاربردی-کارت مقیم در ICC می‌پردازد.

زیرمجموعه ای از API که به اصطلاح مولفه سبک وزن لایهٔ دسترسی به خدمت، خوانده می‌شود، به صورت انحصاری در میزبان محلی پیاده‌سازی می‌شود تا قابلیت کشف برنامه کاربردی-کارت را پشتیبانی کند.

۶-۷ مدل داده

واسط خدمات مشخص شده در استاندارد ISO/IEC 24727-3 در ساختاری از مدل داده‌ها پیش‌بینی شده است که عناصر داده و روابط داخلی آن‌ها را تعریف می‌کند. درحالی‌که آن‌ها برنامه‌های کاربردی ویژه‌ای هستند، عناصر داده و روابط آن‌ها به صورت دائمی از طریق این ساختار مدل داده‌ها حضور دارند. لذا، برنامه‌های کاربردی مشخص مدل داده‌ها توسط برنامه کاربردی-کارخواه از طریق واسط خدمات قابل کشف است.

۶-۸ واسط کارت عمومی

استاندارد ISO/IEC 24727-2 وسایلی برای دسترسی برنامه کاربردی-کارت موجود بر یک ICC تعریف می‌کند. واسط کارت عمومی به صورت تفصیلی که در استاندارد ISO/IEC 24727-2 آورده شده، مجموعه‌ای ثابت از کارکردها را فراهم کرده است.

پیاده‌سازی واسط کارت عمومی شامل موارد زیر است:

- درخواست عمومی را به یک یا تعداد بیشتری درخواست‌های مشخص ترجمه می‌کند

1- Card Capability Description
2- Application Capability Description

- یک یا تعداد بیشتری از تاییدهای مشخص را به تایید عمومی ترجمه می‌کند

استاندارد ISO/IEC 24727-3 کارکرد در دسترس برای پردازش داده، مدیریت امنیت و مدیریت را تعریف می‌کند.

۶-۹ واسط اتصال

استاندارد ISO/IEC 24727-3 توصیفی تفصیلی را از واسط اتصال در دسترس برای مولفه‌ها فراهم می‌کند. فرایندها برای تاثیر بر این اتصال در استاندارد ISO/IEC 24727-4 مشخص شده‌اند. کاربرد اتصال واسط برای ایجاد کانال ارتباطی بین مولفه‌های مجاور در پشتهٔ ارتباطات به کار رفته است.

۶-۱۰ واسط کانال مورد اطمینان

استاندارد ISO/IEC 24727-4 توصیفی تفصیلی از واسط کانال مورد اطمینان دردسترس به مولفه‌های پشته‌ای فراهم کرده است. به‌کار بستن واسط کانال مورد اعتماد برای ایجاد کانال ارتباطی امن بین مولفه‌های مجاور در پشتهٔ قراردادها استفاده می‌شود.

۷ منطق امنیت

استاندارد ISO/IEC 24727 مفاهیم امنیتی و فرایندهای تعریف شده در ISO/IEC 7816-4:2005 تعریف شده‌اند.

استاندارد ISO/IEC 24727 از پیام‌های امنیتی سازگار با ISO/IEC 7826-4 و مشخص شده در استاندارد ISO/IEC 24727-4 استفاده می‌کند.

امنیت در پیاده‌سازی استاندارد ISO/IEC 24727 بستگی به توانایی نگاشت سازوکارهای معماری امنیت تعریف شده در استانداردهای ISO/IEC 24727-3 و ISO/IEC 24727-4 و سازوکارهای معماری امنیت پشتیبانی شده توسط ICC همان‌طور که توسط ISO/IEC 7816-4 مشخص شده است، دارد.

کشف اطلاعات پنهانی ممکن است در بیش از یک شکل پیاده‌سازی شود، به طور مثال:

- استفاده از توصیف قابلیت
- استفاده از ISO/IEC 7816-15 به همان صورت که در استاندارد ISO/IEC 24727-2 و استاندارد ISO/IEC 24727-4 مشخص شده است.

استاندارد ISO/IEC 24727 به جزییات فرایندهای منطق امنیتی از دیدگاه برنامه کاربردی-کارخواه می‌پردازد.

پیوست الف

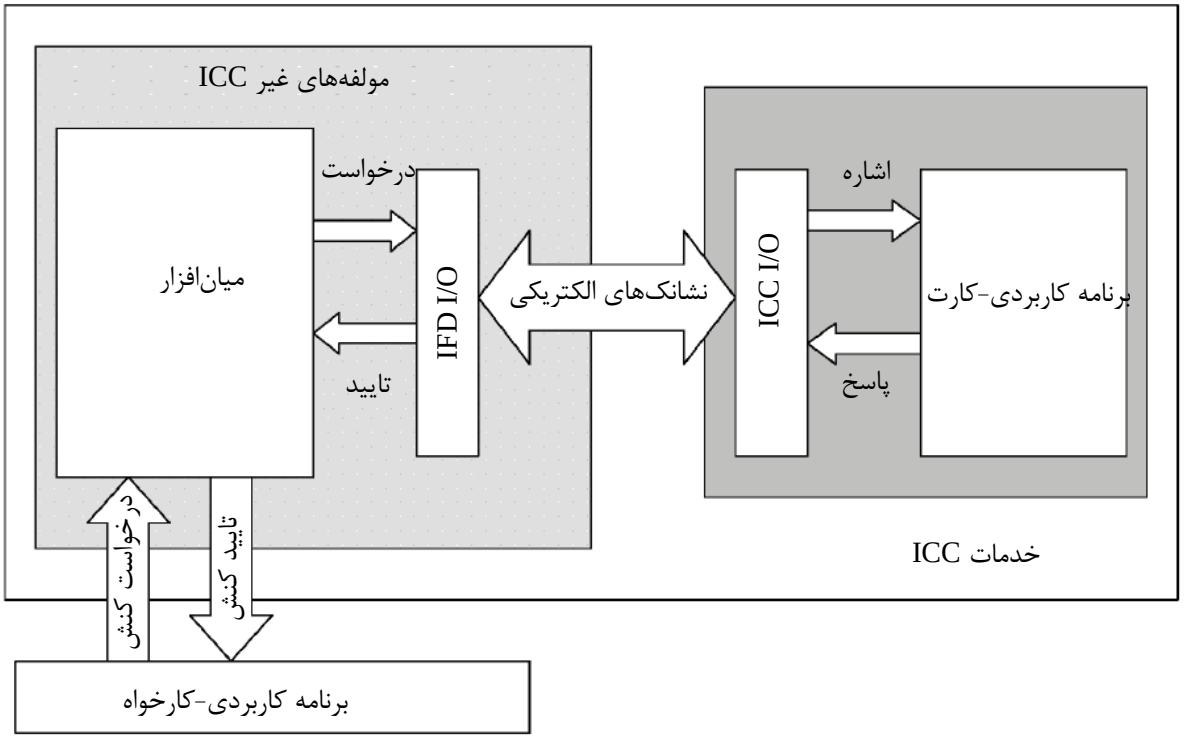
(آگاهی‌دهنده)

مثال‌هایی از پیکربندی پیاده‌سازی

الف-۱ کلیات

پیکربندی پشته‌ی پیش‌بینی شده در این پیوست به صورت تفصیلی مورد بحث قرار می‌گیرد. مشخصات با جزئیات بیشتر پیرامون پیکربندی پشته‌های مختلف در استاندارد ISO/IEC 24727-4 نشان داده شده است. مجموعه پیکربندی پشته‌ها نشان داده شده، تمامی موارد استفاده‌ای را اشاره می‌کند که تاکنون شناخته شده‌اند. هرچند، لازم به ذکر است که مشخصات این پیکربندی‌ها توسط استاندارد ISO/IEC 24727 مورد بررسی قرار نگرفته، در واقع این چنین مشخص‌سازی، عنصر ضروری برای رسیدن به سطوح مطلوب تعامل-پذیری است.

هر نمودار، دیدگاه ساختار فیزیکی برنامه کاربردی-کارخواه مرتبط با برنامه کاربردی-کارت نشان داده شده در شکل الف-۱را نمایش می‌دهد. گسترش ممکن تبادلات درخواست/تایید در واسط برنامه کاربردی در این شکل نشان داده نشده است.



شکل الف-۱- معماری فیزیکی

شکل ۱ در بند ۶ و شکل الف-۱ سامانه یکسانی را از جنبه‌های متفاوت نشان می‌دهند اما. شکل ۱ دید منطقی معماری و شکل الف-۱ دید فیزیکی را نشان می‌دهد. نگاشت مولفه‌های بین دیدگاه‌های منطقی و فیزیکی به پیکربندی پیاده‌سازی انتخابی وابسته است، همان‌طور که در بندهای بیشتر این پیوست ذکر شده و به ویژه در استاندارد ISO/IEC 24727-4 به آن‌ها پرداخته شده است.

در ادامه توصیفی مختصر از معماری فیزیکی شکل الف-۱ آورده شده است:

خدمات ICC : پیاده‌سازی که در آن خدماتی برای برنامه کاربردی-کارخواه فراهم می‌شود و در آن ICC به کار گرفته می‌شود.

ICC : عنصری از خدمات ICC است. این مولفه مشابه با ICC فیزیکی است.

مولفه‌های غیرICC : این عنصر تمامی کارکردهای فراهم شده درون خدمات ICC را نمایش می‌دهد. این عنصر مکمل ICC است.

نشانک الکتریکی: دو قسمت عمده کارکردیِ خدمات ICC، از طریق کانالی با عنوان «نشانک‌های الکتریکی» ارتباط برقرار می‌کنند. به نوع ویژه‌ای از نشانک‌های الکتریکی (به طور مثال، ISO/IEC 7816-3(T=0,T=1) و ISO/IEC 7816-12 USB و ISO/IEC 14443 بدون نیاز به تماس و امنیت لایهٔ انتقال) در استانداردهای مربوط پرداخته شده است.

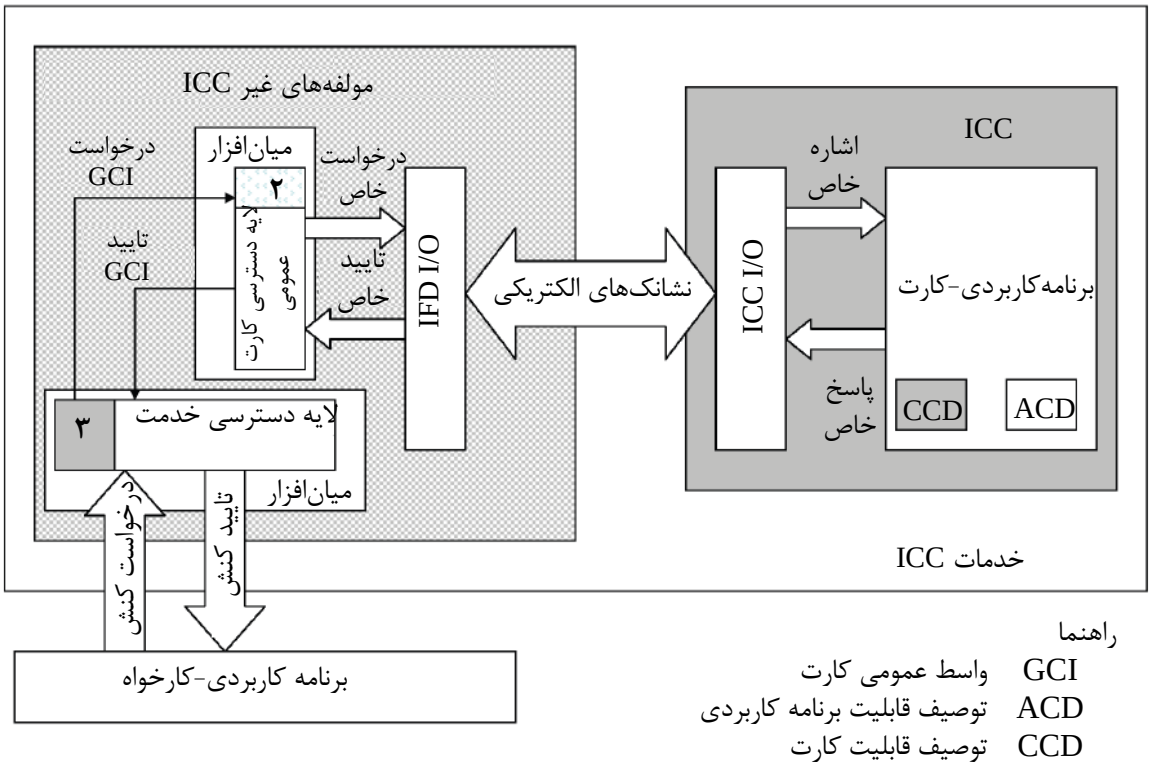
ICC I/O : مولفه ای از ICC است. هدف آن انتقال پیام دریافت شده توسط کانال «نشانک‌های الکتریکی» به درخواست‌هایی است که به برنامه کاربردی-کارت فرستاده می‌شوند. علاوه بر این، این مولفه، تاییدیه‌های دریافت شده از برنامه کاربردی-کارت را به نشانک الکتریکی انتقال داده و آن‌ها را از طریق کانال «نشانک-های الکتریکی» ارسال می‌کند. ICC I/O خارج از هدف و دامنه کاربرد استاندارد ISO/IEC 24727 است.

IFD I/O: این کارکرد، در «مولفه‌های غیرICC» است و دارای مسئولیتی همانند ICC I/O است. IFD I/O خارج از هدف و دامنه کاربرد استاندارد ISO/IEC 24727 است.

برنامه کاربردی-کارت: همان طور که در بند ۳ تعریف شده است.

میان‌افزار: همان طور که در بند ۳ تعریف شده است.

الف-۲ پیکربندی مجزای لایه



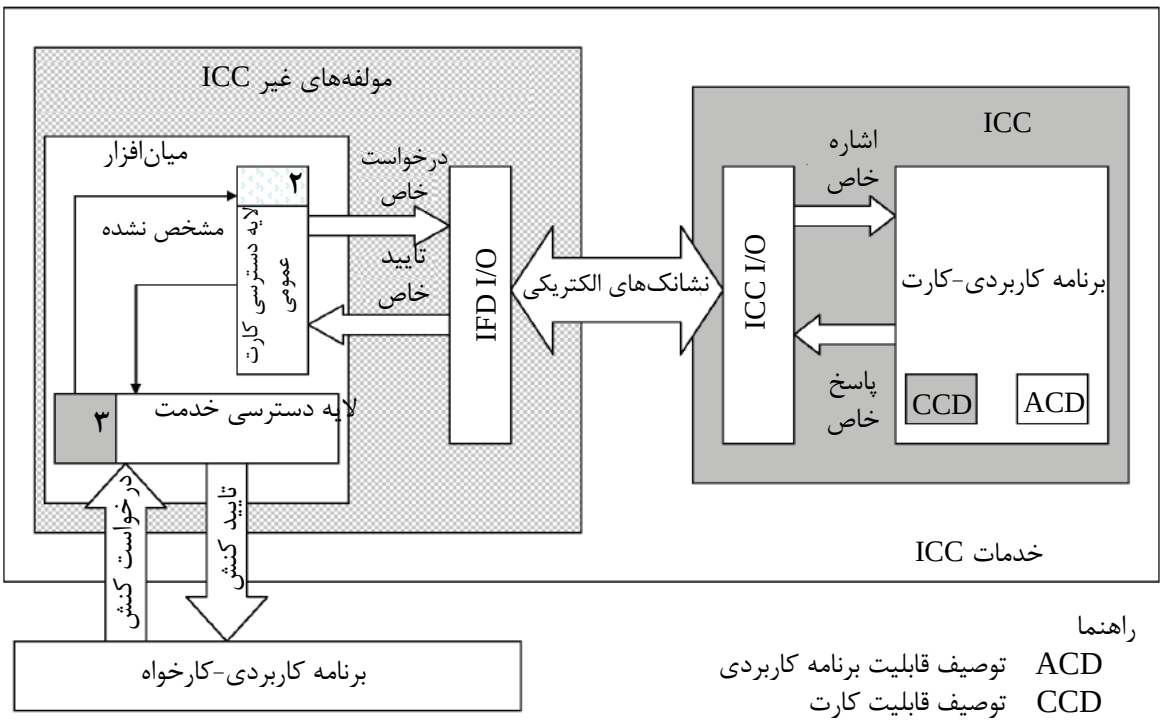
شکل الف-۲- پیاده‌سازی مجزای هر واسط و لایه

این پیکربندی پیاده‌سازی استاندارد ISO/IEC 24727-2 و استاندارد ISO/IEC 24727-3 را به صورت مولفه‌ای مجزا نشان می‌دهد. همان‌طور که در استاندارد ISO/IEC 24727 نشان داده شده، این رده از پیاده‌سازی می‌تواند به صورت **پشته‌ی مات ICC** [1] یا **پشته‌ی کامل شبکه** نشان داده شود.

این پیکربندی برای الزامات مورد نظر پیشنهاد شده است. لایهٔ دسترسی به کارت عمومی، که به عنوان پیشکار ICC عمل می‌کند، می‌تواند انتقال لازم برای ICC موجود و توسعه یافته را فراهم کند.

1- Opaque ICC Stack

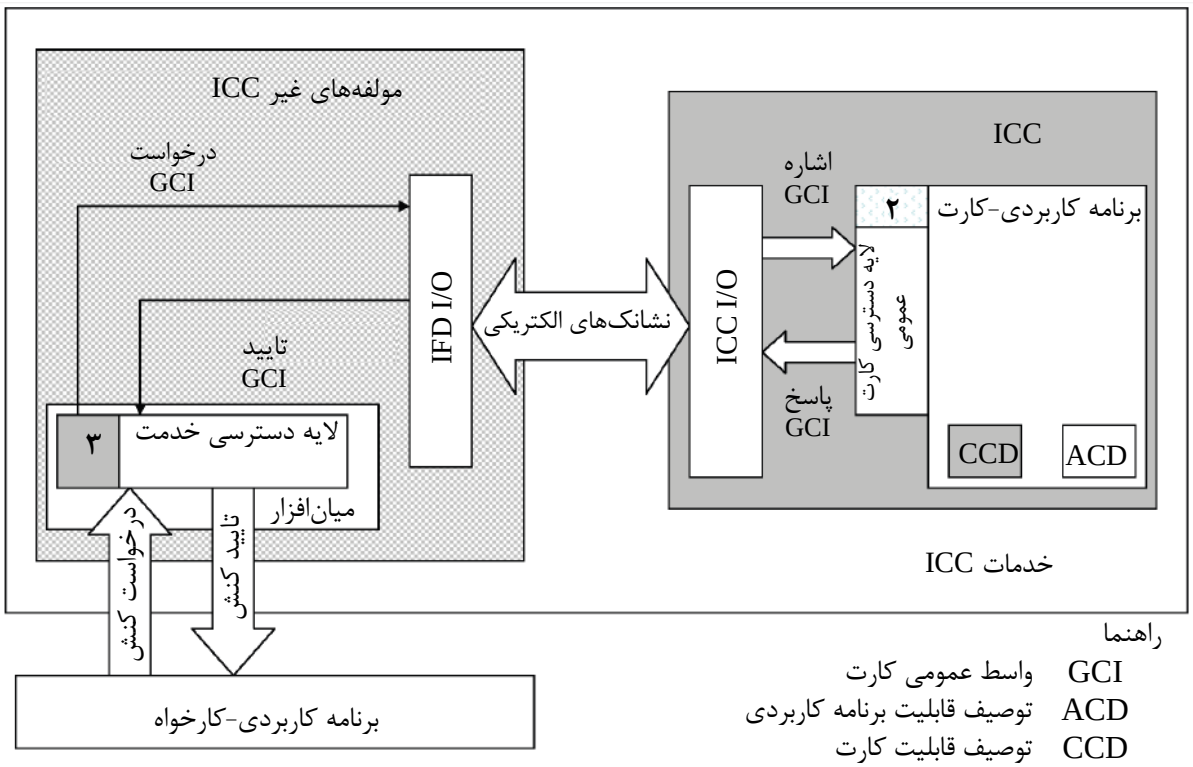
الف-۳ پیکربندی ترکیبی



شکل الف-۳- پیاده‌سازی ترکیبی

این پیکربندی، واسط خدمت، کشف و انجام هر انتقال APUD را به عنوان مولفه نرم‌افزاری منفرد پیشنهاد می‌کند. این برهم‌کنش بین واسط کارت عمومی استاندارد ISO/IEC 24727-2 و لایهٔ دسترسی خدمات استاندارد ISO/IEC 24727-3 در این مورد مشخص نشده است. همان‌طور که در استاندارد ISO/IEC 24727-4 نشان داده شده است، این گروه از پیکربندی پشته می‌تواند به صورت **پشته‌ی Loyal**، **پشته‌ی Loyal از دور**، **پشته‌ی ICC از دور** یا **پشته مقیم در ICC** نشان داده شود.

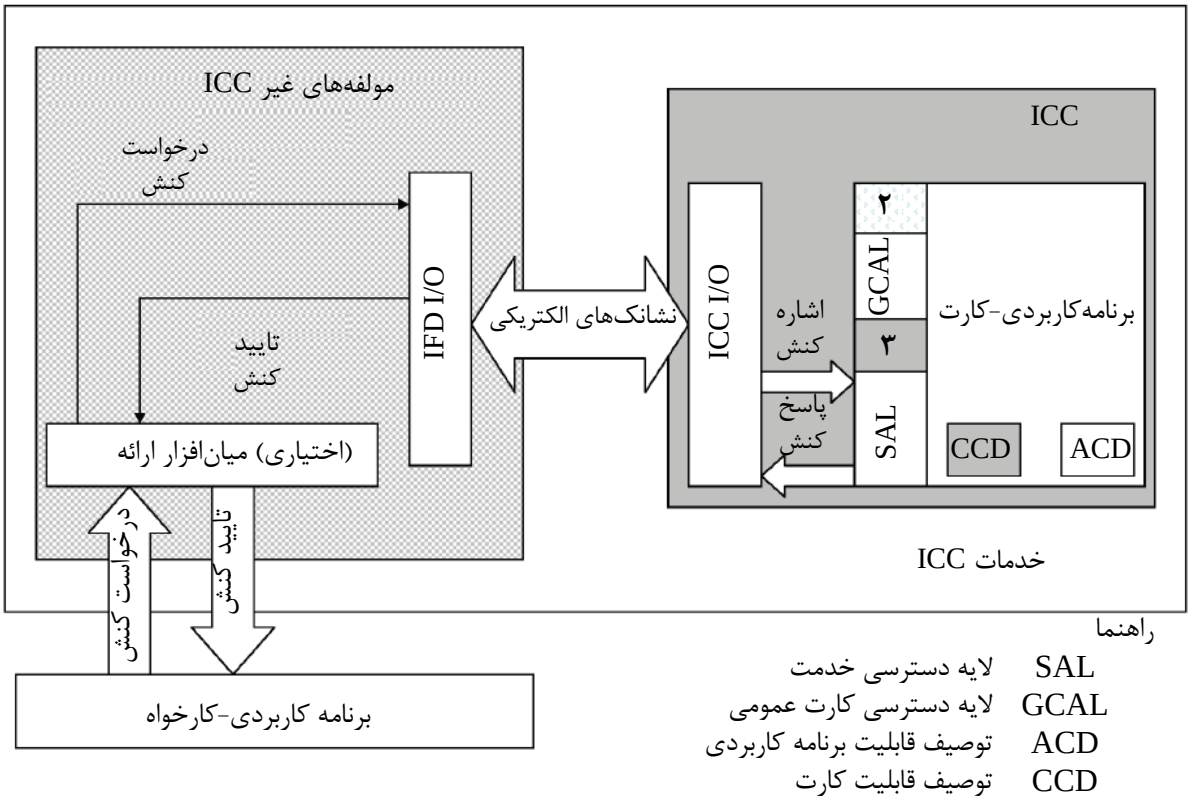
الف-۴ پیکربندی لایهٔ دسترسی ICC کارت عمومی



شکل الف-۴- لایهٔ دسترسی کارت عمومی پیاده‌سازی شده بر ICC

این پیکربندی واسط کارت عمومی و لایهٔ دسترسی پیاده‌سازی شده در ICC را پیشنهاد می‌کند. در استاندارد ISO/IEC 24727-4 به صورت ICC مقیم در پشته نشان داده شده است. در این پیکربندی پشته، دسترسی به برنامه کاربردی-کارت می‌تواند از طریق اتصال مبتنی بر APDU همراه با ENVELOPE APDU نشان داده شده در استاندارد ISO/IEC 24727-2 و/یا به صورت مستقیم در ساختار پیام TLS (اگر ICC دارای اتصال مستقیم شبکه باشد) فراهم شود. TLS پشتیبان از طریق اتصال مستقیم شبکه توسط مجموعه استانداردهای ISO/IEC 7816 مشخص نشده است.

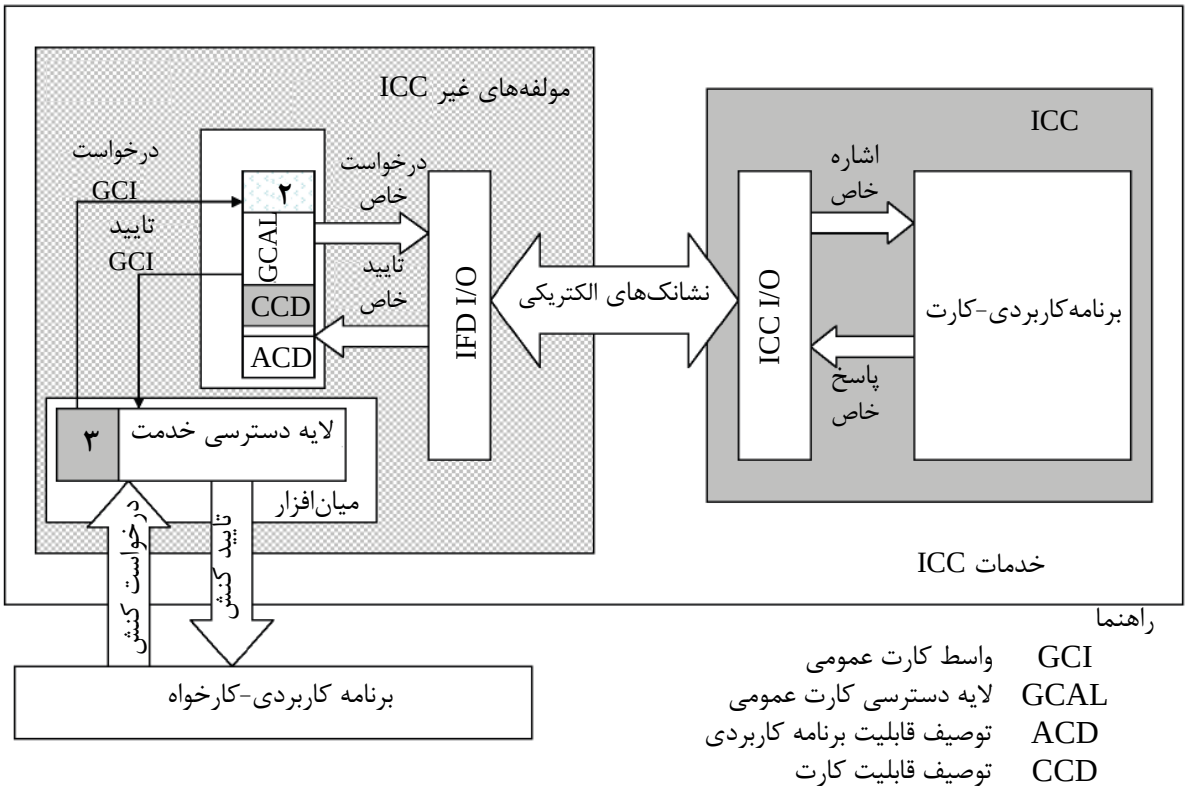
الف-۵ پیاده‌سازی دسترسی خدمات و لایه‌های دسترسی کارت عمومی روی ICC



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

در این پیکربندی، استاندارد ISO/IEC 7816-4 به پنهان‌سازی کنش‌ها از طریق اشیای داده‌ای ASN.1 در قالب ساختارهای BER.TLV می‌پردازد.

الف-۶ مولفه‌های غیر ICC قابل بارگذاری/ ثابت، میزبانِ توصیف قابلیت

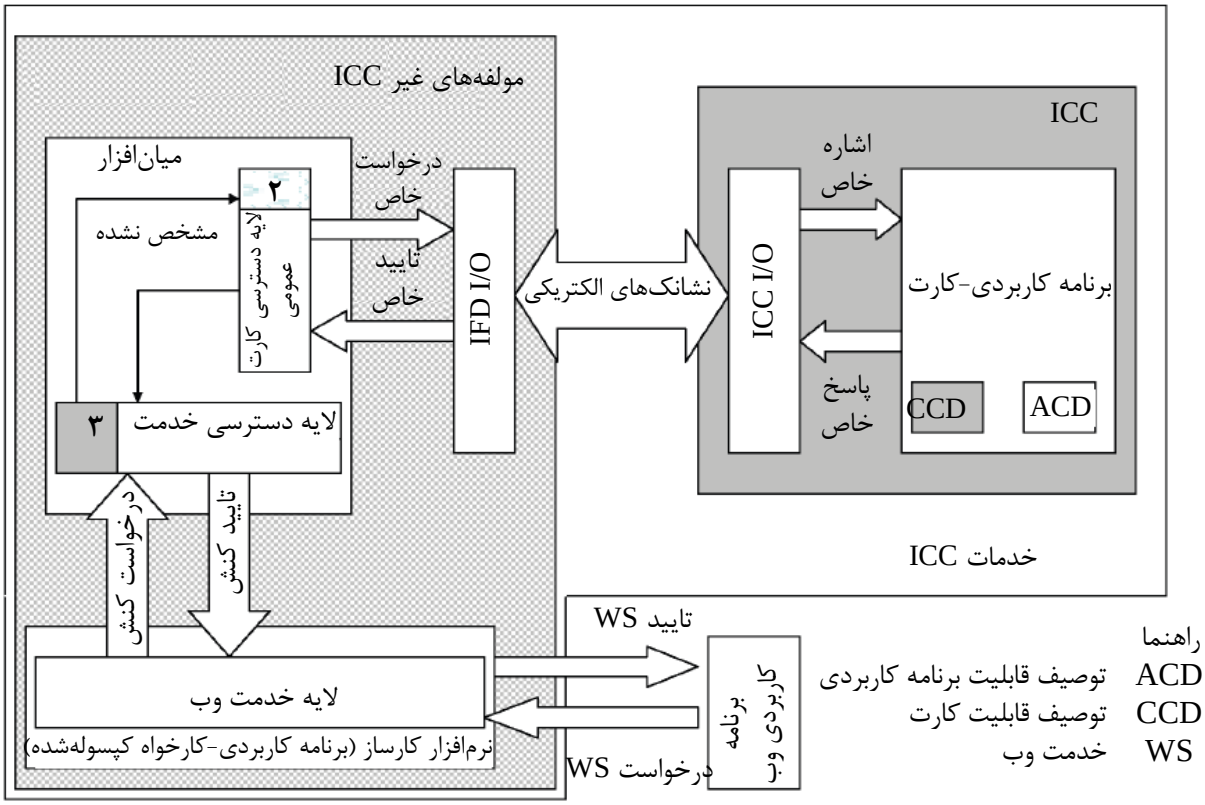


شکل الف-۶- پیکربندیِ قابل بارگذاری یا ثابت

پیکربندی قابل بارگذاری برای تطبیقِ ICC ای پیشنهاد شده است که نمی‌تواند بارگذاری توصیف قابلیت را پشتیبانی کند. CCD و ACD توسط میان‌افزارهای استفاده‌کننده از امکانات off-ICC تعبیه شده‌اند. استاندارد ISO/IEC 24727-2 سازوکارهای نشانک‌دهی مشخص می‌کند که میان‌افزارها می‌توانند از طریق این سازوکارها، به این امکانات اشاره کنند.

پیکربندی ثابت برای تطبیقِ ICC ای پیشنهاد شده است که نمی‌تواند بارگذاری توصیف قابلیت را پشتیبانی کند. علاوه بر این، میان‌افزار مجموعه‌ای معلوم از کاربردهای ICC را پشتیبانی می‌کند. ممکن است توصیف قابلیت به صورت صریح ارائه شود یا به صورت ضمنی در کارکرد میان‌افزار باشد (به عنوان مثال، API قابل بارگذاری).

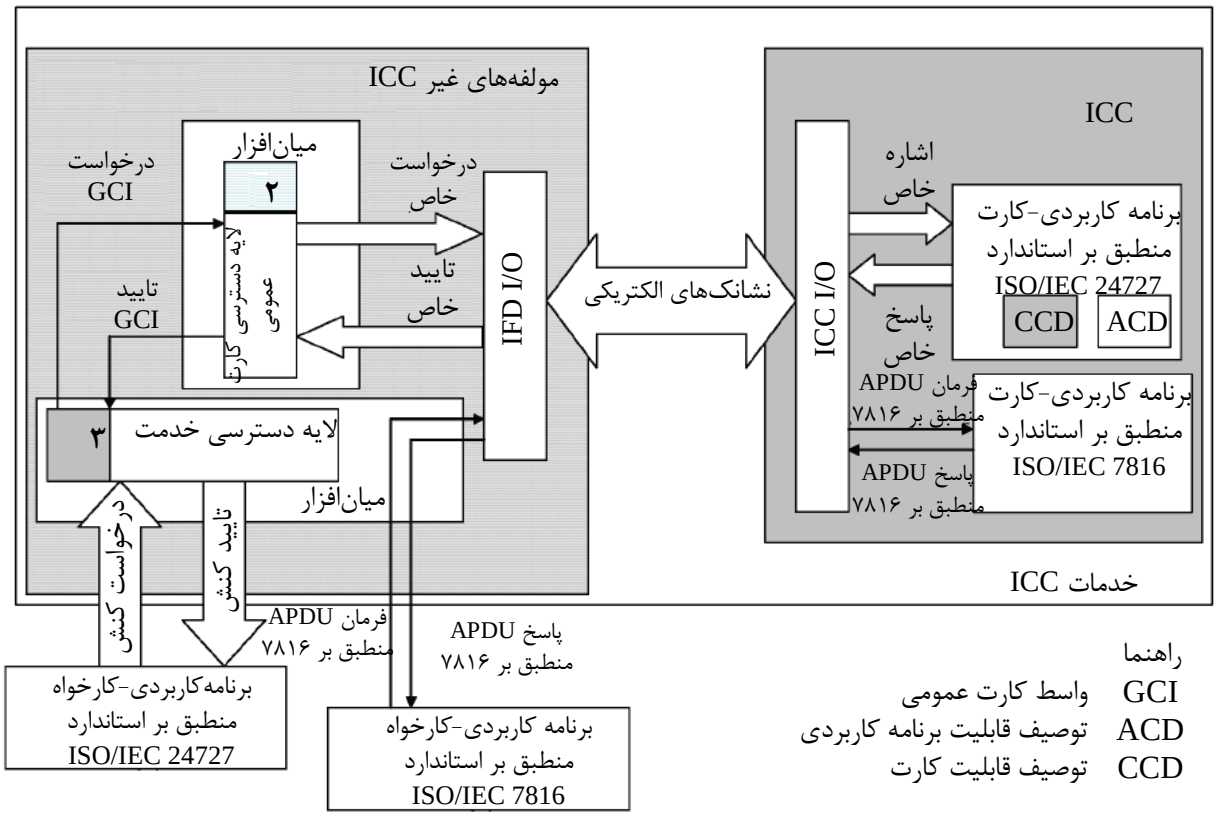
الف-۷ پیکربندی خدمت وب



شکل الف-۷- پیکربندی خدمت وب

این پیکربندی، واسط خدمت وب را پیشنهاد می‌کند که می‌تواند از برنامه‌های کاربردی وب دردسترس باشد. همه‌ی واسط‌های استاندارد ISO/IEC 24727 به صورت رسمی و ترجیحا از طریق ASN.1 مشخص شده‌اند، اما در وهله دوم از طریق توصیفات XML که به ترتیب در استانداردهای ISO/IEC 24727-3 و ISO/IEC24727-4 می‌توان یافت، مشخص شده‌اند.

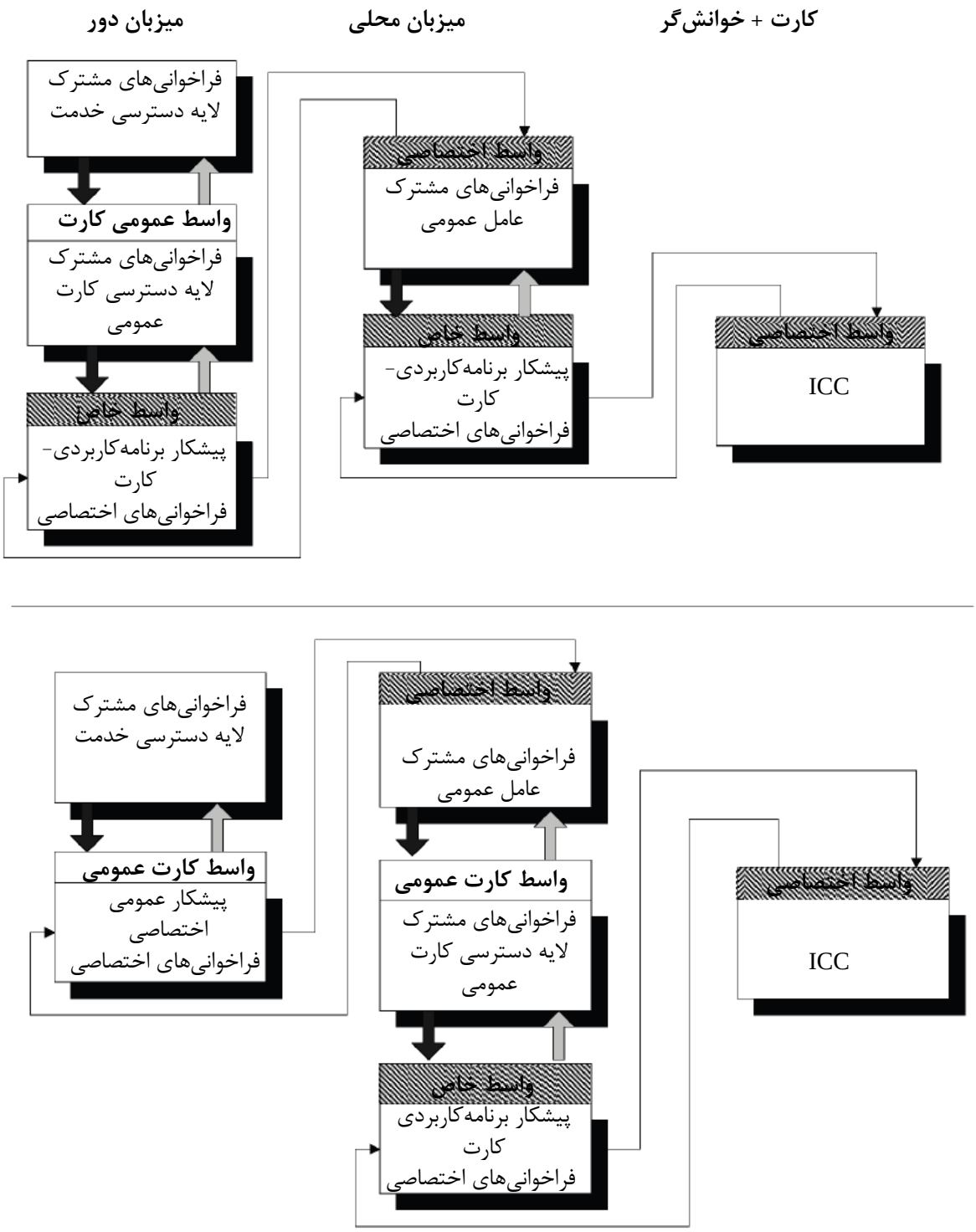
الف-۸ پیکربندی برنامه کاربردی چندگانه



شکل الف-۸- پیکربندی برنامه کاربردی چندگانه

این پیکربندی وجود برنامه کاربردی استاندارد ISO/IEC 24727 را به همراه ICC ای نشان می‌دهد که برنامه‌های کاربردی ISO/IEC 7816 دیگر را پشتیبانی می‌کند. فرایندهای مکان‌یابی و علامت‌گذاری مانند برنامه‌های کاربردی-کارت در استاندارد ISO/IEC 24727-3 و استاندارد ISO/IEC 24727-4 مشخص شده‌اند.

الف-۹ پیاده‌سازی توزیع‌شده پشته



شکل الف-۹- پیاده‌سازی توزیع‌شده پشته

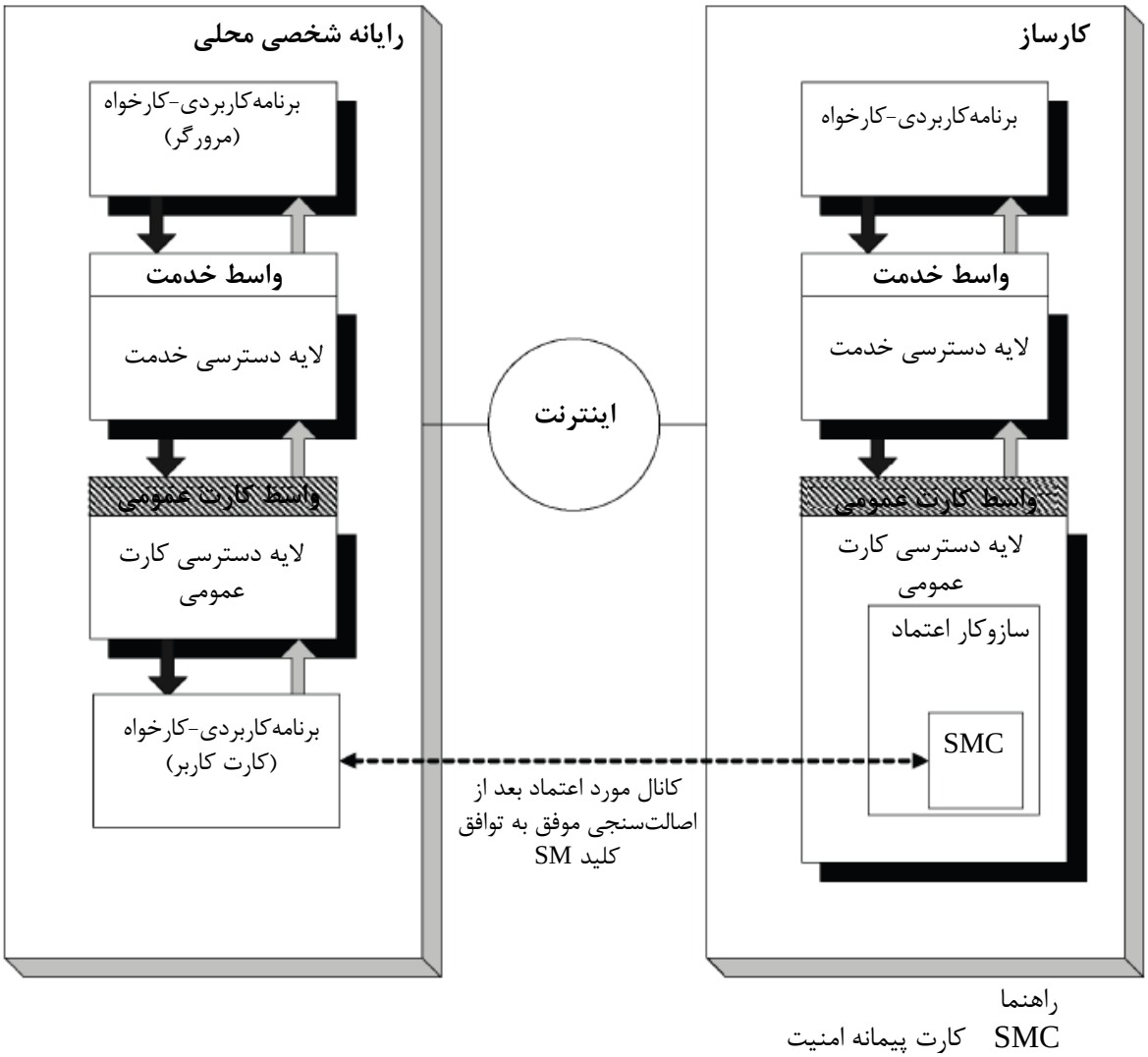
این نمودارها از یک ترکیب (پاسخ مشترک، مستطیل‌های با خط انتهایی پررنگ) برای دسترسی به API

مشخص و واسط کارت عمومی (قاب‌های رشته‌ای) استفاده می‌کنند. این امر تضمین می‌کند که لایه‌های وارد شده در پشته یا موجود در پیشکار (به طور مثال، شبیه‌ساز کارت، ابزارهای آزمون تطابق) بر ضرایب استاندارد تاثیر ندارند (ضرایب استانداردها به‌گونه‌ای ارائه شده‌اند که واسط کارت عمومی و استفاده از پاسخ‌های رایج را عرضه می‌کنند).

این خدمات به صورت اختصاصی استفاده اولیه از اتصال پایه‌ای TLS را فراهم می‌کنند. ممکن است در ادامه استفاده از دیگر قراردادهای TLS شامل قراردادهای به طور کامل اختصاصی ممکن شود.

فرایند عامل پیشکار در استاندارد ISO/IEC 24727-4 مشخص شده است.

الف-۱۰ پیاده‌سازی توزیع‌شده با استفاده از سازوکار مورد اطمینان



شکل الف-۱۰- پیاده‌سازی توزیع‌شده با استفاده از *سازوکار* مورد اطمینان

این پیکربندی استفاده از سازوکار مورد اطمینان مشخص شده در استاندارد ISO/IEC 24727-3 و استاندارد ISO/IEC 24727-4 نمایش می‌دهد. لایهٔ دسترسی کارت عمومی سمت کارساز، درخواستی به واسط عمومی کارساز ارسال می‌کند که نشان دهنده‌ی نیاز به استفاده از سازوکارهای مورد اطمینان است.

سازوکار مورد اطمینان با کمک به SMC، درخواستی امن تولید می‌کند که به کانال مورد اطمینان ارسال و پردازش‌های پیکربندی امن در آنجا انجام می‌شود. هر داده‌ی پاسخ به صورت متنی ساده به لایهٔ دسترسی کارت عمومی تحویل داده می‌شود. استفاده از SMC به صورت ویژه در استاندارد ISO/IEC 24727-3 API نشان داده شده است.

کتاب‌نامه

[1] ETSI/TS 102 221, Smart cards; UICC-Terminal interface; Physical and logical characteristics

[2] ETSI/TS 102 222, Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications

[3] ETSI/TS 102 223, Smart cards; Card Application Toolkit (CAT)

[4] Interoperability Specification for ICCs and Personal Computer Systems, Version 2.0 PC/SC Workgroup, 2004

[5] ISO 3166-1, Codes for the representation of names of countries and their subdivisions — Part 1: Country codes

[6] ISO/IEC 7498-1 | ITU-T Rec. X.200, Information technology— Open Systems Interconnection— Basic Reference Model: The Basic Model

[7] ISO/IEC 7812-1, Identification cards — Identification of issuers — Part 1: Numbering system

[8] ISO/IEC 7816-3, Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols

[9] ISO/IEC 7816-6, Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange

[10] ISO/IEC 7816-8, Identification cards — Integrated circuit cards — Part 8: Commands for security operations

[11] ISO/IEC 7816-9, Identification cards — Integrated circuit cards — Part 9: Commands for card management

[12] ISO/IEC 7816-12, Identification cards - Integrated circuit cards — Part 12: Cards with contacts — USB electrical interface and operating procedures

[13] ISO/IEC 7816-13, Identification cards — Integrated circuit cards — Part 13: Commands for application management in a multi-application environment

[14] ISO/IEC 7816-15, Identification cards — Integrated circuit cards — Part 15: Cryptographic information application

[15] ISO/IEC 8825-1, Information technology — ASN.1 encoding rules: Specification of Basic EncodingRules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

[16] ISO/IEC TR 9577:1999, Information technology — Protocol identification in the network layer

[17] ISO/IEC 9796 (all parts), Information technology — Security techniques — Digital signature schemes giving message recovery

[18] ISO/IEC 9797 (all parts), Information technology — Security techniques — Message Authentication Codes (MACs)

[19] ISO/IEC 9798 (all parts), Information technology — Security techniques — Entity authentication

[20] ISO 9992-2, 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

[21] ISO/IEC 10116, Information technology — Security techniques — Modes of operation for an n-bit block cipher

[22] ISO/IEC 10118 (all parts), Information technology — Security techniques — Hash-functions

[23] ISO/IEC 10536 (all parts), Identification cards — Contactless integrated circuit(s) cards — Closecoupled cards

[24] ISO/IEC 11770 (all parts), Information technology — Security techniques — Key management

[25] ISO/IEC 14443 (all parts), Identification cards — Contactless integrated circuit cards — Proximity cards

[26] ISO/IEC 14888 (all parts), Information technology — Security techniques — Digital signatures with appendix

[27] ISO/IEC 18033 (all parts), Information technology — Security techniques — Encryption algorithms

[28] ISO/IEC 24727-2, Identification cards — Integrated circuit card programming interfaces — Part 2: Generic card interface

[29] ISO/IEC 24727-3, Identification cards — Integrated circuit card programming interfaces — Part 3: Application interface

[30] ISO/IEC 24727-4, Identification cards — Integrated circuit card programming interfaces — Part 4: Application programming interface (API) administration

[31] ISO/IEC 24727-5, Identification cards — Integrated circuit card programming interfaces — Part 5: Testing procedures

[32] ISO/IEC 24727-6, Identification cards — Integrated circuit card programming interfaces — Part 6: Registration authority procedures for the authentication protocols for interoperability