سیستم مدیریت ایزو
www.isomanagement.ir

تماس تلفنی جهت دریافت مشاوره:

۱. مشاور دفتر تهران (آقای محسن ممیز)

۰۹۱۲ ۹۶۳ ۹۳۳۶

۲. مشاور دفتر اصفهان (سرکار خانم لیلا ممیز)

۰۹۱۳ ۳۲۲ ۸۲۵۹

مجموعه **سیستم مدیریت ایزو** با هدف بهبود مستمرعملکرد خود و افزایش رضایت مشتریان سعی بر آن داشته، کلیه استانداردهای ملی و بین المللی را در فضای مجازی نشر داده و اطلاع رسانی کند، که تمام مردم ایران از حقوق اولیه شهروندی خود آگاهی لازم را کسب نمایند و از طرف دیگر کلیه مراکز و کارخانه جات بتوانند به راحتی به استانداردهای مورد نیاز دسترسی داشته باشند.

این موسسه اعلام می دارد در کلیه گرایشهای سیستم های بین المللی ISO پیشگام بوده و کلیه مشاوره های ایزو به صورت رایگان و صدور گواهینامه ها تحت اعتبارات بین المللی سازمان جهانی IAF و تامین صلاحیت ایران می باشد.

هم اکنون سیستم خود را با معیارهای جهانی سازگارکنید...

ISO 9001 14001 18001

CE

GMP GAP 22716

IMS HSE-MS

45001

22000 HACCP

INSO
15712-1
1st Edition
2019
Identical with
ISO/IEC 18328-1:
2015

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

استاندارد ملی ایران
۱-۱۵۷۱۲
چاپ اول
۱۳۹۷

کارت‌های شناسایی- افزاره‌های مدیریت شده توسط کارت مدار مجتمع (ICC)- قسمت ۱: چارچوب کلی

Identification cards- ICC-managed devices- Part 1: General framework

ICS: 35. 240. 15

استاندارد ملی ایران شمارهٔ ۱-۱۵۷۱۲ (چاپ اول): سال ۱۳۹۷

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. gov. ir

وبگاه: http: //www. isiri. gov. ir

Iranian National Standardization Organization (INSO)

No. 2592 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. gov. 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 ماه۱۳۷۱تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشراستانداردهای 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 در کمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شوند 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 بین المللی 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 صدور گواهی 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 افزاره 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- افزاره‌های مدیریت شده توسط کارت مدار مجتمع (ICC)- قسمت ۱: چارچوب کلی»

رئیس:	**سمت و/یا محل اشتغال:**
شجاع چایی‌کار، سامان (دکتری مهندسی کامپیوتر- امنیت اطلاعات)	پژوهشگر- دانشگاه خواجه نصیرالدین طوسی
دبیر:	
علیزاده، مجتبی (دکتری مهندسی کامپیوتر- امنیت اطلاعات)	عضو هیات علمی دانشگاه لرستان- مشاور شرکت پایش کیفیت ماهان پیشگام
اعضا: (اسامی به ترتیب حروف الفبا)	
بصیری، علی اکبر (کارشناسی مهندسی برق- قدرت)	مدیر دفتر تحقیقات- شرکت توزیع برق استان مرکزی
بیت‌الهی، محدثه (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	کارشناس امور استاندارد و فناوری اطلاعات- اداره کل استاندارد استان کرمان
جوانمرد، جواد (کارشناسی ارشد مهندسی کامپیوتر- سخت افزار)	مدرس- دانشگاه آزاد اسلامی واحد خرم‌آباد
حاجی‌وند، محمد (کارشناسی ارشد مهندسی برق- الکترونیک)	کارشناس- شرکت فنی و مهندسی داده‌پردازان افلاک
حیدری، مسعود (کارشناسی مهندسی برق- قدرت)	کارشناس اجرایی- شرکت پایش کیفیت ماهان پیشگام
حیدرنژاد، امین (کارشناسی ارشد مهندسی کامپیوتر- فناوری اطلاعات)	عضو مستقل
خدادادی، تورج (دکتری مهندی کامپیوتر- امنیت اطلاعات)	کارشناس- شرکت پایش کیفیت ماهان پیشگام
خزاعی، هما (کارشناسی مهندسی کامپیوتر- فناوری اطلاعات)	کارشناس امور استاندارد- اداره کل استاندارد استان کرمان

اعضا: (اسامی به ترتیب حروف الفبا)

دهداری سی‌سخت، علیرضا
(کارشناسی ارشد مهندسی کامپیوتر- شبکه‌های کامپیوتری)

سمت و/یا محل اشتغال:
مدرس- دانشگاه آزاد اسلامی واحد کرمان

سالار کریمی، هادی
(کارشناسی مهندسی کامپیوتر- نرم‌افزار)

کارشناس اندازه‌شناسی، اوزان و مقیاس‌ها- اداره کل استاندارد استان کرمان

کرمی‌زاده، ساسان
(دکتری مهندسی کامپیوتر- امنیت اطلاعات)

پژوهشگر- پژوهشکده امنیت پژوهشگاه ارتباطات و فناوری اطلاعات

کریمی، شبیر
(کارشناسی ارشد مهندسی فناوری اطلاعات)

کارشناس- شرکت فنی و مهندسی مهرآفرین افلاک

کولیوند، داود
(کارشناسی مهندسی کامپیوتر- نرم‌افزار)

کارشناس فناوری اطلاعات- شرکت پایش کیفیت ماهان پیشگام

نظرنژاد، مهدی
(کارشناسی ارشد مهندسی برق- مخابرات)

مدرس- دانشگاه آزاد اسلامی واحد خرم‌آباد

ویراستار:

مشرف، بهنوش
(کارشناسی ارشد مهندسی کامپیوتر- شبکه‌های کامپیوتری)

کارشناس استاندارد

فهرست مندرجات

پیش‌گفتار

استاندارد «کارت‌های شناسایی- افزاره‌های مدیریت شده توسط کارت مدار مجتمع (ICC) – قسمت ۱: چارچوب کلی» که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی/منطقه‌ای به عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی ایران شمارهٔ ۵ تهیه و تدوین شده، در پانصد و نود و ششمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۷/۱۱/۱۳ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان 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 زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

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 است و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 18328-1: 2015, Identification cards- ICC-managed devices- Part 1: General framework

مقدمه

این استاندارد یک قسمت از مجموعه استانداردهای ملی ایران شماره ۱۵۷۱۲ است.

این مجموعه استاندارد شامل موارد زیر است:

– قسمت ۱: چارچوب کلی

– قسمت ۲: مشخصه‌های فیزیکی و روش‌های آزمون برای کارت‌های با افزاره‌ها

– قسمت ۳: سازمان، امنیت و فرمان‌ها جهت مبادله

فناوری‌های نوین موجب تولید افزاره‌های انعطاف‌پذیر و مناسب برای عملیات‌های ورودی و خروجی بر روی ICC شده‌اند و دریچه‌های وسیعی از کاربردها و موارد کاربرد گوناگون را گشوده‌اند. نیاز به قابلیت همکاری در پروژه‌های توسعه داده شده جدید، اهمیت وجود استانداردسازی را روشن‌تر کرده است.

کارت‌های مدار مجتمع (ICC)[1] از یک بدنه کارت حاوی یک (یا چند) مدار مجتمع تشکیل می‌شوند. استانداردهای ISO/IEC 7816 و ISO/IEC 14443 الزامات فیزیکی و منطقی ICC، شامل محل قرارگیری تماس[2]، ابعاد کارت، نشانک‌های الکتریکی[3] و پروتکل‌های ارتباطی، سازوکارهای امنیتی و غیره را تعریف می‌کنند.

زمانی‌که افزاره‌های مدیریت شده توسط کارت مدار مجتمع (ICC) بر روی یک ICC قرار می‌گیرند، الزامات متعدد و زیادی در نظر گرفته می‌شود. این الزامات همچنین شامل جنبه‌های فیزیکی و نیز دید منطقی این نوع کارت است. برای افزاره‌های مدیریت شده توسط ICC قرار گرفته بر روی کارت یا داخل کارت، نیاز به برنامه‌های کاربردی مفید و محیط‌های ویژه آن‌ها باید در نظر گرفته شود. طبیعت این نوع افزاره‌ها موجب ایجاد تعاریف گوناگون در جنبه‌های فیزیکی و منطقی گردیده است. هدف این استاندارد، کمینه کردن تفاوت‌های وابسته به فناوری و بیشینه کردن قابلیت همکاری و تبادل است.

1- Integrated Circuit card
2- Contact
3- Electrical signals

کارت‌های شناسایی- افزاره‌های مدیریت شده توسط کارت مدار مجتمع (ICC) – قسمت ۱: چارچوب کلی

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین معماری کلی یک کارت مدار مجتمع (ICC)[1] با افزاره‌های مدیریت شده توسط ICC است. استاندارد ISO/IEC 18328، محتوا و مرزبندی‌های پوشش داده شده و استانداردسازی شده را به‌صورت اجمالی مورد بحث قرار می‌دهد. اصل کلی این استاندارد این است که کلیه فعالیت‌های مربوط به افزاره‌های مدیریت شده توسط ICC، توسط card-IC واپایش[2] می‌شود. این اصل همچنین در مواردی که افزاره‌های مدیریت شده توسط ICC، خارج از کارت قرار داشته باشند نیز معتبر است. این استاندارد برای تمام انواع کارت‌ها صرف‌نظر از فناوری واسط برای ارتباط، کاربرد دارد.

۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌روند:

۱-۲

دکمه

button

افزاره لمسی است که به عنوان یک ورودی واحد استفاده می‌شود.

۲-۲

مدار مجتمع کارت

card-IC

نوعی مدار مجتمع که همراه با سامانه عامل کارت[3] عرضه می‌شود.

۳-۲

افزاره‌های مدیریت شده توسط ICC

ICC-managed devices

افزاره یا افزاره‌هایی که فعالیت آن‌ها فقط توسط ICCها واپایش می‌شود.

1- Integrated Circuit Card (ICC)
2- Control
3- Card operating system

۴-۲

کلیدگان

keypad

آرایه‌ای از چندین دکمه (به زیربند ۲-۱ مراجعه) سازماندهی شده به‌عنوان یک هستار است.

۵-۲

افزاره دریافت اطلاعات زیست‌سنجی

biometric capture device

نوعی حسگر است که وظیفه آن دریافت داده‌های زیست‌سنجی است.

یادآوری- به استاندارد ISO/IEC 17839 مراجعه شود.

۶-۲

نمایشگر الکترونیکی

electronic display

افزاره‌ای الکترونیکی است که جهت نمایش اطلاعات از آن استفاده می‌شود.

۳ نمادها و کوته‌نوشت‌ها

CLF	contactless frontend	انتهای جلویی غیرتماسی
COS	card operating system	سامانه عامل کارت
eID	electronic identification	شناسایی الکترونیکی
eSE	embedded secure element	عنصر امن درون نهاده شده
HCI	host controller interface	واسط واپایشگر میزبان
IC	integrated circuit	مدار مجتمع
ICC	Integrated circuit card	کارت مدار مجتمع

یادآوری- ICC شامل بدنه کارت (یا مدرک مانند مدرک مسافرتی) و یک IC (یا چندین IC) با پیاده‌سازی عملکردهای تعریف شده در استاندارد ISO/IEC 7816-4 است. این ICC مستقل از فناوری واسط فیزیکی است.

I^2C	inter-integrated circuit	مدار میان مجتمع
IFD	interface device	افزاره واسط
LED	light emitting diode	دیود ساطع‌کننده نور

NFC	near field communication	ارتباطات میدان نزدیک
OTP	one-time password	گذرواژه یکبار مصرف
PIN	personal identification number	شماره شناسایی شخصی
SPI	serial peripheral interface	واسط جانبی سری
SWP	single wire protocol	پروتکل تک سیمی
TEE	trusted execution environment	محیط اجرایی قابل اعتماد
UICC	universal integrated circuit card	کارت مدار مجتمع همگانی

۴ چارچوبی برای افزاره‌های مدیریت شده توسط ICC

۴-۱ دسته‌بندی‌های افزاره‌های مدیریت شده توسط ICC

افزاره‌های مدیریت شده توسط ICC، شیوه استفاده و تعاریف کارت‌ها را توسعه داده‌اند. پیاده‌سازی‌های اولیه ICCها، استفاده از افزاره‌های توسعه‌دهنده مانند کلیدگان، نمایشگرهای الکترونیکی و غیره را شامل می‌شوند. انگیزه کلی تدوین استاندارد برای افزاره‌های مدیریت شده توسط ICC در پیوست **الف** توصیف شده است.

به‌طور کلی، یک افزاره مدیریت شده توسط ICC، شامل یک افزاره الکترونیکی مکمل برای سامانه الکترونیکی قرار گرفته بر روی کارت است که اجازه انجام تراکنش‌های داخلی یا تراکنش با جهان پیرامون را می‌دهد. در زیر دسته‌بندی کلی برای افزاره‌های مدیریت شده توسط ICC، از زاویه دید card-IC ارائه شده است:

– افزاره‌های ورودی مانند دکمه، کلیدگان، میکروفون و حسگر ورودی زیست‌سنجی؛

– افزاره‌های خروجی مانند نمایشگر و بلندگو؛

– افزاره‌های ورودی/خروجی مانند صفحه نمایش لمسی؛

– افزاره‌های ارتباطی مانند LED، حسگر نوری، بلندگو، میکروفون؛

– افزاره‌های پشتیبانی مانند منبع تغذیه.

۴-۲ موضوعات هدف در مجموعه استانداردهای ISO/IEC 18328

بسیاری از مدارهای مجتمع مورد استفاده در ICCها امروزی، به طور پیش‌فرض دارای افزاره‌های مدیریت شده توسط ICC بر روی خود card-IC هستند. برای مثال می‌توان به تولیدکننده‌های اعداد تصادفی

(RNG)[1] و کمک پردازنده‌های رمز[2] و غیره اشاره کرد. این افزاره‌های تعبیه شده روی صفحه[3]، از card-IC و سامانه عامل کارت، فقط برای استفاده‌های خاص و تعریف شده توسط سازنده پشتیبانی می‌کنند. امروزه غالباً این افزاره‌ها به‌صورت اختصاصی و مالکانه و مختص به نوع پیاده‌سازی، به یکدیگر متصل می‌شوند. با این‌که در این استاندارد، این‌گونه افزاره‌ها لحاظ نشده‌اند اما هیچ ممانعتی جهت استفاده از سازو کارهای توصیف شده در این مجموعه استاندارد برای چنین افزاره‌های تعبیه شده روی صفحه وجود ندارد.

افزاره‌های توصیف شده در این استاندارد، همواره افزاره‌های الکترونیکی هستند که به card-IC متصل شده‌اند. هرگونه ارسال اطلاعات به/از افزاره باید از سامانه عامل کارت عبور کرده و واپایش شود.

در این استاندارد، پروتکل‌های فیزیکی و منطقی میان واسط‌های سخت‌افزاری card-IC و افزاره‌ها، مورد بحث قرار نمی‌گیرند. در حال حاضر از واسط‌های گوناگونی برای card-IC، مانند واسط‌های SPI یا واسط‌های I^2C استفاده می‌شود. تعاریف این استاندارد، باید مستقل از هرگونه واسط موجود یا واسط‌های احتمالی طراحی شده در آینده باشد. همچنین پیاده‌سازی‌های عینی واسط‌های فیزیکی و الکترونیکی میان card-IC و هر یک از افزاره‌ها و/یا میان گذرگاه‌ها[4] و سخت‌افزارهای فیزیکی خارج از موضوع بحث این استاندارد است.

تنوع گسترده افزاره‌ها با اهداف مختلف و تعداد متعدد سازندگان، که هر کدام از فناوری‌های گوناگونی برای ساخت افزاره‌های خود استفاده می‌کنند و فناوری‌های جدیدی که هر روز اختراع می‌شود، نیاز به یک رویکرد کلی جهت تسهیل سازگاری افزاره‌های جدید، سازندگان جدید و فناوری‌های نوین را آشکار می‌سازد. تعاریف این استاندارد باید تاحد امکان انعطاف‌پذیر بوده تا اجازه پذیرش افزاره‌های جدید در آینده را بدهد.

این استاندارد، کلیه افزاره‌های قابل اتصال به card-IC شامل منابع تغذیه، نمایشگرها، انواع مختلف حسگرها، میکروفون‌ها، دکمه‌ها، کلیدگان‌ها و غیره را پوشش می‌دهد. این فهرست به‌دلیل نیازها و پیشرفت‌های آینده گسترده‌تر نیز خواهد شد. همچنین سازوکار استفاده از افزاره‌های الکترونیکی که خارج از ICC قرار گرفته‌اند، در این استاندارد، پوشش داده شده‌اند. شکل ۱ فهرستی از خصوصیات و سازوکارها را نشان می‌دهد که باید در این مجموعه از استانداردها استانداردسازی شوند.

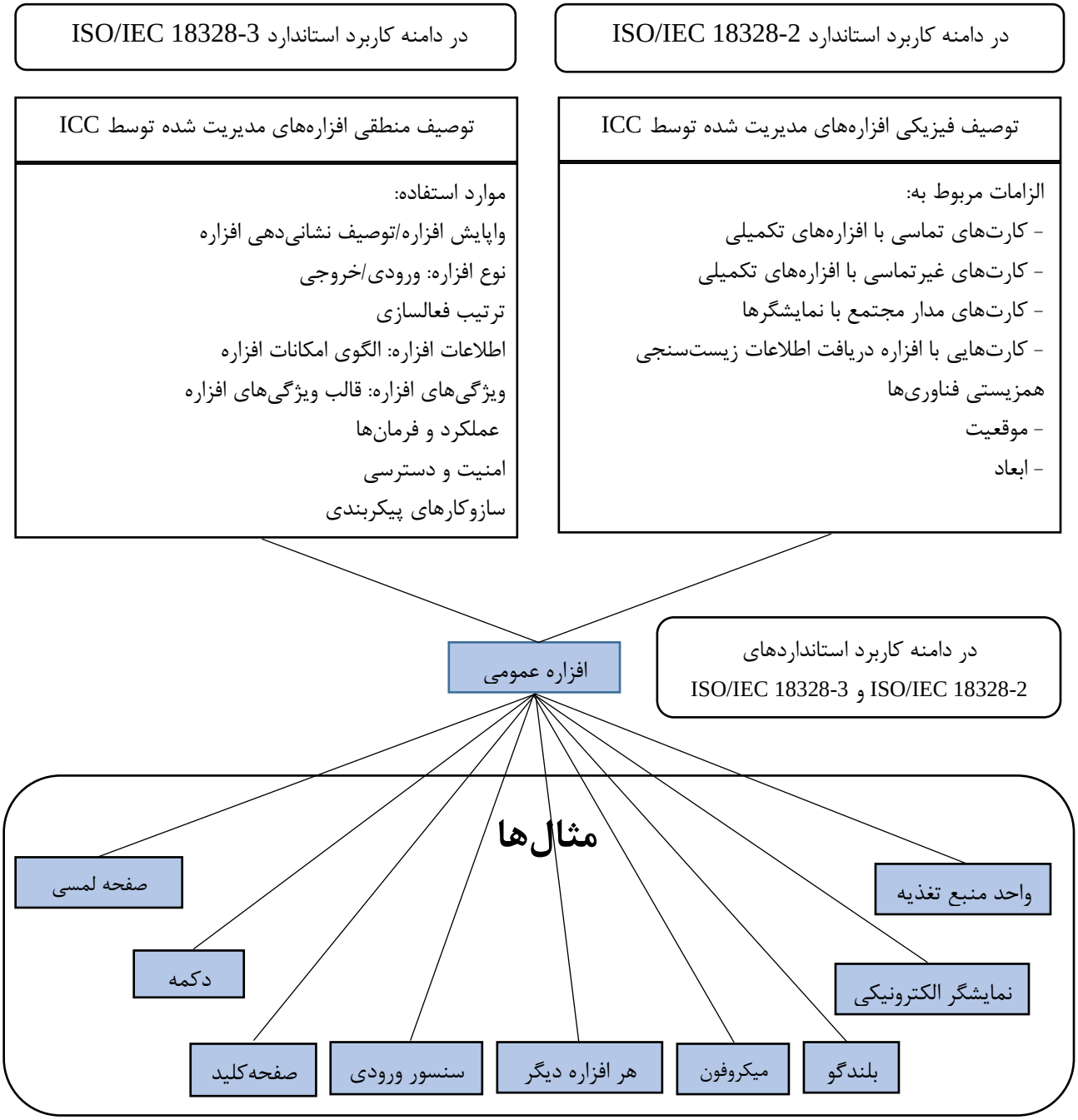
این استاندارد، الزامات عملکردی سامانه عامل کارت و دیگر قسمت‌های نرم‌افزاری را توصیف می‌کند. خصوصیات فیزیکی و روش‌های آزمون و جنبه‌های همزیستی فناوری‌ها برای افزاره‌های مدیریت شده توسط ICCها نیز مورد بررسی قرار می‌گیرند.

تعاریف مربوط به کدبندی مورد نیاز جهت «ارزیابی اعتماد» به داده‌های مدیریت شده مانند هشدار، قلم[5]، رنگ و غیره نیز در دامنه کاربرد این استاندارد است.

1- Random Number Generators
2- Crypto coprocessors
3- On-board devices
4- Buses
5- Font

سازوکارهای توصیف شده در این استاندارد، مستقل از توانایی‌های داخلی افزاره‌ها هستند.

یادآوری- افزاره‌های پیچیده می‌توانند دارای یک واپایشگر یا رانه افزاره[1] جداگانه برای عملکرد باشند. برای مثال یک نمایشگر الکترونیکی ممکن است نیازمند یک رانه الکترونیکی خاص برای فراهم‌سازی و واپایش نشانک‌های فیزیکی به نمایشگر باشد.



شکل ۱- موضوعات هدف در مجموعه استاندارد ISO/IEC 18328

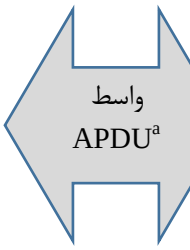
1- Device driver

۴-۳ خلاصه‌ای از معماری سامانه

یکپارچه‌سازی افزاره در ICCها نباید موجب کاهش عملکرد ICCها، به‌خصوص عملکرد کارت‌های مجاورتی[1] شود. تاثیرات احتمالی در دامنه کاربرد سایر قسمت‌های مجموعه استاندارد ISO/IEC 18328 ارائه شده است.

افزاره‌هایی که در مکان‌های متفاوت بر روی ICCهای واقع شده‌اند، همواره از نظر الکتریکی به card-IC متصل هستند. دسترسی منطقی به هر یک از افزاره‌های قرار گرفته بر روی card-IC به‌طور کامل بر عهده سامانه عامل کارت است. شکل ۲ نمای کلی معماری یک ICC با افزاره‌های مدیریت شده توسط ICC را نشان می‌دهد.

مکان‌ها، دسترسی فیزیکی و منطقی، الزامات مکانیکی و الکتریکی، تعاریف مرتبط با امنیت و غیره، موضوع بحث سایر قسمت‌های مجموعه استاندارد ISO/IEC 18328 هستند. برخی قابلیت‌های اختیاری نیز در شکل ۲ نشان داده شده است، برای مثال یک قطعه کد نرم‌افزاری در سامانه عامل کارت، که به‌نام رانه شناخته می‌شود، می‌تواند وظیفه پردازش دسترسی‌های الکتریکی و فعالیت‌های گذرگاه از و/یا به واحدهای مختلف افزاره‌های مدیریت شده توسط ICC را بر عهده داشته باشد. همچنین علاوه بر معماری سامانه ترسیم شده در شکل ۲، پیشنهاد دیگری برای سامانه‌های قدیمی[2] به منظور معماری سامانه در پیوست **پ** ارائه شده است.



[a] Application Protocol and Data Unit (APDU)

شکل ۲ – معماری سامانه card-IC با افزاره‌های مدیریت شده توسط ICC

۴-۴ معماری منطقی

چارچوب منطقی باید هر نوع افزاره مدیریت شده توسط ICC در کاربردهای کنونی و آینده را پوشش دهد. سازوکارها و الگوهای چارچوب باید عملیات‌های پایه و عناصر یا اشیاء داده چنین کاربردهایی را، بدون ایجاد محدودیت در استفاده یا بازتعریف کارکردهای آن‌ها، شامل شوند.

1- Proximity cards
2- Legacy systems

شکل ۱ برخی از الگوهای داده‌ای برجسته و سازوکارهای فراهم شده توسط سامانه عامل را با هدف استفاده از کارکردهای توسعه داده شده در سامانه عامل و برنامه‌های کاربردی، نشان می‌دهد.

معماری منطقی همچنین باید شامل استفاده از افزاره‌های الکتریکی واقع در خارج از کارت باشد. مبادلات و معیارهای امنیتی برای چنین حالتی مشابه با افزاره‌های قرارگرفته بر روی کارت است. هرگونه دسترسی باید توسط ICC واپایش شود؛ در مورد افزاره‌های خارجی، یک قابلیت اضافی برای دنیای خارجی باید تعریف شود. امنیت با استفاده از اصالت‌سنجی[1] و حفظ محرمانگی[2] اطلاعات مبادله شده، تامین می‌شود.

معماری منطقی سامانه در استاندارد ISO/IEC 18328-3 توصیف شده است.

مثال‌هایی از موارد کاربرد افزاره‌های مدیریت شده توسط ICC در پیوست **ب** ارائه شده است.

1- Authenticity
2- Confidentiality

پیوست الف

(آگاهی‌دهنده)

زمینه کاربرد افزاره

الف-۱ کلیات

با افزایش استفاده از فضای سایبری، که فرآیند تصدیق[1] و اصالت‌سنجی در آن‌ها از شفافیت کمتری نسبت به محیط‌های غیربرخط برخوردار است، جرم‌های هویتی به طور چشمگیری افزایش یافته است. مجرمان اغلب از سامانه‌های ضعیف شناسایی، اصالت‌سنجی و عملیات تعیین مجوز و همچنین زیرساخت‌های مورد استفاده توسط اینترنت، برای مقاصد مخرب خود سوء استفاده می‌کنند. بنابراین فرآیند ایمن تایید و اصالت‌سنجی، مهمترین سازوکار امنیتی شده است.

به طور رایج از سه عامل زیر برای حصول اطمینان از انجام صحیح فرآیند اصالت‌سنجی استفاده می‌شود:

- چیزی که می‌دانید، مانند یک گذرواژه؛
- چیزی که دارید، مانند یک ICC یا یک کلید رمزنگاری؛
- چیزی که هستید (ویژگی ماهیتی فرد)، مانند اثر انگشت یا دیگر داده‌های زیست‌سنجی.

قدرت یک سازوکار اصالت‌سنجی به طور عمده به تعداد عامل‌های به‌کار رفته در آن بستگی دارد. این استاندارد، بر اصالت‌سنجی چندعاملی، در حالتی‌که یکی از عامل‌ها یک نمودافزار[2] سخت‌افزاری مانند ICC یا یک سند هویت الکترونیک باشد، تمرکز دارد.

برای اصالت‌سنجی چندعاملی، دو نوع ورودی اختیاری به نمودافزار وجود دارد که به‌نام *داده‌های* فعالسازی نمودافزار[3] و داده‌های ورودی نمودافزار[4] شناخته می‌شوند.

- داده‌های فعالسازی نمودافزار، مانند یک PIN یا اطلاعات زیست‌سنجی، ممکن است جهت فعالسازی نمودافزار و صدور اجازه تولید تاییدکننده اعتبار[5]، مورد نیاز باشند. هنگامی‌که نمودافزار از طریق چیزهایی که گاهی شما می‌دانید یا شما هستید، واپایش می‌شود، داده‌های فعالسازی نمودافزار نیاز است؛

1- Verification
2- Token
3- Token activation data
4- Token input data
5- Authenticator

– داده‌های ورودی نمودافزار، برای مثال یک چالش یا یک داده نانس[1]، ممکن است جهت تولید تاییدکننده اعتبار مورد نیاز باشند. این داده‌ها ممکن است توسط کاربر تولید شده یا یکی از ویژگی‌های خود نمودافزار (مانند یک ساعت بر روی افزاره OTP) باشد.

الف-۲ انگیزه‌های به‌کارگیری افزاره‌های دریافت اطلاعات زیست‌سنجی بر روی کارت‌ها

استفاده از مشخصه‌های زیست‌سنجی جهت اصالت‌سنجی، مزایای بسیاری دارد. مثال‌هایی از این استفاده شامل «بازگشایی»[2] نمودافزارهای متداول اصالت‌سنجی، جلوگیری از رد عضویت[3] یا حصول اطمینان از تکمیل شدن کلیه مراحل ثبت‌نام توسط یک شخص ثابت است. به منظور بهبود فرآیند مرتبط‌سازی[4] یک نمودافزار اصالت‌سنجی به مالک نمودافزار، به‌کارگیری افزاره‌های دریافت اطلاعات زیست‌سنجی بر روی ICCها بسیار مفید است. یکی از رایج‌ترین این افزاره‌ها، حسگرهای اثر انگشت است که از فضای ذخیره‌سازی اثر انگشت و برنامه تصدیق اثر انگشت بر روی کارت بهره می‌برند.

– حسگرهای اثر انگشت قرار گرفته بر روی کارت‌ها، انواع مختلفی از روش‌های اصالت‌سنجی کارت را فراهم می‌کنند: فقط PIN، فقط مشخصه‌های زیست‌سنجی، PIN یا مشخصه‌های زیست‌سنجی، PIN و مشخصه‌های زیست‌سنجی.

– حسگرهای اثر انگشت قرار گرفته بر روی کارت‌ها، انواع مختلفی از روش‌های اصالت‌سنجی افراد را فراهم می‌کنند: از اصالت‌سنجی تک‌عاملی (فقط کارت) تا اصالت‌سنجی‌های ترکیبی دوعاملی یا سه‌عاملی: نمودافزار، PIN و اطلاعات زیست‌سنجی.

– داده‌های اصالت‌سنجی زیست‌سنجی، به طور ایمن بر روی ICC ذخیره و پردازش می‌شوند و بنابراین نسبت به قطع برق و حملات مرد-میانی[5] ایمن هستند.

– تسهیل فرآیند: استفاده از اطلاعات زیست‌سنجی ساده‌تر بوده و مشکلات فراموش نکردن PIN را ندارند.

– افزایش سازگاری و حریم خصوصی: داده‌های اصالت‌سنجی زیست‌سنجی هیچگاه از کارت خارج نمی‌شوند (نیازی به ذخیره این داده‌ها بر روی ذخیره سازهای مرکزی نیست).

– نیازی به زیرساخت جداگانه برای ثبت‌نام و تصدیق نیست.

1- Nonce
2- Unlocking
3- Repudiation of registration
4- Binding
5- Man-in-the-middle attacks

الف-۳ انگیزه استفاده از نمودافزار بر روی ICC

نمودافزار یکی از موارد رایج کاربرد ICCها با افزاره‌های ورودی/خروجی قرار گرفته بر روی کارت است. با ترکیب چنین افزاره‌هایی، کاربردهایی مانند موارد زیر قابل پیاده‌سازی است:

– نمودافزار گذرواژه یکبار مصرف تک‌عاملی[1]: افزاره سخت‌افزاری است که وظیفه تولید رمزهای عبور یکبار مصرف با استفاده از داده جاسازی شده محرمانه‌ای بنام بذر[2]، که گذرواژه با استفاده از آن تولید می‌شود، را بر عهده دارد. این افزاره نیازی به فعالسازی توسط یک عامل ثانویه ندارد. معمولاً گذرواژه یکبار مصرف (برای مثال، شش نویسه[3]) به طور دائمی بر روی افزاره نمایش داده شده و به ورود داده توسط کاربر نیازی ندارد.

– نمودافزار گذرواژه یکبار مصرف چندعاملی[4]: افزاره سخت‌افزاری است که رمزهای عبور یکبار مصرف است که نیازمند فعالسازی از طریق یک عامل اصالت‌سنجی ثانویه هستند (مانند چیزی که می‌دانید و/یا چیزی که هستید)، را تولید می‌کند. عامل ثانویه را می‌توان با استفاده از یک صفحه ورود و/یا یک افزاره دریافت اطلاعات زیست‌سنجی یکپارچه (مانند اثر انگشت)، دریافت کرد. گذرواژه یکبار مصرف غالباً برای مدت کوتاهی بر روی افزاره، نمایش داده می‌شود.

– نمودافزار رمزنگاری چندعاملی[5]: نوعی افزاره سخت‌افزاری حاوی یک کلید رمزنگاری محافظت شده است که نیازمند فعالسازی توسط یک عامل اصالت‌سنجی ثانویه (مانند چیزی که می‌دانید یا چیزی که هستید) است. عامل ثانویه را می‌توان با استفاده از یک صفحه ورود یا یک افزاره دریافت اطلاعات زیست‌سنجی یکپارچه (مانند اثر انگشت)، دریافت کرد. فرآیند اصالت‌سنجی از طریق اثبات در اختیار داشتن افزاره و کلید رمزنگاری، که معمولاً منجر به یک پیام امضا شده رمزی[6] می‌شود، انجام می‌شود. جزئیات عملکرد بستگی به نوع نمودافزار رمزنگاری و پروتکل مورد استفاده دارد.

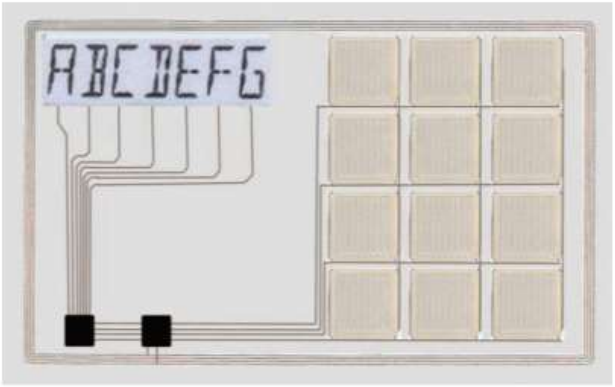
خصوصیات انواع مختلف نمودافزارهای رایج در جدول الف-۱ نشان داده شده است.

1- Single-factor one time password(OTP) token
2- Seed
3- Character
4- Multi-factor one time password(OTP) token
5- Multi-factor cryptographic token
6- Cryptographically signed message

جدول الف-۱- خصوصیات کلیدی موارد کاربرد بیان شده

افزاره	نمایشگر	عناصر ورودی	ملاحظات
نمودافزار گذرواژه یکبار مصرف تک‌عاملی	نمایشگر بخش‌بندی شده[1]	فاقد جزء ورودی	به منبع تغذیه متصل روی صفحه نیاز است
نمودافزار گذرواژه یکبار مصرف چندعاملی	نمایشگر بخش‌بندی شده	کلیدگان و/یا افزاره دریافت اطلاعات زیست‌سنجی	نیازی به منبع تغذیه متصل روی صفحه نیست
نمودافزار رمزنگاری چندعاملی	LED	کلیدگان و/یا افزاره دریافت اطلاعات زیست‌سنجی	نیازی به منبع تغذیه متصل روی صفحه نیست

[1] Segmented display



شکل الف-۱- مثالی از یک نمودافزار گذرواژه یکبار مصرف چندعاملی، به همراه کلیدگان و نمایشگر یکپارچه

پیوست ب

(آگاهی‌دهنده)

موارد کاربرد

ب-۱ تصدیق PIN یا ورود PIN بر روی ICCها

ب-۱-۱ نمایش اطلاعات واپایشی کاربر

در برخی کاربردها از ICCها به عنوان یک عنصر امن بهره می‌برند، برای مثال کارت‌های امضاء[1] که در محیط‌های محافظت نشده با پایانه‌هایی[2] که ممکن است خراب شده یا دستکاری شوند، به‌کار گرفته می‌شوند. کاربر قادر نیست صحت نشست ایجاد شده و قابل اعتماد بودن پایانه را تعیین نماید. وجود نمایشگری بر روی کارت می‌تواند به کاربر این امکان را دهد تا ورودی معتبر بر روی کلیدگان پایانه را، هنگامی‌که ICC قادر به نمایش ورودی بر روی نمایشگر کارت است، واپایش نماید، زیرا ارتباط میان پایانه و ICC معمولاً با استفاده از یک کانال امن، ایمن‌سازی می‌شود. بدین طریق کانال امن میان افزاره واسط و ICC، توسط کاربر قابل بررسی است و از حملات مرد-میانی جلوگیری می‌شود.

می‌توان با خواندن اطلاعات داخلی، که به‌صورت رمزنگاری شده در کارت و در یک کانال امن قرار دارد، یک بررسی مشابه را انجام داد. اگر کارت قادر به نمایش متن آشکار بر روی صفحه نمایش خود باشد، کاربر مطمئن خواهد شد که پایانه قابل اعتماد است.

ب-۱-۲ تصدیق PIN بر روی ICCها

برخی کاربردهای ICCها، دسترسی به کارکردها و داده‌های خاصی را با محافظت از طریق گذرواژه یا PIN، محدود می‌کنند. معمولاً ورودی از طریق کلیدگان پایانه دریافت می‌شود. علاوه بر این، وجود یک کانال امن برای انجام دستور VERIFY ضروری است. کاربردهای با امنیت بالا، مانند کاربردهای امضای رقمی[3] (دیجیتال)، اجباراً از واسط‌ها و پایانه‌های گران‌قیمت برای وارد کردن داده اصالت‌سنجی، از طریق یک کلیدگان مخصوص و امن استفاده می‌کنند.

درصورتی‌که ICC اجازه وارد کردن داده اصالت‌سنجی از طریق کلیدگان واقع بر روی کارت را بدهد، تمام این امکانات غیرضروری هستند. برای این منظور پایانه بهتر است قابلیت اجرای یک فرآیند جهت ورود داده اصالت‌سنجی بر روی کلیدگان کارت و تصدیق داده ورودی، به طور داخلی در خود کارت و بدون نیاز به دخالت پایانه را داشته باشد.

1- Signature cards
2- Terminals
3- Digital

هر دو موارد کاربرد، می‌توانند با یک صفحه نمایش لمسی ترکیب شوند.

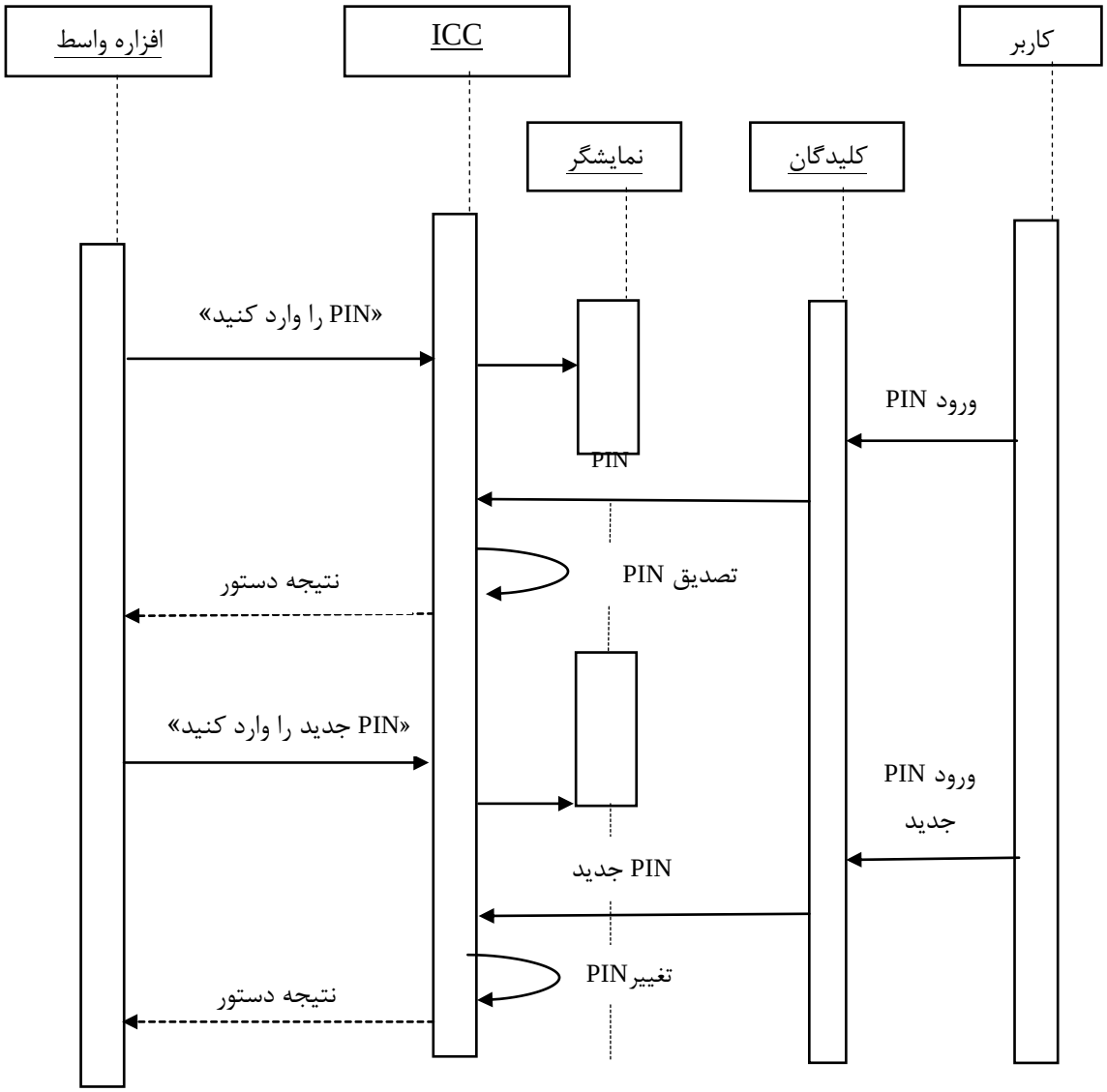
ب-۱-۳ داده مرجع قابل تغییر با نمایشگر روی کارت و کلیدگان

ICCها با نمایشگر الکترونیکی و کلیدگان، امکانات تازه‌ای را برای تغییر PIN یا گذرواژه فراهم می‌کنند. این فرآیند تغییر گذرواژه، با استفاده تعاملی از نمایشگر و کلیدگان، در چند مرحله جداگانه انجام می‌گیرد.

تقاضا برای تصدیق داده و دریافت داده مرجع جدید با نمایش پیغام «PIN را وارد نمایید»، آغاز می‌شود. مقدار جاری بر روی کلیدگان وارد شده و می‌تواند برای تصدیق‌های آینده، به طور موقت در ICC ذخیره شود. به دلایل امنیتی ممکن است نیاز به وارد کردن مجدد این مقدار باشد. برای گرفتن داده مرجع[1] جدید، پیام «PIN را وارد نمائید» نمایش داده می‌شود و مقدار جدید با استفاده از صفحه کلید وارد می‌شود. مقدار می‌تواند در ICC ذخیره شود. همچنین روش اجرایی ممکن است به دلایل امنیتی، تکرار شود.

پس از دریافت تمامی داده‌های مورد نیاز، ICC دستور CHANGE REFERENCE DATA را اجرا می‌کند.

1- Reference data



شکل ب-۱- تغییر داده مرجع با نمایشگر و صفحه کلید متصل به ICC

ب-۲ اعداد موقتی

ب-۲-۱ گذرواژه یکبار مصرف

اصالت‌سنجی کاربر توسط یک هستار دور[1]، ممکن است با استفاده از یک PIN یا گذرواژه انجام گیرد که برای تعیین این‌که آیا کاربر دارای ICC است یا خیر، برای مثال برای کاربردهای غیرتماسی[2] و/یا سازوکارهایی که بر یک واسط دور[3] اجرا می‌شوند. بیشتر کاربردهای امروزی از گذرواژه‌ها و PINهای

1- Remote entity
2- Contactless
3- Remote interface

ایستا[۱]/گذرواژه ایستا استفاده می‌کنند. برای افزایش امنیت، کارت می‌تواند از گذرواژه‌ها و PINهای وابسته به نشست[۲]، که در طول یک نشست توسط ICC تولید می‌شوند، استفاده نماید. این گذرواژه یکبار مصرف، می‌تواند توسط card-IC و مطابق با یک الگوریتم مخصوص تولید شده و توسط همتای دور[۳]، که دارای اطلاعات مشابهی است، بررسی شود.

PIN یا گذرواژه به طور موقت بر روی نمایشگر ICC نشان داده می‌شود و می‌توان از آن در جریان کاربرد استفاده کرد. ورود PIN یا گذرواژه ممکن است از طریق کلیدگان افزاره واسط و/یا ICC انجام شود.

ب-۲-۲ شماره‌های تراکنش[۴]

به‌جای گذرواژه یکبار مصرف، برخی کاربردها از شماره‌های تراکنش استفاده می‌کنند که می‌تواند مالک کارت را شناسایی کنند. شماره‌های تراکنش پویا بر روی نمایشگر ICC فقط در صورتی قابل دسترس هستند که حالت امنیتی اجازه دسترسی به این عملکرد را بدهد. برنامه کاربردی دور می‌تواند شماره تراکنش مورد انتظار را بررسی نماید.

ب-۲-۳ شماره‌های دسترسی کارت

برای اطمینان از اطلاع کاربر از انجام یک کاربرد، به‌خصوص در کاربردهای غیرتماسی، از شماره دسترسی کارت استفاده می‌شود. این شماره جهت برقراری کانال امن بین کارت و پایانه (به مرجع [۱۰] کتاب‌نامه مراجعه شود) استفاده می‌شود. برای جلوگیری از سوءاستفاده (شنود[۵] یا کپی‌برداری از کارت[۶]) و همچنین به منظور افزایش بی‌نظمی[۷] رمزها، یک صفحه نمایش و یک کلیدگان بر روی ICC، به‌صورت هم‌زمان هر دو نیاز را برآورده می‌سازد. کاربرد روی کارت[۸]، یک شماره دسترسی کارت تصادفی/پویا تولید می‌کند (برای مثال بعد از فعالسازی واسط فیزیکی یا انتخاب یک کاربرد) و آن را بر روی نمایشگر کارت نشان می‌دهد. این اطلاعات را می‌توان برای مثال با استفاده از یک خواننده نوری[۹]، پویش[۱۰] نوری انجام داد و/یا توسط متصدی یا مالک کارت، برای مثال با استفاده از کلیدگان واقع بر روی رایانه یا ICC، به منظور تکمیل مرحله تبادل کلید از پروتکل امنیتی و کانال امنیتی، وارد نمود. اطلاعات نمایش داده شده بر روی نمایشگر، می‌تواند به شیوه‌های گوناگونی مثلاً حرفی-رقمی[۱۱]، مبتنی بر نشانک نوری[۱] یا به‌صورت ترکیب با اطلاعات ایستا[۲] و غیره، ارائه شود.

1- Static
2- Session-related
3- Remote counterpart
4- Transaction numbers
5- Eavesdropping
6- Skimming
7- Entropy
8- On-card application
9- Optical reader
10- Scan
11- Alpha-numeric

ب-۳ نمایش داده‌های ذخیره شده داخلی

برنامه‌های کاربردی موجود بر روی یک ICC، داده‌هایی را نگهداری می‌کنند که ممکن است برای کاربر/مالک کارت، جالب و مفید باشد. برای مثال در یک برنامه کاربردی بانکداری، مقدار مانده حساب و/یا موجودی نقدی ممکن است برای مالک کارت جالب باشد، یا در کاربردهای شناسایی، نشانی منزل مالک کارت نمایش داده می‌شود. برنامه کاربردی می‌تواند داده‌های ذخیره شده داخلی را خوانده و آن‌ها را بر روی نمایشگر ICC نمایش دهد. در حالت وجود یک نمایشگر بخش‌بندی شده، این اطلاعات به‌صورت دائمی نمایش داده شده و فقط درصورتی تغییر داده می‌شوند که داده‌های ذخیره شده داخلی تغییر کنند.

نمایش داده‌های ذخیره شده داخلی که فقط توسط مالک کارت قابل دیدن هستند، می‌تواند یک قابلیت امنیتی اضافه، برای اطلاع‌رسانی به کاربر از برقراری یک کانال امن باشد. این داده‌های داخلی را می‌توان بر روی نمایشگر ICC، نمایش داد. کاربر یا مالک کارت می‌توانند از طریق مقایسه با اطلاعات نمایش داده شده، از صحت افزاره واسط یا میان‌افزار[3] اطمینان حاصل کنند.

ب-۴ نمایش داده‌های خارجی دریافت شده

یک برنامه کاربردی بانکداری، نیاز به تایید یک مبلغ توسط مالک کارت دارد. در حالت معمولی، این مبلغ بر روی نمایشگر پایانه نقطه فروش (POS)[4] و/یا افزاره خودپرداز (ATM)[5] نمایش داده می‌شود. امروزه بهتر است مالک کارت به پایانه اعتماد کند و یک رسید برای بررسی مقدار تراکنش ضروری است. با وجود یک نمایشگر متصل به ICC، مالک کارت قادر است مبلغ را مستقل از پایانه، زمانی‌که مقدار مبلغ بر روی نمایشگر کارت نمایش داده می‌شود، بررسی نماید. درصورتی‌که فعالیت نمایشگر با موارد کاربرد بند ب-۴ ترکیب شود، با وجود یک کانال ارتباطی امن، کاربر قادر به تایید صحت پایانه نیز خواهد بود.

1- Optical signal based
2- Static information
3- Middle-ware
4- Point of sale
5- Automated Teller Machine (ATM)

ب-۵ ارزیابی اعتماد با نمایشگر یا LED

به طور کلی از این قابلیت می‌توان برای تقویت اعتماد در جریان کاربردهای مختلف با استفاده از فنون ساده نمایش، مثلاً LED استفاده کرد. این LED توسط card-IC واپایش می‌شود و به مالک کارت می‌گوید که تراکنش به‌درستی در حال انجام و قابل اعتماد است.

ب-۶ دریافت رضایت مشتری با استفاده از افزاره‌های مدیریت شده توسط ICCهای تکمیلی

درصورتی‌که یک ارائه‌دهنده خدمات جهت اعطای دسترسی یک خدمت الکترونیکی به کاربر به اطلاعات وی (مانند نام، نشانی منزل و غیره) نیاز داشته باشد، بهتر است پیش از دریافت اطلاعات کاربر از وی اجازه گرفته شود. به منظور جلوگیری از جمع‌آوری اطلاعات و ردیابی کاربران و حصول اطمینان از این‌که فقط اطلاعات ضروری به ارائه‌دهنده خدمات ارسال می‌شود، دریافت رضایت مشتری از اهمیت ویژه‌ای برخوردار است.

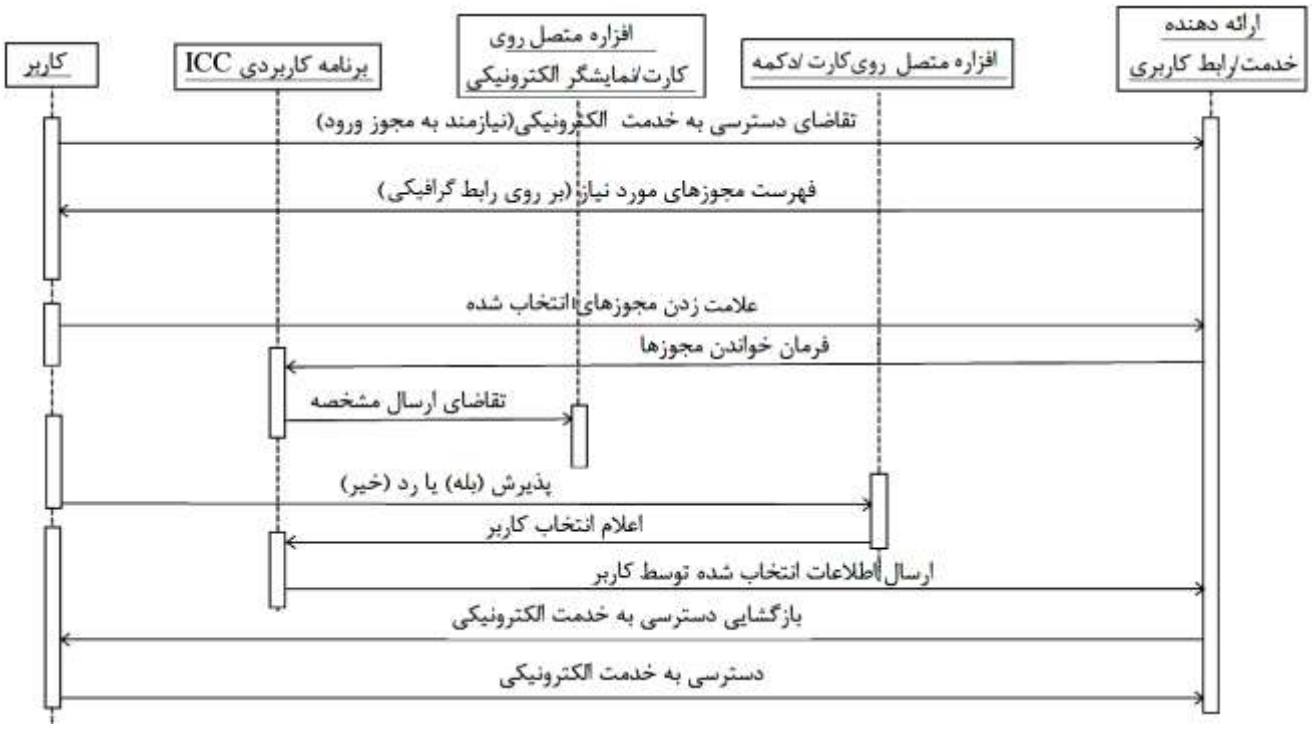
این مورد کاربردی، یک راه‌حل برای چنین ارائه اطلاعات با بهره‌گیری از شیوه‌های غیررمزنگاری با استفاده از یک نمایشگر متصل روی صفحه مدیریت شده توسط ICC و افزاره‌های ورودی (مانند دکمه‌ها، نمایشگر لمسی) را ارائه می‌دهد.

ارائه‌دهنده خدمت یا:

– فهرست ویژگی‌های قابل انتخاب همراه با موارد کاربرد هر یک برای دسترسی به یک خدمت، و تقاضا برای انتخاب و تایید ارسال آن‌ها را بر روی نمایشگر کارت نشان می‌دهد، یا

– فهرست ویژگی‌های قابل انتخاب همراه با موارد کاربرد هر یک برای دسترسی به یک خدمت، و تقاضا برای انتخاب و تایید ارسال آن‌ها را بر روی یک صفحه نمایشگر، برای مثال در قالب یک فرم زبان نشانه‌گذاری اَبَرمتن (HTML)[1] نشان می‌دهد و کاربر با استفاده از کلیدگان متصل به کارت، مواد نشان داده شده برای ارسال به ارائه‌دهنده را تایید می‌کند.

1- Hypertext Markup Language



شکل ب-۲- استفاده از استاندارد ISO/IEC 18328 در ارتباط با امکان دریافت رضایت کاربر

ب-۷ استفاده از استاندارد ISO/IEC 18328 در گوشی‌های همراه[1]

ب-۷-۱ افزاره‌های مدیریت شده توسط eSE

عناصر امنیت پنهان محیط اجرای مورد اعتماد (TEE)[2] محیط ویژه امنی است که بر روی مجموعه تراشه اصلی تلفن همراه اجرا می‌شود و یک محیط مجزای سخت‌افزاری[3] برای سامانه عامل‌های پیشرفته فراهم می‌آورد. این نوع افزونه امنیتی سخت‌افزارهای تلفن همراه، توسط سامانه عامل‌های مختلف مورد استفاده قرار می‌گیرد.

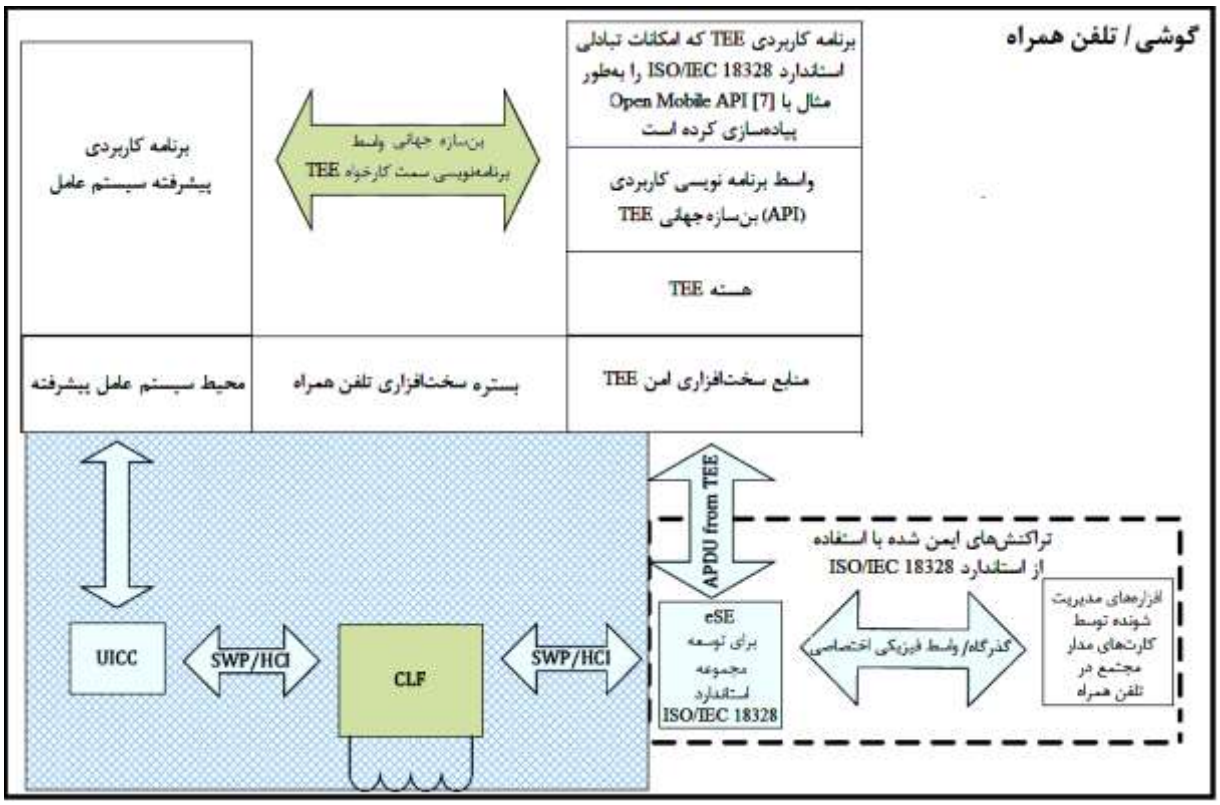
یک عنصر امن (eSE) که درون یک تلفن همراه، مثلاً یک تلفن همراه دارای TEE درون نهاده شده است، می‌تواند میزبان کارکردهای اضافه، ساختمان داده‌ها و قوانین دسترسی همراه با داده‌های محرمانه رمزنگاری مطابق با این استاندارد باشد. چنین عنصر امنی با به‌کارگیری سازوکارهای استاندارد ISO/IEC 18328، فقط دسترسی به یک افزاره اضافی بیرون از کارت (مانند LED، دکمه‌ها، بلندگو و غیره) را واپایش می‌کند. این شیوه استفاده در صورت ترکیب با یک TEE، که توسط عملکردهای این استاندارد توسعه داده شده است، امنیت و قابلیت اعتماد را افزایش می‌دهد، برای مثال بلندگو، LED یا نمایشگر می‌تواند در جریان

1- Handset
2- Trusted Execution Envirement (TEE)
3- Hardware based isolation

تراکنش‌های در حال انجام توسط برنامه کاربردی مبتنی بر TEE، که بر روی صفحه تلفن همراه اجرا می‌شود، فعال شوند.

شکل ب-۳ این مورد کاربرد را، به عنوان مثالی از افزاره‌های خارجی مدیریت شده توسط eSE منطبق با استاندارد ISO/IEC 18328 در یک محیط تلفن همراه، نشان می‌دهد. زمانی‌که یک تراکنش TEE شروع می‌شود، TEE بخش مسئول پردازش افزاره در یک eSE را راه‌اندازی می‌کند. eSE، برای مثال LED را فعال کرده یا صدایی را از طریق بلندگو پخش می‌کند تا به دنیای بیرون اعلام نماید که یک تراکنش TEE، در حال انجام است. پیش از اتمام تراکنش TEE، این اعلان متوقف شود.

وظیفه eSE مطابق با استاندارد ISO/IEC 18328، جایگزین شدن به‌جای واپایش TEE بر منابع سخت‌افزاری امن، با اتکا بر رانه‌های امن واپایش‌کننده افزاره‌های معمولی تلفن همراه نیست. TEE دسترسی بالایی به منابع تلفن همراه، مانند رابط کاربری (کلیدگان و نمایشگر)، شتاب‌دهنده‌های رمزنگاری[1]، عناصر امن و غیره دارد. علاوه بر مسیر راه‌اندارهای امن، TEE می‌تواند یک کانال امن با eSE برقرار کند و دستورات برنامه TEE را در برنامه قرار گرفته در eSE اجرا کرده و بدین طریق مبادلات مبتنی بر استاندارد ISO/IEC 18328 را پیاده‌سازی نماید.



شکل ب-۳- به‌کارگیری استاندارد ISO/IEC 18328 در یک افزاره تلفن همراه

1- Crypto accelerators

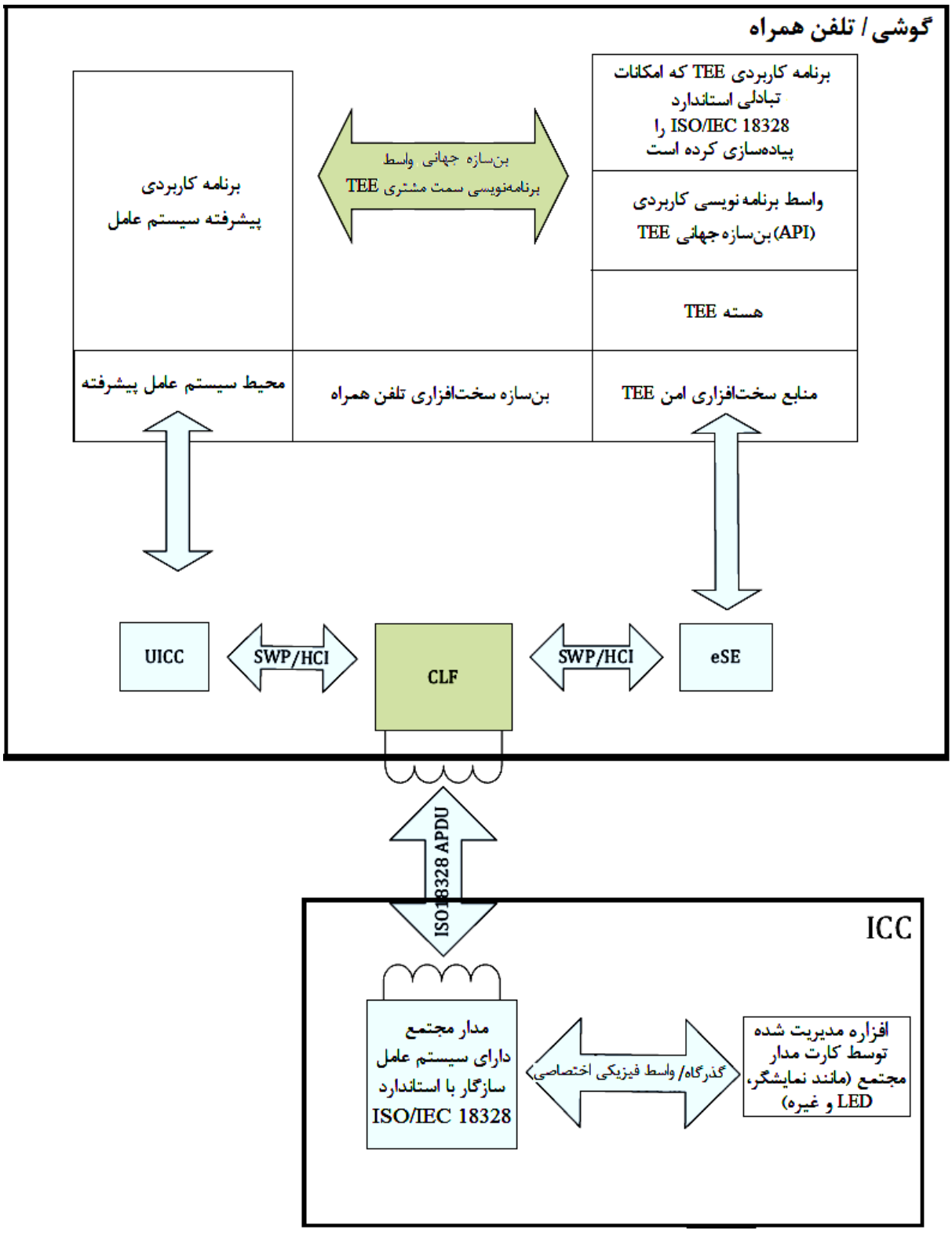
ب-۷-۲ توسعه تراکنش TEE با استفاده از ICC

یک ICC غیرتماسی از تبادل استاندارد ISO/IEC 18328 پشتیبانی می‌کند و به یک کلیدگان، یک LED یا نمایشگر الکترونیکی و غیره مجهز است. این ICC با یک تلفن همراه دارای NFC همراه است. برنامه کاربردی TEE که در محیط TEE اجرا می‌شود، تراکنشی را آغاز نموده و واپایش افزاره متصل به کارت را از طریق واسط NFC بر روی ICC، راه‌اندازی می‌کند.

زمانی‌که ICC و برنامه مربوطه، مجوزهای دسترسی درخواست TEE را بررسی و تایید کردند، واپایشگر متصل به کارت را فعال می‌کنند و برای مثال با یک LED چشمک‌زن، یا پخش صدا کاربر را از در دسترس بودن برنامه کاربردی TEE بر روی تلفن همراه آگاه می‌کنند.

از کاربر خواسته می‌شود (مثلاً از طریق یک نمایشگر الکترونیکی متصل به کارت) به منظور اعتبارسنجی تراکنش با استفاده از امضای رقمی، یک کلید را بفشارد. داده رمزی می‌تواند به TEE برگردانده شود.

شکل ب-۴ این مورد کاربردی را نشان می‌دهد.



شکل ب-۴- استفاده از استاندارد ISO/IEC 18328 همراه با ICC در محیط تلفن همراه

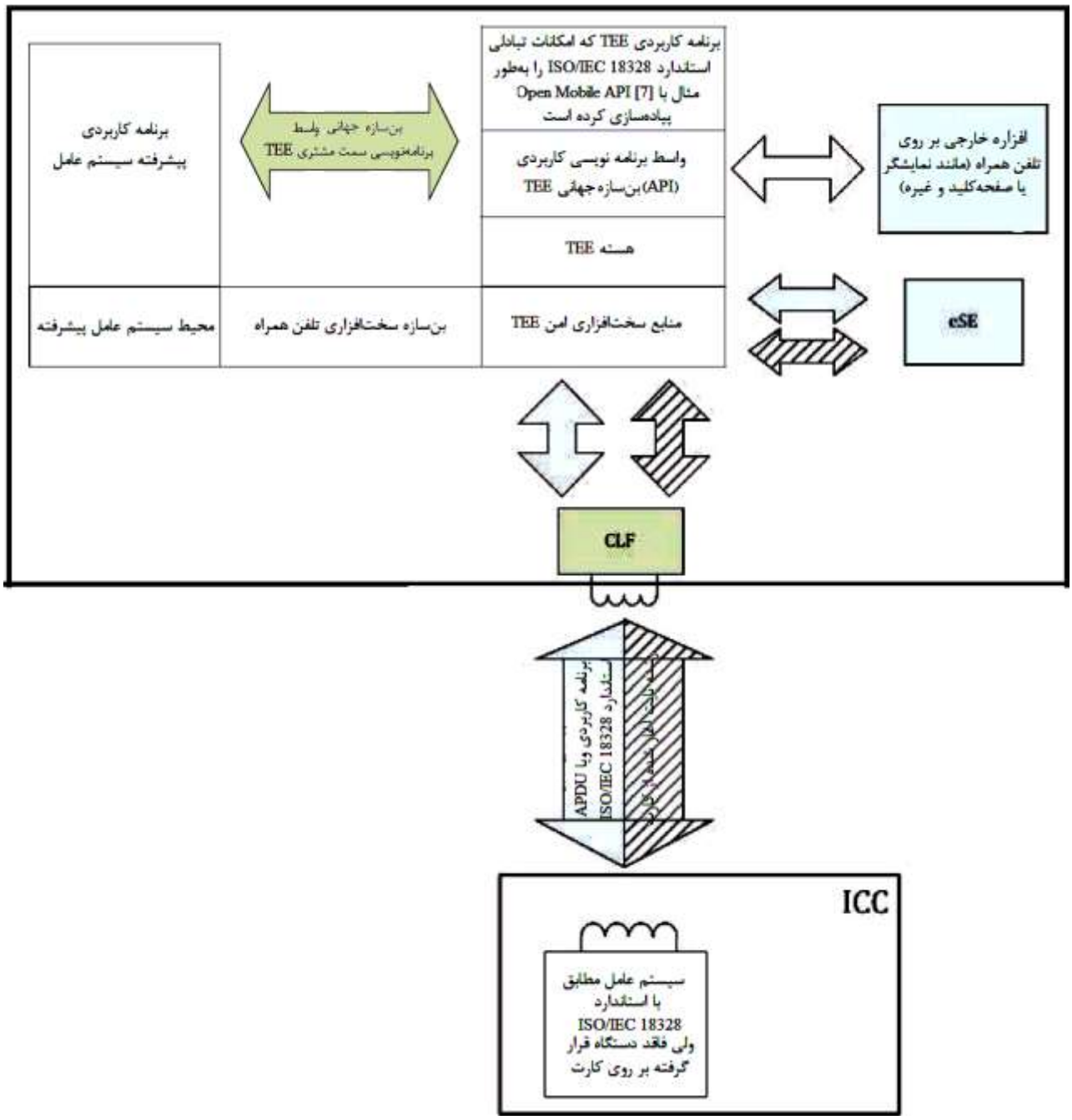
ب-۷-۳ استفاده از افزاره‌های خارج از کارت در یک برنامه کاربردی کارت با پشتیبانی از TEE

یک برنامه کاربردی پشتیبانی‌کننده از TEE بر روی یک موبایل در حال اجرا است. از یک ICC غیرتماسی مطابق با استاندارد ISO/IEC 18328 بدون داشتن هیچ‌گونه افزاره متصل به صفحه، برای اجرای یک برنامه، مثلاً یک برنامه تشخیص هویت که توسط موبایل به عنوان یک IFD راه‌اندازی می‌شود، استفاده می‌شود. در جریان اجرای برنامه، الزام شده است یک نوع داده ورودی کاربر، مثلاً اطلاعات خاص یا PIN، وارد شود.

هنگامی‌که ICC و برنامه مرتبط با آن، مجوزهای درخواست مورد نظر را بررسی و تایید نمایند، یک کانال معکوس صدور دستور را با استفاده از سازوکار «رشته بایت نشئات گرفته از کارت[1]»، را فعال می‌کنند. با در اختیار داشتن این کانال، ICC قادر است رشته دستورها را به برنامه پشتیبانی‌کننده از TEE ارسال نماید، برای مثال دستور خواندن ورودی از کلیدگان و/یا نمایش اطلاعات بر روی نمایشگر تلفن همراه. تمهیدات امنیتی تکمیلی را می‌توان برای حفاظت از این کانال در نظر گرفت (برای مثال رمزنگاری رشته بیت‌ها، رنگ‌ها و قلم‌های تعریف شده به‌صورت موقتی و غیره).

نتیجه دستور «رشته بیت نشئات گرفته از کارت»، به کارت برگشت داده شده و می‌توان از آن در جریان اجرای برنامه استفاده کرد. شکل ب-۵ این مورد کاربرد را نشان می‌دهد.

1- Card-originated byte string



راهنما:

رشته بایت اصلی کارت

APDU برپایه واسط

شکل ب-۵- استفاده از افزاره خارج از کارت با ICC در محیط تلفن همراه

ب-۸ استفاده از مجموعه استاندارد ISO/IEC 18328 در پروتکل‌های امنیتی

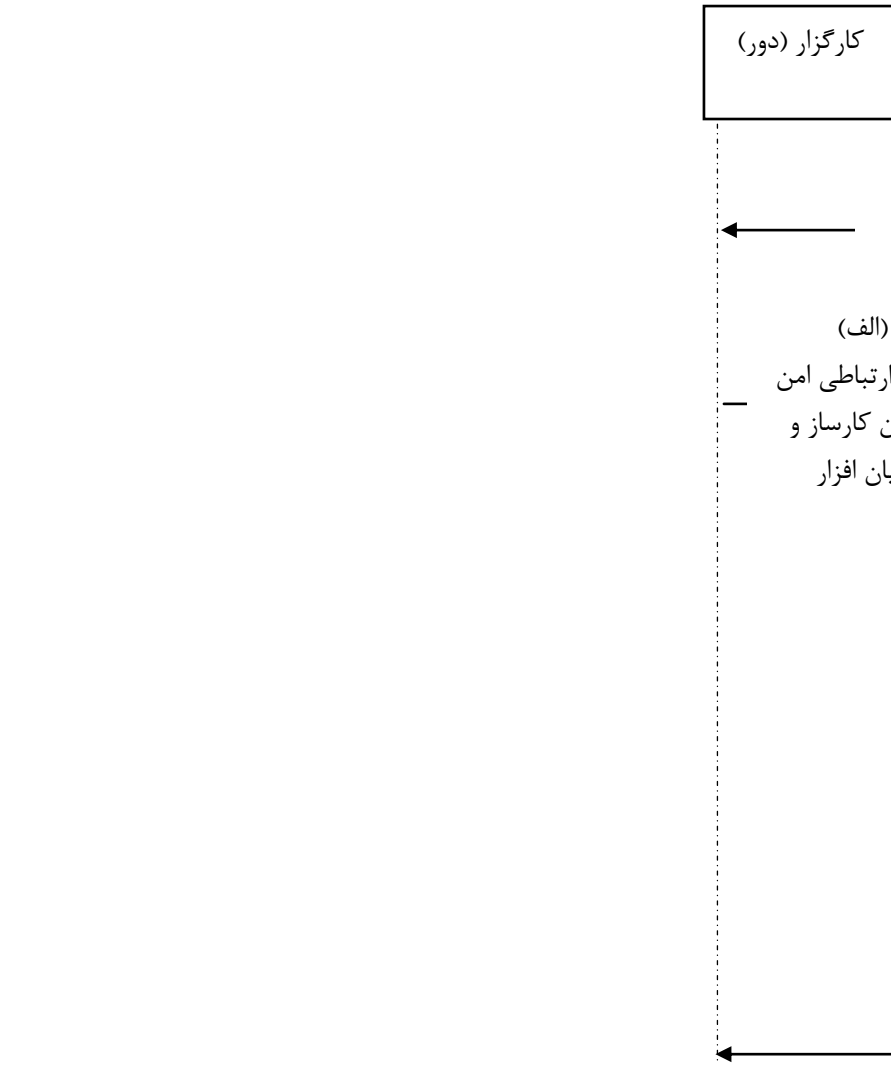
ب-۸-۱ تسهیل ارتباط همتا به همتا[1]

هنگامی‌که پیام‌رسانی امن (SM)[2] میان یک کارساز[3] و یک ICC، به طور همتا به همتا انجام شود، پیام‌رسانی از کلیدهای نشستی که در اختیار میان‌افزار قرار ندارد، استفاده می‌کند. این شیوه امنیتی مانع ارتباط و تبادل اطلاعات با کاربر از طریق رابط کاربری می‌شود: مثلاً برای درخواست داده‌ای از کاربر که به طور امن به ICC بازگردد، مراحل الف تا ث شکل ب-۶ ممکن است ضروری باشد و یکی از دو حالت زیر را ایجاب می‌کند:

– استفاده از یک کانال منطقی دیگر برای ارتباط میان‌افزار و ICC، که با یک پیام‌رسانی امن متفاوت از سازوکار پیاده‌سازی شده میان کارساز و ICC، ایمن شده است؛

– رسیدگی به تغییر زمینه[4] از زمینه SM1 به یک پیام‌رسانی امن دیگر، به طوریکه کلیدهای نشست تنها بین میان‌افزار و ICC به اشتراک گذاشته می‌شوند.

1- End-to-end
2- Secure massaging
3- Server
4- Context switch



راهنما:

الف درحالی‌که SM1 در حال اجراست، به میان‌افزار دستور دریافت داده از کاربر، داده می‌شود.

ب میان‌افزار یک کانال امن با یک واسط گرافیکی کاربر می‌سازد.

پ کاربر از طریق تعامل با واسط گرافیکی کاربر، اطلاعات (مانند گذرواژه، PIN و هر مقدار دخیل در جریان اجرای تراکنش) را وارد می‌کند.

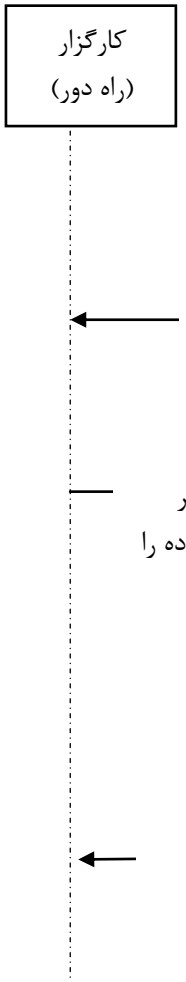
ت داده ورودی کاربر که توسط میان‌افزار جمع‌آوری می‌شود.

ث داده ورودی کاربر رمزنگاری شده توسط کلیدهای نشست SM4، و تحویل داده شده به کارت.

ج اکنون کارت قادر به پردازش ورودی کاربر و برگشت مقادیر نتیجه به کارساز است.

شکل ب-۶- فعالیت‌های انجام شونده در پیام‌رسانی همتا به همتای امن

این مسئله را می‌توان با استفاده از دو افزاره تکمیلی بر روی صفحه ICC حل کرد: یک نمایشگر الکترونیکی و یک کلیدگان. بدین ترتیب می‌توان از طریق نمایشگر الکترونیکی به طور مستقیم به کاربر اطلاع‌رسانی کرد و ورودی مورد انتظار را، با استفاده از کلیدگان، در جریان اجرای پیام‌رسانی امن یعنی SM1، بدون نیاز به رفتن به یک کانال منطقی دیگر یا استفاده از یک شیوه امنیتی اضافی، وارد کرد.



راهنما:

الف درحالی‌که SM1 در حال اجراست، از طریق نمایشگر الکترونیکی به کاربر درخواست ورود اطلاعات، داده می‌شود.

ب کاربر از طریق تعامل با واسط گرافیکی کاربر، اطلاعات (مانند گذرواژه، PIN و هر مقدار دخیل در جریان اجرای تراکنش) را وارد می‌کند.

پ برنامه کاربردی ICC، ورودی را بازیابی می‌کند.

ت اکنون کارت قادر به پردازش ورودی کاربر و برگشت مقادیر نتیجه به کارساز است.

یادآوری- کل تراکنش همتا به همتای میان ICC و کارساز دور، در SM1 اتفاق می افتند.

شکل ب-۷- استفاده از استاندارد ISO/IEC 18328 در پیام‌رسانی امن همتا به همتا

پیوست پ

(آگاهی‌دهنده)

استفاده از card-IC قدیمی[1]

تعریف یک واسط الکتریکی و ارتباط میان card-IC و افزاره/ ریزواپایشگر[2] واپایش افزاره خارج از دامنه کاربرد این استاندارد است. پیاده‌سازی فنی احتمالاً از PINهای ورودی/خروجی دوسویه[3] مانند ورودی/خروجی اهداف عمومی (GPIO)[4]، SPI یا I^2C و دیگر شیوه‌های اتصال افزاره بهره می‌برد.

جهت ایجاد امکان استفاده از card-ICهای قدیمی یا ICCهایی که فاقد پورت‌های تکمیلی هستند، یک مدار دستبرد[5] ممکن است به طور الکتریکی به واسط ارتباطی سازگار ISO یک ICC پیوند شود، برای این‌که بتواند داده‌ها مدنظر یک افزاره مدیریت شده توسط ICC (مانند نمایشگر الکتریکی) را بخواند و آن را بر روی افزاره قرار دهد. مدار دستبرد به عنوان یک خواننده ICC روی صفحه کارت عمل می‌کند. در چنین مواردی و در انطباق با این استاندارد، این مدار دستبرد اجازه ندارد به طور مستقیم اجازه دسترسی به افزاره مدیریت شده توسط ICC را بدهد. جزئیات طراحی و پیاده‌سازی چنین سامانه‌ای خارج از دامنه کاربرد این استاندارد است.

1- Legacy card-IC
2- Microcotroller
3- Bi-directional input/output pins
4- General-Purpose input/output (GPIO)
5- Interception circuit

کتاب‌نامه

[1] ISO/IEC 7816-1. Identification cards- Integrated circuit cards- Part 1: Physical characteristics

یادآوری- استاندارد ملی ایران شماره ۱-۸۲۳۲ (تجدیدنظر اول): سال ۱۳۹۰، کارت‌های شناسایی- کارت‌های دارای مدار مجتمع قسمت ۱: کارت‌های دارای کنتاکت‌ها- مشخصات فیزیکی، با استفاده از استاندارد ISO/IEC 7816-1 Ed 2.0: 2011 تدوین شده است.

[2] ISO/IEC 7816-2, Identification cards- Integrated circuit cards- Part 2: Cards with contacts- Dimensions and location of the contacts

یادآوری- استاندارد ملی ایران شماره ۲-۸۲۳۲ (تجدیدنظر اول): سال ۱۳۹۰، کارت‌های دارای کنتاکت‌ها- ابعاد و محل قرارگیری کنتاکت‌ها، با استفاده از استاندارد ISO/IEC 7816-2 ed2.0: 2011 تدوین شده است.

[3] ISO/IEC 7816-4, Identification cards- Integrated circuit cards- Part 4: Organization, security and commands for interchange

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

یادآوری- استاندارد ملی ایران- ایزو- آی‌ای‌سی شماره ۱-۸۸۲۵: سال ۱۳۹۱، فناوری اطلاعات- قواعد کدبندی نشانه‌گذاری قاعده نحوی انتزاعی یک (ASN.1) ویژگی قواعد کدبندی پایه (BER) قواعد کدبندی متعارف (CER) و قواعد کدبندی متمایز (DER)، با استفاده از استاندارد ISO/IEC 8825-1: 2008 تدوین شده است.

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

یادآوری- مجموعه استانداردهای ملی ایران شماره ۱۴۴۴۳،کارت‌های شناسایی- کارت‌های مدار مجتمع فاقد کنتاکت- کرت‌های مجاورتی، با استفاده از برخی قسمت‌های مجموعه استاندارد ISO/IEC 14443 تدوین شده است.

[6] ISO/IEC 17839 (all parts), Information technology- Biometric System-on-Card

یادآوری- مجموعه استانداردهای ملی ایران به شماره ۲۱۸۵۴، فناوری اطلاعات، سامانه زیست‌سنجی-روی کارت، با استفاده از برخی قسمت‌های مجموعه استاندارد ISO/IEC 17839 تدوین شده است.

[7] TEE Client API Specification. Version 1.0, July 2010, http://www.globalplatform.org/specificationsdevice.asp

[8] TEE INTERNAL API Specification. Version 1.0, Dec 2011, https://globalplatform.org/specs-library/

[9] TEE SYSTEM API Specification. Version 1.0, Dec 2011, https://globalplatform.org/specs-library/

[10] TR-SUPPLEMENT ACCESS CONTROL FOR MACHINE READABLE TRAVEL DOCUMENT, VERSION 1.1, Apr: 2014, http://www.icao.int/Security/mrtd/Downloads/TechnicalReports/NEWTRspostTAG22/TR-SupplementalAccessControlV1.1.pdf

[11] EST/TS 102 613(SWP), V.11.0.0, Sept. 2012

[12] EST/TS 102 622(HCL), V.12.1.0, Oct. 2014

[13] Open mobile A.P.I Version 3.1 , 2015, http://www.simalliance.org/wp-content/uploads/2015/03/SIMalliance_OpenMobileAPI3_1_.pdf