INSO
10821-4
1st.Edition

2017

Identical with
ISO -9564-4
(2016)

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران

۱۰۸۲۱-۴

چاپ اول

۱۳۹۶

دارای محتوای رنگی

خدمات مالی - مدیریت و امنیت شماره شناسایی شخصی (PIN) - قسمت ۴: الزامات رسیدگی PIN در تجارتِ الکترونیک برای تراکنش‌های پرداخت

Financial services — Personal Identification Number (PIN) management and security — Part 4: Requirements for PIN handling in eCommerce for Payment Transactions

ICS: 35.240.40

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 رسمی‌کشور 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 کسب‌وکار است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی‌و 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 الزامات 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، پیاده‌سازی 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، پیاده‌سازی 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 سامانه‌های 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

«خدمات مالی – مدیریت و امنیت شماره شناسایی شخصی (PIN)– قسمت ۴: الزامات رسیدگی PIN در تجارت الکترونیک برای تراکنش‌های پرداخت»

رئیس:	**سمت و/ یا محل اشتغال:**
یزدیان ورجانی، علی (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس و مسئول مرکز آپا دانشگاه تربیت مدرس
دبیر:	
قسمتی، سیمین (فوق لیسانس مهندسی فناوری اطلاعات، تکنولوژی ارتباطات)	مشاور مرکز آپا دانشگاه تربیت مدرس
اعضا: (اسامی به ترتیب حروف الفبا)	
اسدی پویا، سمیرا (فوق لیسانس مهندسی فناوری اطلاعات)	مدیر عامل شرکت مهندسی پویا دانش و کیفیت آوا
ترابی، مهرنوش (فوق لیسانس مهندسی فناوری اطلاعات، تجارت الکترونیک)	کارشناس استاندارد
شیخ‌الاسلامی، محمد کاظم (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس
صالحی، فاطمه (لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس مسئول پرداخت الکترونیک شرکت فناوری اطلاعات و ارتباطات بانک پاسارگاد (فناپ)
قندهاری، آزاده (فوق لیسانس کامپیوتر، نرم‌افزار)	عضو هیات علمی دانشگاه آزاد اسلامی واحد ساوه
کماسی، مهدی (لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس شرکت گسترش سرمایه‌گذاری ایران خودرو
محمدیان، مصطفی (دکتری، برق)	عضو هیات علمی و معاون پژوهشی دانشکده برق و کامپیوتر دانشگاه تربیت مدرس

معروف، سینا کارشناس سازمان فناوری اطلاعات ایران

(لیسانس، مهندسی کامپیوتر، سخت افزار)

ویراستار:

فرهاد شیخ احمد، لیلا کارشناس استاندارد

(فوق لیسانس مهندسی کامپیوتر، نرم‌افزار)

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «خدمات مالی - مدیریت و امنیت شماره شناسایی شخصی (PIN)- قسمت ۴: الزامات رسیدگی PIN در تجارت الکترونیک برای تراکنش‌های پرداخت» که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی به عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی ایران شمارهٔ ۵ تهیه و تدوین شده، د پانصد و نهمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۹۶/۲/۲۵ 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 وخدمات، 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 می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO 9564-4:2016, Financial services — Personal Identification Number (PIN) management and security — Part 4: Requirements for PIN handling in eCommerce for Payment Transactions

مقدمه

این استاندارد یک قسمت از مجموعه استانداردهای ملی ایران شمارهٔ ۱۰۸۲۱ است.

محیط تجارت الکترونیک به طور ذاتی دارای مخاطره بالا است. این موضوع به خصوص برای تراکنش‌های مبتنی بر PIN درست است، چرا که اگر امنیت PIN در این محیط دچار نقص شود، احتمال زیادی وجود دارد که در برخی موارد داده‌های کارت و PIN به طور متقلبانه اخذ و در دستگاه خودپرداز (ATM)[1]، پایانه‌های فروش (POS)[2] یا محیط‌های تجارت الکترونیک مجدد استفاده شود.

برای انجام تراکنش‌های تجارت الکترونیک، دارندگان کارت از افزاره‌های دسترسی به شبکه (NAD)[3] انتخابی خود استفاده می‌کنند. استاندارد ISO 9564-1 از ورود PIN ها روی NAD ها ممانعت می‌کند.

این استاندارد کمینه الزامات امنیتی و شیوه‌هایی را برای افزاره‌های قابل قبول زیر تعریف می‌کند که برای ورود PIN ها در محیط تجارت الکترونیک استفاد می‌شود:

- افزاره‌هایی که سازگار با ISO 9564-1 است (به عنوان مثال افزاره‌های ورود PIN (PEDs)[4]

- افزاره‌هایی که سازگار با ISO 9564-1 نیست، اما از لحاظ کارکردی افزاره‌های امن برای ورود PIN (FSPED)[5] برای استفاده انحصاری با کارت‌های مدار مجتمع (IC)[6] هستند؛

- افزاره‌هایی که سازگار با ISO 9564-1 نیست، اما کارت‌های IC با صفحه کلید و صفحه نمایش یکپارچه (ICCPED)[7] است.

1 - Automatic teller machine
2 - Point of sale
3 - Network access devices
4 - PIN entry devices
5 - Functionally secure PIN entry device
6- Integrated circute
7 - Integrated circuit card PIN entry devices

خدمات مالی - مدیریت و امنیت شماره شناسایی شخصی (PIN)- قسمت ۴: الزامات رسیدگی PIN در تجارت الکترونیک برای تراکنش‌های پرداخت

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین الزاماتی برای استفاده از شماره‌های شناسایی شخصی (PIN) در تجارت الکترونیک است. شماره‌های شناسایی شخصی در دامنه کاربرد، مشابه PINهای دارنده کارت است که به عنوان وسیله‌ای برای درستی‌سنجی دارنده کارت در تراکنش‌های مالی مبتنی بر کارت استفاده می‌شود؛ به ویژه، در دستگاه خودپرداز (ATM)، پایانه‌های فروش (POS)، نازل خودکار سوخت[1] و ماشین‌های خرید محصول[2].

این استاندارد در تراکنش‌های مالی با منشا کارت که نیاز به درستی‌سنجی PIN دارند و سازمان‌های مسئول پیاده‌سازی فنون مدیریت PIN در تجارت الکترونیک کاربردپذیر است.

مفاد این استاندارد برای پوشش موارد زیر در نظر گرفته نشده است:

- کلمات عبور، کدهای عبور، عبارات عبور و سایر رمزهای مشترک که برای اصالت‌سنجی مشتری در بانکداری برخط، بانکداری تلفنی، کیف پول دیجیتال، پرداخت سیار و غیره، استفاده می‌شود،

- مدیریت PIN های دارنده کارت برای استفاده به عنوان وسیله‌ای برای درستی‌سنجی دارنده کارت در سامانه‌های بانکداری خرد، به ویژه، در دستگاه خودپرداز (ATM)، پایانه‌های فروش (POS)، نازل خودکار سوخت ، ماشین‌های خرید محصول، باجه‌های بانکی و سامانه‌های انتخاب / تغییر PIN که در ISO 9564-1 تحت پوشش قرار گرفته،

- پیشکارهای (پراکسی‌های)[3] کارت مانند تلفن‌های همراه یا زنجیرهای کلید[4]،

- الگوریتم‌های تاییدشده برای رمز کردن PIN که در ISO 9564-2 تحت پوشش قرار گرفته،

- حفاظت از PIN در برابر از دست دادن یا سوء استفاده عمدی توسط مشتری یا کارکنان صادرکننده مجاز،

- حریم خصوصی داده‌های تراکنش غیر PIN،

- حفاظت از پیام‌های تراکنش در برابر تغییر یا تعویض، به عنوان مثال پاسخ مجوزدهی برخط،

- حافظت در برابر تکرار[1] تراکنش،

---

1 - Fuel dispenser
2 - Vending machines
3 - Proxies
۴- Key fobs (توکن سخت افزاری) افزاره کوچکی است که کاربران را برای ورود به شبکه اصالت‌سنجی می‌کند.

- کارکرد افزاره‌های مورد استفاده برای ورود PIN که مربوط به کارکردهای صادرکننده به غیر از ورود PIN است،

- فنون مدیریت کلید خاص، و

- دسترسی و ذخیره‌سازی، داده‌های کارت به غیر از PIN توسط برنامه‌های کاربردی مانند کیف پول.

۲ مراجع الزامی

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

در صورتی که 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 الزامی‌است:

2-1 ISO 9564-1, Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems

۳ اصطلاحات و تعاریف

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

۳-۱

پذیرنده

acquirer

نهاد یا نماینده آن است که از کارت‌پذیر، داده‌های مالی مربوط به تراکنش را به بدست می‌آورد و چنین داده‌هایی را در یک سامانه تبادل، مقداردهی اولیه می‌کند.

۳-۲

به خطر افتادن

Compromise

نقض محرمانگی و / یا یکپارچگی <رمزنگاری> است.

1 - Replay

۳-۳

خوانشگر IC تماسی

Contact IC reader

خوانشگر کارت IC است که برای ایجاد ارتباط بین خوانشگر IC تماسی با کارت IC از طریق یک اتصال فیزیکی نیاز به وارد کردن کارت به خوانشگر IC تماسی دارد

۴-۳

تجارت الکترونیک

eCommerce

خرید و فروش محصولات یا خدمات بر روی شبکه‌های باز است

۵-۳

رمز کردن

encipherment

تبدیل داده‌های قابل فهم (متن) به شکل غیرقابل فهم (متن رمزی) است

۶-۳

افزاره ورود PIN امن کارکردی

FSPED

Functionally secure PIN entry device

افزاره‌ای است که با یک کارت IC تماسی به منظور استفاده از PIN برای تولید توکن یکبار مصرف (OTT)[1] غیر برخط ارتباط دارد و حاوی موارد زیر است:

- خوانشگر IC تماسی،

- صفحه کلید عددی یکپارچه، و

- صفحه نمایش حرفی و عددی

یادآوری۱- FSPED، مفهوم PED در استاندارد ISO 9564-1 نیست.

1 - One-time token

۳-۷

کارت مدار مجتمع

ICC

کارت IC

integrated circuit card

نوع کارت ID-1 است که در آن همان طور که در (تمام قسمت‌های) استاندارد ISO/IEC 7816 مشخص شده یک یا چند مدار یکپارچه قرار داده شده است

۳-۸

افزاره ورود PIN کارت مدار مجتمع

ICCPED

integrated circuit card PIN entry device

نوعی کارت ID-1 است که در آن همان طور که در (تمام قسمت‌های) استاندارد ISO/IEC 7816 مشخص شده یک یا چند مدار یکپارچه قرار داده شده است، اما علاوه بر خود تغذیه[1]، قابلیت‌های صفحه کلید و صفحه نمایش یکپارچه را برای استفاده از PIN در تولید OTT غیر برخط را نیز دارد

یادآوری۱- استانداردهایی که توصیف می‌کند این نوع افزاره‌ها در حال تدوین هستند (به مرجع [۸] مراجعه شود)

یادآوری۲- ICCPED، مفهوم PED در استاندارد ISO 9564-1 نیست.

۳-۹

صادرکننده

Issuer

موسسه دارنده حساب که توسط شماره حساب اصلی (PAN)[2] مشخص می‌شود

یادآوری۱- در این استاندارد، ارجاع به صادرکننده ممکن است به یک نماینده اقدام‌کننده از طرف صادرکننده گسترش یابد، به عنوان مثال، انجام کارکردهای صادرکننده مانند صدور کارت و PIN، درستی‌سنجی PIN و مجوزدهی تراکنش.

1 - Self-powered
2 - Primary account number

۳-۱۰

افزاره دسترسی به شبکه

NAD

network access device

افزاره‌ای که قابلیت اجازه دسترسی به نقاط انتهایی عمومی را از طریق یک شبکه باز دارد، به عنوان مثال رایانه شخصی، تلویزیون، تلفن همراه یا حتی لوازم خانگی

یادآوری۱- افزاره‌های POS که در استاندارد ISO 9564-1 با اتصال IP با دسترسی محدود به تعداد پذیرندگان محدود تعریف شده، NAD نیست.

۳-۱۱

شبکه باز

open network

شبکه ارتباطات برای استفاده عمومی است

مثال اینترنت، شبکه‌های تلفن همراه.

۳-۱۲

شماره شناسایی شخصی

PIN

personal identification number

رشته‌ای از ارقام عددی که به عنوان یک رمز مشترک بین دارنده کارت و صادرکننده برای استفاده‌های بعدی برای اعتباردهی استفاده از کارت‌های مجاز ایجاد می‌شود

۳-۱۳

افزاره ورود PIN

PED

PIN entry device

افزاره‌ای برای ورود امن PIN، همان طور که در استاندارد 9564-1 مشخص شده است

۳-۱۴

شماره حساب اصلی

PAN

primary account number

شماره اختصاصی که صادرکننده کارت و دارنده کارت را شناسایی می‌کند و همان طور که در استاندارد ISO/IEC 7812-1 مشخص شده متشکل از یک شماره کارت شناسایی صادرکننده، شناسایی حساب شخصی و همراه با رقم کنترلی[1] است

۳-۱۵

توکن یکبار مصرف

OTT

one-time token

داده‌های اصالت‌سنجی به صورت رمز توسط کارت IC در پاسخ به ورودی PIN تولید و به صورت اختیاری توسط FSPED قالب‌بندی می‌شوند (به عنوان مثال تبدیل به اعشار[2] و / یا کوتاه می‌شوند[3])

۴ مدل تجارت الکترونیک

در تجارت الکترونیک، دارنده کارت و فروشنده معمولا در زمان پرداخت در یک محل نیستند. تجارت الکترونیک در یک محیط شبکه باز رخ می‌دهد و دارنده از کارت افزاره دسترسی شبکه (NAD) برای انجام تراکنش تجارت الکترونیک استفاده می‌کند. در محیط شبکه باز، NAD ممکن است یک تراکنش را با هر فروشنده متصل به شبکه باز شروع کند. در تجارت الکترونیک، افزاره‌ای که PIN به آن وارد شده است ممکن است تحت واپایش (کنترل)[4] فروشنده یا پذیرنده فروشنده نباشد.

برای تراکنش‌های پرداخت کارت بر اساس PIN، مدل تجارت الکترونیک برخی تغییرات اساسی را با توجه به محیط POS معرفی می‌کند:

- NAD ممکن است یک افزاره محاسبات همه منظوره متصل به شبکه باز باشد و در نتیجه نمی‌تواند امن در نظر گرفته شود.

1 - Check sum
2 - Decimalization
3 - Truncation
4 - Control

- NAD ممکن است شامل یک صفحه کلید عددی باشد، برای سازگاری با الزامات صنعت پرداخت، ساخته نشده است.

- NAD تحت واپایش فروشنده، صادرکننده یا پذیرنده فروشنده نیست.

در نتیجه، NAD برای ورود PIN قابل قبول نیست. بند ۵ الزامات برای رسیدگی امن PIN ها را در محیط تجارت الکترونیک مشخص می‌کند.

۵ الزامات رسیدگی PIN

۵-۱ کلیات

PIN نباید به افزاره دسترسی به شبکه (NAD) وارد شود، این موارد شامل رایانه شخصی، تلفن همراه و غیره است، اما به این موارد محدود نمی‌شود.

افزاره‌های شخصی مورد استفاده برای ورود PIN در تجارت الکترونیک باید برای استفاده انحصاری دارنده کارت باشد. استفاده از افزاره‌های ورود PIN عمومی (مشترک) به PEDS تعریف شده در بند ۵-۴ و ۵-۵ محدود می‌شود.

۵-۲ افزاره‌های ورود PIN امن کارکردی (FSPED)

افزاره‌های ورود PIN امن کارکردی (FSPED)، محدود به افزاره‌های ورود PIN کارکرد است که باید توسط صادرکننده برای استفاده در ارتباط با هر یک از کارت‌های IC صادرکننده به منظور تولید OTT غیربرخط تایید شده باشد.

FSPED هایی که از به‌روزرسانی‌های نرم‌افزار پشتیبانی می‌کند باید با صادرکننده کارت یک رابطه رمزنگاری داشته باشد، اما کلیدهای رمزنگاری مرتبط نباید برای رمز کردن PIN استفاده شود. افزاره باید تنها به‌روزرسانی‌های نرم‌افزاری را به کار برد که اصالت‌سنجی رمزنگاری دارند و باید اطمینان حاصل کند که به‌روزرسانی‌های نرم‌افزار در جهت درست به کار می‌رود (به‌روزرسانی‌های قدیمی‌تر پس از این که به‌روزرسانی جدیدتر به کار رفت، نمی‌تواند به کار رود).

FSPED باید شامل خوانشگر IC تماسی برای ارتباط با کارت IC باشد. افزاره نیز باید شامل صفحه کلید برای ورود PIN و صفحه نمایش باشد.

پس از ورود PIN (که ممکن است توسط کارت IC درستی‌سنجی شود) FSPED با کارت IC تعامل می‌کند تا OTT را برای درستی‌سنجی بعدی توسط صادرکننده تولید کند. کارت IC مقدار رمزنگاری را تولید می‌کند. این مقدار ممکن است به طور مستقیم به عنوان OTT استفاده شود یا FSPED ممکن است این مقدار را به OTT قالب‌بندی کند (به عنوان مثال تبدیل به اعشار و / یا کوتاه می‌شوند) که برای کاربر مناسب است که آن را به صورت دستی وارد کند. OTT پس از آن وارد می‌شود یا به NAD به عنوان قسمتی

از تراکنش تجارت الکترونیک منتقل می‌شود و به صادرکننده برای درستی‌سنجی ارسال می‌شود. علاوه بر PIN، ممکن است راه‌حل‌ها قبل از این که OTT بتواند تولید شود، به ورود داده‌های دیگر مربوط به تراکنش در FSPED نیاز داشته باشد. این داده‌های مربوط به تراکنش ممکن است به صورت دستی وارد شود یا از NADبه FSPED منتقل شود. توصیه می‌شود جزئیات چنین تراکنشی (به عنوان مثال مقدار) در FSPED برای دارنده کارت به منظور درستی‌سنجی نمایش داده شود.

FSPED نباید هیچ مشارکتی در رمزنگاری مقدار OTT داشته باشد. با این حال، به عنوان مثال، FSPED ممکن است PIN را با کلید عمومی کارت IC برای انتقال به کارت IC رمز کند.

کارت‌هایی که فقط نوار مغناطیسی دارند، هیچ قابلیت پردازشی ندارد (به عنوان مثال برای درستی‌سنجیPIN) و بنابراین نمی‌توانند برای تولید OTT استفاده شوند.

توصیه می‌شود دارنده کارت توسط صادرکننده راهنمایی شود تا:

- هیچ FSPED ای را از یک منبع نامطمئن مانند کافی نت، مرکز کسب‌وکار هتل و غیره استفاده نکند،

- کارت را از FSPED پس از هر بار استفاده حذف کند،

- از لحاظ فیزیکی از FSPED در مقابل جایگزینی یا تغییر غیر مجاز محافظت کند، و

- استفاده از FSPED را اگر آسیب دیده به نظر می‌رسد متوقف کند.

یادآوری- الزامات این بند مانع استفاده از سازگاری PED استاندارد ISO 9564-1 برای تولید OTT نیست. هر زمان از اصطلاح PED به عنوان یک اصطلاح مستقل در این استاندارد استفاده می‌شود، منظور سازگاری با PED استاندارد ISO 9564-1 است.

FSPED ها باید با الزامات زیر سازگار باشد:

الف- تغییرات غیرمجاز در مشخصه‌های کارکردی افزاره نمی‌تواند بدون نفوذ فیزیکی افزاره ایجاد شود.

ب- افزاره دارای مشخصه‌هایی است که این احتمال را به وجود می‌آورد که نفوذ فیزیکی منجر به آسیب قابل مشاهدهِ قابل تشخیص توسط کاربر نهایی می‌شود.

پ- افزاره نباید مقدار PIN را در هر شکلی به جز برای کارت IC افشا کند. به عنوان مثال، نباید سیگنال‌های دیداری یا شنوایی که مقدار ارقام PIN واردشده را افشا می‌کند، ارائه دهد.

ت- افزاره باید تنها کارکردهای طراحی‌شده خود را انجام دهد.

ث- قابلیت کارکردی پیاده‌سازی‌شده در افزاره باید توسط صادرکننده که دارنده کارت از آن افزاره استفاده می‌کند، تایید شود.

ج- افزاره باید یک افزاره واحد باشد که شامل خوانشگر IC تماسی، پردازنده، صفحه کلید، صفحه نمایش و حافظه می‌شود.

چ- افزاره باید بلافاصله PIN واردشده را هنگامی که PIN به کارت IC ارائه شد یا برای انتقال به کارت IC رمز شد، از کل حافظه افزاره پاک کند.

ح- پس از ورود PIN، OTT باید روی افزاره نمایش داده شود، مگر این که به طور خودکار به NAD منتقل شود.

خ- افزاره باید فقط به‌روزرسانی‌های نرم‌افزاری را به کار ببرد که از نظر رمزنگاری اصالت‌سنجی شده است و باید اطمینان حاصل کند که به‌روزرسانی‌های نرم‌افزاری با ترتیب زمانی درست به کار رود (به‌روزرسانی‌های قدیمی‌تر پس از این که یک به‌روزرسانی جدیدتر به کار رفت، نمی‌تواند به کار رود).

د- افزاره نباید دستورات درستی‌سنجی PIN که از خارج افزاره سرچشمه می‌گیرد را انتقال دهد.

۵-۳ افزاره‌های ورود PIN کارت مدار مجتمع (ICCPED)

افزاره‌های ورود PIN کارت مدار مجتمع (ICCPED)، کارت‌های IC دارای تغذیه‌ای هستند که با قابلیت‌های صفحه کلید و صفحه نمایش یکپارچه شده اند. پس از ورود PIN، ICCPED تولید و OTT را نمایش می‌دهد. این OTT سپس به NAD به عنوان قسمتی از تراکنش تجارت الکترونیکی وارد شده و برای درستی‌سنجی به صادرکننده ارسال می‌شود.

ICCPED باید الزامات الف، ب، ت، ث، چ و ح در بند ۵-۲ و همچنین الزامات زیر را برآورده سازد:

الف- ICCPED نباید مقدار PIN را در هر شکلی به جز برای کارت IC افشا کند. به عنوان مثال، نباید سیگنال‌های دیداری یا شنیداری که مقدار ارقام PIN واردشده را افشا می‌کند، ارائه دهد؛

ب- ICCPED باید یک افزاره واحد باشد که ، پردازنده، صفحه کلید، صفحه نمایش، منبع تغذیه و حافظه در یک محل مشهود در برابر دستکاری[1] را شامل IC می‌شود؛

پ- ICCPED باید PIN مرجع را تنها در حافظه امن قسمت ICC افزاره ذخیره کند و بلافاصله PIN تراکنش را هنگامی که PIN درستی‌سنجی شد، از تمام حافظه‌های دیگر پاک کند.

۵-۴ افزاره‌های ورود PIN با رابطه کلیدگذاری به پذیرنده

این مدل می‌تواند به عنوان گسترش محیط نقطه فروش موجود در نظر گرفته شود که در آن دارنده کارت PED مدیریت‌شده توسط پذیرنده با شیوه‌ای مشابه PEDS در محیط‌های سنتی نقطه از فروش است.

که در آن رابطه کلیدگذاری رمزنگاری بین PED و پذیرنده وجود دارد، الزامات استاندارد ISO 9564-1 کاربردپذیر است. علاوه بر این، الزامات زیر باید برآورده شود:

الف- PED باید خودش را برای پذیرنده برای هر تراکنش اصالت‌سنجی کند؛

1 - Tamper-evident

ب- PED باید هر فرمان از سوی پذیرنده را اصالت‌سنجی کند؛

پ- این PED ها نباید از ورود دستی PAN پشتیبانی کند.

این PED ها ممکن است از درستی‌سنجی PIN غیربرخط برای کارت‌های IC استفاده کند و ممکن است از درستی‌سنجی PIN برخط برای نوار مغناطیسی یا کارت‌های IC استفاده کند. توصیه می‌شود پذیرندگانی که تراکنش‌های تجارت الکترونیک نوار مغناطیسی PIN برخط را می‌پذیرند منشاء تراکنش را اصالت‌سنجی کرده یا روش‌های دیگری برای کاهش حملات حدس PIN جعلی داشته باشند.

۵-۵ افزاره ورود PIN با رابطه کلیدگذاری به صادرکننده

جایی که رابطه کلیدگذاری رمزنگاری بین PED و صادرکننده وجود دارد، باید الزامات ISO 9564-1 به کار رود. علاوه بر این، الزامات زیر باید برآورده شود:

الف- PED باید خودش را برای صادرکننده در هر تراکنش اصالت‌سنجی کند؛

ب- PED نباید دستورات PIN را به کارت IC ارسال کند، تا از حملات تهی کردن PIN ممانعت شود؛

پ- PED باید هر فرمان از سوی صادرکننده را اصالت‌سنجی کند. این سازوکار باید بر ارائه‌دهنده و مدیریت‌کننده افزاره‌های صادرکننده تکیه کند، به شکل الف-۶ مراجعه شود.

ت- PED نباید از ورود دستی PAN پشتیبانی کند.

توصیه می‌شود صادرکنندگانی که پیام‌های درستی‌سنجی PIN برخط نوار مغناطیسی را قبول می‌کنند، منشاء تراکنش را اصالت‌سنجی کنند یا روش‌های دیگری را برای کاهش حملات حدس PIN جعلی داشته باشند.

۶-۵ خلاصه رده PED

جدول ۱ رده‌های PED قابل قبول را خلاصه می‌کند.

جدول ۱ - رده‌های افزاره ورودی PIN

رده افزاره ورودی	FSPED	ICCPED	9564-1 PED
مرجع	۲-۵	۳-۵	۴-۵ و ۵-۵
متصل به NAD در زمان تراکنش	مجاز	مجاز	مجاز
استفاده از کارت IC	مجاز	کاربرد ندارد	مجاز
استفاده از کارت نوار مغناطیسی	غیرمجاز	کاربرد ندارد	مجاز
ورود دستی PAN در افزاره	غیرمجاز	غیرمجاز	غیرمجاز

رده افزاره ورودی	FSPED	ICCPED	9564-1 PED
ورود PIN			
PED در زمان تراکنش اصالت‌سنجی شده	کاربرد ندارد	کاربرد ندارد	اجباری
OTT به صورت برخط تولیدشده	بله	بله	اختیاری
PIN به صورت برخط درستی‌سنجی شده	خیر	خیر	بله
OTT به طور خودکار به NAD منتقل شده	مجاز	مجاز	مجاز
افزاره نمایش OTT برای ورود دستی OTT به NAD	مجاز	مجاز	مجاز
ارتقاء نرم‌افزار	مجاز	اختیاری، با استفاده از یک دست‌نوشته (اسکریپت) کارت توسط صادرکننده	اختیاری

پیوست الف

(آگاهی‌دهنده)

نمونه جریان‌ها برای درستی‌سنجی PIN در تجارت الکترونیک

الف-۱ کلیات

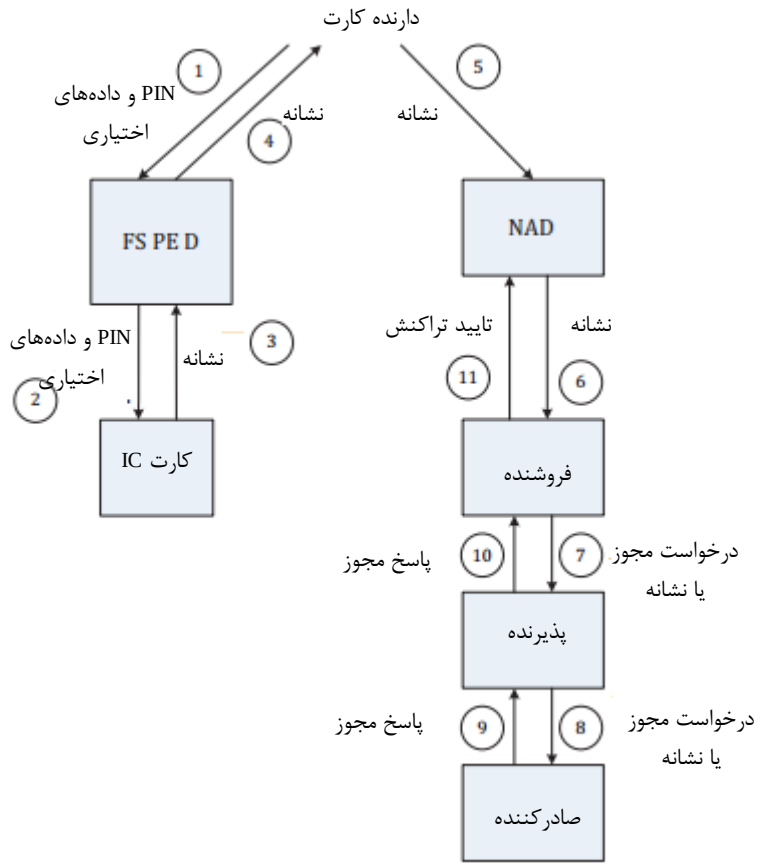
این پیوست همبندی‌های[1] مختلف جریان PIN را نشان می‌دهد.

- غیربرخط، که در آن PIN به صورت محلی توسط دارنده کارت IC پردازش می‌شود
  - با استفاده از FSPED (به شکل الف-۱ یا الف-۴ مراجعه شود) یا سازگاری PED استاندارد ISO9564-1 (به شکل الف-۴ مراجعه شود) از طریق پذیرنده،
  - با استفاده از FSPED از طریق صادرکننده (به شکل الف-۳ مراجعه شود) و
  - با استفاده از ICCPED (به شکل الف-۲ مراجعه شود)؛
- برخط، که در آن PIN برای درستی‌سنجی به صادرکننده ارسال می‌شود،
  - که در آن رابطه رمزنگاری بین PED و پذیرنده وجود دارد (به شکل الف-۵ مراجعه شود)، و
  - که در آن رابطه رمزنگاری بین PED و صادرکننده وجود دارد (به شکل الف-۶ مراجعه شود).

الف-۲ ورود PIN با تولید OTT

شکل الف-۱ فرانامه‌ای (سناریویی) را نشان می‌دهد که در آن دارنده کارت IC در یک FSPED قرار داده می‌شود که سپس در آن PIN وارد می‌شود و OTT ای را تولید کرده که مصرف‌کننده در NAD آنها وارد می‌کند.

1 - Topologies

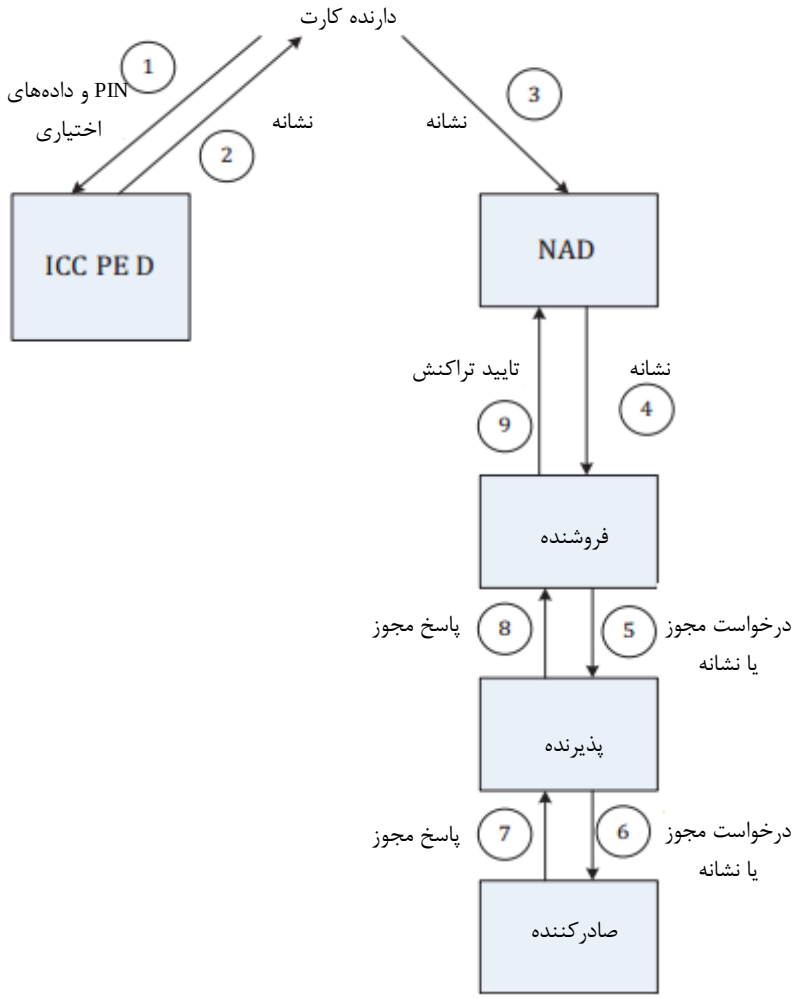


یادآوری- داده اختیاری می‌تواند شامل مقدار تراکنش و / یا حساب مقصد باشد.

شکل الف-۱ – ورود PIN با تولید OTT (FSPED)

در این مورد، کارت IC در یک FSPED قرار داده می‌شود. دارنده کارت PIN خود را در FSPED وارد می‌کند، PIN توسط کارت IC درستی‌سنجی می‌شود و پاسخ به FSPED باز می‌گردد که OTT را (معمولا رشته‌ای از ارقام) به عنوان پاسخی برای ورودی به عنوان قسمتی از تراکنش تجارت الکترونیک آنها نمایش می‌دهد. OTT به فروشنده در نشست برخط منتقل می‌شود و فروشنده تراکنش پرداخت را با استفاده از OTT دریافت‌شده از دارنده کارت ادامه می‌دهد. این کار ممکن است یک فرآیند دو مرحله‌ای باشد که در آن در اولین گام آن OTT (از طریق پذیرنده) به صادرکننده فرستاده می‌شود؛ زمانی که تایید از سمت صادرکننده می‌آید، گام دوم «درخواست مجوز» است یا می‌تواند یک فرایند یک مرحله‌ای باشد که در آن OTT با درخواست مجوز ترکیب می‌شود. فقط فرایند یک مرحله‌ای در شکل الف-۱ ارائه شده است.

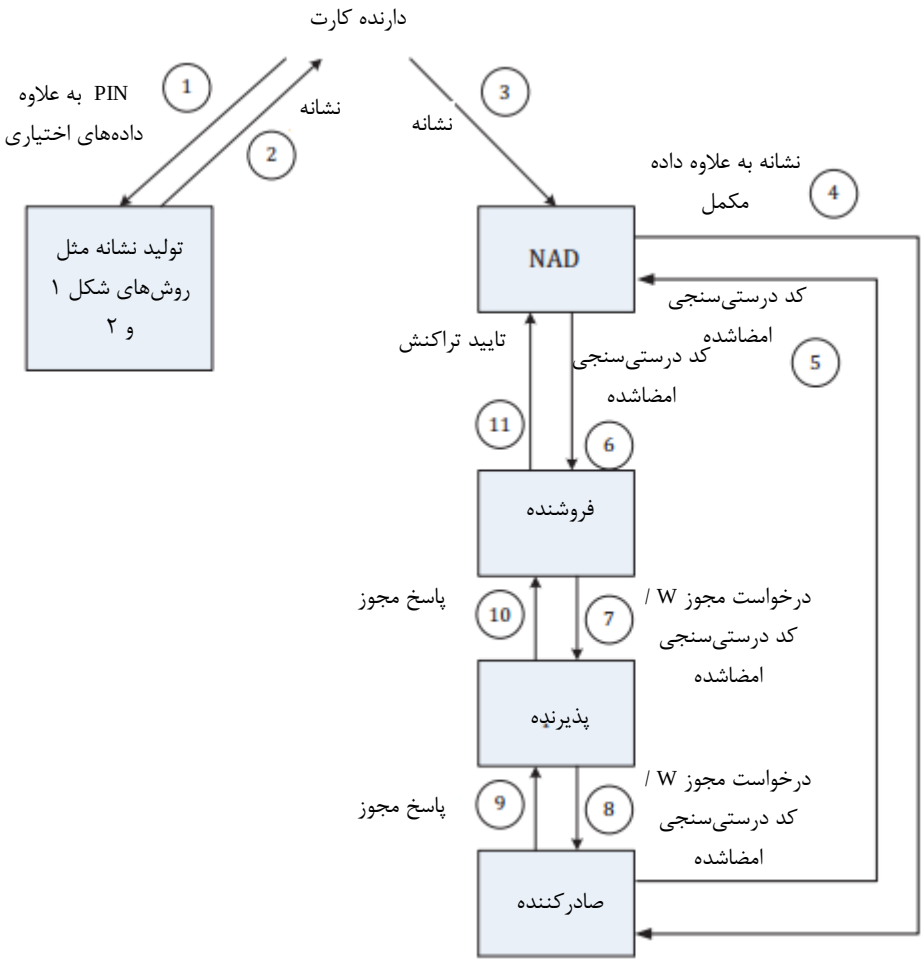
یادآوری- داده اختیاری می‌تواند شامل مقدار تراکنش و/ یا حساب مقصد باشد.



یادآوری- داده اختیاری می‌تواند شامل مقدار تراکنش و / یا حساب مقصد باشد.

شکل الف-۲ - ورود PIN با تولید OTT (ICCPED)

دارنده کارت، PIN خود را در صفحه کلید ICCPED خود وارد می‌کند، PIN توسط ICCPED درستی‌سنجی می‌شود و پاسخ OTT توسط ICCPED برای ورودی به عنوان قسمتی از تراکنش تجارت الکترونیک آنها نشان داده می‌شود. OTT به فروشنده در نشست برخط منتقل می‌شود و فروشنده تراکنش پرداخت را با استفاده از OTT دریافت‌شده از دارنده کارت ادامه می‌دهد. این کار ممکن است یک فرآیند دو مرحله‌ای باشد که در اولین گام آن OTT از طریق پذیرنده به صادرکننده فرستاده می‌شود و زمانی که تایید از سمت صادرکننده می‌آید، گام دوم درخواست مجوز است یا می‌تواند یک فرایند یک مرحله‌ای باشد که در آن OTT با درخواست مجوز ترکیب می‌شود. فقط فرایند یک مرحله‌ای در شکل الف-۲ ارائه شده است.



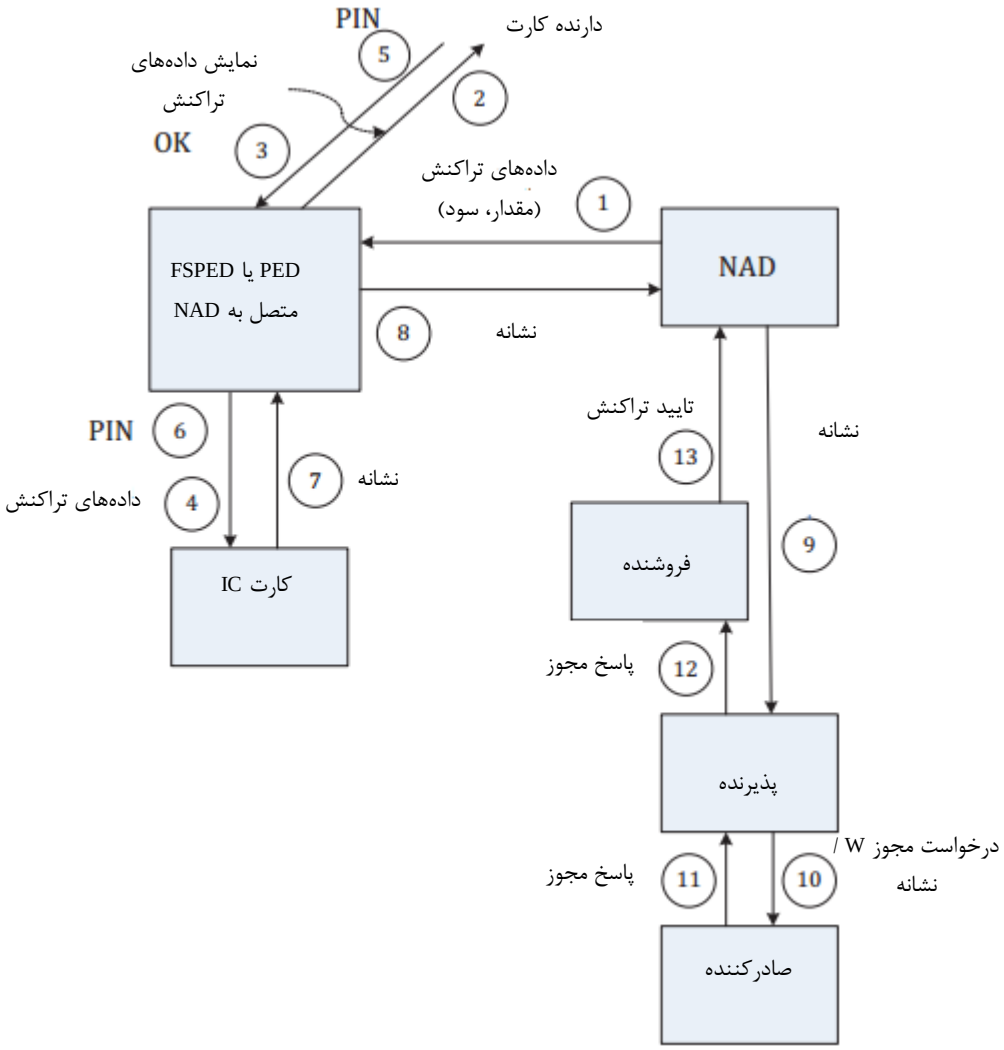
یادآوری- داده اختیاری می‌تواند شامل مقدار تراکنش و/ یا حساب مقصد باشد.

شکل الف-۳ - تولید OTT با صادرکننده درستی‌سنجی مستقیم OTT

این جریان شبیه به جریان نشان داده شده در شکل الف-۱ و الف-۲ است، به جز آن که OTT به طور مستقیم برای درستی‌سنجی از دارنده کارت NAD به صادرکننده ارسال شود. اگر درستی‌سنجی موفقیت آمیز باشد، صادرکننده یک کد درستی‌سنجی امضاشده را به NAD دارنده کارت باز می‌گرداند. این کد سپس به فروشنده که امضای دیجیتال کد را درستی‌سنجی می‌کند و آن را به پیام درخواست مجوز از طریق پذیرنده به صادرکننده انتقال می‌دهد، ارائه می‌شود.

یادآوری- امنیت 3-D[1] می‌تواند به این جریان نگاشت شود.

۱- امنیت 3D یا امنیت کارساز ۳ حوزه‌ای، پروتکل امنیتی برای جلوگیری از تقلب در تراکنش‌های با کارت اعتباری به صورت برخط است.



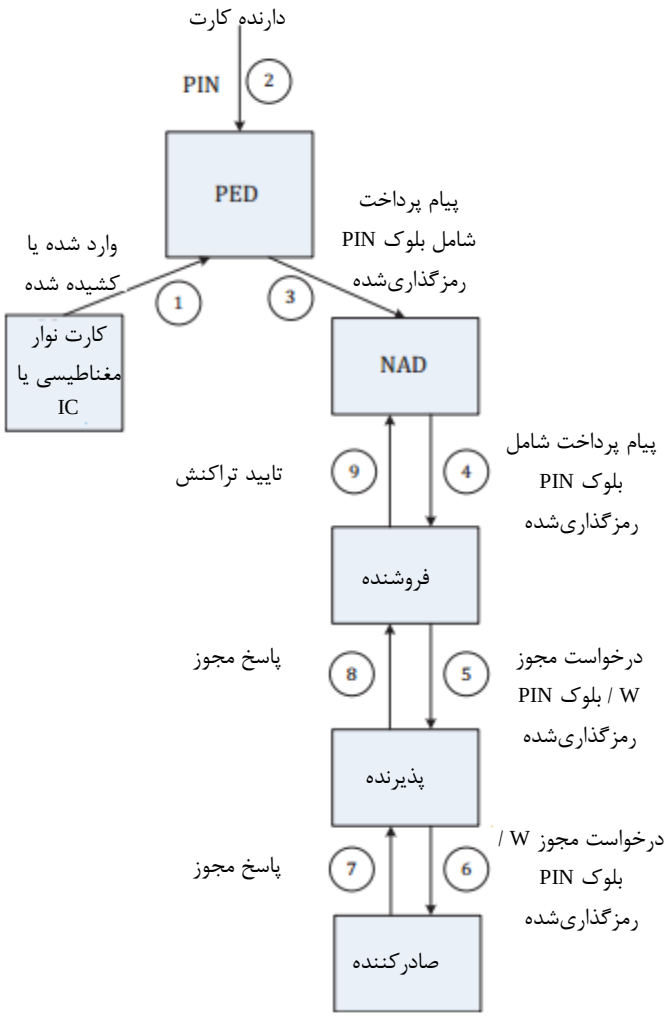
شکل الف-۴- درستی‌سنجی دارنده کارت با داده‌های تراکنش در OTT

در این مورد، دارنده کارت PIN خود را به PED یا FSPED ارائه می‌کند. PIN به صورت رمز با داده‌های تراکنش مانند مقدار تراکنش ترکیب می‌شود و این مزیت را دارد که به شکل یک OTT در آید (به عنوان مثال MAC با کلید خاص کارت IC که می‌تواند از صادرکننده نیز برگرفته شود ایجاد می‌شود). صادرکننده سپس قادر است درستی‌سنجی کند که PIN به درستی توسط اعتبار OTT همراه با داده‌های تراکنش وارد شده است.

در این الگو می‌تواند در رابطه با این که PED یا FSPED چگونه داده‌های تراکنش را از NAD، دریافت می‌کند و همچنین این که آیا PIN واردشده قبل یا بعد از داده‌های تراکنش از NAD به PED یا FSPED منتقل شده است تغییراتی وجود باشد. فلشی که در شکل از سمت سوی مصرف‌کننده به NAD است، نشان می‌دهد دارنده کارت داده تراکنش را تایید می‌کند. علاوه بر این، کارت IC ممکن است مقدار شناسایی بزرگتری تولید کند که PED یا FSPED برای تولید OTT که از طریق بقیه تراکنش فرستاده می‌شود، کوتاه / قالب‌بندی شود.

الف-۳ درستی‌سنجی PIN برخط افزاره ورود PIN سازگار با ISO 9564-1

شکل الف-۵ یک جریان مثال را نشان می‌دهد که در آن PED سازگار بـا ISO 9564-1 بـرای ورود PIN در تنظیمات تجارت الکترونیک استفاده می‌شود.

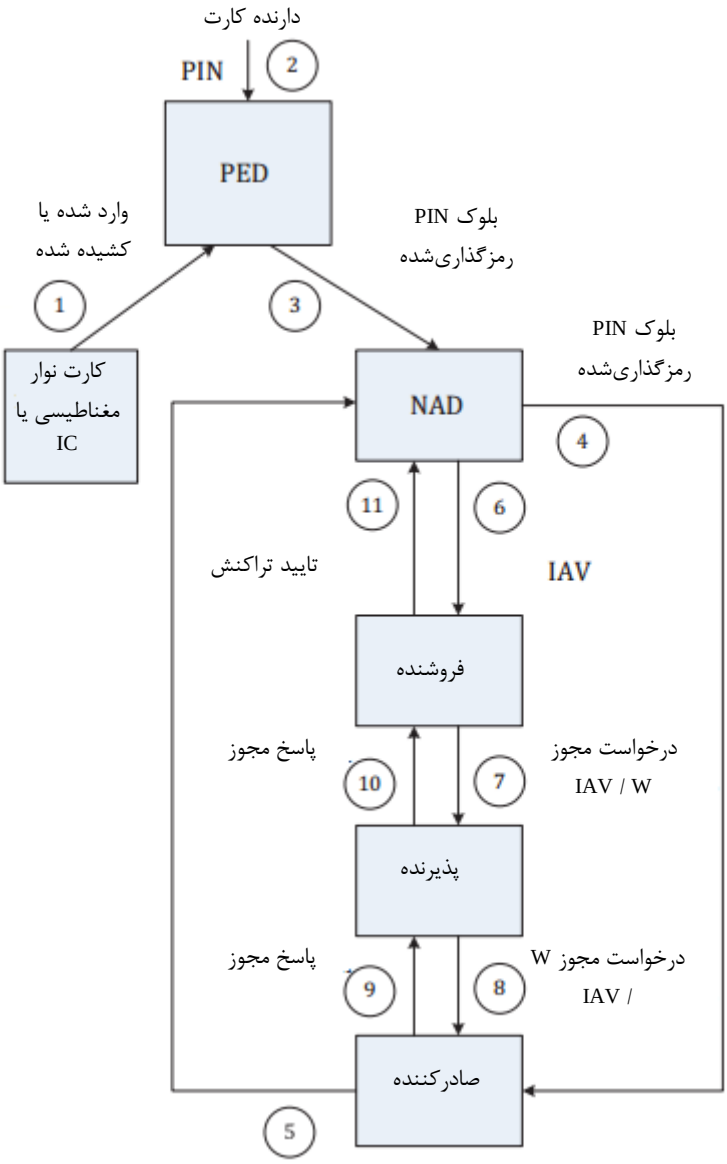


شکل الف-۵ – درستی‌سنجی PIN برخط با PED سازگار با ISO 9564-1

پس از آن که NAD تراکنش پرداخت را با PED، آغاز کرد، دارنـده کـارت، کـارت را در PED قـرار داده یـا می‌کشد، که یک استفاده خصوصی PED سازگار با ISO 9564- 1 است که در ایـن مـورد بـه NAD متصـل است. NAD می‌تواند یک افزاره شخصی یا در یک محل عمومی باشد. دارنده کارت، PIN خود را وارد می‌کند و PED یک بلوک PIN رمزگذاری شده را ایجاد می‌کند که از PED به NAD ارسال می‌شود که از آنجـا بـه فروشنده برخط منتقل می‌شود که آن را از طریق پذیرنده خود به صادرکننده کارت به عنـوان نقطـه فـروش تراکنش پرداخت معمول با PIN می‌فرستد. هنگامی که پاسخ مجوز از صادرکننده به فروشنده بـازمی‌گـردد، فروشنده می‌تواند تصمیم‌گیری کند و تراکنش را به دارنده کارت در نشست برخط اعلام یا رد کند.

الف-۴ درستی‌سنجی PIN برخط با رابطه کلیدگذاری مستقیم بین PED و صادرکننده

شکل الف-۶ یک جریان مثال را نشان می‌دهد که در آن رابطه کلیدگذاری مستقیم بین PED سازگار با ISO 9564-1 و صادرکننده کارت مصرف‌کننده وجود دارد.



یادآوری- بلوک PIN رمزگذاری‌شده هنگامی که صادرکننده دارای رابطه کلیدگذاری با PED است، به طور مستقیم از NAD به صادرکننده می‌رود.

شکل الف-۶ – درستی‌سنجی PIN برخط با رابطه کلیدگذاری مستقیم بین PED و صادرکننده

پس از آن که NAD تراکنش پرداخت را با PED شروع کرد، دارنده کارت، کارت را در PED قرار داده یا می‌کشد، PED در این مورد دارای ارتباط مستقیم با صادرکننده کارت است، به این معنی که PED شامل یک کلید رمزنگاری شناخته شده برای صادرکننده است. به همین دلیل، زمانی که NAD بلوک PIN

رمزگذاری شده را از PED دریافت می‌کند، می‌تواند آن را به طور مستقیم به صادرکننده ارسال کند. صادرکننده درستی‌سنجی PIN را انجام می‌دهد و تاییدی مبنی بر درست بودن PIN را در قالب میزان اصالت‌سنجی صادرکننده (IAV)[1] باز می‌گرداند. این IAV از طریق NAD به فروشنده ارسال می‌شود. پس از دریافت IAV، فروشنده برای تراکنش تصمیم‌گیری می‌کند و با یک درخواست اصالت‌سنجی عادی ادامه می‌دهد.

1 - Issuer authentication value

کتاب‌نامه

[1] ISO/IEC 7810:2003, Identification cards — Physical characteristics

[2] ISO/IEC 7811 (all parts), Identification cards — Recording technique

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

[4] ISO/IEC 7812-2, Identification cards — Identification of issuers — Part 2: Application and registration procedures

[5] ISO/IEC 7813:2006, Information technology — Identification cards — Financial transaction cards

[6] ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics

[7] ISO 13491-1, Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods

[8] ISO/IEC 18328-1, Identification cards — ICC-managed devices — Part 1: General framework

[9] ISO/IEC 18328-2, Information technology — ICC-managed devices — Part 2: Physical characteristics and test methods for cards with devices

[10] ISO/IEC 18328-3, Identification card — ICC-managed devices — Part 3: Organization, security and commands for interchange