INSO

11957-2
1st.Edition

2017

Identical with
ISO-13491-2
(2017)

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران
۱۱۹۵۷-۲

چاپ اول

۱۳۹۶

خدمات مالی – افزاره‌های رمزنگاری امن (خرده‌فروشی) – قسمت ۲: بازبینه‌های انطباق امنیتی برای افزاره‌های استفاده‌شده در تراکنش‌های مالی

Financial services — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions

ICS: 35.240.40

shaghool.ir

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

shaghool.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 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 می کند. ترویج دستگاه بین المللی 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)
Contact point 4-
5- Codex Alimentarius Commission

shaghool.ir

کمیسیون فنی تدوین استاندارد
«خدمات مالی – افزاره‌های رمزنگاری امن (خرده‌فروشی) – قسمت ۲: بازبینه‌های انطباق امنیتی برای افزاره‌های استفاده‌شده در تراکنش‌های مالی»

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
صادقی، محسن	شرکت مدیریت امن الکترونیکی کاشف
صالحی، فاطمه (لیسانس مهندسی کامپیوتر، نرم‌افزار)	مدیر اجرایی نرم‌افزار - شرکت توسعه فناوری اطلاعات گردشگری ایران
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

shaghool.ir

معروف، سینا کارشناس - سازمان فناوری اطلاعات ایران

(لیسانس، مهندسی کامپیوتر، سخت افزار)

ویراستار:

فرهاد شیخ احمد، لیلا کارشناس استاندارد

(فوق لیسانس مهندسی کامپیوتر، نرم‌افزار)

shaghool.ir

فهرست مندرجات

عنوان **صفحه**

shaghool.ir

پیش‌گفتار

استاندارد «خدمات مالی – افزاره‌های رمزنگاری امن (خرده‌فروشی) –قسمت ۲: بازبینه‌های انطباق امنیتی برای افزاره‌های استفاده‌شده در تراکنش‌های مالی» 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، در پانصد و نهمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۹۶/۰۳/۰۹ 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 13491-2:2017, Financial services — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions

shaghool.ir

مقدمه

این استاندارد یک قسمت از مجموعه استانداردهای ملی ایران شمارهٔ ۱۱۹۵۷ است.

این استاندارد مشخصه‌های منطقی و فیزیکی و همچنین مدیریت افزاره‌های رمزنگاری امن (SCDs)[1] را مشخص می‌کند. از این افزاره‌ها در محیط خدمات مالی خرده‌فروشی برای حفاظت از پیام‌ها، کلیدهای رمزنگاری[2] و دیگر اطلاعات حساس استفاده می‌شود.

امنیت خدمات مالی خرده‌فروشی به شدت به امنیت افزاره‌های رمزنگاری وابسته است.

الزامات امنیتی بر این اساس به وجود آمده‌اند که پوشه‌های رایانه‌ای می‌توانند دسترسی یابند و دستکاری شوند، در خطوط ارتباطی می‌تواند «شنود[3]» شود و داده‌های مجاز یا ورودی‌های واپایشی (کنترلی)[4] در افزاره سامانه می‌تواند با ورودی‌های غیرمجاز جایگزین شود. افزاره‌های رمزنگاری معین (برای مثال پودمان‌های (ماژول‌های)[5] امنیتی میزبان) در مراکز پردازش به نسبت بالای امنیتی هستند اما بخش عمده افزاره‌های رمزنگاری که در حال حاضر در خدمات مالی خرده‌فروشی به کار گرفته می‌شوند (برای مثال افزاره‌های ورود شماره شناسایی شخصی (PIN)[6] و غیره) در محیط‌های نا امن قرار دارند. بنابراین وقتی پین‌ها، کدهای اصالت‌سنجی پیام (MACs)[7] ، کلیدهای رمزنگاری و دیگر داده‌های حساس در این افزاره‌ها پردازش می‌شوند این مخاطره[8] وجود دارد که افزاره بتواند دستکاری شده یا داده‌ها در معرض خطر افشا یا تغییر قرار گیرد.

استفاده مناسب از افزاره‌های رمزنگاری که مشخصه‌های منطقی و فیزیکی مناسبی داشته باشند و با مدیریت درست آنها بتوان اطمینان حاصل کرد که مخاطره زیان مالی کاهش یافته است. برای اطمینان از مناسب بودن امنیت فیزیکی و منطقی SCDs نیاز است آنها را ارزشیابی کرد.

این استاندارد، بازبینه‌های انطباق امنیتی را برای ارزشیابی SCDs استفاده‌شده در سامانه‌های خدمات مالی مطابق با ISO 13491-1 ارائه می‌دهد. چارچوب‌های ارزشیابی دیگری نیز وجود دارند که ممکن است برای ارزشیابی‌های امنیتی رسمی مناسب باشند برای مثال ISO/IEC 15408-1، ISO/IEC 15408-3 و ISO/IEC 19790 که خارج از دامنه کاربرد این استاندارد است.

---

1 - Secure cryptographic devices
2 - Cryptographic
3- Tapped
4 - Control
5 - Modules
6 - Personal Identification Number
7 - Message authentication codes
8 - Risk

shaghool.ir

برای اطمینان از این که این افزاره‌ها قابلیت‌های عملیاتی مناسبی دارند و به اندازهٔ کافی از داده‌های موجود حفاظت می‌شود، مشخصه‌های افزاره مناسب لازم است. برای اطمینان از این که افزاره قانونی است و تغییر به شیوه‌ای غیرمجاز، برای مثال «اِشکال[1]»، در افزاره ایجاد نشده است و این که هیچ‌کدام از داده‌های حساسی (برای نمونه: کلیدهای رمزنگاری) که در افزاره هستند، افشا نشده اند یا تغییری در آنها راه نیافته است، به مدیریت مناسب افزاره نیاز است.

«امنیت مطلق» در عمل دست نایافتنی است. امنیت رمزنگاری به هر مرحله چرخه حیات SCD و همچنین به ترکیب مکمل رویه‌های مدیریت افزاره مناسب و مشخصه‌های رمزنگاری امن وابسته است. این رویه‌های مدیریتی اقدامات پیشگیرانه‌ای را به کار می‌گیرند تا از فرصت نفوذ به امنیت افزاره رمزنگاری بکاهند. هرگاه مشخصه‌های افزاره در پیشگیری یا تشخیص نقض امنیتی ناتوان شوند، می‌توان اقدامات یادشده را برای تشخیص هر چه ممکن‌ترِ هر گونه دسترسی غیرمجاز به داده های حساس یا محرمانه به کار برد.

1 - Bugging

shaghool.ir

خدمات مالی – افزاره‌های رمزنگاری امن (خرده‌فروشی) –قسمت ۲: بازبینه‌های انطباق امنیتی برای افزاره‌های استفاده‌شده در تراکنش‌های مالی

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین بازبینه‌هایی است برای ارزشیابی افزاره‌های رمزنگاری امن (SCDs) که در فرآیندهای رمزنگاری رایج در محیط خدمات مالی به کار می‌روند؛ آن گونه که در ISO 9564-1، ISO9564-2، ISO 16609، ISO 11568-1، ISO 11568-2 و ISO 11568-4 مشخص شده است. کارت‌های پرداخت مدار مجتمع (IC)[1] تا زمان صدور، مشمول الزامات مشخص‌شده در این استاندارد هستند و پس از آن، دیگر افزاره «شخصی» تلقی می‌شود و بیرون از دامنه کاربرد این استاندارد است.

این استاندارد، به مسائل برآمده از انکار خدمت[2] SCDs نمی‌پردازد.

در بازبینه‌های داده شده در پیوست‌های الف تا ح، اصطلاح «امکان‌پذیر نیست[3]» برای بیان این معنا به کار گرفته شده است که اگرچه حمله‌ای خاص از لحاظ فنی امکان‌پذیر است اما از لحاظ اقتصادی مقرون به صرفه نیست، زیرا هزینه انجام آن حمله بیش از هر گونه منفعتی است که از یک حمله موفق به دست می‌آید. افزون بر حمله‌هایی که تنها برای دستیابی به بُرد[4] اقتصادی انجام می‌شوند باید حمله‌های ویرانگری را که برای آسیب‌رسانی به «شهرت نیک» انجام می‌شوند، نیز در نظر داشت.

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:

---

1 - Integrated circuit
2 - Denial of service
3 - Not feasible
4 - Gain

shaghool.ir

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

2-2 ISO 11568-1, Banking — Key management (retail) — Part 1: Principles

2-3 ISO 11568-2, Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle

یادآوری- استاندارد ملی ایران شماره ۱۰۳۰۷-۲: سال ۱۳۸۷، بانکداری -مدیریت کلید (خرد) قسمت دوم-رمزهای متقارن - مدیریت کلید و چرخه حیات آنها با استفاده از استاندارد ISO 11568-2 : 2005 تدوین شده است.

2-4 ISO 11568-4, Banking — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle

2-5 ISO 13491-1, Financial services — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods

یادآوری- استاندارد ملی ایران شماره ۱۱۹۵۷-۱: سال ۱۳۸۷، بانکداری-دستگاه‌های رمز نگاری امن(خرد)قسمت ۱-مفاهیم، الزامات و روشهای ارزشیابی با استفاده از استاندارد ISO 13491-1 : 2007 تدوین شده است.

2-6 ISO 16609, Financial services — Requirements for message authentication using symmetric techniques

2-7 ISO/IEC 18031, Information technology — Security techniques — Random bit generation

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف استاندارد ISO 13491-1 و اصطلاحات و تعاریف زیر به کار می‌رود:

ISO و IEC پایگاه‌های دادهٔ اصطلاح شناختی‌ای برای استفاده در استانداردسازی در نشانی‌های زیر دارند:

- دانشنامه الکترونیکی IEC: در http://www.electropedia.org در دسترس است.

- بُن‌سازه مرورکننده برخط[1] ISO: در http://www.iso.org/obp در دسترس است.

۳-۱

ممیز

auditor

شخصی از طرف پشتیبان یا نهاد بازنگری ممیزی که مهارت‌های مناسبی برای وارسی[2]، ارزیابی[3]، بازنگری[4] و ارزشیابی[5] میزان انطباق یک ارزشیابی غیررسمی دارد.

1 - Online browsing platform
2 - Check
3 - Assess
4 - Review
5 - Evaluate

shaghool.ir

۲-۳

یکپارچگی داده

data integrity

ویژگی‌ای که نشان می‌دهد داده‌ها به شیوه‌ای غیرمجاز تغییر نکرده اند یا از بین نرفته اند.

۳-۳

واپایش دوگانه

dual control

فرآیند به‌کارگیری دو یا چند هستار (معمولا افراد) که در همکاری با یکدیگر برای حفاظت از کارکردها یا اطلاعات حساس کار می‌کنند؛ آنجا که هیچ هستار منفردی - به تنهایی - توان دسترسی یا استفاده از مواد را ندارد.

یادآوری ۱- کلید رمزنگاشتی نمونه ای از مواد مورد دسترسی یا استفاده است.

۴-۳

نمایندگی ارزشیابی

evaluation agency

سازمانی مورداعتماد هستارهای طراح، سازنده و پشتیبان[1] که (با استفاده از مهارت‌ها و ابزارهای تخصصی) مطابق ISO 13491 به ارزشیابی SCD می‌پردازد.

یادآوری ۱- ارزشیابی مطابق با ISO 13491-1 است.

۵-۳

یای انحصاری

exclusive or

پیمانه[2]-دوی جمع بیت به بیت بردارهای دوتایی با طول یکسان است.

1 - Sponsoring entities
2- Modulo

shaghool.ir

۶-۳

بازبینه انطباق امنیتی

security compliance checklist

فهرستی از ادعاهای ممیزی‌پذیر که بر اساس نوع افزاره سازماندهی شده باشد.

یادآوری ۱- بازبینه آن گونه که در این استاندارد مشخص شده است.

۷-۳

وضعیت حساس

sensitive state

شرایط افزاره که دسترسی به واسط[1] کاروَر[2] امن را فراهم می‌کند و تنها، زمانی که افزاره در واپایش دوگانه یا چندگانه قرار دارد، می‌توان وارد آن شد.

۴ استفاده از بازبینه‌های انطباق امنیتی

۱-۴ کلیات

این بازبینه‌ها باید برای ارزیابی قابل پذیرش بودن تجهیزات رمزنگاری که امنیت سامانه به آنها بستگی دارد، استفاده شود. بسته به روش ارزشیابی منتخب، مسئولیت پشتیبان، نهاد تصویب‌کننده یا نهاد اعتباردهی است که برخی یا تمام بازبینه‌ها را بپذیرد تا:

الف- نمایندگی‌های ارزشیابی را برای استفاده تأمین‌کنندگان یا مشارکت‌کنندگان در سامانه تأیید کند؛ و

ب- نهاد بازنگری ممیزی را برای بازنگری بازبینه‌های ممیزی تکمیل‌شده ایجاد کند.

پیوست‌های الف تا ح بازبینه‌هایی را ارائه می‌دهند که کمینه ارزشیابی را برای ارزیابی قابل‌پذیرش بودن تجهیزات رمزنگاری تعریف می‌کنند که باید به کار گرفته شود. آزمون‌های بیشتر ممکن است برای نمایش [وضعیت] «در لحظه» [تجهیزات] - در زمان ارزشیابی - آزمون‌های بیشتری انجام داد.

این ارزشیابی ممکن است آن گونه که در ISO 13491-1 مشخص شده است، «غیررسمی»، «نیمه‌رسمی»[3] یا «نیمه‌رسمی روشن»[4] باشد. اگر ارزشیابی «رسمی» انتخاب شود، آنگاه نباید بازبینه‌ها را آنچنان که در اینجا

1- Interface
2 - Operator
3 - Semi-formal
4 - Strict semi-formal

shaghool.ir

ارائه شده‌اند، به کار گرفت، بلکه باید درگاهی باشند برای کمک به آماده‌سازی «ادعاهای رسمی» که در چنین ارزشیابی لازم هستند.

یادآوری- از آنجا که این ادعاهای رسمی، از آنجا که به طور ذاتی معیارهای دیگری را دربردارند، از دامنه کاربرد این استاندارد بیرون هستند.

افزاره‌های رمزنگاری هم از طریق مشخصه‌های ذاتی خود و هم مشخصه‌های محیطی که در آن هستند – امنیت را به دست می‌آورند. هنگام تکمیل این بازبینه‌های ممیزی باید محیطی را که این افزاره در آن قرار دارد نیز مدنظر قرار داد، برای مثال افزاره‌ای که قرار است در محل‌های عمومی استفاده شود، ممکن است نسبت به افزاره‌ای که در یک محیط واپایش‌شده کار می‌کند، امنیت ذاتی بیشتری نیاز داشته باشد. برای آنکه نمایندگی‌های ارزشیابی‌کننده، از بررسی محیط خاصی که قرار است افزاره ارزشیابی شونده در آن قرار گیرد، بی‌نیاز شوند؛ در پیوست ح این استاندارد دسته‌بندی پیشنهادی برای این محیط‌ها ارائه می‌شود. بنابراین، می‌توان از نمایندگی‌های ارزشیابی‌کننده خواست که افزاره مفروض را برای کار در محیطی خاص ارزشیابی کنند. چنین افزاره‌ای را تنها هنگامی می‌توان در تسهیلات موجود به کار گرفت که خود آن تسهیلات از پیش ارزشیابی شده باشند تا از فراهم آمدن محیطی مطمئن اطمینان حاصل شود. . با این حال، بازبینه‌های ممیزی را می‌توان در محیطی به غیر از محیط‌های معرفی‌شده - در دسته‌بندی‌های محیطی پیشنهاد شده در پیوست ح - نیز به کار گرفت.

چهار روش ارزشیابی که در ISO 13491-1 تعیین شده‌اند، در بندهای ۴-۲، ۴-۳، ۴-۴ و ۴-۵ توضیح داده می‌شود.

۴-۲ ارزشیابی غیررسمی

ممیز مستقل باید - به عنوان قسمتی از یک ارزشیابی غیررسمی - بازبینه(های) مناسبی را برای افزاره در حال ارزشیابی تکمیل کند.

۴-۳ ارزشیابی نیمه‌رسمی

در روش نیمه‌رسمی، پشتیبان که ممکن است سازنده باشد، باید افزاره را در اختیار یک نمایندگی ارزشیابی‌کننده بگذارد تا مطابق بازبینه(های) مناسب آزمایش شود.

۴-۴ ارزشیابی نیمه‌رسمی روشن

در روش نیمه‌رسمی روشن، پشتیبان که ممکن است سازنده باشد باید افزاره را در اختیار یک نمایندگی ارزشیابی‌کننده قرار دهد تا مطابق بازبینه(های) مناسبی که از سوی نهاد تصویب‌کننده معین شده، آزمایش شود.

shaghool.ir

۵-۴ ارزشیابی رسمی[1]

در روش رسمی، سازنده یا پشتیبان باید افزاره را در اختیار یک نمایندگی ارزشیابی مجاز بگذارد تا مطابق ادعاهای رسمی که بازبینه(های) مناسبی در آنها به عنوان ورودی به کار رفته است، آزمایش شود.

1 - Formal evaluation

shaghool.ir

پیوست الف

(الزامی)

مشخصه‌های مشترک فیزیکی، منطقی و مدیریتی افزاره برای تمام افزاره‌های رمزنگاری امن

الف-۱- کلیات

این پیوست برای استفاده در تمام ارزشیابی‌ها بوده و باید پیش از به کارگیری هرگونه «بازبینه(های) انطباق امنیتی» مختصّ افزاره تکمیل شود.

لازم است بیانیه‌های زیر در این بازبینه انطباق امنیتی توسط ممیز به عنوان «درست (T)»، «نادرست (F)» یا «کاربرد ندارد (N/A)[1]» مشخص شود. علامت «نادرست» لزوماً نشان‌دهنده عمل غیر قابل قبول نیست بلکه باید به صورت مکتوب توضیح داده شود. بیانیه‌هایی که به صورت «کاربرد ندارد» نشان داده می‌شوند نیز باید به صورت مکتوب توضیح داده شوند.

الف-۲- مشخصه‌های افزاره

الف-۲-۱- مشخصه‌های امنیت فیزیکی

الف-۲-۱-۱-کلیات

تمام افزاره‌ها باید معیارهای مندرج در الف-۲-۱-۲ را برای مشخصه‌های امنیت عمومی و معیارهای مندرج در الف-۲-۱-۵ برای مشخصه‌های پاسخگو بودن به دستکاری[2] و مندرج در الف-۲-۱-۳ برای مشخصه‌های آشکارکنندهٔ دستکاری[3] را برآورده کنند. علاوه بر این، افزاره‌های دیگر باید معیارهای مندرج در الف-۲-۱-۴ را برای مشخصه‌های مقاوم بودن در برابر دستکاری[4] برآورده کند.

الف-۲-۱-۲- مشخصه‌های امنیتی عمومی

نمایندگی ارزشیابی‌کننده، میزان آسیب‌پذیری افزاره موردنظر را در برابر فنون حمله فیزیکی و منطقی که در زمان ارزشیابی شناخته شده‌اند، ارزشیابی می‌کند. برخی از آنها در اینجا آورده شده است (اما محدود به این موارد نمی‌شود):

- حمله‌های شیمیایی (حلّال‌ها)؛

1 - Not Applicable
2 - Tamper responsive characteristics
3 - Tamper-evident characteristics
4 - Tamper-resistant characteristics

shaghool.ir

- حمله‌های پویشی[1] (پویش میکروسکوپ الکترونی)؛
- حمله‌های مکانیکی (سوراخ‌کردن، بریدن، کاوش کردن و غیره)؛
- حمله‌های حرارتی (حد بالا یا حد پایین دما؛
- حمله‌های پرتوای (پرتو ایکس)؛
- نشت اطلاعات از طریق کانال‌های (جانبی) پنهان (منبع تغذیه، زمان‌سنج و غیره)؛
- حمله‌های شکست؛

و نتیجه آن در جدول الف-۱ درج شده‌اند:

جدول الف-۱- مشخصه‌های امنیتی عمومی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
الف-۱	تعیین PIN، کلید یا دیگر اطلاعات محرمانه توسط پویش امکان‌پذیر نیست (برای مثال با تشعشعات الکترومغناطیسی از افزاره با یا بدون همکاری کاروَر افزاره).			
الف-۲	هر نوع تهویه و شکاف دیگر در پودمان چنان قرار می‌گیرد و محافظت می‌شود که استفاده از شکاف برای کاوش مولفه پودمان برای افشای پین‌های رمزگذاری نشده، کدهای دسترسی یا کلیدهای رمزنگاری یا به قصد غیرفعال کردن سازوکارهای حفاظتی افزاره امکان‌پذیر نیست.			
الف-۳	تمام داده‌های حساس و کلیدهای رمزنگاری، از جمله پس‌ماندها[2]، در پودمان امنیتی ذخیره شده‌اند.			
الف-۴	تمام سازوکارهای انتقال درون افزاره به گونه‌ای پیاده‌سازی می‌شوند که پایش افزاره برای افشای غیرمجاز هرگونه اطلاعاتی از این دست امکان‌پذیر نیست.			
الف-۵	هنگامی که افزاره در حال کار است، همهٔ درگاه های دسترسی به شبکهٔ مدار درونی افزاره با یک یا چند قفل ضد سرقت[3] یا سازوکارهای امنیتی مشابه و در «موقعیت بسته» قفل شده‌اند.			
الف-۶	طراحی افزاره به گونه‌ای است که با مولفه‌های موجود در بازار و خرده‌فروشی‌ها نمی‌توان افزاره مشابه آن را ساخت.			
الف-۷	اگر افزاره اعداد تصادفی یا شبه‌تصادفی تولید می‌کند، تولید این اعداد			

1- Scanning
2 - Residues
3 -Pick resistant locks

shaghool.ir

	مطابق با ISO 18031 است.			
الف-۸	اگر افزاره اعداد تصادفی یا شبه‌تصادفی تولید می‌کند تأثیر بر خروجی این اعداد امکان‌پذیر نیست برای مثال با تغییر شرایط محیطی افزاره، مانند: بازنشانی[1] یا راه‌اندازی دوباره افزاره یا دستکاری منبع انرژی/تزریق الکترومغناطیسی.			

الف-۲-۱-۳- مشخصه‌های آشکارکنندهٔ دستکاری

نمایندگی ارزشیابی‌کننده موارد درج شده در جدول الف-۲ را نتیجه‌گیری کرده است:

جدول الف-۲- مشخصه‌های آشکارکنندهٔ دستکاری

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
الف-۹	افزاره به گونه‌ای طراحی و ساخته شده است که دست بردن در آن با هدف: - انجام هر گونه افزودن، جایگزینی یا تغییر (برای مثال: نصب اِشکال) در سخت‌افزار یا نرم‌افزار افزاره یا - تعیین یا تغییر هرگونه اطلاعات حساس (برای مثال پین‌ها، کدهای دسترسی و کلیدهای رمز) و در پی آن بازگرداندن دوباره آن، بی آن که نیاز به مهارت‌های تخصصی و تجهیزاتی که از دسترس همگانی دور هستند، امکان‌پذیر نیست بی آن که: الف- آسیب بزرگی به آن وارد شود؛ آن هم آسیبی که به احتمال زیاد تشخیص داده می¬شود، یا ب- نبود طولانی مدت افزاره در محلی که برایش در نظر گرفته شده است و ناپدید شدن و برگشتن دوباره آن تشخیص داده نشود {از چشم‌ها پنهان مانده باشد}			

الف-۲-۱-۴- مشخصه‌های آشکارکنندهٔ دستکاری

نمایندگی ارزشیابی‌کننده موارد درج شده در جدول الف-۳ را نتیجه‌گیری کرده است:

1- Resetting

shaghool.ir

جدول الف-۳- مشخصه‌های مقاوم بودن در برابر دستکاری

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
الف-۱۰	افزاره با بکارگیری محافظ فیزیکی در برابر نفوذ محافظت شده است، چنان که نفوذ امکان‌پذیر نیست.			
الف-۱۱	حتی پس از دسترسی نامحدود و بدون مزاحمت به افزاره، کشف اطلاعات محرمانه در افزاره هدف امکان‌پذیر نیست.			

الف-۲-۱-۵- مشخصه‌های پاسخگو بودن به دستکاری

نمایندگی ارزشیابی‌کننده موارد درج شده در الف-۴ را نتیجه‌گیری کرده است:

جدول الف-۴- مشخصه‌های پاسخگو بودن به دستکاری

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
الف-۱۲	افزاره با ویژگی‌هایی که هرگونه تلاش ممکن را برای دستکاری افزاره تشخیص می‌دهد در برابر نفوذ محافظت می‌شود و به سرعت تمام کلیدهای رمزنگاری و داده‌های حساس را پس از تشخیص چنین تلاشی پاک می‌کند.			
الف-۱۳	برداشتن مجاز یا غیرمجاز محفظه یا دریچه[1] برای درگاه دسترسی به مولفه‌های داخلی افزاره، به صورت سبب پاک شدن خودکار و بی‌درنگ کلیدهای رمزنگاری ذخیره شده در افزاره می‌شود.			
الف-۱۴	روشی تعریف‌شده وجود دارد که اطمینان حاصل می‌کند داده‌های محرمانه یا هرگونه کلید رمزنگاری که برای رمزگذاری داده‌های محرمانه به کار رفته است - هنگامی که واحد به طور دائمی از خدمت جدا می‌شود (از دور خارج می‌شود) - از روی آن پاک می‌شود. همچنین روشی تعریف‌شده وجود دارد که اطمینان حاصل می‌کند - هنگام از دور خارج شدن دائمی واحد-، هرگونه کلید رمزنگاری نگهداری‌شده در واحد که ممکن است در آینده قابل استفاده باشد از «واحد» پاک شده است یا در تمام تسهیلاتی که آن واحد قادر به ایجاد ارتباطات رمزنگاری محافظت شده با آن باشد نامعتبر است.			
الف-۱۵	سازوکارهای تشخیص دستکاری/ پاک کردن کلید حتی با قطع برق کار			

1 - Opening

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	می‌کنند.			
الف-۱۶	اگر افزاره مجهز به سازوکاری برای تشخیص جدا شدن از محیط عملیاتی خود نیست، غلبه بر سازوکارهای تشخیص دستکاری یا کشف اطلاعات محرمانه در افزاره هدف، - حتی در صورت جدا شدن از محیط عملیاتی- ، امکان‌پذیر نیست. به خطر افتادن افزاره نیازمند مجموعه تجهیزات و مهارت‌هایی است که در حال حاضر موجود نیست. به عنوان مثالی ممکن، کشف چنین اطلاعاتی نیازمند زمان کافی برای مثال یک ماه آمادگی، شامل تحلیل افزاره‌های دیگر و دست کم یک هفته تلاش برای به خطر افتادن افزاره، پس از دسترسی نامحدود و بدون مزاحمت به افزاره هدف است.			
الف-۱۷	اگر افزاره دارای سازوکاری برای تشخیص جدا شدن از محیط عملیاتی خود است، غلبه بر سازوکارهای تشخیص نفوذ یا کشف اطلاعات محرمانه در افزاره هدف امکان‌پذیر نیست. به خطر افتادن این افزاره نیازمند مجموعه مهارت‌هایی است که در حال حاضر وجود نداشته و به تجهیزاتی نیاز دارد که نه در محل افزاره موجود است و نه امکان انتقال آن به محل افزاره وجود دارد. به عنوان مثالی ممکن، کشف چنین اطلاعاتی نیازمند زمان کافی - برای مثال یک ماه آمادگی -، شامل تحلیل افزاره‌های دیگر و کمینه ۱۲ ساعت دسترسی نامحدود و بدون مزاحمت به افزاره هدف است.			

الف-۲-۲- مشخصه‌های منطقی امنیتی

نمایندگی ارزشیابی‌کننده موارد درج شده در جدول الف-۵ را نتیجه‌گیری کرده است:

جدول الف-۵- مشخصه‌های امنیتی منطقی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
الف-۱۸	افزاره دارای قابلیت‌های خودآزمایی است که می‌تواند به صورت دستی یا خودکار آغاز شود و به وسیله آن می‌توان مطمئن شد که کارکردهای اصلی آن به‌درستی کار می‌کند.			
الف-۱۹	افزاره فقط کارکردهایی را که برای آن طراحی شده است، انجام می‌دهد.			
الف-۲۰	تشخیص کلید یا دیگر اطلاعات محرمانه با استفاده از حالت‌های			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	آزمایش مخصوص یا تشخیصی امکان‌پذیر نیست.			
الف-۲۱	الگوریتم‌های رمزنگاری، حالت‌های عملیاتی و طول کلیدهای رمزنگاری که توسط افزاره استفاده می‌شود مطابق با ISO 11568-1، ISO 11568-2 و ISO 11568-4 است.			
الف-۲۲	مدیریت کلید افزاره مطابق با ISO 11568-1، ISO 11568-2 و ISO 11568-4 بوده و از هر کلید تنها برای یک مقصود رمزنگاری استفاده می‌شود (هر چند انواع مختلفی از یک کلید می‌توانند برای مقاصد مختلف استفاده شوند).			
الف-۲۳	قابلیت کارکردی پیاده‌سازی‌شده برای افزاره به گونه‌ای است که با هیچ روشی نمی‌توان اطلاعات محرمانه با متن رمزگذاری‌نشده (برای مثال پین‌ها یا کلیدهای رمزنگاری) یا اطلاعات محرمانه که با کلیدهای قانونی رمزگذاری نشده است را از آنها بدست آورد مگر با شیوه‌های مجاز (برای مثال با نامه‌رسان‌های PIN[1]).			
الف-۲۴	اگر افزاره از چندین مولفه تشکیل شده باشد، انتقال کلیدهای رمزنگاری محرمانه درون افزاره از مولفه با امنیت بیشتر به مولفه‌ای با امنیت کمتر، امکان‌پذیر نیست.			
الف-۲۵	بارگذاری کلیدها زمانی انجام می‌شود که: - افزاره در حالت حساس باشد؛ یا - عمل بارگذاری کلیدها، افزاره را در حالتی قرار دهد که تمام سازوکارهای حفاظت در برابر دستکاری در افزاره فعال شود.			
الف-۲۶	کارکردهای کاروَر زیر که ممکن است بر امنیت افزاره‌ها تأثیر بگذارند، تنها زمانی مجاز هستند که افزاره در وضعیت حساس باشد، یعنی تحت واپایش دوگانه یا چندگانه باشد: - فعال یا غیرفعال‌کردن کارکردهای افزاره؛ یا - تغییر گذرواژه‌ها یا داده‌هایی که افزاره را در وضعیت حساس قرار می‌دهند.			
الف-۲۷	واسط امن کاروَر با افزاره چنان طراحی شده که برای ورود به این حالت حساس لازم است بیش از یک گذرواژه (یا برخی سازوکارهای معادل			

1 -PIN Mailers

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	برای واپایش دوگانه یا چندگانه) وارد شود.			
الف-۲۸	واسط کاروَر امن با افزاره چنان طراحی شده است که بعید است افزاره ندانسته در وضعیت حساس رها شود.			
الف-۲۹	اگر وضعیت حساس با چند محدودیت ایجاد شده باشد (برای مثال محدودیت در تعداد فراخوانی‌های کارکرد و محدودیت زمان)، وقتی اولین محدودیت به سر برسد، افزاره به حالت طبیعی برمی‌گردد.			
الف-۳۰	در صورتی که از گذرواژه‌ها یا داده‌های رمزگذاری‌نشده برای واپایش گذار به وضعیت حساس استفاده شود، از این داده‌ها به شیوه‌ای همانند دیگر اطلاعات محرمانه یا حساس محافظت می‌شود.			
الف-۳۱	اگر به هر دلیلی کلیدهای رمزنگاری از دست بروند، برای مثال با قطع طولانی‌مدت برق، افزاره وارد حالت غیرعملیاتی خواهد شد.			
الف-۳۲	تنها فراخوانی‌های کارکرد و کارکردهای کاروَر حساس که در افزاره وجود دارد، کارکردهایی هستند که توسط پشتیبان یا سامانه‌ای که افزاره در آن کار می‌کند، تأیید شده‌اند.			
الف-۳۳	کلیدها هرگز از رمزگذاری با یک نوع کلید به رمزگذاری با نوع دیگری از همان کلید منتقل نمی‌شود.			

الف-۳- مدیریت افزاره

الف-۳-۱- ملاحظات عمومی

نهاد مسئول تکمیل بازبینه ممیزی - در هر مرحله‌ای از چرخهٔ عمر - اطمینان مرتبط با همان مرحله را برای موارد زیر – جدول الف-۶ ایجاد می‌کند:

جدول الف-۶ - ملاحظات عمومی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
الف-۳۴	برای ممیزی و واپایش، هویت افزاره (برای مثال شماره ردیف آن) با نشانه‌گذاری یا برچسب‌گذاری بیرونی آشکارکنندهٔ دستکاری مشخص می‌شود یا با یک دستور از طریق واسط یا صفحه نمایش که هویت خود را نشان می‌دهد.			
الف-۳۵	زمانی که افزاره در مرحله‌ای از چرخه عمر است که کلیدهای رمزنگاری را شامل می‌شود، هویت این کلیدها می‌تواند به آسانی از روی هویت			

shaghool.ir

	افزاره قابل تشخیص باشد (به این ترتیب اگر گزارش شود که افزاره از دست رفته یا دزدیده شده است، می‌توان این کلیدها را نامعتبر کرد).			
الف-۳۶	تمام کلیدهای فیزیکی که برای بازکردن قفل یا راه‌اندازی افزاره استفاده می‌شود به دقت واپایش شده و تنها در اختیار افراد مجاز هستند.			
الف-۳۷	اگر افزاره شامل کلیدهای رمزنگاری محرمانه باشد و حمله‌ای به افزاره صورت گیرد یا افزاره دزدیده شود، رویه‌هایی وجود دارد تا بی‌درنگ پس از ردیابی حمله یا ربوده شدن افزاره، طرف مسئول امنیت را آگاه کنند.			
الف-۳۸	اگر افزاره هنوز کلید رمزنگاری محرمانه نداشته باشد و حمله‌ای به آن صورت گیرد یا افزاره دزدیده شود، رویه‌هایی وجود دارد که از جایگزینی افزاره‌ای که به آن حمله شده است یا آن را دزدیده‌اند با افزاره‌ای که قانونی است اما هنوز کلید رمزنگاری محرمانه ندارد، جلوگیری شود.			
الف-۳۹	در صورتی که هیچ گونه وضعیت حساسی در افزاره نباشد، - بارگذاری کلیدهای رمزگذاری‌نشده - تحت واپایش دوگانه انجام می‌شود..			

الف-۳-۲- محافظت از افزاره توسط سازنده

سازنده افزاره یا ممیز مستقل به نهاد بازنگری ممیزی – دربارهٔ موارد درج شده در جدول الف-۷ – اطمینان قابل قبولی داده‌اند:

جدول الف-۷- محافظت از افزاره توسط سازنده

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد
الف-۴۰	طراحی سخت‌افزاری و نرم‌افزاری افزاره به گونه‌ای است که تمام قابلیت‌های کارکردی افزاره، کارکردهای قانونی و مستند بوده و هیچ کارکرد غیرمجازی (برای مثال «اسب تراوا»[1]) در افزاره وجود ندارد.			
الف-۴۱	افزاره، - از جمله نرم‌افزار آن -، در محیطی واپایش شده تحت نظر کارکنان شایسته تولید و انبار شده است تا از هرگونه تغییرات غیرمجاز در مشخصه‌های فیزیکی یا کارکردی افزاره جلوگیری شود.			

1- Trojan Horse

shaghool.ir

الف-۳-۳- محافظت از افزاره در فاصلهٔ مراحل ساخت و پس از ساخت

سازنده افزاره و کسانی که مسئول انتقال و انبارکردن افزاره - پیش از بارگذاری کلید مالی اولیه - هستند یا ممیز مستقل، موارد درج شده در جدول الف-۸ را تضمین می‌کند:

جدول الف-۸- محافظت از افزاره در فاصلهٔ مراحل ساخت و پس از ساخت

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
الف-۴۲	افزاره - در پی ساخت و پیش از بارگیری -، در نواحی محافظت شده یا مهر و موم شده و درون بسته‌بندی با مشخصه آشکارکنندهٔ دستکاری نگهداری شده چنان که دسترسی غیرمجاز به آن قابل تشخیص باشد.			
الف-۴۳	افزاره در بسته‌بندی با مشخصه آشکارکنندهٔ دستکاری جابجا می‌شود و برای تشخیص دسترسی غیرمجاز به آن بازرسی می‌شود یا: - پیش از آن که کلیدهای رمزنگاری در آن بارگذاری شود توسط کارکنان شایسته بازرسی می‌شود تا اطمینان حاصل شود که هیچ گونه تغییر فیزیکی یا کارکردی در آن اعمال نشده است، یا - افزاره با اطلاعات محرمانه تحویل داده شده است تا در صورت تشخیص دستکاری، این اطلاعات پاک شود. به این ترتیب کاربر از اصالت و به خطر نیافتادن افزاره اطمینان حاصل می‌کند. **یادآوری**- مثالی از این نوع اطلاعات کلید خصوصی، جفت کلید نامتقارن با کلید عمومی افزاره است که با یک کلید خصوصی که تنها سازنده از آن آگاه است امضا شده است.			

الف-۳-۴- محافظت از افزاره هنگام بارگذاری کلید مالی اولیه و پیش از مرحله پیش از استفاده

مسئولان انبارکردن و انتقال افزاره - هنگام بارگذاری کلید مالی اولیه - یا ممیز مستقل، به نهاد بازنگری ممیزی – دربارهٔ موارد درج شده در جدول الف-۹ – اطمینان قابل قبولی داده‌اند:

جدول الف-۹- محافظت از افزاره هنگام بارگذاری کلید مالی اولیه و پیش از مرحله پیش از استفاده

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
الف-۴۴	سازوکارهای انتقال که به وسیله آنها کلیدهای رمزگذاری‌نشده، مولفه‌های کلید یا گذرواژه‌ها به افزاره وارد شده‌اند چنان محافظت و /یا بازرسی می‌شوند تا مانع انجام هرگونه پایشی شوند که ممکن است به			

shaghool.ir

	افشای غیرمجاز هرگونه کلید، مولفه یا گذرواژه بیانجامد.			
الف-۴۵	تنها زمانی تضمین منطقی حاصل شود که تغییر فیزیکی یا کارکردی غیرمجازی در افزاره ایجاد نشده است، کلیدهای اولیه به شیوه‌ای واپایش‌شده در افزاره بارگذاری می‌شوند.			

الف-۳-۵- محافظت از افزاره هنگام مرحله پیش از استفاده و پیش از نصب

مسئولان انبارکردن و انتقال افزاره در پی بارگذاری کلید اولیه یا ممیز مستقل، موارد درج شده در جدول الف-۱۰ تضمین کرده اند که برای نهاد بازنگری ممیزی قابل‌پذیرش است:

جدول الف-۱۰- محافظت از افزاره هنگام مرحله پیش از استفاده و پیش از نصب

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
الف-۴۶	هر افزاره نصب نشده‌ای چنان واپایش می‌شود که از دسترسی غیرمجاز به آنها جلوگیری شود یا دسترسی غیرمجاز به آن‌ها تشخیص داده شود و سوابق آنها چنان نگهداری و ممیزی می‌شود که دزدیده‌شدن یا گم‌شدن آنها تشخیص داده شود و گزارش شود.			

الف-۳-۶- محافظت از افزاره در پی نصب

پذیرنده یا ممیز مستقل که برای نهاد بازنگری ممیزی تضمین داده‌اند که واپایش‌ها و رویه‌های موجود لحاظ شده‌اند تا از موارد درج شده در جدول الف-۱۱ اطمینان حاصل کنند.

جدول الف-۱۱- محافظت از افزاره در پی نصب

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
الف-۴۷	اگر - به هر دلیلی – افزاره، به نگهداری کردن از کلیدهای معتبر پایان دهد: - باید هر چه زودتر افزاره را از خدمت کنار گذاشت. - باید امکان انجام تراکنش‌ها را از افزاره گرفت. تا زمانی که دست کم دو تَن کارشناس کارآزموده و شایسته افزاره را بازرسی نکرده باشند و نیآزموده باشند و مشخص نکرده باشند که هیچگونه تغییر فیزیکی یا کارکردی در افزاره رخ نداده است، نباید کلیدهای تازه را در افزاره بارگذاری کرد.			
الف-۴۸	گر افزاره گم شده باشد یا آن را دزدیده باشند و دوباره آن را به جای خود باز گردانده باشند یا اگر نسبت به وقوع دستکاری غیرمجاز در			

shaghool.ir

	افزاره – به هر دلیلی – شک وجود داشته باشد، باید همهٔ کلیدهای رمزنگاشتی افزاره را پاک کرد و تا زمانی که «واحد» - برابر آنچه در بند الف-۳-۳ آمده است – بازرسی و آزمایش نشده باشد، نباید کلیدهای تازه را در آن بارگذاری کرد.			
الف-۴۹	رویه‌های واپایش و ممیزی خودکار و/ یا دستی پیاده‌سازی شده است تا نصب دوباره و غیرمجاز افزاره‌ای که پیش از این استفاده‌شده یا افزاره‌ای که شامل کلید(های) افزاره است که پیش از این استفاده‌شده، تشخیص داده شود. این نمونه‌ها بررسی می‌شوند و در صورت رویارویی با فعالیتی مشکوک، افزاره در زودترین زمان ممکن از خدمت خارج می‌شود. هنگامی که هر تراکنش کلید(های) استفاده‌شده در تراکنش را تشخیص دهد، می‌توان از نرم‌افزار میزبان برای تشخیص خودکار موارد زیر استفاده کرد: الف- خارج شدن افزاره از خدمت، و ب- نصب متعاقب یک افزاره که شامل کلید(های) افزاره است که پیش از این از خدمت خارج شده است.			
الف-۵۰	وقتی افزاره در حال تعمیر یا نصب است، رویه‌های به کار گرفته شده تا اطمینان حاصل شود افزاره توسط افرادی که این کارکردها را انجام می‌دهند در معرض خطر قرار نگرفته است.			
الف-۵۱	وقتی از واسط امن کاروَر با افزاره استفاده می‌شود، افزاره ورود داده و کابل‌های متصل به افزاره به دقت بازرسی شده تا اطمینان حاصل شود هیچ سخت‌افزاری به صورت غیرمجاز در آنها وارد نشده است.			
الف-۵۲	اگر افزاره در برابر دستکاری مشهود باشد، رویه‌های وجود دارد تا از بازرسی منظم این شواهد اطمینان حاصل کند.			

الف-۳-۷- محافظت از افزاره پس از خارج شدن از خدمت

افراد مسئول خروج افزاره از خدمت یا ممیز مستقل، موارد درج شده در جدول الف-۱۲ تضمین کرده اند که برای نهاد بازنگری ممیزی قابل پذیرش است:

جدول الف-۱۲- محافظت از افزاره پس از خارج شدن از خدمت

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
الف-۵۳	افزاره به گونه‌ای واپایش شده است که در صورت نصب دوباره آن از دسترسی غیرمجاز به آن جلوگیری شود و چنان ممیزی شده است که گم‌شدن یا دزدیده‌شدن آن تشخیص داده شده و گزارش می‌شود.			

shaghool.ir

الف-۵۴	اگر افزاره به طور دائمی از خدمت خارج شده باشد، هرگونه کلید موجود در افزاره که برای هر مقصود رمزنگاری استفاده‌شده، از روی افزاره پاک می‌شود.			
الف-۵۵	اگر بدنه افزاره به گونه‌ای باشد که مشخصه‌های آشکارکنندهٔ دستکاری را ارائه کند و افزاره به طور دائمی از خدمت خارج شود، بدنه افزاره تخریب می‌شود. محل انبار بدنه تا زمان تخریب آن واپایش و ممیزی می‌شود.			

shaghool.ir

پیوست ب

(الزامی)

افزاره‌های با قابلیت کارکردی ورود PIN

ب-۱- کلیات

رویه ارزشیابی افزاره‌های ورود PIN به شرح زیر است:

- بازبینه‌های پیوست الف تکمیل شود؛ و
- بازبینه‌های این پیوست تکمیل شود.

بیانیه‌هایی که ذیل این بازبینه انطباق امنیتی می‌آیند لازم است توسط ممیز به عنوان «درست (T)»، «نادرست (F)» یا «کاربرد ندارد (N/A)» مشخص شود. علامت «نادرست» لزوماً نشان‌دهنده عمل غیر قابل قبول نیست بلکه باید به صورت مکتوب توضیح داده شود. بیانیه‌هایی که به صورت «کاربرد ندارد» علامت‌گذاری شده نیز باید به صورت مکتوب توضیح داده شوند.

ب-۲- مشخصه‌های افزاره

ب-۲-۱- مشخصه‌های امنیت فیزیکی

ب-۲-۱-۱- مشخصه‌های امنیت فیزیکی عمومی

نمایندگی ارزشیابی‌کننده موارد درج شده در جدول ب-۱ نتیجه گرفته است:

جدول ب-۱- مشخصه‌های امنیت فیزیکی عمومی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ب-۱	مسیر صفحه‌کلید تا واحد پردازنده رمزنگاری به صورت فیزیکی محافظت شده تا هیچ روش امکان‌پذیری برای تشخیص داده‌های عبوری بین آنها وجود نداشته باشد بدون این که: - سبب پاک‌شدن کلیدهای رمزنگاری افزاره شود (به الف-۲-۱-۵ مراجعه شود)؛ یا - سبب آسیب جدی به آن شود چنان که مانع از ادامه استفاده از آن شود (به الف-۲-۱-۳ مراجعه شود)؛ یا الزامات بند ب-۲۷ برآورده شود.			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ب-۲	اگر بتوان از افزاره ورود PIN برای ورود داده‌هایی که رمزگذاری نخواهند شد استفاده کرد، مسیر نمایش به صورت فیزیکی محافظت می‌شود یا الزامات بند ب-۲۲ برآورده می‌شود.			
ب-۳	مسیر خوانشگر کارت نوار مغناطیسی تا واحد پردازنده رمزنگاری به صورت فیزیکی محافظت شده است چنان که دسترسی و/ یا جایگزین کردن داده‌های عبوری بدون این که سبب پاک شدن کلیدهای رمزنگاری خصوصی شود به هیچ روش امکان‌پذیر نیست یا الزامات ب-۲۸ برآورده می‌شود.			
ب-۴	اگر ورود PIN با صدایی قابل شنیدن همراه باشد، صدای هر رقم PIN واردشده متمایز از صدای رقم‌های واردشده دیگر است.			
ب-۵	اگر افزاره ورود PIN دارای صفحه نمایش است، این صفحه نمایش هیچ‌کدام از ارقام PIN را افشا نمی‌کند بلکه نواری از نمادهایی نامشخص مانند ستاره را به جای ارقام PIN واردشده نشان می‌دهد.			
ب-۶	افزاره ورود PIN به یک حفاظ حریم خصوصی مجهز است یا چنان طراحی شده که دارنده کارت می‌تواند هنگام ورود PIN با بدن خود جلوی مشاهده PIN را بگیرد.			
ب-۷	هر اثر باقی‌مانده از پین‌ها یا کلیدهای رمزنگاری استفاده‌شده هنگام تراکنش در پودمان مقاوم بودن در برابر دستکاری یا پاسخگو به دستکاری نیز ذخیره می‌شود یا پس از تکمیل تراکنش به سرعت بازنویسی می‌شوند. **یادآوری**- پین‌های رمزگذاری‌نشده همواره پس از رمزگذاری به سرعت بازنویسی می‌شوند.			
ب-۸	شکاف خوانشگر IC که کارت IC درون آن وارد می‌شود فضای کافی برای قرار گرفتن « اِشکال» افشای PIN را ندارد و بزرگ کردن آن برای جاشدن «اِشکال» افشای PIN امکان‌پذیر نیست. امکان ندارد که کارت IC و هر نوع شی خارجی دیگر با هم درون شکاف ورود کارت جا شوند. دریچه ورودی کارت IC به صورت تمام رخ در دید دارنده کارت قرار دارد چنان‌که هر نوع انسداد یا اشیا مشکوک در دریچه قابل‌تشخیص است. **یادآوری**- اگر پین‌ها تنها با محافظت منطقی (رمزنگاری) به کارت IC منتقل می‌شوند، مطابقت با این الزام برای افزاره ورود PIN نیاز نیست.			
ب-۹	خوانشگر IC چنان ساخته شده است که دارنده کارت می‌تواند سیم‌های			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	خارج شده از شکاف خوانشگر IC را که به یک ضبط کننده یا فرستنده (اِشکال بیرونی) وصل است، مشاهده کند. **یادآوری**- اگر پین‌ها با محافظت منطقی (رمزگذاری‌شده) تنها به کارت IC منتقل می‌شوند، مطابقت با این الزام برای افزاره ورود PIN نیاز نیست.			
ب-۱۰	صفحه کلید PIN و خوانشگر IC با هم در یک افزاره آشکارکنندهٔ دستکاری (مطابق ISO 13491-1) یکپارچه شده‌اند یا در دو افزاره مجزا هستند که هر کدام در یک افزاره آشکارکنندهٔ دستکاری قرار دارد. **یادآوری**- در صورتی که پین‌ها تنها با محافظت منطقی (رمزنگاری) به کارت IC منتقل می‌شوند، خوانشگر IC غیر مجتمع نیاز به مطابقت با این الزام ندارد.			

ب-۲-۱-۲- مشخصه‌های پاسخگو به دستکاری

نمایندگی ارزشیابی‌کننده موارد درج شده در جدول ب-۲ نتیجه گرفته است:

جدول ب-۲- مشخصه‌های پاسخگو به دستکاری

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ب-۱۱	افزاره در برابر نفوذ توسط ویژگی‌ها چنان محافظت شده است که هرگونه تلاش امکان‌پذیر برای دستکاری افزاره را تشخیص می‌دهد و به سرعت پس از تشخیص چنین تلاشی کلیه کلیدهای رمزنگاری و داده‌های حساس را پاک می‌کند.			
ب-۱۲	جداشدن بدنه یا دریچه افزاره، چه ورود با دسترسی مجاز و چه غیرمجاز به مولفه‌های داخلی افزاره سبب پاک‌شدن خودکار و به سرعت کلیدهای رمزنگاری ذخیره شده در افزاره می‌شود.			
ب-۱۳	روش تعریف‌شده‌ای وجود دارد که اطمینان حاصل می‌کند هنگامی که افزاره به طور دائمی از خدمت خارج می‌شود (انهدام)، داده‌های محرمانه یا هر نوع کلید رمزنگاری که از آن برای رمزگذاری داده‌های محرمانه استفاده‌شده، از روی آن پاک شود. همچنین روشی تعریف‌شده وجود دارد که اطمینان حاصل می‌کند هنگام انهدام دائمی، هرگونه کلید رمزنگاری موجود در واحد که ممکن است در آینده قابل استفاده باشد از روی آن پاک شود یا این کلیدها در تمام تسهیلاتی که آن واحد			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	امکان ایجاد ارتباط رمزنگاری محافظت شده با آنها را دارد نامعتبر شود.			
ب-۱۴	هرگونه سازوکارهای تشخیص دستکاری/پاک کردن کلید حتی هنگام قطع برق کار می‌کند.			
ب-۱۵	اگر افزاره، سازوکاری برای تشخیص جدا شدن از محیط عملیاتی خود ندارد، غلبه بر سازوکارهای تشخیص دستکاری یا کشف اطلاعات محرمانه در افزاره هدف، حتی در صورت جدا شدن از محیط عملیاتی، امکان‌پذیر نیست. به خطر افتادن افزاره نیازمند مجموعه تجهیزات و مهارت‌هایی است که در حال حاضر موجود نیست. **یادآوری**- به عنوان مثالی ممکن، کشف چنین اطلاعاتی نیازمند زمان کافی برای مثال یک ماه آمادگی، شامل تحلیل افزاره‌های دیگر و دست کم یک هفته تلاش برای به خطر افتادن افزاره، پس از دسترسی نامحدود و بدون مزاحمت به افزاره هدف است.			
ب-۱۶	اگر افزاره، سازوکاری برای تشخیص جدا شدن از محیط عملیاتی خود داشته باشد، غلبه بر سازوکارهای تشخیص دستکاری یا کشف اطلاعات محرمانه در افزاره هدف امکان‌پذیر نیست. به خطر افتادن افزاره باید نیازمند مجموعه مهارت‌هایی داشته باشد که در حال حاضر موجود نیست و به تجهیزاتی نیاز دارد که نه در محل افزاره موجود است و نه امکان انتقال آن به محل افزاره وجود دارد. **یادآوری**- به عنوان مثالی ممکن، کشف چنین اطلاعاتی نیازمند زمان کافی برای مثال یک ماه آمادگی، شامل تحلیل افزاره‌های دیگر و دست کم ۱۲ ساعت دسترسی نامحدود و بدون مزاحمت به افزاره هدف، است.			
ب-۱۶-الف	اگر افزاره، سازوکاری برای تشخیص جدا شدن از محیط عملیاتی خود داشته باشد، غلبه بر سازوکارهای تشخیص جدا شدن امکان‌پذیر نیست. به خطر افتادن افزاره باید نیازمند مجموعه مهارت‌هایی باشد که در حال حاضر موجود نیست و به تجهیزاتی نیاز دارد که نه در محل افزاره موجود است و نه امکان انتقال آن به محل افزاره وجود دارد.			

ب-۲-۲- مشخصه‌های امنیتی منطقی

سازنده افزاره ورود PIN یا نمایندگی ارزشیابی‌کننده مستقل موارد درج شده در جدول ب-۳ تضمین کرده‌اند که نهاد بازنگری ممیزی آن را می‌پذیرد:

shaghool.ir

جدول ب-۳- مشخصه‌های امنیتی منطقی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ب-۱۷	محافظت از PIN هنگام انتقال درون پایانه (توصیه می‌شود دست کم یکی از این موارد اعمال شود). - اگر افزاره ورود پین (PED)[1] و خوانشگر IC مجتمع نشده باشند و روش درستی‌سنجی دارنده کارت که کارت IC به آن نیاز دارد، PIN رمزگذاری‌شده است، بلوک PIN بین PED و خوانشگر IC با استفاده از یک کلید رمزگذاری اصالت‌سنجی‌شده کارت IC است، رمزگذاری شده است یا بلوک PIN مطابق با ISO 9564-1 با استفاده از یک کلیدرمزگذاری اصالت‌سنجی‌شده کارت IC به کارت IC رمزگذاری‌شده، ارسال شده است. - اگر PED و خوانشگر IC مجتمع نشده باشند و روش درستی‌سنجی دارنده کارت با PIN رمزگذاری‌نشده تعیین می‌شود، بلوک PIN از PED به خوانشگر IC مطابق با ISO 9564-1 رمزگذاری می‌شود (خوانشگر IC سپس PIN را رمزگشایی می‌کند تا آن را به صورت رمزگذاری نشده به کارت IC ارسال کند). - اگر PED و خوانشگر IC مجتمع شده‌اند و روش درستی‌سنجی دارنده کارت با روش PIN رمزگذاری‌شده تعیین می‌شود، بلوک PIN با استفاده از کلیدرمزگذاری اصالت‌سنجی‌شده کارت IC رمزگذاری می‌شود. - اگر PED و خوانشگر IC مجتمع شده‌اند و روش درستی‌سنجی دارنده کارت با PIN رمزگذاری نشده انجام می‌گیرد، در صورتی که به طور کامل بلوک PIN از طریق افزاره‌ای با رمزنگاری امن که الزامات ISO 9564-1 را برآورده می‌کند، ارسال می‌شود، رمزگذاری نیاز نیست. اگر PIN رمزگذاری‌نشده از طریق محیطی محافظت نشده به خوانشگر IC ارسال شود، بلوک PIN مطابق ISO 9564-1 رمزگذاری			

1 - PIN entry device

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	می‌شود.			
ب-۱۸	رمزگذاری PIN فقط با استفاده از قالب بلوک PIN و الگوریتم رمزگذاری مشخص‌شده در ISO 9564-1، انجام می‌شود.			
ب-۱۹	اگر افزاره ورود PIN قابلیت کارکردی بارگیری نرم‌افزار داشته باشد، افزاره هرگونه نرم‌افزار بارگیری‌شده را رد می‌کند (کلیدهای رمزنگاری افزاره نیز می‌تواند به طور خودکار پاک شود) مگر این که افزاره با موفقیت رمزنگاری کد بارگیری‌شده را اصالت‌سنجی کند.			
ب-۲۰	در صورتی که افزاره ورود PIN به بیش از یک پذیرنده متصل باشد، هرگونه تغییرات بارگیری‌شده در جدول واپایش انتخاب مجموعه کلید پذیرنده، تنها در صورتی از سوی افزاره پذیرفته می‌شود که رمزنگاری این داده‌های بارگیری‌شده با موفقیت اصالت‌سنجی شود.			
ب-۲۱	PED دارای مشخصه‌هایی است که از تعیین کامل PIN جلوگیری می‌کند یا به شکل قابل ملاحظه‌ای آن را از این کار منصرف می‌کند (برای مثال فن استفاده از یک کلید یکتا به ازای هر تراکنش برای جلوگیری از حمله یا محدودکردن تعداد دفعات مجاز ورود PIN در هر دقیقه برای منصرف کردن حمله یا با استفاده از یک قالب بلوک PIN که شامل داده‌های تصادفی است).			
ب-۲۲	در صورتی که صفحه‌کلید هم برای ورود PIN و هم داده‌های دیگر استفاده می‌شود، صفحه نمایش چنان تحت واپایش افزاره قرار دارد که در صورت نمایان بودن داده‌های خروجی یا برآورده شدن الزامات بند ب-۲، پیام «PIN را وارد کنید» یا پیام معادل آن نتواند نمایش داده شود.			
ب-۲۳	افزاره ورود PIN تنها پین‌هایی را قبول می‌کند که بین چهار تا دوازده رقم داشته باشد.			
ب-۲۴	نگاشت مقادیر عددی PIN وارد شده در کدگذاری داخلی مطابق با ISO 9564-1 است.			
ب-۲۵	افزاره ورود PIN برای پذیرندگان مختلف از شکاف‌های کلید مختلف استفاده می‌کند و هیچ یک از کارکنان پذیرنده به هیچ روشی نمی‌توانند کلید مربوط به پذیرنده دیگر را معلوم کرده یا آن را تغییر دهند.			
ب-۲۶	افزاره ورود PIN برای پذیرندگان مختلف از کلیدهای مختلف استفاده می‌کند و ابزارهای انتخاب کلید که در یک تراکنش مشخص استفاده			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	می‌شود، واپایش می‌شود (برای مثال انتخاب از یک جدول داخلی) در نتیجه هیچ راه امکان‌پذیری وجود ندارد که عمدی یا سهوی، کلید پذیرنده دیگر را انتخاب کرد.			
ب-۲۷	مسیر بین صفحه‌کلید تا واحد پردازنده رمزنگاری به صورت منطقی محافظت می‌شود (برای مثال کدگذاری شده است) یا الزامات بند ب-۱ برآورده می‌شوند.			
ب-۲۸	مسیر بین خوانشگر کارت نوار مغناطیسی تا واحد پردازشگر رمزنگاری به صورت منطقی محافظت شده یا الزامات بند ب-۳ برآورده می‌شود.			

ب-۳- مدیریت افزاره

ب-۳-۱- محافظت از افزاره ورود PIN هنگام بارگذاری کلید اولیه

مسئولان بارگذاری کلید اولیه یا ممیز مستقل، موارد درج شده در جدول ب-۴ تضمین کرده‌اند که پشتیبان آن را می‌پذیرد.

جدول ب-۴- محافظت از افزاره ورود PIN هنگام بارگذاری کلید اولیه

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ب-۲۹	افزاره ورود PIN تعمیرشده با کلید اصلی بارگذاری نمی‌شود (مگر به‌صورت تصادفی).			
ب-۳۰	از فنون خودکار استفاده می‌شود و رویه‌های دستی به کارگیری و پیروی می‌شود تا اطمینان حاصل شود که هر افزاره ورود PIN دست کم از لحاظ آماری یک کلید منحصر به فرد را ارائه می‌دهد که برای هیچ کس معلوم نبوده و پیش از این هرگز برای هیچ افزاره ورود PIN دیگری استفاده نشده است (مگر به‌صورت تصادفی).			

ب-۳-۲- محافظت از افزاره ورود PIN پس از نصب

پذیرنده یا ممیز مستقل تضمینی برای نهاد بازنگری ارائه کرده است که واپایش‌ها و رویه‌های لحاظ شده است تا از موارد جدول ب-۵ اطمینان حاصل شود.

جدول ب-۵- محافظت از افزاره ورود PIN پس از نصب

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد

shaghool.ir

ب-۳۱	افزاره ورود PIN چنان نصب شده که ورود PIN به وسیله دوربین‌های نظارتی یا فردی که در کنار افزاره ایستاده، قابل مشاهده نباشد.			
ب-۳۲	محل قرارگیری و/ یا اقدامات مدیریت افزاره در افزاره ورود PIN به گونه‌ای است که عدم حضور آن یا دسترسی غیرمجاز (حمله) به آن در عرض ۲۴ ساعت تشخیص داده می‌شود.			

shaghool.ir

پیوست پ

(الزامی)

افزاره‌های با قابلیت کارکردی مدیریت PIN

پ-۱- کلیات

کارکردهای مدیریت PIN شامل موارد زیر است:

- صدور PIN؛
- درستی‌سنجی PIN؛ و
- ترجمه PIN.

یادآوری ۱- ورود PIN در پیوست ب مطرح شده است.

یادآوری ۲- الزامات این پیوست برای افزاره‌های پایانه فروش (POS)[1] و خودپرداز (ATM)[2] که ترجمه PIN را برای ارسال به کارت‌های IC انجام می‌دهند، به کار نمی‌رود.

رویه ارزشیابی افزاره‌هایی که قابلیت کارکردی مدیریت PIN را شامل می‌شود، به شرح زیر است:

- بازبینه‌های پیوست الف تکمیل شود؛
- بازبینه‌های این پیوست تکمیل شود؛ و
- نتایج این دو بازبینه برای نهاد بازنگری ممیزی ارسال شود.

لازم است بیانیه‌ها در این بازبینه انطباق امنیتی توسط ممیز به عنوان «درست (T)»، «نادرست (F)» یا «کاربرد ندارد (N/A)» مشخص شود. علامت «نادرست» لزوماً نشان‌دهنده عمل غیر قابل قبول نیست بلکه باید به صورت مکتوب توضیح داده شود. بیانیه‌هایی که به صورت «کاربرد ندارد» نشان داده می‌شوند نیز باید به صورت مکتوب توضیح داده شوند.

1 - Point of sale
2 - Automatic teller machine

shaghool.ir

پ-۲- مشخصه‌های افزاره

پ-۲-۱- مشخصه‌های امنیت فیزیکی

سازنده افزاره مدیریت PIN یا نمایندگی ارزشیابی‌کننده مستقل موارد درج شده در جدول پ-۱ تضمین کرده اند که نهاد بازنگری ممیزی آن را می‌پذیرد.

جدول پ-۱- مشخصه‌های امنیت فیزیکی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
پ-۱	یک یا چند سازوکار زیر وجود دارد تا مهاجم را از جداکردن غیرمجاز افزاره از محل عملیاتی خود منصرف کند: - وزن افزاره بیش از ۴۰ کیلوگرم است یا به سازه‌ای که بیش از ۴۰ کیلوگرم است یا اندازه‌ای مشابه دارد به وسیله یک قفل ضدسرقت، قفل شده است، چنان که نتوان بدون باز کردن قفل، آن را از سطح آن جدا کرد. - افزاره دارای سازوکارهایی است که جدا کردن افزاره از محل عملیاتی‌اش سبب پاک شدن خودکار کلیدهای رمزنگاری درون افزاره می‌شود؛ و - جدا کردن افزاره هیچ سودی نخواهد داشت زیرا مشخصه‌های مقاوم بودن در برابر دستکاری یا پاسخگو بودن به دستکاری آن، اطمینان حاصل می‌کند که استخراج کلیدهای رمزنگاری یا دیگر داده‌های محرمانه امکان‌پذیر نیست.			

پ-۲-۲- مشخصه‌های امنیت منطقی

سازنده افزاره مدیریت PIN یا نمایندگی ارزشیابی‌کننده مستقل موارد درج شده در جدول پ-۲ تضمین کرده‌اند که نهاد بازنگری ممیزی آن را می‌پذیرد.

جدول پ-۲- مشخصه‌های امنیت منطقی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
پ-۲	هر اثر باقی‌مانده از پین‌ها یا کلیدهای رمزنگاری استفاده‌شده هنگام تراکنش در پودمان مقاوم بودن در برابر دستکاری یا پاسخگو بودن به دستکاری ذخیره‌شده است یا پس از آن که نیازی به آنها نباشد، به سرعت بازنویسی می‌شوند.			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	یادآوری- پین‌های رمزگذاری‌نشده همواره پس از رمزگذاری به سرعت بازنویسی می‌شود.			
پ-۳	هنگامی که PIN از یک شماره حساب یا داده‌ای دیگر مشتق می‌شود، کلیدهای استفاده‌شده در این فرآیند برای هیچ منظور دیگری استفاده نمی‌شود.			
پ-۴	زمانی که مرجع درستی‌سنجی PIN محاسبه می‌شود، کلیدهایی که در این فرآیند استفاده شده‌اند، برای هیچ منظور دیگری استفاده نمی‌شوند.			
پ-۵	در صورتی که در محیط عملیاتی موردنظر از جستجوی فراگیر PIN حفاظت نمی‌شود، پایش داخلی آمارها به گونه‌ای انجام می‌گیرد که تعداد دفعات مشخصی از درستی‌سنجی PIN اشتباه مجاز است. هنگام محاسبه تعداد دفعات فراخوانی درستی‌سنجی PIN نادرست، اگر چند فراخوانی شامل یک جفت PIN/PAN درست مشابه باشد، آنها شمرده نمی‌شوند.			
پ-۶	تعیین هیچ‌کدام از کلیدهای درستی‌سنجی PIN از روی مقادیر مرجع PIN، پین‌های متناظر و داده‌های غیرمحرمانه مرتبط امکان‌پذیر نیست.			
پ-۷	قابلیت کارکردی ترجمه PIN با بند ISO 9654-1 مطابقت دارد. فرآیند ترجمه، پین‌ها را از خطر افشا شدن محافظت می‌کند.			
پ-۸	تمام کلیدهایی که بلوک‌های PIN ورودی با آنها رمز می‌شوند برای هیچ مقصود دیگری استفاده نمی‌شود. به ویژه به هیچ روشی نمی‌توان از این کلیدها برای رمزگذاری یک تعداد کلید رمزگذاری‌نشده منتخب استفاده کرد و تمام کلیدهایی که بلوک‌های PIN را رمزگشایی می‌کند، نمی‌توانند برای مقاصد دیگری به کار روند. به خصوص روشی برای استفاده از این کلید برای رمزگشایی تعداد کلیدهای منتخب وجود ندارد.			
پ-۹	هیچ ترجمه‌ای از قالب‌های بلوک PIN ورودی به قالب بلوک PIN دیگر وجود ندارد که در بند ISO 9654-1 نیامده باشد.			
پ-۱۰	برای جلوگیری از سوءاستفاده از قابلیت ترجمه افزاره برای تعیین PIN فراگیر روش‌های زیر به کار می‌رود: - محیط عملیاتی از این سوءاستفاده جلوگیری می‌کند؛ یا - تمام ترجمه‌های PIN بین قالب‌هایی صورت می‌گیرد که			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	PIN را به صورت کارکردی از بخش خاص شماره حساب رمز می‌کنند و برای قابلیت ترجمه PIN لازم است که ارقام شماره حساب در بلوک PIN ورودی با ارقام شماره حساب متناظر در بلوک PIN خروجی مطابقت داشته باشند.			
ب-۱۱	افزاره تولید PIN تنها برای صدور PIN رمزگذاری‌نشده تحت واپایش دوگانه می‌تواند فعال شود.			

پ-۳- مدیریت افزاره

الزامات مدیریت افزاره مشابه الزامات مطرح شده در پیوست ث است.

shaghool.ir

پیوست ت

(الزامی)

افزاره‌های با قابلیت کارکردی اصالت‌سنجی پیام

ت-۱- کلیات

افزاره‌های اصالت‌سنجی پیام، کد اصالت‌سنجی پیام (MAC) را برای یکپارچگی داده‌ها و درستی‌سنجی منشاء ادعاشده محاسبه می‌کنند.

سه نوع ورودی وجود دارد:

- کلیدهای رمزنگاری؛
- پیام‌هایی که اصالت‌سنجی می‌شود (که به دنبال یک MAC برای افزاره‌های درستی‌سنجی MAC می‌آید)؛ و
- ورودی کاروَر (برای مثال انتخاب کلید اصالت‌سنجی پیام).

دو نوع خروجی برای افزاره‌های تولید MAC وجود دارد: کد درستی‌سنجی کلید رمزنگاری که وارد شده یا از آن استفاده‌شده است و کد اصالت‌سنجی پیام (MAC) محاسبه‌شده. برای افزاره‌های درستی‌سنجی MAC نیز دو نوع خروجی وجود دارد: کد درستی‌سنجی کلید رمزنگاری که وارد شده یا از آن استفاده‌شده است و پاسخ‌های بله / خیر که با استفاده از کلید نشان داده شده، نشان می‌دهند آیا MAC پیام درست بوده یا خیر.

برخی افزاره‌ها از کلیدهای MAC متفاوتی، برای مثال از کلیدهای یک‌سویه، برای تولید و درستی‌سنجی استفاده می‌کنند. رویه ارزشیابی افزاره‌های اصالت‌سنجی پیام به شرح زیر است:

- بازبینه‌های پیوست الف تکمیل شود؛
- بازبینه‌های این پیوست تکمیل شود؛
- نتایج هر دو بازبینه برای نهاد بازنگری ممیزی ارسال شود.

بیانیه‌های این بازبینه انطباق امنیتی لازم است توسط ممیز به عنوان «درست (T)»، «نادرست (F)» یا «کاربرد ندارد (N/A)» مشخص شود. علامت «نادرست» لزوماً نشان‌دهنده‌ی عمل غیر قابل قبول نیست بلکه باید به صورت مکتوب توضیح داده شود. بیانیه‌هایی که به صورت «کاربرد ندارد» نشان داده می‌شوند نیز باید به صورت مکتوب توضیح داده شوند.

shaghool.ir

ت-۲- مشخصه‌های امنیت منطقی افزاره

سازنده افزاره اصالت‌سنجی پیام یا نمایندگی ارزشیابی‌کننده مستقل موارد درج شده در جدول ت-۱ تضمین کرده‌اند که نهاد بازنگری ممیزی آن را می‌پذیرد.

جدول ت-۱- مشخصه‌های امنیت منطقی افزاره

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ت-۱	اگر افزاره اصالت‌سنجی پیام می‌تواند به صورت دستی فعال شود و کلیدهای MAC مختلفی را شامل شود، افزاره، هویت کلیدهای استفاده‌شده را نشان می‌دهد.			
ت-۲	طول MAC تولیدشده یا درستی‌سنجی‌شده مطابق با ISO 16609 است.			
ت-۳	MAC با استفاده از الگوریتم تأییدشده مطابق با ISO 16609 تولید می‌شود که فرستنده و گیرنده بر آن توافق دارند.			
ت-۴	افزاره فقط تأیید یا انکار MAC را که برای درستی‌سنجی ارائه می‌شود، بیرون می‌دهد و هرگز MAC را به صورت رمزگذاری‌نشده بیرون نمی‌دهد.			
ت-۵	اگر افزاره برای تولید یا درستی‌سنجی MAC از دو کلید استفاده کند، فن به کاررفته باید مطابق ISO 16609 باشد.			
ت-۶	اگر افزاره اصالت‌سنجی پیام برای استفاده از کلیدهای یک‌سویه MAC طراحی شده باشد، از هر کلید MAC تنها برای یک نوع کارکرد MAC استفاده می‌شود، یعنی MAC متن دریافتی را درستی‌سنجی می‌کند یا MAC را برای متن در حال ارسال تولید می‌کند و بیرون می‌دهد.			

shaghool.ir

پیوست ث

(الزامی)

افزاره‌های با قابلیت کارکردی تولید کلید

ث-۱- کلیات

کارکردهای تولید کلید شامل موارد زیر است:

- تولید عدد تصادفی یا شبه‌تصادفی[1] با هدف تولید کلید متقارن یا مولفه کلید متقارن؛
- تولید عدد اول تصادفی یا شبه‌تصادفی با هدف تولید کلید خصوصی و کلید عمومی جفت کلید نامتقارن؛ و
- کارکرد(های) محاسبه مقدار رمز برای سامانه‌های توزیع کلید عمومی.

دو نوع افزاره برای تولید و ورود کلیدها وجود دارد که یکی از این دو نوع نیاز به «جلوگیری از به خطر افتادن» دارد زیرا به خطر افتادن افزاره می‌تواند سبب افشای کلیدهایی شود که پیش‌تر توسط افزاره مقدم بر به خطر افتادن تولید یا وارد شده است. نوع دیگر تنها به «تشخیص به خطر افتادن» نیاز دارد زیرا افزاره هیچ اطلاعاتی را نگهداری نمی‌کند که در صورت افشا، به وسیله آنها بتوان کلیدهایی که به افزاره رمزنگاری مقدم بر به خطر افتادن وارد شده را افشا کرد.

رویه ارزشیابی افزاره‌های تولید کلید به شرح زیر است:

- بازبینه‌های پیوست الف تکمیل شود؛
- بازبینه‌های این پیوست تکمیل شود؛ و
- نتایج هر دو بازبینه برای نهاد بازنگری ممیزی ارسال شود.

بیانیه‌های این بازبینه انطباق امنیتی لازم است توسط ممیز به عنوان «درست (T)»، «نادرست (F)» یا «کاربرد ندارد (N/A)» مشخص شود. علامت «نادرست» لزوماً نشان‌دهنده‌ی عمل غیر قابل قبول نیست بلکه باید به صورت مکتوب توضیح داده شود. بیانیه‌هایی که به صورت «کاربرد ندارد» نشان داده می‌شوند نیز باید به صورت مکتوب توضیح داده شوند.

1 - Pseudo-random

shaghool.ir

ث-۲- مشخصه‌های افزاره

ث-۲-۱- مشخصه‌های امنیت فیزیکی

سازنده افزاره تولید کلید یا نمایندگی ارزشیابی‌کننده مستقل موارد درج شده در جدول ث-۱ تضمین کرده‌اند که نهاد بازنگری ممیزی آن را می‌پذیرد.

جدول-ث-۱- مشخصه‌های امنیت فیزیکی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ث-۱	یک یا چند سازوکار زیر وجود دارد تا مهاجم را از جداکردن غیرمجاز افزاره از محل عملیاتی خود منصرف کند: - وزن افزاره بیش از ۴۰ کیلوگرم است یا به سازه‌ای که بیش از ۴۰ کیلوگرم است یا اندازه‌ای مشابه دارد به وسیله یک قفل ضدسرقت، قفل شده است، چنان که نتوان بدون باز کردن قفل، آن را از سطح آن جدا کرد. - افزاره دارای سازوکارهایی است که جدا کردن افزاره از محل عملیاتی‌اش سبب پاک شدن خودکار کلیدهای رمزنگاری درون افزاره می‌شود؛ و - جدا کردن افزاره هیچ سودی نخواهد داشت زیرا مشخصه‌های مقاوم بودن در برابر دستکاری یا پاسخگو بودن به دستکاری آن اطمینان حاصل می‌کند که استخراج کلیدهای رمزنگاری یا دیگر داده‌های محرمانه امکان‌پذیر نیست.			

ث-۲-۲- مشخصه‌های امنیت منطقی

سازنده افزاره تولید کلید یا نمایندگی ارزشیابی‌کننده مستقل موارد درج شده در جدول ث-۲ تضمین کرده‌اند که نهاد بازنگری ممیزی آن را می‌پذیرد.

جدول-ث-۲- مشخصه‌های امنیت منطقی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ث-۲	کارکردهای مدیریت کلید افزاره چنان طراحی که افشای هیچ کلیدی بدون تبانی افراد مورداعتماد انجام نخواهد شد. به خصوص که: - کلیدهای بالاترین سطح افزاره دست کم در دو مولفه تحت			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	واپایش دوگانه، به صورت دستی بارگذاری می‌شوند، و/یا – هر کارکرد که برای ورود یا خروج مولفه‌های کلید استفاده می‌شود تا زمانی که دست کم دو گذرواژه مختلف وارد نشده باشد، کار نمی‌کند.			
ث-۳	افزاره کلید حقیقی را به مولفه‌های کلید تجزیه می‌کند چنان که هیچ بیت «فعال» کلیدی را نمی‌توان بدون دانستن کل مولفه‌های مورد نیاز تعیین کرد (برای مثال مولفه‌ها برای تشکیل یک کلید XOR می‌شوند یا از فن به اشتراک‌گذاری محرمانه استفاده می‌شود).			
ث-۴	روش‌های تولید کلید مطابق با ISO 11568 است.			
ث-۵	هر فراخوانی برای دریافت کلیدهای تولیدشده، کلیدی متفاوت و از لحاظ آماری منحصر به فرد را دریافت خواهد کرد (مگر به صورت تصادفی).			
ث-۶	در صورتی که افزاره قادر به تولید جفت کلیدهای نامتقارن باشد، کلید خصوصی هنگام فرآیند تولید به شکلی قابل‌فهم نمایان نمی‌شود.			
ث-۷	در صورتی که افزاره قادر به تولید جفت کلیدهای نامتقارنی باشد که از آن استفاده نمی‌کند، این جفت کلید و تمام عناصر تشکیل‌دهنده رمز مرتبط با آن، به سرعت پس از فرآیند انتقال حذف می‌شود.			
ث-۸	افزاره هیچ کلید رمزگذاری‌نشده را بیرون نمی‌دهد مگر تحت واپایش دوگانه. این واپایش دوگانه به دو صورت زیر اجرا می‌شود: – افزاره نیازمند این است که دست کم در مدت کمتر از ۵ دقیقه دو گذرواژه به صورت درست در افزاره وارد شود، پیش از آن که افزاره کلید را بیرون بدهد؛ و – افزاره نیازمند این است که پیش از این که افزاره، کلیدی را بیرون بدهد، دست کم دو کلید مختلف فیزیکی (با علامت «تکثیر تجاری ممنوع») با هم درون این واحد قرار داده شود.			
ث-۹	کارکردهای کاروَر زیر (اگر وجود داشته باشند) نیاز به استفاده خاص از وضعیت‌های «حساس» دارد: – ورود دستی داده‌های واپایش (برای مثال کد درستی‌سنجی کلید) برای امکان‌پذیر کردن خروج، ورود یا استفاده از کلید؛ و			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	- مجاز کردن جابجایی افزاره بدون فعال شدن سازوکار پاک‌کردن کلید.			
ث-۱۰	تمام کارکردهای اختصاصی شرایط زیر را دارند: - به طور کامل، معادل با مجموعه‌های استاندارد و کارکردهای تأییدشده هستند؛ یا - محدود به استفاده از کلیدهایی هستند که با خاصیت تفکیک کلید، نمی‌توانند با کلیدها یا کلیدهای تغییرداده‌شده کارکردهای غیراختصاصی استفاده شوند.			
ث-۱۱	اعداد تصادفی و اعداد شبه‌تصادفی مطابق با ISO 18031 است.			

ث-۳- مدیریت افزاره

سازنده افزاره تولید کلید یا سازمانی که از این افزاره استفاده می‌کند یا نماینده‌گی ارزشیابی‌کننده مستقل موارد درج شده در جدول ث-۳ تضمین کرده اند که نهاد بازنگری ممیزی آن را تأیید می‌کند.

جدول ث-۳- مدیریت افزاره

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ث-۱۲	از استفاده غیرمجاز از افزاره با یکی از روش‌های زیر جلوگیری می‌شود یا تشخیص داده می‌شود: - افزاره دارای مشخصه‌های فیزیکی یا کارکردی (برای مثال گذرواژه‌ها یا کلیدهای فیزیکی با امنیت بالا) است که امکان استفاده از افزاره تنها تحت واپایش دوگانه وجود دارد و هنگامی که در وضعیت قابل‌استفاده قرار دارد افزاره همچنان در نظارت مداوم دست کم دو نفر است که اطمینان می‌دهند هر استفاده غیرمجاز از افزاره را تشخیص خواهند داد؛ و - افزاره همیشه یا قفل است یا در یک محفظه دارای مشخصه آشکارکنندهٔ دستکاری مهر و موم شده است یا در نظارت مداوم دست کم دو فرد مجاز است که اطمینان می‌دهند هر نوع استفاده غیرمجاز از افزاره را تشخیص خواهند داد.			
ث-۱۳	وقتی افزاره آماده به کار یا در حال استفاده است، از دسترسی غیرمجاز			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	به مدار داخلی آن با روش‌های زیر ممانعت به عمل می‌آید: - تسهیلاتی که افزاره در آن کار می‌کند دارای نظارت و واپایش‌های کافی است تا از هرگونه دسترسی غیرمجاز به افزاره که می‌تواند منجر به افشای موفق کلیدهای رمزنگاری یا هرگونه داده محرمانه دیگر شود، جلوگیری کند؛ و - افزاره در نظارت مداوم دست کم دو فرد مورداعتماد قرار دارد که شایستگی و توانایی مشاهده هرگونه تلاش برای دسترسی غیرمجاز به افزاره را دارند و می‌توانند پیش از به ثمر رسیدن حمله از آن جلوگیری کنند.			
ث-۱۴	واپایش‌هایی وجود دارد تا از جداشدن افزاره امنیتی از تسهیلاتی که در آن خدمت‌دهی می‌کند، جلوگیری کند، مگر این که اطمینان حاصل شود هیچ اطلاعاتی درون افزاره باقی نمانده که بتوان با آنها به کلیدهای رمزنگاری را که تا به حال در افزاره بوده، افشا کرد.			
ث-۱۵	وقتی افزاره در حال استفاده نیست، با روش‌های زیر از هرگونه دسترسی غیرمجاز به مدار داخلی آن جلوگیری می‌شود: - تسهیلاتی که افزاره در آنها استفاده می‌شود دارای نظارت و واپایش کافی برای جلوگیری از دسترسی غیرمجاز به افزاره است؛ و - افزاره تحت واپایش دوگانه درون گاوصندوقی که امکان نفوذ به آن وجود ندارد، انبار می‌شود و هر رخداد بازکردن یا بستن گاوصندوق تحت واپایش دوگانه ثبت می‌شود؛			
ث-۱۶	وقتی افزاره در حال استفاده نیست، از دسترسی تشخیص داده نشده به مدار داخلی آن به روش‌های زیر ممانعت به عمل می‌آید: - تسهیلاتی که افزاره در آن کار می‌کند دارای نظارت و واپایش‌های کافی است تا از دسترسی غیرمجاز به افزاره پیش از این که متعاقبا در حالت فعال شدن دوباره قرار گیرد، جلوگیری شود؛ و - افزاره تحت واپایش دوگانه در یک محفظه دارای مشخصه آشکارکنندهٔ دستکاری انبار می‌شود که هر رخداد بازکردن و بستن آن تحت واپایش دوگانه ثبت می‌شود.			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ث-۱۷	هنگامی که افزاره آماده به کار یا در حال استفاده است، به روش‌های زیر از دسترسی تشخیص داده نشده به مدار داخلی آن جلوگیری می‌شود: - تسهیلاتی که افزاره در آن کار می‌کند دارای نظارت کافی و واپایش‌هایی است که هرگونه دسترسی غیرمجاز به افزاره را پیش از استفاده متعاقب از آن برای هر کارکرد رمزنگاری تشخیص می‌دهد؛ و - افزاره در نظارت مداوم دست کم دو فرد مورداعتماد است که شایستگی تشخیص چنین دسترسی را دارند.			
ث-۱۸	واپایش‌هایی وجود دارد تا نصب دوباره غیرمجاز افزاره‌ای که پیش از این از تسهیلات برداشته شده را تشخیص دهد.			

shaghool.ir

پیوست ج

(الزامی)

افزاره‌های با قابلیت کارکردی انتقال و بارگذاری کلید

ج-۱- کلیات

کارکردهای انتقال و بارگذاری کلید شامل موارد زیر است:

- خروج کلیدها از یک افزاره رمزنگاری امن (SCD) به SCD دیگر به سه شکل رمزگذاری‌نشده، مولفه یا رمزگذاری شده؛
- خروج مولفه کلید از SCD به بسته‌بندی آشکارکنندهٔ دستکاری (برای مثال درون یک پاکت بدون منفذ)؛
- ورود مولفه‌های کلید به SCD از بسته‌بندی‌های آشکارکنندهٔ دستکاری؛ و
- ذخیره موقتی کلید به سه شکل رمزگذاری‌نشده، مولفه یا رمزگذاری‌شده در SCD هنگام انتقال آن.

دو نوع افزاره وجود دارد که می‌تواند برای انتقال کلیدها به این روش استفاده شود. یک نوع فقط مولفه تک کلید (از مجموعه دست کم دو مولفه) را منتقل می‌کند. نوع دیگر کلید کلی را به شکل رمزگذاری‌نشده انتقال می‌دهد. این ممیزی دو نوع افزاره را مد نظر قرار می‌دهد.

رویه‌های ارزشیابی افزاره‌های انتقال و بارگذاری کلید به شرح زیر است:

- بازبینه‌های پیوست الف تکمیل شود؛
- بازبینه‌های این پیوست تکمیل شود؛ و
- نتایج هر دو بازبینه برای نهاد بازنگری ممیزی ارسال شود.

بیانیه‌های این بازبینه انطباق امنیتی لازم است توسط ممیز به عنوان «درست (T)»، «نادرست (F)» یا «کاربرد ندارد (N/A)» مشخص شود. علامت «نادرست» لزوماً نشان‌دهنده‌ی عمل غیر قابل قبول نیست بلکه باید به صورت مکتوب توضیح داده شود. بیانیه‌هایی که به صورت «کاربرد ندارد» نشان داده می‌شوند نیز باید به صورت مکتوب توضیح داده شوند.

shaghool.ir

ج-۲- مشخصه‌های افزاره

ج-۲-۱- مشخصه‌های امنیت فیزیکی

افزاره انتقال و بارگذاری کلید یا نمایندگی ارزشیابی‌کننده مستقل موارد درج شده در جدول ج-۱ تضمین کرده‌اند که نهاد بازنگری ممیزی آن را می‌پذیرد:

جدول ج-۱- مشخصه‌های امنیت فیزیکی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ج-۱	یک یا چند سازوکار مهاجم را از جداشدن غیرمجاز افزاره از محل عملیاتی‌اش منصرف می‌کند: - افزاره دارای سازوکارهای پاسخگو بودن به دستکاری است چنان که جدا کردن افزاره از محل عملیاتی آن سبب پاک‌شدن خودکار کلیدهای رمزنگاری موجود در آن می‌شود؛ و - مشخصه‌های مقاوم بودن در برابر دستکاری یا پاسخگو بودن به دستکاری افزاره اطمینان می‌دهد که استخراج کلیدهای رمزنگاری یا دیگر داده‌های محرمانه امکان‌پذیر نیست.			

ج-۲-۲- مشخصه‌های امنیت منطقی

سازنده افزاره، انتقال و بارگذاری کلید یا نمایندگی ارزشیابی‌کننده مستقل موارد درج شده در جدول ج-۲ تضمین کرده‌اند که نهاد بازنگری ممیزی آن را می‌پذیرد:

جدول ج-۲- مشخصه‌های امنیت منطقی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ج-۲	کلیدها در برابر جایگزینی و تغییر محافظت می‌شوند.			
ج-۳	کارکردهای مدیریت کلید افزاره چنان طراحی شده که افشای هیچ‌کدام از کلیدها بدون تبانی افراد مورداعتماد ممکن نیست. به خصوص: - بالاترین سطح کلیدهای افزاره، در صورت متقارن بودن، در دست کم دو مولفه و به صورت دستی بارگذاری می‌شود؛ و - تمام کارکردهایی که برای ورود یا خروج مولفه‌های کلید استفاده می‌شوند تنها تحت واپایش دوگانه کار می‌کنند.			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ج-۴	افزاره هیچ کلید رمزگذاری‌نشده‌ای را بیرون نمی‌دهد مگر تحت واپایش دوگانه. این واپایش دوگانه به دو صورت زیر اجرا می‌شود: - افزاره نیاز دارد که پیش از این که افزاره کلیدی را بیرون دهد، دست کم در مدت کمتر از ۵ دقیقه دو گذرواژه به صورت درست در افزاره وارد شود؛ - افزاره نیاز دارد که پیش از این که افزاره کلیدی را بیرون بدهد، دست کم دو کلید مختلف فیزیکی که نتوان مشابه آنها را ساخت با هم درون این واحد قرار داده شود.			
ج-۵	این کارکردهای کاروَر، نیازمند استفاده از وضعیت حساس است: - تولید داده‌های واپایشی (برای مثال کد درستی‌سنجی کلید) برای خروج، ورود یا استفاده از کلید؛ - مجاز کردن جابجایی افزاره بدون فعال شدن سازوکار پاک‌کردن کلید؛ و - تغییر گذرواژه‌ها یا داده‌هایی که افزاره را به وضعیت حساس وارد می‌کند.			
ج-۶	فقط فراخوانی‌های کارکرد و کارکردهای کاروَر حساس که در افزاره موجود است، جز کارکردهایی است که توسط پشتیبان یا سامانه‌ای که افزاره در آن کار می‌کند، تأیید شده است. هر کارکرد افزوده (اختصاصی) دیگر نیز: - به طور کامل معادل با مجموعه استانداردها و کارکردهای تأییدشده است؛ یا - بر اساس خاصیت تفکیک کلید، محدود به کلیدهای صرفاً کاربردی بوده و نمی‌توان با کلیدها، کلیدهای تغییریافته یا داده‌های حساس کارکردهای غیراختصاصی از آن استفاده کرد.			
ج-۷	وقتی افزاره با کلیدهای رمزنگاری بارگذاری شده، در عمل هیچ راهی وجود ندارد که بتوان قابلیت‌های کارکردی افزاره را تغییر داد، بدون آن که این کار سبب پاک‌شدن خودکار و به سرعت کلیدهای رمزنگاری ذخیره‌شده درون افزاره شده یا سبب شود این تغییرات پیش از استفاده			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	بعدی از افزاره برای بارگذاری کلید تشخیص داده شوند.			
ج-۸	افزاره هیچ اطلاعاتی را نگهداری نمی‌کند که کلیدی که به افزاره رمزنگاری دیگر منتقل کرده است را افشا کند. **یادآوری**- این مورد در کاربردهای زیر اعمال نمی‌شود: - استفاده KLD برای بارگذاری چند پودمان امنیت سخت‌افزار (HSM)[1] با یک کلید پرونده اصلی[2] (برای مثال هنگامی که از HSMها برای اشتراک‌گذاری در بارگذاری با یک پایگاه‌داده کلید استفاده می‌شود.)؛ و - استفاده از KLD برای تولید کلیدهای منحصر به فرد به ازای هر افزاره، بارگذاری آنها در PED و سپس انتقال پرونده کلیدها به HSM.			

ج-۳- مدیریت افزاره

سازنده افزاره انتقال و بارگذاری کلید یا سازمانی که این افزاره در آن به کار گرفته می‌شود یا نمایندگی ارزشیابی‌کننده مستقل، به صورت جدول ج-۳ تضمینی ارائه کرده است که نهاد بازنگری ممیزی آن را می‌پذیرد:

جدول ج-۳- مدیریت افزاره

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ج-۹	سازوکارهایی که برای انتقال کلیدها، مولفه‌ها یا گذرواژه‌ها به درون افزاره یا خارج از آن به کار می‌روند چنان تحت محافظت یا بازرسی قرار دارند که از هرگونه پایش که بتواند منجر به افشای غیرمجاز کلیدها، مولفه‌ها یا گذرواژه‌ها شود، جلوگیری کند.			
ج-۱۰	اگر افزاره نیاز به «جلوگیری از به خطر افتادن» داشته باشد، هنگامی که افزاره در حال استفاده نیست، به روش‌های زیر از هرگونه دسترسی غیرمجاز به مدار داخلی آن جلوگیری می‌شود: - تسهیلاتی که افزاره در آن کار می‌کند دارای نظارت و واپایش کافی برای جلوگیری از دسترسی غیرمجاز به افزاره			

1 - Hardware Security Module
2 - Master file key

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	است؛ و - افزاره تحت واپایش دوگانه درون گاوصندوقی که امکان نفوذ به آن وجود ندارد، نگهداری شده و هر رخداد بازکردن یا بستن گاوصندوق تحت واپایش دوگانه ثبت می‌شود.			
ج-۱۱	اگر افزاره نیاز به «جلوگیری از به خطر افتادن» داشته باشد، هنگامی که افزاره آماده به کار یا در حال استفاده است، به روش‌های زیر از هرگونه دسترسی غیرمجاز به مدار داخلی آن جلوگیری می‌شود: - تسهیلاتی که افزاره در آن کار می‌کند دارای نظارت و واپایش کافی برای جلوگیری از دسترسی غیرمجاز به افزاره است؛ و - افزاره در نظارت مداوم دست کم دو فرد مورداعتماد است که شایستگی و توانایی مشاهده هرگونه تلاش برای دسترسی غیرمجاز به افزاره را دارند و می‌توانند پیش از به ثمر رسیدن حمله از آن جلوگیری کند.			
ج-۱۲	اگر افزاره فقط به «تشخیص به خطر افتادن» نیاز داشته باشد، هنگامی که از افزاره استفاده نمی‌شود، به روش‌های زیر از دسترسی تشخیص داده نشده به مدار داخلی آن جلوگیری می‌شود: - تسهیلاتی که افزاره در آن کار می‌کند دارای نظارت کافی و واپایش‌های کافی بوده تا هرگونه دسترسی غیرمجاز به افزاره پیش از استفاده متعاقب از آن تشخیص داده شود؛ - افزاره در نظارت دوگانه و در محفظه دارای مشخصه آشکارکنندهٔ دستکاری نگهداری شده چنان که هر رخداد باز و بسته‌کردن آن تحت واپایش دوگانه واپایش و ثبت می‌شود؛ و - اگر از محفظه دارای مشخصه آشکارکنندهٔ دستکاری استفاده شود، این محفظه به طور منظم توسط دست کم دو فرد مورداعتماد که شایستگی و توانایی مشاهده هرگونه دسترسی غیرمجاز به افزاره را داشته باشند، پایش می‌شود.			
ج-۱۳	اگر افزاره فقط به «تشخیص به خطر افتادن» نیاز داشته باشد، هنگامی افزاره آماده به کار یا در حال استفاده است، به روش‌های زیر			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	از دسترسی تشخیص داده نشده به مدار داخلی آن پیش از استفاده دوباره از آن جلوگیری می‌شود: - تسهیلاتی که افزاره در آن کار می‌کند دارای نظارت کافی و واپایش‌هایی است تا هرگونه دسترسی غیرمجاز به افزاره پیش از استفاده متعاقب از آن برای کارکرد رمزنگاری تشخیص داده شود؛ و - افزاره در نظارت مداوم دست کم دو فرد مورداعتماد قرار دارد که شایستگی و توانایی مشاهده هرگونه دسترسی غیرمجاز به آن را دارند.			
ج-۱۴	واپایش‌هایی وجود دارد که سبب می‌شود جدا شدن غیرمجاز افزاره از محل مجاز آن و بازگرداندن غیرمجاز آن به محل مجاز آن تشخیص داده شود.			
ج-۱۵	مولفه کلید در نظارت مستقیم شخصی که اجازه دسترسی به این مولفه‌ها را دارد و تنها در صورت تضمین منطقی از عدم وجود «اِشکال» یا هر سازوکار دیگر افشا در مسیر انتقال مولفه‌های کلید از افزاره تولید کلید به خود افزاره انتقال، در افزاره بارگذاری می‌شوند.			
ج-۱۶	در صورتی که افزاره شامل مولفه‌های کلید رمزگذاری‌نشده باشد، در نظارت مداوم شخصی قرار دارد که اجازه دسترسی به این مولفه را دارد (و به مسئولیت‌های خود در قبال اطمینان از محرمانه ماندن این مولفه آگاه است) یا در یک محفظه امنیتی قفل‌شده یا مهر و موم شده قرار دارد و هیچ فردی به غیر از افراد مجاز به دسترسی به آن، امکان باز کردن آن را ندارد.			
ج-۱۷	افزاره تنها زمانی برای واردکردن مولفه درون یک افزاره رمزنگاری استفاده می‌شود که این کار در نظارت مستقیم شخصی که اجازه دسترسی به این مولفه را دارد انجام می‌شود و زمانی که تضمین کامل وجود دارد که هیچ « اِشکال» یا سازوکار افشای دیگری در مسیر انتقال مولفه‌های کلید از افزاره انتقال کلید به افزاره رمزنگاری وجود ندارد.			
ج-۱۸	برای انتقال کلید به افزاره رمزنگاری امن دیگر - از یک مسیر ارتباطی امن استفاده می‌شود؛ - از یک افزاره انتقال کلید استفاده می‌شود؛			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	- از یک مسیر رمزنگاری امن استفاده می‌شود؛ یا - این کار در یک محیط امن انجام می‌شود.			
ج-۱۹	هیچ شخصی با دانستن یا دسترسی به یکی از گذرواژه‌ها یا کلیدهای فیزیکی که برای خروج کلید از افزاره نیاز است، دسترسی به گذرواژه‌های دیگر یا کلیدهای فیزیکی دیگر این افزاره را نمی‌داند.			
ج-۲۰	کلیدهای رمزگذاری‌نشده تنها زمانی در این افزاره بارگذاری می‌شوند که افزاره در نظارت مستقیم دست کم دو فرد مجاز باشد و هر دوی آنها اطمینان یابند که هیچ «اِشکال» یا سازوکار افشای دیگری در مسیر انتقال کلید از افزاره تولید کلید به خود افزاره انتقال کلید وجود ندارد.			
ج-۲۱	از این افزاره تنها زمانی برای واردکردن کلیدهای رمزگذاری‌نشده در یک افزاره رمزنگاری دیگر استفاده می‌شود که افزاره در نظارت مستقیم دست کم دو فرد مجاز باشد و هر دوی آنها اطمینان یابند که هیچ «اِشکال» یا سازوکار افشای دیگری در مسیر انتقال کلید از افزاره انتقال کلید به افزاره رمزنگاری وجود ندارد.			
ج-۲۲	قابلیت کارکردی لازم برای ورود، خروج یا انتقال کلیدهای رمزنگاری از منابع بیرونی اطمینان می‌دهد که این کلیدها به یک یا چند شکل زیر است: - با نوعی مناسب از کلید رمزگذاری کلید متقارن رمزگذاری می‌شود؛ - با کلید عمومیِ نامتقارن گیرنده رمزگذاری می‌شود؛ - با کلید ورود که به خصوص و برای مدت و دفعات فراخوانی‌های کارکرد محدود ایجادشده، رمزگذاری می‌شود؛ - مولفه‌های کلید تحت واپایش دوگانه یا چندگانه از طریق واسط امن کاروَر چنان وارد می‌شوند که حتی در صورت آگاهی کامل، هیچ مولفه‌ای، هیچ اطلاعات مفیدی از حتی یک بیت کلید رمزگذاری ارائه نمی‌دهد؛ و - کلیدهای عمومی تحت واپایش دوگانه وارد شده یا با کلیدهای مناسب رمزگذاری شده یا امضا می‌شوند تا از اعتبار آن‌ها اطمینان حاصل شود.			

shaghool.ir

shaghool.ir

پیوست چ

(الزامی)

افزاره‌هایی با قابلیت کارکردی امضای دیجیتال

چ-۱- کلیات

افزاره‌های امضای دیجیتال، امضاهای دیجیتال را برای یکپارچگی داده‌ها و اعتبار آنها تولید کرده یا این امضاها را تایید می‌کنند. در برخی موارد، با واپایش سخت‌گیرانه، ممکن است از این امضاهای دیجیتال برای انکارناپذیری[1] نیز استفاده شود. برای تولید ورودی‌ها از پیام و کلید رمزنگاری شخصی تشکیل می‌شود. برای درستی‌سنجی، ورودی‌ها از پیام و کلید رمزنگاری عمومی تشکیل شده است. در هر دو کارکرد، محاسبه درون محدوده یک افزاره رمزنگاری امن (SCD) انجام می‌شود.

کلید عمومی که برای درستی‌سنجی اعتبار امضای دیجیتال به کار برده می‌شود و همچنین داده‌هایی که توسط امضای دیجیتال محافظت شده، داده محرمانه محسوب نمی‌شوند. با این حال باید از یکپارچگی کلید عمومی اطمینان حاصل کرد.

رویه ارزشیابی افزاره تولید کلید به شرح زیر است:

- بازبینه‌های پیوست الف تکمیل شود؛
- اگر افزاره قابلیت‌های کارکردی تولید کلید را دارد، بازبینه‌های ارائه‌شده در پیوست ث تکمیل شود؛
- بازبینه‌های این پیوست تکمیل شود؛ و
- نتایج تمام مجموعه‌ها برای نهاد بازنگری ممیزی ارسال شود.

بیانیه‌های این بازبینه انطباق امنیتی لازم است توسط ممیز به عنوان «درست (T)»، «نادرست (F)» یا «کاربرد ندارد (N/A)» مشخص شود. علامت «نادرست» لزوماً نشان‌دهنده‌ی عمل غیر قابل قبول نیست بلکه باید به صورت مکتوب توضیح داده شود. بیانیه‌هایی که به صورت «کاربرد ندارد» نشان داده می‌شوند نیز باید به صورت مکتوب توضیح داده شوند.

1- non-repudiation

shaghool.ir

چ-۲- مدیریت افزاره

چ-۲-۱- ملاحظات عمومی

سازنده افزاره امنیتی و کاربر آن، یک یا چند فرد یا سازمان که از این افزاره استفاده می‌کنند الزامات زیر را تضمین کرده‌اند که نهاد بازنگری ممیزی آن را می‌پذیرد و الزامات جدول چ-۱ تکمیل شده است:

جدول چ-۱- ملاحظات عمومی

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
چ-۱	در صورتی که ادعای انکارناپذیری شود: - جفت کلید عمومی و خصوصی نامتقارن در افزاره امضای دیجیتال تولید می‌شوند؛ - کلید خصوصی نامتقارن به هیچ وجه، از جمله برای پشتیبان‌گیری یا بایگانی، به بیرون از افزاره امضای دیجیتال اصلی فرستاده نمی‌شود؛ و - سازوکارهایی برای واپایش استفاده از کلیدهای خصوصی ارائه می‌شود.			

چ-۲-۲- مدیریت افزاره برای درستی‌سنجی امضای دیجیتال

نمایندگی مستقل داخلی یا خارجی مدیریت افزاره امضای دیجیتال را ارزشیابی کرده و به نتایج جدول چ-۲ رسیده است:

جدول چ-۲- مدیریت افزاره برای درستی‌سنجی امضای دیجیتال

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
چ-۲	انقیاد[1] برای ممیزی و واپایش، میان کلید عمومی و هویت صاحب کلید خصوصی به روش‌های زیر تعیین می‌شود: - استفاده از گواهی‌های کلید عمومی وقتی گواهی کلید عمومی از یک نهاد صدور گواهی مجاز دریافت شود؛ - استفاده از گواهی‌های کلید عمومی و رویه‌های مناسب			

1 - Binding

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	مدیریت گواهی؛ یا - سازوکارهای معادل دیگر برای تعیین انکارناپذیری هویت صاحب کلید خصوصی متناظر.			
چ-۳	کارکردهای مدیریت کلید افزاره مطابق با ISO 11568 بوده و به خصوص از استفاده از کلید امضا برای مقاصد دیگر جلوگیری می‌شود.			

shaghool.ir

پیوست ح

(الزامی)

دسته‌بندی محیط‌ها

ح-۱- کلیات

محیط‌ها بر اساس ارزشیابی مخاطره که توسط پشتیبان و مطابق ISO 13491-1 انجام شده، تعیین می‌شود.

ح-۲- محیط‌های واپایش‌نشده

هیچ الزام امنیتی برای محیط‌های واپایش‌نشده وجود ندارد.

ح-۳- محیط‌های واپایش‌شده

محیط‌های واپایش‌شده مشابه اتاق‌های رایانه معمولی هستند که در آنها واپایش دسترسی وجود دارد که فقط به کارکنان مجاز اجازه دسترسی داده می‌شود. محیط واپایش شده تحت واپایش دسترسی دقیق‌تر قرار داشته و هم ورودی‌ها و هم داخل آنها در نظارت قرار دارد.

هدف از ایجاد این محیط‌های واپایش‌شده محدودکردن نوع حمله‌هایی است که ممکن است به افزاره صورت گیرد (برای مثال با غیرممکن‌کردن استفاده از انواع ویژه‌ای از تجهیزات) و کاهش زمان (برخی از انواع) حمله (به جدول ح-۱ مراجعه شود).

تمام رویه‌های امنیتی سازماندهی‌شده به‌خوبی مستند و اجرا می‌شوند. بازنگری‌های دوره‌ای این رویه‌های توسط ممیز انجام شده و نتایج ممیزی به نهاد بازنگری ممیزی ارسال می‌شود.

جدول ح-۱- محیط‌های واپایش‌شده

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ح-۴	دسترسی با قفل‌های فیزیکی و نظارت مداوم نقاط دسترسی محافظت می‌شود و تنها به کارکنان مجاز و مورداعتماد و اشخاص همراه آنها اجازه دسترسی داده می‌شود.			
ح-۵	هرگونه دسترسی افرادی غیر از کارکنان مجاز و مورداعتماد ثبت می‌شود و این اطلاعات در جای امنی نگهداری شده و به صورت دوره‌ای ممیزی می‌شود.			
ح-۶	افزاره‌ها شرایط زیر را دارند: - در تمام مدت تحت نظر دست کم دو نفر قرار دارد که دستور دارند افزاره‌ها را در مورد نشانه‌های حمله یا حضور هر شخص			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	دیگر در افزاره‌ها وارسی کنند؛ یا - در دید دوربین ویدئویی (از طریق سامانه ویدئویی امن) قرار دارد و هر X/2 دقیقه یکبار پایش می‌شود یا حرکت نزدیک به افزاره‌ها به صورت خودکار توسط افرادی که به خصوص موظف به وارسی نشانه‌های حمله به افزاره‌ها هستند تشخیص داده می‌شود. **یادآوری**- زمان «X/2 دقیقه» نصف زمان «X دقیقه» است که برای نفوذ موفقیت‌آمیز به افزاره با مقاصد زیر تخمین زده شده است تا از موارد زیر جلویری کند: - هرگونه افزودن، جایگزینی یا تغییر (برای مثال نصب اِشکال) در سخت‌افزار یا نرم‌افزار افزاره؛ یا - تعیین یا تغییر هرگونه اطلاعات حساس (برای مثال پین‌ها، کدهای دسترسی و کلیدهای رمزنگاری) و در پی آن نصب دوباره افزاره بدون نیاز به مهارت‌های تخصصی و تجهیزاتی که به طور عمومی در دسترس نیست و بدون ایجاد صدمه‌ای جدی در افزاره که با احتمال بالا تشخیص داده می‌شود. در نصب سامانه ویدئویی باید دقت شود تا اطمینان حاصل شود فرصت‌هایی برای سرک کشیدن[1] به وجود نمی‌آید.			
ح-۷	هیچ نقطه‌ای برای ورود و خروج افراد یا تجهیزات وجود ندارد که بدون نظارت مداوم نقاط دسترسی باشد، برای مثال در نظارت نگهبانانی است که وظیفه دارند از ورود و خروج تجهیزات بدون مجوز کتبی با امضای شخصی معتبر جلوگیری کنند. شخص مجوزدهنده نباید همان شخصی باشد که قصد جابجایی تجهیزات را دارد.			
ح-۸	دسترسی غیرمجاز به محیط واپایش شده یا ورود و خروج تجهیزات از کف یا سقف آن امکان‌پذیر نیست.			

ح-۴- محیط‌های که به شکل کمینه واپایش‌شده

هدف الزامات جدول ح-۲ تشخیص حمله یا دزدی در بیشینه زمان مشخص است.

1 -Shoulder surfing

shaghool.ir

جدول ح-۲- محیط‌های واپایش‌شده کمینه

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ح-۱	دسترسی مجاز به وسیله قفل‌های فیزیکی یا بر نقاط دسترسی نظارت‌شده محدود به کارکنان مجاز و افراد همراه آنها است.			
ح-۲	محیط دارای تسهیلاتی است که می‌توان افزاره‌های امنیتی را در صورت نصب چنین افزاره‌هایی با سازوکارهای چفت و بست قفل کرد.			
ح-۳	محیط واپایش‌شده کمینه تا زمانی که تمام کلیدها و دیگر داده‌های محرمانه ذخیره‌شده در افزاره‌های درون این محیط از بین نرفته یا این افزاره‌ها از آنجا خارج نشده باشند، دست‌نخورده باقی می‌ماند.			

ح-۵- محیط‌های امن

محیط امن یک لایه حفاظتی را دور افزاره نا امن به وجود می‌آورد و توصیه می‌شود به طور قابل‌ملاحظه‌ای از محیط‌های واپایش‌شده امن‌تر باشد. این محیط‌ها می‌توانند اتاق‌هایی باشند که به همین منظور طراحی و ساخته شده‌اند یا می‌توانند گاوصندوق یا محفظه‌ای امن باشد. محیط‌های امن هرچه که باشند، تنها افراد با دسترسی مجاز به افزاره‌ها باید دسترسی به محیط امن را داشته باشند. محیط‌های امن اغلب درون یک محیط واپایش شده قرار دارند. (به جدول ح-۳ مراجعه شود.)

تمام رویه‌های امنیتی سازمانی به دقت مستند و نصب می‌شود. بازنگری‌های دوره‌ای این رویه‌های توسط ممیز انجام شده و نتایج ممیزی به نهاد بازنگری ممیزی ارسال می‌شود.

جدول ح-۳- محیط‌های امن

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ح-۹	دسترسی با روش‌های زیر محدود شده است: - به وسیله قفل‌های فیزیکی و نظارت مداوم روی نقاط دسترسی؛ - با دو نفر از افراد مجاز و مورداعتماد؛ و - افرادی می‌توانند وارد شوند که دو نفر از کارکنان مجاز و مورداعتماد آنها را همراهی کنند. نقاط دسترسی که روی آنها نظارتی انجام نمی‌شود چنان قفل شده و مجهز به زنگ هشدار هستند که هرگونه ورود یا خروج نگهبانان را آگاه کند.			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
ح-۱۰	هر فرد (افراد) غیرمجازی که نیاز باشد وارد محیط امن شود باید تمام مدتی که در محیط حضور دارد در نظارت دست کم دو فرد مجاز و مورداعتماد باشد.			
ح-۱۱	تمام دسترسی‌ها به محیط امن ثبت شده و این گزارش‌ها در جای امنی نگهداری شده و به صورت دوره‌ای ممیزی می‌شود.			
ح-۱۲	تمام نقاط دسترسی ممکن به محیط امن: - همواره تحت نظر دست کم دو فرد مجاز و مورداعتماد قرار دارند که وظیفه دارند افزاره را برای یافتن نشانه‌های حمله وارسی کنند؛ یا - در دید دوربین‌های ویدئویی (از طریق یک سامانه ویدئویی) قرار دارند. این دوربین‌ها چنان در مدار قرار می‌گیرد که هرگاه حرکتی را نزدیک افزاره‌ها تشخیص دهند یا مدار تشخیص نفوذ فعال شود به صورت خودکار زنگ هشدار را به صدا در می‌آورند. حتی اگر هشداری به صدا در نیاید دوربین دست کم هر ده دقیقه یکبار پایش می‌شود. تصاویر دوربین توسط افرادی که موظف به وارسی محیط امن برای یافتن نشانه‌های حمله هستند مشاهده می‌شود.			
ح-۱۳	تمام نقاط ورود و خروج افراد و تجهیزات در نظارت مداوم نگهبانانی قرار دارد که وظیفه دارند از ورود و خروج تجهیزات بدون مجوز کتبی با امضای شخصی معتبر جلوگیری کنند. شخص مجوزدهنده نباید همان شخصی باشد که قصد جابجایی تجهیزات را دارد.			
ح-۱۴	اگر محیط امن در یک اتاق امن پیاده‌سازی شده باشد، افزاره(های) موجود در محیط امن (از طریق یک سامانه ویدئویی امن) در دید دوربین امنیتی قرار می‌گیرند. این دوربین چنان در مدار قرار می‌گیرد که هرگاه حرکتی را نزدیک افزاره‌ها تشخیص دهد یا مدار تشخیص دستکاری فعال شود به صورت خودکار زنگ هشدار را به صدا در می‌آورد. حتی اگر هشداری به صدا در نیاید دوربین دست کم هر ده دقیقه یکبار پایش می‌شود. تصاویر دوربین توسط افرادی که موظف به وارسی محیط امن برای یافتن نشانه‌های حمله هستند مشاهده می‌شود.			
ح-۱۵	محیط امن فرصت پنهان‌کاری فعالیت و انبارکردن ابزارها و تجهیزات را			

shaghool.ir

شماره	بیانیه انطباق امنیتی	درست	نادرست	کاربرد ندارد
	تا حد ممکن کاهش می‌دهد.			
ح-۱۶	محیط امن تا زمانی که تمام کلیدها و دیگر داده‌های محرمانه ذخیره‌شده در افزاره‌های درون محیط از بین نرفته یا این افزاره‌ها از آن خارج نشده باشند، به همین ترتیب باقی می‌ماند.			
ح-۱۷	افزاره به دو صورت در محیط امن قرار می‌گیرد: - افزاره و میزبان آن هر دو در این محیط امن قرار دارند و برای جلوگیری از اتصال هرگونه افزاره غیرمجاز به افزاره موردنظر و میزبان آن واپایش‌هایی صورت می‌گیرد تا اطمینان حاصل شود که حمله‌های فراگیر (به پین‌ها) با استفاده از درخواست‌های کارکردی قانونی امکان‌پذیر نیست؛ یا - افزاره چنان است که شامل سازوکارهایی امنیتی است که از حمله‌های فراگیر محافظت می‌کند.			

shaghool.ir

کتاب‌نامه

[1] ISO 9564-2, Financial services — Personal Identification Number (PIN) management and security — Part 2: Approved algorithms for PIN encipherment

[2] ISO/IEC 15408-1, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

[3] ISO/IEC 15408-2, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

[4] ISO/IEC 15408-3, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components

[5] ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules

shaghool.ir