INSO-
ISO/IEC

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

استاندارد ملی ایران

# الزامات امنیتی پودمان‌های رمزنگاشتی زیرساخت کلید عمومی(PKI)

# Security Requirements of PKI Cryptographic Modules

ICS: 35.040

**سازمان ملی استاندارد ایران**

تهران - خیابان ولیعصر، ضلع جنوبی میدان ونک، پلاک ۱۲۹۴، صندوق پستی: ۶۱۳۹-۱۴۱۵۵
تلفن: ۵-۸۸۸۷۹۴۶۱
دورنگار: ۸۸۸۸۷۰۸۰ و۸۸۸۸۷۱۰۳
کرج - شهر صنعتی، صندوق پستی ۱۶۳-۳۱۵۸۵
تلفن: ۸- ۲۸۰۶۰۳۱(۰۲۶۳) )
دورنگار: ۲۸۰۸۱۱۴ (۰۲۶۳)
پیام نگار: standard@isiri.org.ir
وب‌گاه : www.isiri.org
بخش فروش، تلفن: ۲۸۱۸۹۸۹ (۰۲۶۳) ، دورنگار: ۲۸۱۸۷۸۷ (۰۲۶۳)

**Iran National Standardization Organization**

Central Office: No.1294 Valiaser Ave. Vanak corner, Tehran, Iran
P. O. Box: 14155-6139, Tehran, Iran
Tel: +98 (21) 88879461-5
Fax: +98 (21) 88887080, 88887103

Headquarters: Standard Square, Karaj, Iran
P.O. Box: 31585-163
Tel: +98 (263) 2806031-8
Fax: +98 (263) 2808114
Email: standard @ isiri.org.ir
Website: www.isiri.org
Sales Dep.: Tel: +98(263) 2818989, Fax.: +98(263) 2818787

**به نام خدا**

## آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان*، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی 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 وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود . پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون‌های فنی 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.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1]،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی 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 نیازمندی های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه-بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سامانه‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون ( واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، کالیبراسیون ( واسنجی ) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

---

* سازمان ملی استاندارد ایران

1 - International Organization for Standardization
2 - International Electrotechnical Commission
3 - International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

## کمیسیون فنی تدوین استاندارد

## «الزامات امنیتی پودمان‌های رمزنگاشتی زیرساخت کلید عمومی(PKI)»

| **رئیس :** | **سمت و/ یا نمایندگی** |
| --- | --- |
| فیاضی، اسماعیل<br>(فوق لیسانس نرم‌افزار و حقوق) | جانشین مدیرعامل شرکت ره‌آورد سامانه‌های امن |
| **دبیر:** | |
| فلاح چای، سیدمهدی<br>(فوق لیسانس مخابرات رمز) | کارشناس مسؤول مرکز دولتی صدور گواهی الکترونیکی ریشه |
| **اعضاء** : ( اسامی به ترتیب حروف الفبا) | |
| اروجلو، آرزو<br>(فوق لیسانس مخابرات) | کارشناس تدوین استاندارد سازمان تنظیم مقررات رادیویی |
| امین مقدم، عماد<br>(فوق لیسانس مخابرات رمز) | کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه |
| بداغی، امیرحسین<br>(فوق لیسانس مهندسی برق الکترونیک) | کارشناس IT ی سازمان فناوری اطلاعات ایران |
| پوربابایی، هادی<br>(کارشناس مهندسی کامپیوتر نرم‌افزار) | مدیر طرح و برنامه شرکت خدمات انفورماتیک راهبر |
| تیمورنژاد، علی<br>(فوق لیسانس فناوری اطلاعات) | کارشناس PKI شرکت پیام پرداز |
| حسینی، ریحانه<br>(لیسانس مهندسی کامپیوتر) | کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه، دانشجوی فوق لیسانس مهندسی IT |
| راستی، رامبد<br>(لیسانس مهندسی برق الکترونیک) | نماینده سازمان نظام صنفی کمیسیون افتا و مدیرگروه امنیت شرکت گام الکترونیک |
| سبزی نژاد،محمد<br>(دکترای رمز) | کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه |
| سپهی،رضا<br>(دکترای مهندسی کامپیوتر) | مدیر تحقیق و توسعه PKI |

| | |
|---|---|
| شادمان، مهدی<br>(لیسانس مهندسی کامپیوتر) | رییس گروه شبکه و سخت افزار سازمان ثبت اسناد و املاک کشور |
| شاهی، فرید<br>(لیسانس مهندسی کامپیوتر نرم‌افزار) | سرپرست آزمایشگاه PKI ی مرکز تحقیقات صنایع انفورماتیک ایران |
| طاهری،احسان<br>(لیسانس مهندسی کامپیوتر نرم‌افزار) | کارشناس توکن کیا۳ شرکت پیام پرداز |
| عابدی، اسماعیل<br>(لیسانس مهندسی کامپیوتر) | کارشناس مرکز دولتی صدور گواهی الکترونیکی ریشه، دانشجوی فوق لیسانس مدیریت تکنولوژی |
| قورچیان، رضا<br>(فوق لیسانس IT) | کارشناس ارشد مگانفت (مرکزصدور گواهی الکترونیکی میانی نفت) |
| کریمی، داود<br>(فوق لیسانس IT) | مدیرامنیت سازمان امور مالیاتی کشور |
| گوکی، رضا<br>(لیسانس مهندسی کامپیوتر - نرم‌افزار) | کارشناس امنیت اطلاعات شرکت ره آورد سامانه های امن |
| محلوجی، نرگس<br>(لیسانس مهندسی کامپیوتر - نرم‌افزار) | کارشناس نرم‌افزار سازمان امور مالیاتی کشور |
| ناظمی، علی احسان<br>(فوق لیسانس مهندسی کامپیوتر) | مشاور اجرایی مدیرعامل شرکت داده پردازی ایران |
| هادی پور، حمیدرضا<br>(لیسانس مهندسی برق الکترونیک ) | معاون زیرساخت کلید عمومی و رئیس مرکز میانی عام |
| هایراپطیان، کارین<br>(فوق لیسانس مهندسی معماری کامپیوتر) | کارشناس PKI شرکت داده پردازی ایران |

## فهرست مندرجات

**عنوان** **صفحه**

## پیش‌گفتار

استاندارد « الزامات امنیتی پودمان‌های رمزنگاشتی زیرساخت کلید عمومی (PKI) » که پیش نویس آن در کمیسیون‌های مربوط توسط مرکز دولتی صدور گواهی الکترونیکی ایران تهیه و تدوین شده است و در سیصد و دومین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۱۳۹۲/۱۰/۲۳ مورد تصویب قرار گرفته است ، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه صنایع ، علوم و خدمات ، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود ، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین ، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد .

منابع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است :

FIPS PUB 140-2:2001, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Security Requirements for Cryptographic Modules

Smart Card Security User Group, Smart Card Protection Profile (SCSUG-SCPP), Version 3.0: 2001, Common Criteria for Information Technology Security Evaluation

**مقدمه**

در یک زیرساخت کلید عمومی(PKI)[۱]، پودمان‌های رمزنگاشتی[۲] نظیر کارت‌های هوشمند و توکن‌های USB نقش مهمی در امنیت بسترهای اطلاعاتی ایفا می‌نمایند. در این زیرساخت انجام سازوکارهای مختلف رمزنگاشتی توسط پودمان‌های رمزنگاشتی امکان‌پذیر می‌باشد. در پودمان‌های مزبور اطلاعات حساس و محرمانه کاربران نهایی از جمله کلیدهای رمزنگاشتی[۳] (به عنوان مثال کلید خصوصی امضای الکترونیکی(رقمی)) و اسم‌رمزها[۴] ذخیره می‌گردد، بنابراین باید در آن‌ها تدابیر امنیتی لازم جهت مقابله با دسترسی‌های غیرمجاز، شنود، دستکاری[۵]، حملات رمزشکنی و حملات فیزیکی مختلف اتخاذ شده باشد.

در این استاندارد، الزامات امنیتی پودمان‌های رمزنگاشتی با قابلیت PKI در چهار سطح امنیتی مختلف تعیین شده‌است؛ بدین ترتیب که هر سطح امنیتی، امنیت بالاتری را در مقایسه با سطح پایین‌تر ارائه می‌کند. در نرم‌افزارها و بسترهای اطلاعاتی مختلف با توجه به میزان حساسیت و اهمیت آن‌ها باید سطح امنیتی مناسب برای پودمان‌های رمزنگاشتی انتخاب گردد. این سطوح امنیتی متناظر است با سطوح تضمین چهارگانه زیرساخت کلید عمومی ایران است که در مستند «خط‌مشی‌های زیرساخت کلید عمومی ایران» به آن اشاره شده است. مستند مزبور از طریق وب‌گاه مرکز دولتی صدور گواهی الکترونیکی ریشه به آدرس www.rca.gov.ir منتشر شده است.

---

۱ - Public Key Infrastructure

۲ - Cryptpgraphyc Module

3 -Cryptographic Key

۴ - Password

۵ - Manipulate

# الزامات امنیتی پودمان‌های رمزنگاشتی زیرساخت کلید عمومی(PKI)

## ۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین الزامات پودمان رمزنگاشتی است که جهت امن‌سازی بسترهای اطلاعاتی به‌کار می‌رود. در پودمان رمزنگاشتی اطلاعات حساس و محرمانه کاربران نهایی نظیر کلیدهای رمزنگاشتی ذخیره و نگهداری می‌شود. همچنین انجام عملیات و سازوکارهای مختلف رمزنگاشتی توسط این پودمان‌ها امکان‌پذیر است.

پودمان‌های رمزنگاشتی ممکن است به صورت سخت‌افزاری، نرم‌افزاری یا ترکیبی از نرم‌افزار و سخت‌افزار، پیاده‌سازی شوند. الزامات امنیتی ارائه شده در این استاندارد کلیه پودمان‌های رمزنگاشتی نرم‌افزاری و سخت‌افزاری با قابلیت PKI را شامل می‌شود.

## ۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد محسوب می شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

**2-1** National Institute of Standards and Technology Communications Security Establishment:2010, Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program[CMVP]

**2-2** PKCS#11:2004, Cryptographic Token Interface Standard, Version 2.20, RSA Laboratories

## ۳ مرورکلی

در این استاندارد الزامات امنیتی برای چهار سطح امنیتی مختلف و در یازده حوزه زیر بیان شده‌است:

۱- مشخصات پودمان رمزنگاشتی
۲- درگاه‌ها[۱] و واسط‌های پودمان رمزنگاشتی
۳- نقش‌ها، خدمات و احراز هویت[۲]
۴- مدل حالت متناهی
۵- امنیت فیزیکی
۶- محیط عملیاتی
۷- مدیریت کلیدهای رمزنگاشتی
۸- تداخل/ سازگاری الکترومغناطیسی(EMC)[۳]
۹- خودآزمایی
۱۰- تضمین طراحی
۱۱- کاهش سایر حملات

سازندگان پودمان‌های رمزنگاشتی جهت دریافت درستی‌سنجی امنیتی باید متناسب با سطح امنیتی مورد نظر، الزامات این استاندارد را در مرحله تولید، توسعه و عرضه محصولات خود اعمال کنند. سپس پودمان تولید شده باید به همراه واسط‌ها و نرم‌افزارهای وابسته، به آزمایشگاه‌های ارزیابی الزامات این استاندارد ارائه شود. علاوه بر این باید مستند «خط‌مشی‌های امنیتی پودمان رمزنگاشتی» منطبق با الزامات مستندسازی که در این استاندارد آورده شده‌است، به آزمایشگاه ارائه شود.

آزمایشگاه‌های ارزیابی الزامات امنیتی باید ارزیابی خود را در حوزه‌های یازده‌گانه به‌صورت مستقل روی پودمان به عمل آورده و برای هر حوزه، سطح امنیتی پودمان را برآورد نمایند. در نهایت، سطح امنیتی کلی پودمان با توجه به سطح امنیتی اخذ شده در هر حوزه تعیین و یک درستی‌سنجی امنیتی متناسب با این سطح امنیتی برای آن صادر می‌شود.

در ادامه خلاصه‌ای از الزامات بیان شده در این استاندارد به تفکیک سطوح امنیتی چهارگانه ارائه می‌شود.

**سطح اول امنیتی**

سطح اول، پایین‌ترین سطح امنیتی می‌باشد که تعیین‌کننده الزامات امنیتی اولیه و پایه (نظیر الگوریتم‌ها و توابع مصوب[۱]) برای پودمان‌های رمزنگاشتی است. در این سطح، الزامات امنیت فیزیکی در نظر گرفته نشده و

---

۱ - Ports

۲ - Authentication

۳ - Electromagnetic Compatibility

رویه کنترل دسترسی[۲] به واحدهای اطلاعاتی حیاتی موجود در پودمان رمزنگاشتی نسبت به سایر سطوح امنیتی در سطح پایین‌تری اعمال می‌شود. این سطح امنیتی به اجزای نرم‌افزاری و ثابت‌افزاری[۳] اجازه می‌دهد تا در سامانه‌های محاسباتی همه منظوره که دارای حساسیت امنیتی کمتری هستند یا جایی که صرف هزینه کمتر، از اولویت بالاتری برخوردار است، انتخاب گردد.

**سطح دوم امنیتی**

در سطح دوم امنیتی باید علاوه بر الزامات تعیین شده در سطح اول، الزامات امنیت فیزیکی از قبیل قابلیت آشکارساز نفوذ[۴] و پشتیبانی از سازوکار احراز هویت نقش‌محور[۵] نیز در پودمان‌های رمزنگاشتی اعمال گردد.

آشکارساز نفوذ می‌تواند به واسطه استفاده از پوشش‌های[۶] نشان‌دهنده دستکاری، مهر و موم یا قفل برروی روکش قابل برداشت پودمان اعمال گردد. این پوشش‌ها باید به گونه‌ای طراحی شده باشند که دسترسی فیزیکی به کلیدها و واحدهای اطلاعاتی حیاتی، مستلزم برداشتن آن‌ها باشد.

در سطح دوم امنیتی به طورکمینه باید احراز هویت نقش‌محور در پودمان رمزنگاشتی پشتیبانی گردد، به این ترتیب که مجوز کاربر نهایی بر اساس نقش وی (به عنوان مثال کاربر نهایی یا متصدی رمز[۷]) بررسی شده و خدمات و دسترسی‌های متناظر با آن نقش، به کاربر نهایی اعطا گردد.

**سطح سوم امنیتی**

در سطح سوم امنیتی علاوه بر سازوکارهای امنیتی آشکارساز نفوذ بیان شده در سطح دوم، الزامات امنیتی دیگری نیز در نظر گرفته شده که قدرت تشخیص یا واکنش به یک دسترسی فیزیکی - به منظور دسترسی، استفاده یا تغییر در واحدهای اطلاعاتی حیاتی در پودمان رمزنگاشتی - را داشته باشند. سازوکارهای امنیت فیزیکی، ممکن است شامل استفاده از یک محفظه[۸] سخت و مدارهای تشخیص و واکنش به نفوذ باشد که در صورت بازشدن روکش یا در پودمان رمزنگاشتی، کلیدها و کلیه واحدهای اطلاعاتی حیاتی رمز نشده را امحاء[۹] کند.

---

۱- در این استاندارد منظور از الگوریتم‌ها و توابع مصوب، الگوریتم‌های رمزنگاشتی مورد تایید در استاندارد ملی «الزامات الگوریتم‌های رمزنگاشتی در زیرساخت کلید عمومی ایران» به شماره .... می‌باشد.

2 - Access Control
3 - Firmware
4 - Tamper evidence
5 - Role-base Authentication
6 - Coating
7 - Crypto Officer
8 - Enclosure
9 - Zeroization

در این سطح علاوه بر احراز هویت نقش‌محور، احراز هویت هویت‌محور[1] نیز جهت اعمال کنترل دسترسی لازم است؛ به این ترتیب که پودمان رمزنگاشتی ابتدا کاربر نهایی را احراز هویت کرده و سپس بررسی می‌کند که آیا کاربر نهایی هویت‌شناسی شده، می‌تواند مجوز یک نقش خاص را دریافت کرده و به خدمات متناظر با آن نقش دسترسی داشته باشد.

سطح سوم امنیت نیازمند برونداد و درونداد واحدهای اطلاعاتی حیاتی رمز نشده[2] (ازجمله آن‌هایی که با استفاده از رویه‌های تقسیم دانش[3] وارد یا خارج می‌شوند) با استفاده از درگاه‌هایی که به‌صورت فیزیکی از هم جدا هستند یا واسط‌هایی که به‌صورت منطقی با استفاده از مسیرهای امن از یکدیگر جدا شده‌اند، می‌باشد. همچنین واحدهای اطلاعاتی حیاتی یا کلیدهای رمزنگاشتی می‌توانند به‌صورت رمزشده به پودمان وارد یا از آن خارج شوند.

**سطح چهارم امنیتی**

سطح چهارم امنیتی، بالاترین سطح از امنیت که در این استاندارد تعریف شده‌است را فراهم می‌کند. در این سطح، سازوکارهای امنیت فیزیکی طیف وسیعی از حفاظت‌های پودمان رمزنگاشتی را به همراه روش‌های تشخیص و واکنش به همه دسترسی‌های غیرمجاز فراهم می‌کنند. هر نوع دستکاری پودمان رمزنگاشتی، به احتمال خیلی بالا منجر به تشخیص و امحای واحدهای اطلاعاتی حیاتی رمز نشده خواهد شد. پودمان‌های رمزنگاشتی دارای سطح امنیتی چهار برای به کارگیری در محیط‌هایی که محافظت فیزیکی در آن‌ها وجود ندارد، مفید هستند. همچنین در سطح چهارم امنیتی، یک پودمان رمزنگاشتی در برابر شرایط محیطی نظیر نوسانات ولتاژ یا تغییر درجه حرارت نیز باید محافظت شود.

## ۴ اهداف توابع امنیتی

الزامات امنیتی مشروح در این استاندارد مربوط به طراحی و پیاده‌سازی امن پودمان‌های رمزنگاشتی می‌باشد. این الزامات از اهداف امنیتی سطح بالای ذیل برای یک پودمان رمزنگاشتی استخراج می‌شوند:

- به‌کارگیری و پیاده‌سازی صحیح توابع امنیتی مصوب جهت محافظت از اطلاعات حساس
- محافظت پودمان رمزنگاشتی در مقابل استفاده یا انجام عملیات غیرمجاز
- جلوگیری از دسترسی غیرمجاز به محتویات پودمان رمزنگاشتی شامل کلیدهای رمزنگاشتی رمز نشده

1 - Identity -base Authentication
2 - Plain text
3 - Split knowledge procedures

- جلوگیری از تغییر غیرمجاز و تشخیص داده نشده پودمان رمزنگاشتی و الگوریتم‌های رمزنگاشتی، شامل تغییر، جایگزینی، درج و حذف غیرمجاز کلیدهای رمزنگاشتی و پارامترهای امنیتی حیاتی(CSP)[1]
- فراهم‌کردن نشانگرهایی[2] جهت اعلام وضعیت عملیاتی پودمان رمزنگاشتی
- اطمینان از عملکرد درست پودمان رمزنگاشتی در حالت عملیاتی مصوب
- آشکارسازی خطاها در عملیات صورت‌گرفته توسط یک پودمان رمزنگاشتی و جلوگیری از افشای اطلاعات حساس و محرمانه در اثر بروز این خطاها

## ۵ الزامات امنیتی

در این بخش الزامات امنیتی که طبق این استاندارد، پودمان‌های رمزنگاشتی ملزم به پیروی از آن‌ها هستند، آورده شده‌است. این الزامات امنیتی حوزه‌های مختلف مربوط به طراحی و پیاده‌سازی پودمان‌های رمزنگاشتی را پوشش می‌دهد. این بخش‌ها عبارتند از: مشخصات پودمان رمزنگاشتی، درگاه‌ها و واسط‌های پودمان رمزنگاشتی، نقش‌ها، خدمات و احراز هویت، مدل‌های حالت، امنیت فیزیکی، محیط عملیاتی، مدیریت کلیدهای رمزنگاشتی، تداخل و یا سازگاری الکترومغناطیسی، خودآزمایی و ضمانت طراحی و کاهش سایر حملات.

در جدول ۱ خلاصه الزامات امنیتی پودمان‌های رمزنگاشتی در بخش‌ها و حوزه‌های نام برده شده، آورده شده‌است.

---

۱ - Critical Security Parameters

2 - Indicator

**جدول ۱- چکیده الزامات امنیتی**

| سطح امنیتی / حوزه امنیتی | سطح اول | سطح دوم | سطح سوم | سطح چهارم |
|---|---|---|---|---|
| **مشخصات پودمان رمزنگاشتی** | • مشخصات و معماری اجزای مختلف پودمان رمزنگاشتی شامل سخت‌افزار، نرم‌افزار، ثابت‌افزار و ارتباطات آن‌ها<br>• الگوریتم‌های مصوب<br>• حالت‌های عملیاتی مصوب<br>• دستورالعمل خط‌مشی امنیتی | | | |
| **درگاه‌ها و واسط‌های پودمان رمزنگاشتی** | • واسط‌های الزامی و اختیاری<br>• توصیف همه واسط‌ها و همه مسیرهای درونداد و برونداد داده | | درگاه‌های داده برای واحدهای اطلاعاتی حیاتی محافظت نشده به صورت منطقی یا فیزیکی از سایر درگاه‌ها جدا شده‌اند. | |
| **نقش‌ها، خدمات و احراز هویت** | تفکیک منطقی نقش‌ها و خدمات الزامی و اختیاری. | احراز هویت کاربر به‌صورت نقش‌محور یا هویت‌محور. | احراز هویت کاربر به‌صورت هویت‌محور. | |
| **مدل حالت متناهی** | • توصیف مدل حالت متناهی<br>• حالت‌های الزامی و حالت‌های اختیاری<br>• نمودار انتقال حالت و مشخص‌نمودن چگونگی انتقال از یک حالت به حالت دیگر | | | |
| **امنیت فیزیکی** | استفاده از تجهیزات درجه-تولیدی | قفل‌ها یا آشکارساز نفوذ | تشخیص و واکنش به دستکاری برای درپوش‌ها[آ] و درب‌ها | • تشخیص و واکنش به دستکاری پوسته[ب].حفاظت در برابر شکست‌های محیطی[پ] و آزمون شکست‌های محیطی[ت]. |

**ادامه جدول ۱- چکیده الزامات امنیتی**

| سطح امنیتی / حوزه امنیتی | سطح اول | سطح دوم | سطح سوم | سطح چهارم |
|---|---|---|---|---|
| **محیط عملیاتی** | • تک‌کاربر<br>• کد قابل اجرا<br>• فن‌های یکپارچه‌سازی مصوب | رخنمون‌های حفاظتی[ث] مرجع که در استاندارد سطح دوم ارزیابی کیفیت (EAL2)[ج] ارزیابی شده‌اند به همراه سازوکارها و ممیزی کنترل دسترسی احتیاطی توصیف شده | • رخنمون‌های حفاظتی مرجع<br>• مسیرهای مطمئن ارزیابی شده در استاندارد سطح سوم ارزیابی کیفیت (EAL3)<br>• مدل‌سازی خط و مشی امنیتی | • رخنمون‌های حفاظتی مرجع<br>• مسیرهای مطمئن ارزیابی شده در استاندارد سطح چهارم ارزیابی کیفیت (EAL4) |
| **مدیریت کلیدهای رمزنگاشتی** | سازوکارهای مدیریت کلید شامل: تولید کلید[چ]، برقراری کلید[ح]، توزیع کلید، درونداد و برونداد کلید، ذخیره‌سازی کلید و امحاء کلید | | | |
| | کلیدهای خصوصی و مخفی که به روش‌های دستی استقرار یافته‌اند، ممکن‌است به‌صورت متن آشکار وارد یا خارج شوند. | | کلیدهای خصوصی و مخفی که به روش‌های دستی استقراریافته‌اند، باید به‌صورت رمزشده یا با استفاده از رویه‌های تقطیع دانش، وارد یا خارج شوند. | |
| **تداخل/ سازگاری الکترومغناطیسی** | به<br>47 CFR FCC Part 15. Subpart B, Class A (Business use)<br>Applicable FCC requirements (for radio)<br>مراجعه شود | | به<br>47 CFR FCC Part 15. Subpart B, Class B (Home use)<br>مراجعه شود | |
| **خودآزمایی** | آزمون‌های آغازین شامل[خ]: آزمون‌های الگوریتم رمزنگاشتی، آزمون یکپارچگی و یکپارچگی[د] نرم‌افزار یا ثابت‌افزارها، آزمون توابع حیاتی، آزمون‌های شرایطی. | | | |

**ادامه جدول ۱- چکیده الزامات امنیتی**

| سطح امنیتی / حوزه امنیتی | سطح اول | سطح دوم | سطح سوم | سطح چهارم |
|---|---|---|---|---|
| **ضمانت طراحی** | • مدیریت پیکربندی[ذ]<br>• نصب و تولید امن<br>• طرح و خط و مشی مرتبط<br>• مستندات راهنما | • سامانه مدیریت پیکربندی<br>• توزیع امن<br>• توصیف کارکردی | پیاده‌سازی به زبان سطح بالا | • مدل‌های رسمی<br>• توضیحات جزئی (اثبات-های غیر رسمی)<br>• پیش‌شرط‌ها و پس‌شرط‌ها |
| **کاهش سایر حملات** | توصیفی از اقدامات کاهش‌دهنده آسیب در برابر حملاتی که در این استاندارد الزاماتی برای آن‌ها ارائه نشده است. | | | |

آ Cover

ب Envelope

پ Environmental Failure Protection (EFP)

ت Environmental Failure Testing (EFT)

ث Protection Profiles

ج Evaluation Assurance Level

چ Key Establishment

ح Key Distribution

خ Power Test

د Integrity

ذ Configuration Management (CM)

### ۱-۵ مشخصات پودمان رمزنگاشتی

یک پودمان رمزنگاشتی مجموعه‌ای شامل سخت‌افزار، نرم‌افزار، ثابت‌افزار یا ترکیبی از آن‌ها می‌تواند باشد که برای پیاده‌سازی فرایندها یا توابع رمزنگاشتی (شامل الگوریتم‌های رمزنگاشتی و به طور اختیاری، الگوریتم‌های تولید کلید) در یک محدوده رمزنگاری تعریف شده به‌کار می‌رود. یک پودمان رمزنگاشتی در صورت پشتیبانی از الگوریتم‌های رمزنگاشتی متقارن، الگوریتم‌های رمزنگاشتی نامتقارن، توابع چکیده‌ساز[1] و مولدهای اعداد تصادفی، در حالت عملیاتی مصوب، باید به‌طورکمینه از یک تابع یا الگوریتم امنیتی مصوب و مورد تایید در هریک از محورهای نام برده شده استفاده کند.لازم به ذکر است که در پودمان‌های موضوع این استاندارد کمینه پشتیبانی از یک الگوریتم نامتقارن، تابع چکیده ساز و مولد اعداد تصادفی مصوب الزامی می‌باشد.

پشتیبانی الگوریتم‌های رمزنگاشتی غیرمصوب نیز می‌توانند در حالت عملیاتی غیرمصوب[2] مورد استفاده قرار گیرند. در پودمان رمزنگاشتی باید قابلیت انتخاب توابع و الگوریتم‌های مصوب توسط کاربر نهایی وجود داشته باشد. درخصوص سطوح امنیتی یک و دو، زمان عملکرد پودمان رمزنگاشتی در حالت عملیاتی مصوب را در مستند خط‌مشی امنیتی پودمان می‌توان تعیین کرد. اما برای سطوح امنیتی سه و چهار، عملکرد پودمان در یک حالت عملیاتی مصوب، باید توسط پودمان رمزنگاشتی نشان داده شود (به عبارتی، پودمان باید دارای نشان‌گر وضعیت حالت عملیاتی مصوب داشته باشد).

اگر پودمان رمزنگاشتی متشکل از اجزای نرم‌افزاری یا ثابت‌افزاری باشد، حاوی پردازنده‌ها و اجزای نرم‌افزاری خواهد بود که از اجزای نرم‌افزار و ثابت‌افزار نگهداری می‌کنند. به طور مثال پودمان رمزنگاشتی ممکن است به سه حالت زیر وجود داشته باشد:

۱- به‌صورت نرم‌افزاری باشد و در داخل یک رایانه شخصی اجرا شود.

۲- به‌صورت سخت‌افزاری باشد و کلیه سازوکارهای سخت‌افزاری را به‌صورت مستقل اجرا کند.

۳- به‌صورت سخت‌افزاری تولید شود و برخی سازوکارها را به‌صورت سخت‌افزاری و برخی دیگر را به‌صورت نرم‌افزاری و در داخل یک رایانه شخصی که به آن متصل شده‌است اجرا کند.

الزامات قید شده در این استاندارد باید برای همه سخت افزارها، نرم‌افزارها و ثابت افزارهای خاص امنیت موجود در پودمان رمزنگاشتی اعمال شود. الزامات هر یک از سه جزء سخت‌افزار، نرم‌افزار یا ثابت‌افزار که بر روی پودمان امنیتی تاثیری ندارند، شامل این استاندارد نخواهند شد. این الزامات در مورد ریزکدها[3] و

1 - Hash Function
2 - Non Approved Mode of Operation
3 - Microcode

نرم‌افزارهای سامانه‌ای که کد منبع آن‌ها در دسترس سازنده نمی‌باشد یا در مورد هر یک از اجزای پودمان رمزنگاشتی که ارتباطی با امنیت ندارند، اعمال نمی‌گردد.

- مستندسازی باید مشخصات اجزای مختلف پودمان رمزنگاشتی شامل سخت‌افزار، نرم‌افزار و ثابت‌افزار را توصیف و محدوده رمزنگاری احاطه کننده این اجزا را تعیین کند. پیکربندی فیزیکی پودمان رمزنگاشتی نیز باید در مستند شرح داده شود؛

- در مستندسازی باید هر بخش از سخت‌افزار، نرم‌افزار و ثابت‌افزار پودمان رمزنگاشتی که از اعمال الزامات این استاندارد مستثنی شده است با ذکر دلایل تعیین گردد؛

- در مستندسازی باید درگاه‌های فیزیکی، واسط‌های منطقی و کلیه مسیرهای درونداد و برونداد اطلاعات در پودمان رمزنگاشتی مشخص گردد؛

- در مستندسازی باید کنترل‌های دستی یا منطقی پودمان رمزنگاشتی، شاخص‌های وضعیت فیزیکی و منطقی و خصوصیات کاربردپذیر فیزیکی، منطقی و الکتریکی معرفی گردند.

- در مستندسازی کلیه توابع امنیتی مصوب و غیرمصوب توسط این استاندارد که در پودمان رمزنگاشتی به کار گرفته می‌شوند و حالت‌های عملیاتی مصوب و غیرمصوب، باید معرفی شوند؛

- مستندسازی باید شامل نمودار بستک[۱] نمایش‌دهنده تمامی اجزای سخت‌افزاری اصلی پودمان رمزنگاشتی و ارتباط آن‌ها شامل تمامی پردازنده‌ها، میانگیرهای[۲] درونداد و برونداد، میانگیرهای متن اصلی/متن رمزی، میانگیرهای کنترلی، مخزن کلید، حافظه کاری و حافظه برنامه باشد. همچنین مستندسازی باید شامل طرح فنی اجزای سخت‌افزاری، نرم‌افزاری و ثابت‌افزاری باشد. باید برای مستند کردن طرح، زبان‌های توصیفی سطح بالا برای نرم‌افزار/ثابت افزار یا الگو واره‌ها برای سخت افزار مورد استفاده قرار گیرند ؛

- در مستندسازی باید کلیه اطلاعات مرتبط با امنیت، شامل کلیدهای رمزنگاشتی مخفی و خصوصی(هم آشکار و هم رمزشده)، داده احراز هویت (مثل اسم‌رمزها یا شماره شناسایی(Pin)[۳])، واحدهای اطلاعاتی حیاتی و سایر اطلاعات محافظت شده (مانند رویدادهای ممیزی‌شده و داده ممیزی) که آشکار شدن یا دستکاری آن‌ها می‌تواند امنیت پودمان رمزنگاشتی را به خطر اندازد، تعیین شود؛

---

۱ - Block Diagram

۲ -Buffers

۳ - Personal Identification Name

- مستندسازی باید خط‌مشی امنیتی پودمان رمزنگاشتی را تعیین کند. این خط‌مشی امنیتی[1] باید شامل قواعد مشتق از الزامات تعیین شده در این استاندارد و قواعد مشتق از الزامات تکمیلی در نظر گرفته شده توسط سازنده باشد. الزامات مربوط به مستند خط‌مشی امنیتی پودمان رمزنگاشتی در پیوست آورده شده است.

### ۵-۲ درگاه‌ها و واسط‌های پودمان رمزنگاشتی

یک پودمان رمزنگاشتی باید کلیه جریان‌های اطلاعاتی و نقاط دسترسی فیزیکی را به درگاه‌های فیزیکی و واسط‌های منطقی درونداد و برونداد، محدود کند. واسط‌های پودمان رمزنگاشتی باید به‌صورت منطقی از یکدیگر مجزا باشند. هرچند، ممکن است یک درگاه فیزیکی را به اشتراک گذارند (به طور مثال، داده‌های درونداد و داده‌های برونداد ممکن است از درگاه مشابهی استفاده کنند) یا ممکن است روی یک یا چند درگاه فیزیکی توزیع شوند (به طور مثال، داده‌های درونداد ممکن است هم از طریق درگاه ترتیبی و هم از طریق درگاه موازی وارد شوند). واسط برنامه‌نویسی برنامه کاربردی(API)[2] مربوط به جزء نرم‌افزاری یک پودمان رمزنگاشتی، ممکن است به عنوان یک یا چند واسط منطقی تعریف شود. یک پودمان رمزنگاشتی باید این چهار واسط منطقی را داشته باشد («درونداد» و «برونداد» از زاویه دید پودمان تعیین می‌شوند):

#### ۵-۲-۱ واسط درونداد داده[3]

همه داده‌های درونداد (به جز داده‌های کنترلی که از طریق واسط دروندادهای کنترلی وارد می‌شوند)که به پودمان رمزنگاشتی وارد یا توسط پودمان رمزنگاشتی پردازش می‌شوند (شامل داده‌های متن آشکار، داده‌های رمزشده، کلیدهای رمزنگاشتی و سایر واحدهای اطلاعاتی حیاتی، داده‌های احراز هویت و اطلاعات اعلان وضعیت از طرف پودمان دیگر) باید از طریق واسط «درونداد داده« وارد شوند.

#### ۵-۲-۲ واسط برونداد داده[4]

همه داده‌های برونداد ( به جز داده‌های وضعیت که از طریق واسط برونداد وضعیت خارج می‌شوند) که از پودمان رمزنگاشتی خارج می‌شوند (شامل داده‌های متن آشکار، داده‌های رمزشده، کلیدهای رمزنگاشتی، واحدهای اطلاعاتی حیاتی، داده‌های احراز هویت و اطلاعات کنترلی برای پودمان دیگر) باید از طریق واسط « برونداد داده« خارج شوند. در هنگام بروز خطا و در حین خودآزمایی (طبق ۵-۹) باید از برونداد داده‌ها از طریق واسط برونداد داده جلوگیری کرد.

1 - Security Policy
2 - Application Programming Interface
3 - Input Data Interface
4 - Output Data Interface

### ۵-۲-۳ واسط درونداد کنترلی[1]

کلیه دستورات درونداد، سیگنال‌ها و داده‌های کنترلی (شامل فراخوانی توابع و کنترل‌های دسترسی نظیر سوده‌ها[2]، دکمه‌ها و صفحه‌کلیدها) که جهت کنترل عملیات پودمان رمزنگاشتی به کار می‌روند، باید از طریق واسط « درونداد کنترلی» وارد شوند.

### ۵-۲-۴ واسط برونداد وضعیت[3]

همه سیگنال‌های برونداد ، نشانگرها و داده‌های وضعیتی (شامل مقادیر بازگشتی و نشانگرهای فیزیکی نظیر دیودهای نوری و صفحه‌های نمایش) که جهت نشان دادن وضعیت پودمان رمزنگاشتی به کار می‌روند، باید از طریق واسط « برونداد وضعیت» خارج شوند.

تمام انرژی الکتریکی خارجی که به پودمان رمزنگاشتی وارد می‌شود (شامل انرژی تامین شده از منابع خارجی یا باتری‌ها) باید از طریق درگاه انرژی وارد شود. هنگامی که تمام انرژی مورد نیاز در درون محدوده رمزنگاری پودمان رمزنگاشتی تامین یا محافظت می‌شود (برای مثال یک باتری داخلی)، دیگر نیازی به یک درگاه انرژی نیست.

پودمان رمزنگاشتی باید در درونداد، بین داده درونداد و درونداد کنترلی و در برونداد، بین داده برونداد و برونداد وضعیت تمایز قائل شود. کلیه داده‌های درونداد به پودمان رمزنگاشتی از طریق واسط «درونداد داده» باید فقط از مسیر داده درونداد عبور کنند. کلیه داده‌های برونداد از پودمان از طریق واسط « برونداد داده» باید فقط از مسیرداده برونداد عبور کنند. در هنگام اجرای عملیات تولید کلید، وارد کردن دستی کلید و امحاء کلید، مسیر داده برونداد باید به صورت منطقی از مدارات الکتریکی و فرایندها قطع شده باشد. به منظور جلوگیری از برونداد غیر عمدی و ناخواسته اطلاعات حساس، دو فرایند داخلی مستقل باید لازم باشد تا داده را از طریق هر واسط برونداد که بر روی آن کلیدهای رمزنگاشتی، واحدهای اطلاعات حیاتی یا داده-های حساس رمز نشده خارج می‌شوند، خارج کند (به طور مثال دو پرچم[4] نرم‌افزاری متفاوت تنظیم شود که یکی از آن‌ها توسط کاربر مقداردهی می‌شود و یا دو مدخل سخت‌افزاری که به‌صورت پیوسته از دو رفتار مجزا تنظیم شوند).

### ۵-۲-۵ الزامات درگاه‌ها و واسط‌های پودمان رمزنگاشتی برای سطوح امنیتی اول و دوم

برای سطوح اول و دوم، درگاه‌های فیزیکی و واسط‌های منطقی که برای درونداد و برونداد مواردی نظیر کلیدهای رمزنگاشتی ، اجزای کلید رمزنگاشتی، داده‌های احراز هویت و واحدهای اطلاعاتی حیاتی رمز نشده

1 - Control Input Interface
۲ - Switch
3 - Status Output Interface
4 - Flag

به کار می‌روند، ممکن است به‌صورت فیزیکی و منطقی با درگاه‌ها و واسط‌های دیگر پودمان رمزنگاشتی به اشتراک‌گذاشته شوند.

### ۵-۲-۶ الزامات درگاه ها و واسط‌های پودمان رمزنگاشتی برای سطوح امنیتی سوم و چهارم

برای سطوح سوم و چهارم:

- درگاه(های) فیزیکی مورد استفاده برای درونداد و برونداد اجزای کلید، داده‌های احراز هویت و واحدهای اطلاعاتی حیاتی رمز نشده، باید به‌صورت فیزیکی از سایر درگاه‌های پودمان رمزنگاشتی جدا باشند.

یا

- واسط‌های منطقی استفاده شده برای درونداد و برونداد اجزای کلید، داده‌های احراز هویت و واحدهای اطلاعاتی حیاتی رمز نشده، باید به‌صورت منطقی از سایر واسط‌های استفاده کننده از یک مسیر مورد اعتماد جدا باشد.

و

- اجزای کلید، داده‌های احراز هویت و سایر واحدهای اطلاعاتی حیاتی رمز نشده باید به‌صورت مستقیم وارد پودمان رمزنگاشتی شوند (به طور مثال از طریق یک مسیر مورد اعتماد یا یک کابل متصل). (به زیربند ۵-۷-۴ مراجعه شود).

## ۵-۳ نقش‌ها، خدمات و احراز هویت

یک پودمان رمزنگاشتی باید نقش‌های مجاز برای کاربران [۱] و خدمات متناظر را در هر نقش پشتیبانی کند. یک کاربر می‌تواند چندین نقش را اتخاذ کند. در صورتی که پودمان رمزنگاشتی از کاربران همزمان پشتیبانی کند، پودمان رمزنگاشتی باید به‌صورت داخلی بین نقش‌ها و خدمات مرتبط با کاربران مختلف تفکیک ایجاد کند. یک کاربر برای اجرای خدماتی که در آن‌ها کلیدهای رمزنگاشتی و واحدهای اطلاعاتی حیاتی دچار تغییر، جایگزینی یا دستکاری نمی‌شوند، (برای مثال نمایش وضعیت، خودآزمایی یا سایر خدماتی که بر روی امنیت پودمان اثرگذار نیستند) نیازی به اتخاذ یک نقش مجاز ندارد.

ممکن است در یک پودمان رمزنگاشتی، سازوکارهای احراز هویت مورد نیاز باشند، که به منظور درستی‌سنجی دسترسی یک کاربر نهایی به پودمان و بررسی اینکه آیا کاربر مجاز است نقش درخواستی را به عهده گرفته و خدمت‌های موجود در آن نقش را اجرا کند، مورد استفاده قرار می‌گیرند.

### ۵-۳-۱ نقش‌ها

یک پودمان رمزنگاشتی باید نقش‌های مجاز[۲] زیر را برای کاربران پشتیبانی کند:

---

۱ - Operators

2 - Authorized roles

۱- نقش کاربر نهایی[1]: این نقش به منظور اجرای خدمت‌های امنیتی عمومی از قبیل عملیات رمزنگاشتی و سایر توابع امنیتی مصوب تعریف می‌شود.

۲- نقش متصدی رمز[2]: این نقش به منظور اجرای مقدار دهی اولیه یا توابع مدیریتی (به عنوان مثال، مقدار دهی اولیه پودمان، درونداد/برونداد کلیدهای رمزنگاشتی و واحدهای اطلاعات حیاتی و ...) تعریف می‌شود. در صورتی که پودمان رمزنگاشتی به متصدیان اجازه اجرای خدمات تعمیر و نگهداری را بدهد، آنگاه پودمان باید نقش مجاز زیر را پشتیبانی کند:

۳- نقش تعمیرکننده و نگهداری کننده[3]: این نقش به منظور تعمیر و نگهداری فیزیکی و/یا اجرای خدمات منطقی (مانند عیب‌یابی سخت‌افزاری/ نرم‌افزاری) تعریف می‌شود. همه کلیدهای خصوصی و مخفی رمز نشده و واحدهای اطلاعاتی حیاتی محافظت نشده، در هنگام درونداد یا برونداد نقش تعمیر و نگهداری، باید امحاء شوند.

یک پودمان رمزنگاشتی علاوه بر نقش‌های فوق ممکن است نقش‌ها یا زیرنقش‌های دیگری را نیز پشتیبانی کند.

مستندسازی باید تمام نقش‌های مجاز پشتیبانی شده توسط پودمان رمزنگاشتی را تعیین کند.

### ۵-۳-۲ خدمات

خدمات به کلیه عملیات یا توابعی که می‌تواند توسط یک پودمان رمزنگاشتی اجرا شود، اتلاق می‌شود. درونداد‌های خدمت[4] باید در بر گیرنده تمام درونداد‌های داده یا کنترلی پودمان رمزنگاشتی باشد که خدمت-ها، عملیات یا توابع خاصی را راه اندازی یا کسب می‌کنند. برونداد‌های خدمت[5]، باید شامل کلیه داده‌ها و وضعیت‌های برونداد باشد که نتیجه اجرای خدمات، عملیات یا توابع راه اندازی شده یا بدست آماده توسط درونداد‌های خدمت هستند. هر درونداد خدمت باید همراه با یک برونداد خدمت باشد.

یک پودمان رمزنگاشتی باید خدمات زیر را برای متصدیان فراهم کند:

۱- نمایش وضعیت: اعلان وضعیت فعلی پودمان رمزنگاشتی

۲- اجرای خودآزمایی‌ها: آماده‌سازی و اجرای خودآزمایی‌ها بر اساس توضیحات زیربند ۵-۹.

۳- اجرای توابع امنیتی مصوب: اجرای کمینه یک تابع امنیتی مصوب به کار رفته در یک حالت عملیاتی مصوب در هر یک از الگوریتم‌ها و توابع رمزنگاشتی که در زیربند ۵-۱ تعین شده است.

---

1 - User Role
2 - Crypto Officer
3 - Maintenance Role
4 - Service inputs
5 - Service outputs

یک پودمان رمزنگاشتی ممکن‌است علاوه بر خدمات شرح داده شده در بالا خدمات، عملیات یا توابع دیگری - چه مصوب و چه غیرمصوب – را نیز فراهم کند. خدماتی خاص ممکن است برای بیش از یک نقش فراهم باشند (به طور مثال خدماتی درونداد کلید ممکن است در نقش کاربر و نقش متصدی رمز فراهم باشند.

اگر در یک پودمان رمزنگاشتی، قابلیت کنارگذار[1] به منظور ارائه خدمات مختلف بدون پردازش رمزنگاشتی (مانند انتقال متن آشکار از طریق پودمان، بدون رمزبندی) وجود داشته باشد، آنگاه:

- به منظور جلوگیری از کنارگذار غیرعمدی داده رمز نشده در اثر خطای سیگنال، دو عمل داخلی مستقل جهت فعال‌سازی قابلیت کنارگذار باید مورد نیاز باشد (مانند دو پرچم نرم‌افزاری یا سخت‌افزاری متفاوت که یکی از آن‌ها ممکن است توسط کاربر مقداردهی شده باشد).

- نشانگر وضعیت پودمان باید به منظور مشخص نمودن موارد زیر، اعلان داشته باشد:
  - قابلیت کنارگذار فعال نشده و پودمان فقط خدمات را با پردازش رمزنگاشتی ارائه می‌دهد ( متن آشکار رمزشده‌است).
  - قابلیت کنارگذار فعال شده و پودمان خدمات را بدون پردازش رمزنگاشتی ارائه می‌دهد (متن آشکار رمزشده نیست).
  - قابلیت کنارگذار به‌صورت متناوب فعال و غیرفعال می‌شود و پودمان برخی خدمات را با پردازش رمزنگاشتی و برخی خدمات را بدون پردازش رمزنگاشتی ارائه می‌دهد (برای مثال، برای پودمان‌های دارای چند کانال ارتباطی، متن آشکار رمز شده یا نشده به پیکربندی هر کانال بستگی دارد).

مستندسازی باید موارد زیر را مشخص کند:

- کلیه خدمات، عملیات یا توابع مصوب و غیرمصوب که توسط پودمان رمزنگاشتی فراهم شده‌اند.

- برای هر خدمت ارائه شده توسط پودمان، درونداد‌های خدمت، برونداد‌های خدمت متناظر و نقش‌های مجاز که در آن‌ها خدمت می‌تواند اجرا شود.

- هر خدمت ارائه شده توسط پودمان رمزنگاشتی که برای آن، کاربر نیازمند به عهده گرفتن یک نقش مجاز نیست و اینکه این خدمت‌ها چگونه کلیدهای رمزنگاشتی یا واحدهای اطلاعاتی حیاتی را دچار تغییر، افشا یا جابجایی نمی‌کنند، یا در غیر این صورت چگونه بر امنیت پودمان تاثیر می‌گذارند.

### ۵-۳-۳ احراز هویت کاربر

سازوکارهای احراز هویت در یک پودمان رمزنگاشتی برای احراز هویت کاربر جهت دسترسی به پودمان و بررسی اینکه آیا این کاربر مجاز است یک نقش درخواستی را به عهده گیرد و خدمت‌های موجود در آن را اجرا کند، مورد نیاز می‌باشد. بسته به سطح امنیتی و به منظور کنترل دسترسی به پودمان، به طور کمینه یکی از سازوکارهای زیر باید توسط پودمان رمزنگاشتی پشتیبانی شود:

1 - Bypass

۱- احراز هویت «نقش‌محور»: اگر سازوکار احراز هویت «نقش محور» توسط یک پودمان رمزنگاشتی پشتیبانی شود، پودمان باید دارای امکان انتخاب ضمنی یا صریح یک یا چند نقش توسط کاربر و احراز هویت این نقش یا نقش‌های انتخابی باشد. در این روش احراز هویت شناسه شخصی کاربر در پودمان رمزنگاشتی مورد نیاز نیست. در یک پودمان رمزنگاشتی ممکن است قابلیت انتخاب نقش‌ها و انجام عملیات احراز هویت روی نقش‌های انتخابی با یکدیگر ترکیب شوند. اگر پودمان رمزنگاشتی به کاربر اجازه تغییر نقش‌ها را بدهد، آنگاه انجام عملیات احراز هویت روی نقشی که از قبل احراز هویت نشده باشد، لازم است.

۲- احراز هویت «هویت‌محور»: اگر سازوکار احراز هویت «هویت‌محور» در یک پودمان رمزنگاشتی پشتیبانی شود، پودمان باید دارای امکان احراز هویت شخصی کاربر، انتخاب ضمنی یا تضمینی یک یا چند نقش توسط کاربر و بررسی مجوز وی برای بر عهده گرفتن نقش یا نقش‌های انتخابی باشد. احراز هویت شخصی متصدی، انتخاب نقش‌ها و احراز هویت نقش‌های انتخابی ممکن است با یکدیگر ترکیب شوند. اگر پودمان رمزنگاشتی اجازه تغییر نقش‌ها را به کاربر بدهد، آن‌گاه مجوز کاربر احراز هویت شده‌ای که پیش از این احراز نشده، به منظور بر عهده گرفتن هر نقشی باید بررسی شود.

یک پودمان رمزنگاشتی ممکن است اجازه اجرای کلیه خدمات مجاز یک نقش را به یک کاربر احراز هویت شده بدهد یا ممکن است اجرای هر خدمت یا مجموعه‌ای از خدمات، مستلزم انجام فرآیند احراز هویت جداگانه و مستقل باشد.

وقتی که نشست[1] یک پودمان رمزنگاشتی با نرم‌افزار به هر دلیل (به عنوان مثال جداشدن پودمان رمزنگاشتی از سامانه یا قطع و وصل منبع تغذیه) بسته شود، نتایج احراز هویت قبلی کاربر نباید باقی مانده و باید مجدد عملیات احراز هویت صورت گیرد.

احراز هویت جهت مجوزدهی به نقش‌ها در پودمان‌های رمزنگاشتی ممکن است به روش‌های مختلفی از جمله اسم‌رمز یا شماره شناسایی شخصی(PIN) ، احراز هویت مبتنی بر کلید و یا احراز هویت زیست‌سنجشی صورت گیرد. در هر صورت اطلاعات مربوط به احراز هویت در پودمان رمزنگاشتی باید در مقابل افشاسازی[2]، تغییر و یا جایگزینی غیرمجاز محافظت گردند.

سازوکارهای احراز هویت به روش‌های مختلفی می‌توانند مقدار دهی اولیه شوند. در صورتی که یک پودمان رمزنگاشتی دارای مقادیر اولیه برای احراز هویت کاربر در اولین دسترسی به پودمان نباشد، آنگاه باید

1 - Session
2 - Compromise

روش‌های مجاز دیگری باید برای کنترل دسترسی به پودمان و راه اندازی اولیه سازوکارهای احراز هویت استفاده شود.

سازوکار احراز هویت پشتیبانی شده توسط پودمان رمزنگاشتی باید موارد ذیل را تضمین کند:

- در صورت استفاده از سازوکار احراز هویت مبتنی بر اسم‌رمز یا PIN، باید در تعداد دفعات سعی در وارد نمودن اسم‌رمز نادرست محدودیت اعمال گردد و در صورت عبور تعداد دفعات سعی در وارد نمودن اسم‌رمز نادرست از مقدار آستانه تعیین شده، پودمان رمزنگاشتی باید وارد حالت خطا شود و بدین ترتیب پودمان رمزنگاشتی باید غیر فعال گردد؛

- برای هر بار اجرای عملیات احراز هویت ، احتمال یک سعی تصادفی منجر به موفقیت و یا احتمال وقوع خطا در پذیرش باید کمتر از ۱ در ۱,۰۰۰,۰۰۰ باشد (به عنوان مثال حدس زدن یک اسم‌رمز یا PIN و یا خطا در پویش‌گرهای زیست‌سنجشی)؛

- برای چندین بار انجام سازوکار احراز هویت در طی یک دقیقه، احتمال یک سعی تصادفی منجر به موفقیت یا احتمال وقوع خطا در پذیرش باید کمتر از ۱ در ۱۰۰,۰۰۰ باشد؛

- بازخورد یا نمایش داده‌های احراز هویت به کاربر باید غیر آشکار و پنهان صورت گیرد (به عنوان مثال نباید اسم‌رمز در زمان درونداد آن به‌صورت آشکار نمایش داده‌شود) همچنین این بازخورد نباید امنیت سازوکار احراز هویت را به خطر اندازد.

مستندسازی باید موارد زیر را مشخص کند:

- سازوکار احراز هویت پشتیبانی شده توسط پودمان رمزنگاشتی؛
- انواع داده‌های احراز هویت مورد نیاز پودمان رمزنگاشتی جهت پیاده‌سازی سازوکارهای احراز هویت ؛
- روش‌های احراز هویت به کاررفته جهت کنترل دسترسی به پودمان در اولین بار و آماده‌سازی سازوکارهای احراز هویت و
- استحکام[۱] سازوکار احراز هویت پشتیبانی شده توسط پودمان

سازوکارهای احراز هویت برای هر سطح امنیتی باید به شرح ذیل در پودمان‌های رمزنگاشتی اعمال گردد:

### ۴-۳-۵ الزامات احراز هویت کاربر در سطح امنیتی اول

در سطح امنیتی اول پیاده‌سازی سازوکارهای احراز هویت جهت اعمال کنترل دسترسی به پودمان رمزنگاشتی مورد نیاز نمی‌باشد. اگر سازوکارهای احراز هویت در یک پودمان رمزنگاشتی پشتیبانی نشود، قابلیت انتخاب ضمنی یا تضمینی نقش یا نقش‌ها باید به کاربر داده شود.

---

۱ - Strength

### ۵-۳-۵ الزامات احراز هویت کاربر در سطح امنیتی دوم

در سطح امنیتی دوم باید احراز هویت «نقش‌محور»جهت کنترل دسترسی به پودمان رمزنگاشتی به کار گرفته شود.

### ۵-۳-۶ الزامات احراز هویت کاربر در سطوح امنیتی سوم و چهارم

در سطح امنیتی سوم و چهارم باید احراز هویت «هویت‌محور» جهت کنترل دسترسی به پودمان رمزنگاشتی به کار گرفته شود.

## ۵-۴ مدل حالت متناهی

عملکرد یک پودمان رمزنگاشتی باید با استفاده از یک مدل حالت متناهی مشخص شود که به صورت یک نمودار و/یا جدول انتقال حالت نشان داده می‌شود. نمودار و/یا جدول انتقال حالت شامل موارد زیر است:

- کلیه حالت‌های عملیاتی و خطای پودمان رمزنگاشتی؛
- گذرهای متناظر از یک حالت به حالت دیگر؛
- رویدادهای درونداد که باعث گذر از یک حالت به حالت دیگر می‌شوند؛ و
- رویدادهای برونداد که نتیجه گذر از یک حالت به حالت دیگر هستند.

### ۵-۴-۱ حالت‌های عملیاتی و خطای پودمان رمزنگاشتی

یک پودمان رمزنگاشتی باید دارای حالت‌های عملیاتی یا خطای ذیل باشد:

۱- حالت‌های خاموش/روشن: حالت‌هایی برای منبع تغذیه اصلی، فرعی و منبع تغذیه پشتیبان. این حالات ممکن است بین منابع مختلف تغذیه اعمال شده به پودمان رمزنگاشتی، تمایز قائل شوند.

۲- حالت‌های متصدی رمز: حالت‌هایی که در آن‌ها خدمت‌های متصدی رمز (مانند آماده‌سازی اولیه یا مدیریت کلیدهای رمزنگاشتی) اجرا می‌شوند.

۳- حالت‌های درونداد کلید/واحدهای اطلاعاتی حیاتی: حالت‌هایی برای زمان درونداد کلیدهای رمزنگاشتی و واحدهای اطلاعاتی حیاتی می‌باشند.

۴- حالت‌های کاربر نهایی[1]: حالت‌هایی که در آن‌ها دریافت خدمت‌های امنیتی، اجرای عملیات رمزنگاشتی یا اجرای سایر توابع مصوب یا -غیر مصوب برای کاربر نهایی مجاز امکان پذیر است.

۵- حالت‌های خودآزمایی[2]: حالت‌هایی که در آن‌ها پودمان رمزنگاشتی در حال انجام فرآیند خودآزمایی می‌باشد.

---

1 - User State

2 -Self test State

۶- حالت‌های خطا[1]: حالت‌هایی که در آن پودمان رمزنگاشتی با خطا مواجه می‌شود (به عنوان مثال بروز خطا در طی فرآیند خودآزمایی). حالت‌های خطا ممکن است شامل خطاهای سخت[2] باشند که در اثر خرابی تجهیزات رخ داده و در آن‌ها پودمان رمزنگاشتی نیازمند تعمیر، خدمت یا نگهداری باشد. همچنین حالت‌های خطا ممکن است در اثر وقوع خطاهای نرم[3] قابل بازگشت باشند که ممکن است راه اندازی اولیه یا بازنشانی پودمان نیاز باشد. به جز مواردی که در اثر خطاهای سخت به وجود می‌آیند و نیازمند تعمیر و نگهداری پودمان رمزنگاشتی هستند، بازگشت از سایر حالت‌های خطا باید امکان پذیر باشد.

۷- یک پودمان رمزنگاشتی ممکن است شامل سایر مدل‌های حالت، البته نه محدود به آن‌ها، باشد :

۸- حالت‌های کنارگذار: حالت‌هایی که در آن‌ها قابلیت کنارگذار فعال شده و خدمات بدون پردازش رمزنگاشتی (مانند انتقال متن آشکار در درون پودمان رمزنگاشتی) ارائه می‌شوند.

۹- حالت‌های تعمیر و نگهداری: حالت‌هایی برای تعمیر و نگهداری پودمان رمزنگاشتی شامل آزمون‌های نگهداری فیزیکی و منطقی. در صورتی که پودمان رمزنگاشتی دارای نقش تعمیر و نگهداری باشد، حالت تعمیر و نگهداری به طور حتمی باید وجود داشته باشد.

در مستندسازی باید مدل‌های حالت تعریف شده برای پودمان رمزنگاشتی از طریق نمودارها و جداول (شامل توصیف کامل سطوح دسترسی برای هر حالت و چگونگی گذار از یک حالت به حالت دیگر، درونداد و یا برونداد داده‌ها و نیز داده‌های کنترلی ) شرح داده شود.

### ۵-۵ امنیت فیزیکی

یک پودمان رمزنگاشتی باید سازوکارهای امنیت فیزیکی را جهت جلوگیری از دسترسی فیزیکی غیرمجاز به محتویات پودمان رمزنگاشتی به کار بندد و پس از نصب، مانع از استفاده غیرمجاز یا تغییر پودمان شود. کلیه اجزای سخت‌افزار، نرم‌افزار، ثابت‌افزار و اجزای داده‌ای درون محدوده رمزنگاری باید محافظت شوند.

یک پودمان رمزنگاشتی به طور کامل نرم‌افزاری،که امنیت فیزیکی آن به طور انحصاری توسط سامانه میزبان تامین می‌شود، مخاطب الزامات امنیت فیزیکی این استاندارد نیست.

الزامات امنیت فیزیکی برای سه آرایش مختلف از تراشه‌ها تعریف شده‌است:

۱. پودمان‌های رمزنگاشتی تک-تراشه‌ای[4]: دربرگیرنده یک تراشه مدار مجتمع(IC)[5] است که به عنوان یک افزاره مستقل به‌کار می‌روند و یا ممکن است در داخل یک محفظه یا محصولی که به‌صورت فیزیکی محافظت نشده‌است، تعبیه گردد. از نمونه‌های پودمان رمزنگاشتی تک-تراشه‌ای، می‌توان تراشه‌هایی با یک IC یا کارت‌های هوشمند تک-تراشه‌ای را نام برد.

---

1 - Error States
2 - Hard Error
3 - Soft Error
4 - Single-chip cryptography module
5 -Integrated Circuit

۲. پودمان رمزنگاشتی چند-تراشه‌ای تعبیه شده[1]: که از دو یا چند تراشه مدار مجتمع متصل به هم تشکیل شده‌اند و در داخل یک محفظه یا محصولی که محافظت فیزیکی ندارد، تعبیه شده‌اند. از نمونه‌های پودمان‌های رمزنگاشتی چند-تراشه‌ای تعبیه شده می‌توان تطبیق‌دهنده‌ها[2] و تخته‌مدار گسترش[3] را نام برد.

۳. پودمان رمزنگاشتی چند-تراشه‌ای خودکفا[4]: که از دو یا چند مدار مجتمع متصل به هم تشکیل شده‌اند و در داخل یک محفظه یا محصولی که محافظت فیزیکی دارد، تعبیه شده‌اند. از نمونه‌های پودمان‌های رمزنگاشتی چند-تراشه‌ای خودکفا می‌توان مسیریاب‌های رمز کننده یا رادیوهای امن را نام برد.

بر اساس سازوکارهای امنیت فیزیکی پودمان رمزنگاشتی، تلاش‌های غیر مجاز برای دسترسی فیزیکی، استفاده یا تغییر باید در شرایط ذیل با احتمال بالایی تشخیص داده خواهد شود :

- پس از تلاش، از روی علائم نمایان برجا مانده ( به عبارتی، آشکارسازی نفوذ)

و/یا

- در حین تلاش، به نحوی که پودمان بتواند واکنش مناسبی به منظور محافظت از کلیدهای خصوصی و داده‌های اطلات حیاتی اتخاذ نمود (به عبارتی، پاسخگویی به دستکاری).

جدول زیر به‌صورت خلاصه الزامات امنیت فیزیکی را برای هر یک از چهار سطح امنیت بیان می‌کند.

1 - Multiple-chip embedded cryptographic module
2 - Adapters
3 - Expansion Board
4 - Multiple-chip standalone cryptographic module

**جدول ۲- خلاصه الزامات امنیت فیزیکی**

| | عمومی | تک-تراشه‌ای | چند-تراشه‌ای تعبیه شده | چند-تراشه‌ای خودکفا |
|---|---|---|---|---|
| **سطح امنیتی اول** | استفاده از قطعات صنعتی و به تولید انبوه رسیده[آ]. | هیچ الزامات دیگری تعریف نشده‌است. | در صورت امکان، محفظه و درپوش پودمان رمزنگاشتی از مواد صنعتی تهیه شود. | محفظه و درپوش پودمان رمزنگاشتی از مواد صنعتی تهیه شود. |
| **سطح امنیتی دوم** | آشکارسازی نفوذ برای پوشش، محفظه یا پلمپ پودمان رمزنگاشتی | پوشش مات و غیر شفاف آشکار کننده نفوذ برای پوشش تراشه یا محفظه | پوشش مات و غیر شفاف آشکار کننده نفوذ و محفظه‌ای با مهر و موم‌های آشکارساز نفوذ یا قفل‌های مقاوم برای درب‌ها یا پوشش‌های قابل برداشت. | محفظه مات و غیر شفاف با مهر و موم‌های آشکارساز نفوذ یا قفل‌های مقاوم برای درب‌ها یا پوشش‌های قابل برداشت. |
| **سطح امنیتی سوم** | امحاء خودکار واحدهای حیاتی در هنگام دسترسی به واسط تعمیر و نگهداری[ب]. مدارهای پاسخگو به نفوذ و امحاء کننده. منفذهای محافظت شده. | پوشش سخت و مات آشکارساز نفوذ روی تراشه یا محفظه مقاوم در برابر برداشتن و نفوذ. | استفاده از مواد سخت، مات و مقاوم در برابر ضربه و لرزش برای بسته بندی مدارو تراشه‌ها یا نیازمندی‌های امنیتی سطح سه برای پودمان‌های چندتراشه‌ای خودکفا. | استفاده از مواد سخت، تیره‌رنگ و مقاوم در برابر ضربه و لرزش مدار و تراشه‌ها با امکان ایجاد خسارت زیاد در صورت بازشدن یا هر نوع نفوذ دیگر |
| **سطح امنیتی چهارم** | حفاظت در برابر شکست‌های محیطی برای درجه حرارت و ولتاژ | استفاده از پوشش سخت، مات و مقاوم در برابر برداشتن، بر روی تراشه | تشخیص نفوذ به محفظه به همراه مدارهای پاسخگویی به نفوذ و امحاء | تشخیص و پاسخگویی به نفوذ به همراه پوسته‌ای که در مقابل نفوذ واکنش نشان می‌دهد و نیز مدارهای امحاء |

[آ] Production-grade componenet

[ب] Maintenance Interface

به طور کلی سطح اول امنیت کمترین نیاز به محافظت فیزیکی را دارد. در سطح دوم سازوکار آشکارسازی نفوذ افزوده شده‌است. در سطح سوم، استفاده از جلدها و روکش‌ها با قابلیت تشخیص نفوذ و سازوکار

پاسخگویی به نفوذ، برای روکش‌ها و درهای قابل برداشت، اضافه شده‌است و در سطح چهارم، الزامات تشخیص و پاسخگویی به نفوذ برای تمام اجزای محوطه افزوده شده‌است. همچنین آزمون و محافظت در برابر شکست‌های محیطی نیز در سطح چهارم مورد نیاز می‌باشند. توجه داشته باشید که قابلیت‌های تشخیص نفوذ (به عنوان مثال تشخیص نفوذ از طریق حس‌گرهای تعبیه شده در پودمان) و پاسخگویی به نفوذ (امحای حافظه پس از تشخیص نفوذ) نمی‌توانند جایگزین قابلیت آشکارسازی نفوذ (آشکارسازی نفوذ برای پوشش، محفظه یا پلمپ پودمان رمزنگاشتی) شوند.

زمانی که پودمان رمزنگاشتی به منظور اجازه دسترسی فیزیکی طراحی شده باشد، نیازمندی‌های امنیتی برای واسط دسترسی تعمیر و نگهداری تعیین می‌شوند (به عنوان مثال، توسط فروشنده پودمان یا مراجع مجاز دیگر).

### ۵-۵-۱ الزامات عمومی امنیت فیزیکی

الزامات زیر برای هر سه آرایش مختلف از تراشه‌ها باید تامین شوند:

- مستندسازی باید سطح امنیتی پیاده‌سازی شده را توصیف کند.
- مستندسازی باید سازوکار امنیت فیزیکی را توصیف کند.
- درصورتی که پودمان رمزنگاشتی شامل یک نقش تعمیر و نگهداری باشد که نیازمند دسترسی فیزیکی است، آنگاه:
  - یک واسط دسترسی تعمیر و نگهداری باید تعریف گردد.
  - واسط دسترسی فیزیکی باید شامل تمام مسیرهای دسترسی فیزیکی به محتویات پودمان رمزنگاشتی شامل کلیه درب‌ها و روکش‌های قابل برداشت، باشد.
  - تمام درب‌ها و پوشش‌های قابل برداشت موجود در واسط دسترسی تعمیر و نگهداری باید با استفاده از سازوکارهای امنیت فیزیکی مناسب محافظت شوند.
  - کلیه کلیدهای خصوصی و مخفی و واحدهای اطلاعاتی حیاتی رمز نشده، در هنگام دسترسی به واسط تعمیر و نگهداری باید امحاء گردند.
  - مستندات باید واسط دسترسی تعمیر و نگهداری و چگونگی امحاء کلیدهای رمزنگاشتی و واحدهای اطلاعاتی حیاتی رمز نشده را در زمان دسترسی به این واسط را توصیف نمایند.

۱- الزامات عمومی امنیت فیزیکی برای سطح امنیتی اول

الزامات زیر در سطح اول باید رعایت شوند:

- استفاده از اجزای رده صنعتی و به تولید انبوه رسیده که باید فنون اثرناپذیری استاندارد[1] را شامل شوند (برای مثال، پوششی که مدارات پودمان رمزنگاشتی را در مقابل آسیب‌های محیطی محافظت کند).

1 - Standard Passivation techniques

- در هنگام اجرای تعمیر و نگهداری فیزیکی، هر نوع داده مخفی، کلید خصوصی یا واحدهای اطلاعاتی حیاتی[1] که در پودمان رمزنگاشتی به صورت رمز نشده ذخیره شده‌اند، باید امحاء شود. فرایند امحاء باید به صورت نظام‌مند توسط کاربر یا به‌صورت خودکار توسط پودمان رمزنگاشتی انجام شود.

۲- الزامات عمومی امنیت فیزیکی برای سطح امنیتی دوم

علاوه بر الزامات عمومی سطح امنیتی اول، زمانی که تلاشی برای دسترسی فیزیکی به پودمان امنیتی صورت گرفته، پودمان باید آشکارسازی از نفوذ را (به عنوان مثال از طریق پوشش، محفظه یا مهر و موم) ارائه کند.

۳- الزامات عمومی امنیت فیزیکی برای سطح امنیتی سوم

علاوه بر الزامات عمومی سطح اول و دوم الزامات زیر نیز باید در سطح سوم درنظر گرفته‌شود:

- در صورتی که پودمان دارای هر گونه درب یا پوشش قابل برداشت[2] بوده یا واسط دسترسی تعمیر و نگهداری در آن تعریف شده باشد، باید دارای مدارهای پاسخگو به نفوذ و امحاء باشد. مدار پاسخگو به نفوذ و امحاء در هنگام بازشدن درب، برداشته‌شدن پوشش یا دسترسی به واسط دسترسی تعمیر و نگهداری، باید تمامی کلیدهای مخفی و واحدهای اطلاعاتی حیاتی رمز نشده را امحاء کند. زمانی‌که کلیدهای مخفی و خصوصی و واحدهای اطلاعاتی حیاتی رمز نشده در پودمان رمزنگاشتی قرار دارند، پاسخگو به نفوذ و مدار امحاء باید عملیاتی باقی بماند.
- اگر پودمان رمزنگاشتی دارای مجاری یا شکاف‌های تهویه باشد، باید به شکلی تعبیه شوند که مانع دسترسی یا کاوش داخل محفظه پودمان شوند (به طور مثال، وجود ۹۰ درجه انحنا در محل‌هایی که سوراخ یا شکاف وجود دارد یا انسداد آن‌ها با مواد محکم.).

۴- الزامات عمومی امنیت فیزیکی برای سطح امنیتی چهارم

علاوه بر الزامات امنیتی سطح اول و دوم و سوم، در سطح چهارم باید ویژگی‌های حفاظت در مقابل شکست محیطی یا آزمون‌های تحمل شکست محیطی (توصیف شده در زیربند ۵-۵-۵) نیز درنظر گرفته شود.

### ۵-۵-۲ الزامات ویژه پودمان‌های تک-تراشه‌ای

علاوه بر الزامات عمومی امنیت فیزیکی بیان شده در زیربند ۵-۵-۱، پودمان‌های تک‌تراشه‌ای در هر یک از چهار سطح امنیت، باید الزامات خاص زیر را داشته باشند:

۱- الزامات ویژه پودمان‌های تک-تراشه‌ای برای سطح اول امنیتی
هیچ الزاماتی در این سطح در نظر گرفته نشده‌است.

---

1 - Critical
2 - Removable cover

۲- الزامات ویژه پودمان‌های تک-تراشه‌ای برای سطح دوم امنیتی
در این سطح پودمان رمزنگاشتی با اعمال الزامات ذیل باید مجهز به قابلیت آشکارسازی نفوذ در مقابل نفوذ و دسترسی غیرمجاز به مدار الکترونیکی و تراشه پودمان رمزنگاشتی باشد:

- پودمان رمزنگاشتی باید با یک پوشش آشکارساز نفوذ، پوشانده شود (مانند یک ماده تاثیرناپذیر آشکارساز نفوذ یا یک ماده آشکارساز نفوذ که روی سطح تاثیرناپذیر را می‌پوشاند) یا در درون محفظه‌ای با قابلیت آشکارسازی نفوذ قرار بگیرد تا از مشاهده مستقیم، پروب‌گذاری[1] یا دستکاری پودمان جلوگیری کرده و آشکارسازی از تلاش برای دستکاری یا برداشتن پودمان ارائه دهد.
- محفظه یا پوشش آشکارساز نفوذ باید مات و کدر باشد به طوری‌که طیف مرئی[2] نتواند از آن عبور کند (یعنی اجزاء درونی پودمان از پشت آن قابل دیدن نباشد).

۳- الزامات ویژه پودمان‌های تک-تراشه‌ای برای سطح سوم امنیتی
علاوه بر سطح اول و دوم امنیت، الزامات زیر نیز باید در سطح سوم، لحاظ شود:

- پودمان رمزنگاشتی باید با یک پوشش سخت و مات با قابلیت آشکارسازی نفوذ پوشانده شود (به عنوان مثال تراشه از طریق یک پوشش اپاکسی[3] مات و سخت پوشانده شود) یا محفظه‌ای که پودمان در آن قرار داده می‌شود به نحوی پیاده‌سازی شود که هر گونه تلاشی برای برداشتن یا نفوذ به آن باید با احتمال بالایی سبب خسارت جدی به پودمان رمزنگاشتی شود (به عبارتی، پودمان نتواند کار کند).

۴- الزامات ویژه پودمان‌های تک-تراشه‌ای برای سطح چهارم امنیتی
علاوه بر الزامات سه سطح قبلی، الزامات زیر نیز باید در سطح چهارم امنیت، اعمال شود:

- پودمان باید با یک پوشش سخت، تیره و نیز مقاوم در برابر برداشتن پوشیده شود به طوری که خاصیت کششی و شکنندگی آن به نحوی باشد که سعی در تراشیدن یا بریدن آن موجب آسیب‌دیدن پودمان شود (به عبارتی، موجب از کار افتادن پودمان شود).
- پوشش مقاوم در برابر برداشتن باید آن گونه خاصیت حل‌شدنی داشته باشد به نحوی که حل‌شدن پوشش با احتمال بسیار زیادی باعث آسیب دیدن پودمان رمزنگاشتی شود (به عبارتی، موجب از کار افتادن پودمان شود).

### ۵-۵-۳ پودمان چند-تراشه‌ای تعبیه شده

علاوه بر الزامات عمومی امنیت فیزیکی بیان شده در زیربند ۵-۵-۱، پودمان‌های چند-تراشه‌ای تعبیه شده در هر یک از چهار سطح امنیت، باید الزامات زیر را داشته باشند:

---

1 - Probe
2 - Visible Spectrum
۳ - epoxy

۱- الزامات ویژه پودمان‌های چند-تراشه‌ای برای سطح امنیتی اول

درصورتی که پودمان رمزنگاشتی درون یک محفظه یا پوشش قابل برداشت قرار داشته باشد، باید از محفظه یا پوشش تولید شده در رده صنعتی استفاده شود.

۲- الزامات ویژه پودمان‌های چند-تراشه‌ای برای سطح امنیتی دوم

علاوه بر الزامات سطح اول، در سطح دوم باید الزامات زیر نیز لحاظ گردد. این الزامات به دو شکل تامین می‌گردد:

یا

- اجزای پودمان رمزنگاشتی باید با یک پوشش آشکارساز نفوذ یا با ماده‌ای که اثرات دستکاری بر روی آن نقش بندد پوشیده شوند یا در درون یک محفظه آشکارساز نفوذ قرار گیرند تا از مشاهده مستقیم، پروب‌گذاری[1] یا دستکاری پودمان جلوگیری شده و آشکارسازی از تلاش برای نفوذ یا برداشتن اجزای پودمان ارائه دهد و
- این محفظه یا پوشش آشکارساز نفوذ نباید طیف نور قابل دیدن را از خود عبور دهد.

یا

- پودمان رمزنگاشتی باید به طور کامل در درون یک محفظه فلزی یا پلاستیک سخت رده صنعتی قرارگیرد که ممکن است دارای درب یا پوشش‌های قابل برداشت باشد،
- این محفظه باید مات و کدر بوده و طیف نور قابل دیدن را نباید از خود عبور دهد. و
- در صورتی که پودمان داری هرگونه درب یا پوشش قابل برداشت باشد، با استفاده از قفل‌های مکانیکی ضد سرقت[2] با کلیدهای فیزیکی یا منطقی باید قفل شوند یا با مهر و موم‌های آشکارساز نفوذ (برای مثال، نوار چسب یا مهر و موم هولوگرام) باید محافظت شوند.

۳- الزامات ویژه پودمان‌های چند-تراشه‌ای برای سطح امنیتی سوم

علاوه بر سطح اول و دوم، الزامات ذیل نیز در این سطح مورد نیاز می باشد:

یا

- تراشه‌ها باید با یک پوشش سخت که طیف نور قابل دیدن نتواند از آن عبور کند یا ماده‌ای مقاوم در برابر ضربه ولرزش، پوشانده شوند.

یا

- الزامات کاربردی پودمان رمزنگاشتی چند-تراشه‌ای خودکفا در سطح سوم باید اعمال شود (طبق زیربند ۵-۵-۴).

---

۱ - Probe

2 - Pick-resistant

۴-الزامات ویژه پودمان‌های چند-تراشه‌ای برای سطح امنیتی چهارم

علاوه بر الزامات سطح اول و دوم و سوم، الزامات زیر نیز در سطح چهارم باید لحاظ شود:

- اجزای پودمان رمزنگاشتی باید با ماده‌ای مقاوم در برابر ضربه و لرزش پوشیده شود یا داخل محفظه‌ای با پوسته حفاظت شده که قابلیت تشخیص نفوذ دارد(مانند یک لایه پولیستری انعطاف‌پذیر که اطراف آن را یک سیم‌پیچ فرا گرفته‌است)، قرار گیرد. همچنین باید نفوذهایی نظیر بریده‌شدن، سوراخ‌شدن، آسیاب‌شدن، خردشدن یا ذوب‌شدن را تشخیص دهد تا از دسترسی به کلیدهای خصوصی و محرمانه و واحدهای اطلاعاتی حیاتی رمز نشده جلوگیری کند.

- پودمان رمزنگاشتی باید شامل مدار پاسخگو به تهدید و امحاء باشد که به طور مداوم بر نفوذ به محفظه پودمان رمزنگاشتی نظارت داشته باشد و به محض تشخیص یک نفوذ باید بی‌درنگ کلیه کلیدهای خصوصی و محرمانه و واحدهای اطلاعاتی حیاتی را امحاء کند. تا زمانی که کلیدهای خصوصی و محرمانه یا واحدهای اطلاعاتی حیاتی رمز نشده در درون پودمان رمزنگاشتی قرار دارند، مدار پاسخگویی به نفوذ و امحاء باید عملیاتی باقی بماند.

### ۵-۵-۴ پودمان رمزنگاشتی چند-تراشه‌ای خودکفا

علاوه بر الزامات امنیتی عمومی ذکر شده در زیربند ۵-۵-۱، موارد زیر به پودمان‌های رمزنگاشتی چندتراشه‌ای خودکفا اختصاص دارند:

۱-الزامات ویژه پودمان‌های چند-تراشه‌ای خودکفا برای سطح امنیتی اول

پودمان رمزنگاشتی باید به طور کامل در یک محفظه فلزی یا پلاستیک فشرده از رده صنعتی قرار گرفته که ممکن است دارای درب یا پوشش قابل برداشت باشد.

۲-الزامات ویژه پودمان‌های چند-تراشه‌ای خودکفا برای سطح امنیتی دوم

در این سطح علاوه بر الزامات سطح اول، الزامات زیر نیز باید اعمال گردد:

- محفظه پودمان رمزنگاشتی باید مات و کدر بوده و طیف نور قابل دیدن نتواند از آن عبور کند.
- درصورتی که محفظه پودمان رمزنگاشتی شامل هر گونه درب یا پوشش قابل برداشت باشد، آنگاه این درب‌ها یا پوشش‌ها با قفل‌های مکانیکی ضد سرقت دارای کلیدهای منطقی یا فیزیکی باید قفل شده یا با استفاده از مهر و موم‌های آشکارساز نفوذ (مانند نوار یا برچسب پلمب) حفاظت شوند، مانند نوار چسب یا مهر و موم هولوگرام.

۳-الزامات ویژه پودمان‌های چند-تراشه‌ای خودکفا برای سطح امنیتی سوم

علاوه بر الزامات امنیتی سطح اول و دوم، برای این سطح امنیتی موارد زیر نیز باید اعمال گردد:

- بخش چند تراشه مدار الکترونیکی داخل پودمان باید با ماده‌ای سخت و مقاوم در برابر ضربه و لرزش که برای طیف نور قابل دیدن مات و غیر شفاف است، پوشیده شود.

یا

- پودمان رمزنگاشتی باید در درون یک محفظه محکم قرار بگیرد به نحوی که هر گونه تلاش برای برداشتن یا نفوذ به این محفظه با احتمال زیادی سبب آسیب جدی به پودمان شود (به عبارتی، پودمان از کار بیافتد).

۴- الزامات ویژه پودمان‌های چند-تراشه‌ای خودکفا برای سطح امنیتی چهارم

علاوه بر الزامات امنیتی سطح اول، دوم و سوم، موارد زیر نیز باید در این سطح اعمال گردد:

- مواد یا محفظه مقاوم در برابر ضربه و لرزش پودمان رمزنگاشتی باید با استفاده از یک پوشش تشخیص نفوذ بسته بندی شوند. تشخیص نفوذ از طریق به کارگیری سازوکارهای تشخیص نفوذ نظیر سوده‌های پوششی[1] (مانند ریزسوده‌ها[2]، سوده‌های حساس به مغناطیس، محرک‌های مغناطیسی دائمی و ..)، تشخیص‌دهنده‌های حرکت[3] (مانند مادون قرمز، ریزموج و یا ماوراء صوت) یا سایر سازوکارهای تشخیص نفوذ شرح داده شده برای پودمان‌های چندتراشه‌ای تعبیه شده، انجام می‌شود. سازوکارهای تشخیص نفوذ، باید حملات و نفوذهایی نظیر برش، سوراخ‌کاری، آسیاب‌شدن، پودرشدن یا حل‌شدن ماده یا محفظه مقاوم به منظور دستیابی به کلید خصوصی و محرمانه و واحدهای اطلاعاتی حیاتی رمز نشده را تا حد امکان تشخیص دهد.
- پودمان رمزنگاشتی باید شامل مدار پاسخگویی به نفوذ و امحاء باشد که باید به طور مداوم پوسته تشخیص نفوذ را نظارت کرده و به محض تشخیص دادن یک نفوذ باید فوری تمام کلیدهای رمزنگاشتی خصوصی و محرمانه و واحدهای اطلاعاتی حیاتی رمز نشده را امحا کند. تا زمانی که کلیدهای رمزنگاشتی و واحدهای اطلاعاتی حیاتی رمز نشده در درون پودمان رمزنگاشتی قرار دارند، مدار پاسخگویی به نفوذ و امحاء باید عملیاتی باقی بماند.

### ۵-۵-۵ آزمون/حفاظت در برابر شکست‌های محیطی

تجهیزات الکترونیکی و مدارها برای استفاده در یک محدوده خاصی از شرایط محیطی طراحی شده‌اند. به‌صورت عمدی یا تصادفی، خارج‌شدن از بازه عادی ولتاژ و حرارت می‌تواند باعث رفتارهای غیرقابل پیش‌بینی یا از کار افتادن تجهیزات و مدارها شود و بدین ترتیب امنیت پودمان به خطر بیافتد. حصول

1 - Switch
2 - Micro Switch
3 - Motion Detector

اطمینان از اینکه امنیت فیزیکی یک پودمان در شرایط محیطی غیر عادی به خطر نمی‌افتد، با بـه کـارگیری خواص EFP و EFT، می‌تواند محقق شود.
برای سطوح امنیتی اول، دوم و سوم، یک پودمان رمزنگاشتی نیازی به بکارگیری قابلیت‌هـای EFP یـا EFT ندارد. اما در سطح چهارم، پودمان رمزنگاشتی باید خواص EFP یا EFT را به کار بندد.

### ۵-۵-۵-۱ ویژگی‌های حفاظت در برابر شکست‌های محیطی (پیشنهاد ۱)

شرایط غیرعادی یا نوسانات اتفاقی یا عمدی خارج از محـدوده عملیـاتی پودمـان رمزنگاشـتی ممکـن اسـت امنیت آن را به خطر بیاندازد، ویژگی‌های EFP، باید پودمان رمزنگاشتی را در برابر این شرایط حفظ کنند. به ویژه، پودمان رمزنگاشتی باید بر نوسانات حرارت و ولتاژ نظارت کرده و در زمان برونداد از بازه عملیاتی عادی آن‌ها پاسخ مناسب را به دنبال داشته باشد.
ویژگی‌های EFP باید شامل مدارات یا تجهیزات الکترونیکی باشد که به طـور مـداوم درجـه حـرارت و ولتـاژ عملیاتی پودمان رمزنگاشتی را اندازه‌گیری می‌کنند. در صورت برونداد ولتاژ یا درجه حـرارت از بـازه عـادی، مدار محافظتی باید یا (۱) پودمان را به‌صورت امن خاموش کند تا از عملیات بعـدی جلـوگیری کنـد یـا (۲) بلافاصله کلیه کلیدهای خصوصی و محرمانه و واحدهای اطلاعاتی حیاتی رمز نشده را امحاء کند.

مستندات باید محدوده‌های عملیاتی عادی پودمان و ویژگی‌های حفاظت در برابر شکست‌های محیطی به کار رفته در پودمان را توصیف کنند.

### ۵-۵-۵-۲ رویه‌های آزمون شکست‌های محیطی[1] (پیشنهاد ۲)

آزمون شکست‌های محیطی (EFT) باید ترکیبی از تحلیل‌ها، شبیه‌سازی‌ها و آزمون‌های پودمان رمزنگاشتی باشد تا اطمینان دهد که شرایط محیطی یا نوسانات (عمدی یا تصادفی) خـارج از محـدوده عملیـاتی عـادی پودمان امنیت پودمان را با خطر مواجه نمی‌کند.

EFT باید تضمین کند که اگر درجه حرارت یا ولتاژ عملیاتی پودمان از محدوده عملیاتی مجـاز خـود خـارج شود و منجر به بروز خطا در تجهیزات یا مدار درونی آن شود، به هیچ وجه امنیت پودمان بـه خطـر نخواهـد افتاد. بازه حرارتی مورد آزمایش، باید از ۱۰۰- درجه سلسـیوس تـا ۲۰۰+ درجـه سلسـیوس ( ۱۵۰- درجـه فارنهایت تا ۴۰۰+ درجه فارنهایت) باشد. بازه ولتاژ مورد آزمایش، از کمترین ولتاژ منفی ( نسبت بـه زمـین) که باعث امحاء مدارها یا تجهیزات الکترونیکی می‌شود تا کمترین ولتاژ مثبت ( نسبت بـه زمـین) کـه باعـث امحای مدارها یا تجهیزات الکترونیکی می‌شود، را باید شامل شود.

مستندات باید محدوده عملیاتی عادی پودمـان رمزنگاشـتی و آزمون‌هـای شکسـت محیطـی انجـام شـده را توصیف کنند.

1 - Environment Failure Test

### ۵-۶ محیط عملیاتی

محیط عملیاتی به مدیریت اجزای سخت‌افزار، نرم‌افزار و/ یا ثابت‌افزاری که برای عملکرد پودمان رمزنگاشتی مورد نیاز هستند، اتلاق می‌شود. محیط عملیاتی ممکن است غیر قابل تغییر (مانند ثابت‌افزارموجود در حافظه فقط خواندنی(ROM)[1] یا نرم‌افزار موجود در رایانه‌ای با درونداد و برونداد غیرفعال ) یا قابل تغییر (مانند ثابت‌افزاری که در حافظه تصادفی(RAM)[2] قرار گرفته یا نرم‌افزارهایی که با استفاده از رایانه‌های همه منظوره اجرا می‌شوند) باشد. سامانه‌عامل، یک مولفه مهم از محیط عملیاتی پودمان رمزنگاشتی است.

۱- محیط عملیاتی همه‌منظوره: به یک سامانه‌عامل (به عبارتی، مدیر منابع) همه منظوره تجاری اتلاق می‌شود که اجزای نرم‌افزاری و ثابت‌افزاری موجود در محدوده رمزنگاری را مدیریت می‌کند. این محیط عملیاتی، همچنین وظیفه مدیریت سامانه و فرایندهای کاربران، شامل برنامه‌های کاربردی همه منظوره مثل برنامه‌های پردازشگر متن را بر عهده دارد ( به عنوان نمونه‌ای از یک محیط عملیاتی همه منظوره می‌توان سامانه‌عامل ویندوز را نام برد).

۲- محیط عملیاتی محدود : به یک محیط عملیاتی مجازی غیرقابل تغییر و ایستا (مانند ماشین مجازی جاوا[3] موجود در یک افزاره جانبی رایانه‌ای غیرقابل برنامه‌ریزی[4]) اتلاق می‌شود که نیازی به استقرار در یک سامانه عامل همه منظوره ندارد.

۳- محیط عملیاتی قابل تغییر : به یک محیط عملیاتی اتلاق می‌شود که ممکن است برای قابلیت افزودن/ حذف/تغییر، پیکربندی شده باشد و/یا ممکن است توانایی‌های یک سامانه‌عامل همه منظوره (مانند استفاده از یک سامانه‌عامل رایانه‌ای، سامانه‌عامل کارت هوشمند قابل پیکربندی یا ثابت‌افزار قابل برنامه‌ریزی) را داشته باشد. در صورتی که در یک سامانه عامل، نرم‌افزارها یا ثابت‌افزارها توسط کاربر قابل تغییر باشند و/یا کاربر بتواند نرم‌افزارها یا ثابت‌افزارهایی که بخشی از حوزه ارزیابی پودمان نیستند را بارگذاری و اجرا کند، به این سامانه‌عامل محیط عملیاتی قابل تغییر گفته می‌شود.

در صورتی‌که محیط عملیاتی از نوع قابل تغییر است، الزامات سامانه‌عامل در زیربند ۵-۶-۱ باید اعمال شود و اگر محیط عملیاتی از نوع محدود باشد، نیازی به اعمال الزامات زیربند ۵-۶-۱ نیست.

در مستندسازی باید اجزا و قابلیت‌های محیط عملیاتی یا ثابت‌افزار مورد استفاده در پودمان رمزنگاشتی تشریح گردد.

---

1 - Read only memory
2 - Random Access Memory
3 - JAVA Virtual machine
4 - non-Programmable PC Card

### ۵-۶-۱ الزامات سامانه‌عامل

الزامات امنیتی محیط عملیاتی به تفکیک سطوح امنیتی مختلف در ذیل آورده شده‌است:

۱- الزامات سامانه عامل برای سطح امنیتی اول

- فقط برای سطح امنیتی اول، سامانه‌عامل باید محدود به یک حالت عملیاتی تک کاربری باشد (یعنی، با صراحت از کاربران همزمان جلوگیری شود).
- فقط برای سطح اول، پودمان رمزنگاشتی در حین انجام عملیات باید از دسترسی سایر فرایندها به کلیدهای خصوصی و مخفی، واحدهای اطلاعاتی حیاتی و مقادیر تولید کلید میانی رمز نشده جلوگیری کند. فرایندهایی که توسط پودمان رمزنگاشتی اجرا می‌شوند متعلق به خود پودمان هستند نه متعلق به فرایند یا کاربر بیرونی. فرایندهای غیر رمزنگاشتی نباید پودمان رمزنگاشتی را در حین اجرا، دچار وقفه کنند.
- پیاده‌سازی تمام نرم‌افزارها و ثابت‌افزارهای پودمان رمزنگاشتی باید به نحوی باشد که کدهای مرجع و اجرایی را در برابر افشا و تغییر غیرمجاز محافظت کند؛
- یک سازوکار رمزنگاشتی با استفاده از یک روش مصوب (مانند کد تشخیص احراز هویت پیام (MAC))[1] یا امضای رقمی) جهت اطمینان از حفظ یکپارچگی اجزای نرم‌افزاری و ثابت‌افزار پودمان رمزنگاشتی باید اعمال گردد. در صورتی که از یک روش احراز هویت مصوب برای آزمون یکپارچگی استفاده شود، این سازوکار رمزنگاشتی می‌تواند به عنوان بخشی از آزمون یکپارچگی نرم‌افزار/ثابت افزار[2] (زیربند ۵-۹-۱) به کار گرفته شود.

۲- الزامات سامانه عامل برای سطح امنیتی دوم

در این سطح علاوه بر الزامات ذکرشده در سطح اول، الزامات ذیل نیز باید اعمال گردد:

- کلیه نرم‌افزارها و ثابت‌افزارها، کلیدهای رمزنگاشتی و واحدهای اطلاعاتی حیاتی و اطلاعات کنترلی و وضعیت، باید تحت کنترل موارد زیر باشد:
  - یک سامانه‌عامل که الزامات عملیاتی توصیف شده در رخنمون‌های حفاظتی مربوط به توسعه نرم‌افزار و ارزیابی شده در استاندارد معیار مشترک(CC)[3] سطح دوم تضمین ارزیابی(EAL2)[4] را برآورده می‌کند.

  یا

  - یک سامانه‌عامل معادل قابل اعتماد.

---

1 - Message Authentication Code

2 - Firmware

۳ - Common Criteria

4 -Evaluation Asurance Level 2

- به منظور محافظت از داده‌های متن آشکار، ثابت افزار و نرم‌افزار رمزنگاشتی، کلیدهای رمزنگاشتی، واحدهای اطلاعات حیاتی، اطلاعات احراز هویت و اطلاعات محرمانه دیگر، سازوکارهای کنترل دسترسی اجباری باید برای اهداف ذیل به کار گرفته شوند:
  - تعیین مجموعه‌ای از نقش‌ها که بتوانند نرم‌افزار و ثابت‌افزار ذخیره شده در پودمان رمزنگاشتی را اجرا نمایند.
  - تعیین مجموعه‌ای از نقش‌ها که بتوانند اجزای نرم‌افزاری یا ثابت‌افزاری پودمان رمزنگاشتی را که در درون محدوده رمزنگاشتی ذخیره شده‌اند از قبیل: پارامترهای رمزنگاشتی، داده‌های رمزنگاشتی (مثل کلیدهای رمزنگاشتی و داده‌های ممیزی)، واحدهای اطلاعاتی حیاتی و داده‌های متن آشکار، تغییر دهد (به عبارتی، نوشتن، جایگزینی یا حذف داده).
  - تعیین مجموعه‌ای از نقش‌ها که بتوانند اجزای نرم‌افزاری رمزنگاشتی از قبیل: داده‌های رمزنگاشتی (مثل کلیدهای رمزنگاشتی و داده‌های ممیزی)، واحدهای اطلاعاتی حیاتی و داده‌های رمز نشده ذخیره شده در محدوده رمزنگاری را بخوانند.
  - تعیین مجموعه‌ای از نقش‌ها که بتوانند کلیدهای رمزنگاشتی و واحدهای اطلاعاتی حیاتی را وارد کنند.
  - امکان تعریف واحدهای اطلاعاتی خصوصی به طوریکه فقط توسط نقش‌های خاص و پس از احراز هویت، این نقش‌ها در دسترس باشد؛
  - امکان تعریف واحدهای اطلاعاتی حساس[1] به طوریکه به‌صورت رمزبندی شده داخل پودمان رمزنگاشتی نگهداری شوند؛
  - امکان تعریف واحدهای اطلاعاتی غیر قابل استخراج[2] که به‌صورت رمزبندی شده در داخل پودمان رمزنگاشتی نگهداری می‌شوند و قابل استخراج از پودمان رمزنگاشتی (حتی به صورت اطلاعات رمزبندی شده) نمی‌باشند؛
- سامانه‌عامل باید کلیه متصدیان و فرایندهای اجرایی را از تغییر دادن فرایندهای رمزنگاشتی اجرایی باز دارد. در این مورد، فرایندهای اجرایی به تمام فرایندهای رمزنگاشتی یا غیر رمزنگاشتی اتلاق می‌شود که غیر از فرایندهای سامانه عاملی باشند (به عبارتی، فرایندهایی که توسط کاربر تنظیم می‌شوند).
- سامانه‌عامل باید یک سازوکار ممیزی جهت ثبت تغییرات، دسترسی‌ها، حذف‌ها و افزودن داده‌های پودمان رمزنگاشتی، فراهم کند.
  - رویدادهای زیر باید توسط سازوکار ممیزی ثبت شوند:

1 - Sensitive
2 - unextractable

- سعی در درونداد نامعتبر داده‌ها برای توابعی که توسط متصدی رمز اجرا می‌شوند.
- افزودن یا حذف یک کاربر به/از نقش متصدی رمز

○ سازوکار ممیزی باید توانایی ممیزی رویدادهای زیر را داشته باشد:

- عملیات لازم جهت پردازش داده‌های ممیزی ذخیره شده در فرایند ممیزی
- درخواست‌های استفاده از سازوکارهای مدیریت داده‌های احراز هویت
- استفاده از یک تابع متصدی رمز که مرتبط با امنیت است.
- درخواست‌های دسترسی به داده‌های احراز هویت کاربر که مرتبط با پودمان رمزنگاشتی است.
- استفاده از یک سازوکار احراز هویت (مانند سازوکار درونداد به سامانه) متناظر با پودمان.
- درخواست‌های صریح جهت بر اتخاذ نقش متصدی رمز
- تخصیص یک تابع به نقش متصدی رمز

۳- الزامات سامانه عامل برای سطح امنیتی سوم

در این سطح علاوه بر الزامات ذکرشده در سطوح اول و دوم، الزامات ذیل نیز باید اعمال گردد:

- تمام نرم‌افزار و ثابت‌افزار رمزنگاشتی، کلیدهای رمزنگاشتی، واحدهای اطلاعاتی حیاتی و اطلاعات کنترلی و وضعیت باید تحت کنترل موارد زیر باشد:

○ یک سامانه‌عامل که الزامات عملیاتی توصیف شده در رخنمون‌های حفاظتی مربوط به توسعه نرم‌افزار را طبق استاندارد CC در سطح سوم تضمین ارزیابی[1]، برآورده سازد.

یا

○ یک سامانه‌عامل معادل ارزیابی شده قابل اعتماد.

- انتقال کلیه اطلاعات مخفی و محرمانه نظیر کلیدهای رمزنگاشتی، داده‌های کنترلی و اطلاعات احراز هویت باید از طریق یک سازوکار قابل اعتماد (مانند یک درگاه فیزیکی درونداد/برونداد اختصاصی یا یک مسیر مطمئن[2]) صورت گیرد. این کانال امن در واقع بین پودمان رمزنگاشتی و نرم‌افزاری که از پودمان رمزنگاشتی استفاده می‌کند باید تشکیل گردد و در آن کلیه اطلاعات باید به‌صورت رمزبندی شده تبادل گردد. کانال مذکور می‌تواند از طریق توافق، یک کلید نشست بین نرم‌افزار و پودمان رمزنگاشتی ایجاد گردد. در مستندسازی باید چگونگی ایجاد کانال امن در پودمان رمزنگاشتی به طور کامل تشریح گردد؛
- علاوه بر الزامات ممیزی مطرح شده در سطح دوم امنیتی، رویدادهای زیر نیز باید توسط ساز وکار ممیزی

1 - Evaluation Asurance Level 3 (EAL3)

۲ - Trusted Path

ثبت شود:

- تلاش‌های صورت گرفته برای استفاده از قابلیت مسیر مطمئن و
- شناسایی راه‌انداز و مقصد مسیر مطمئن

۴- الزامات سامانه عامل برای سطح امنیتی چهارم

علاوه بر الزامات مطرح شده در سه سطح قبلی، در سطح چهارم موارد ذیل نیز باید درنظر گرفته‌شود:

- تمام نرم‌افزار و ثابت‌افزار، کلیدهای رمزنگاشتی و واحدهای اطلاعاتی حیاتی و اطلاعات کنترلی و وضعیت باید تحت کنترل موارد زیر باشد:
  - یک سامانه‌عامل که الزامات عملیاتی توصیف شده در رخنمون‌های حفاظتی مربوط به توسعه نرم‌افزار را طبق استاندارد CC در سطح چهارم تضمین ارزیابی(EAL4)[1]، برآورده سازد.

یا

- یک سامانه‌عامل معادل ارزیابی شده و قابل اعتماد.

### ۷-۵ مدیریت کلیدهای رمزنگاشتی

الزامات امنیتی برای مدیریت کلید رمزنگاشتی، تمام چرخه حیات کلیدهای رمزنگاشتی، اجزای کلید رمزنگاشتی و واحدهای اطلاعاتی حیاتی به‌کار رفته توسط پودمان رمزنگاشتی را دربر می‌گیرد. در پودمان‌های رمزنگاشتی مدیریت کلید شامل تولید کلید و عدد تصادفی، استقرار کلید، توزیع کلید، درونداد و برونداد کلید، ذخیره‌سازی کلید و امحاء کلید است. یک پودمان رمزنگاشتی ممکن است سازوکارهای مدیریت کلید سایر پودمان‌های امنیتی را نیز به‌کار بندد. کلیدها و واحدهای اطلاعاتی حیاتی رمزبندی شده، به آن دسته از کلیدها و واحدهای اطلاعاتی حیاتی اتلاق می‌شود که با استفاده از یک الگوریتم یا تابع امنیتی مصوب رمزبندی شده باشند. کلیدها و واحدهای اطلاعاتی حیاتی که با استفاده از الگوریتم‌های غیرمصوب رمزبندی می‌گردند، در حوزه این استاندارد به عنوان رمز نشده در نظر گرفته می‌شوند.

کلیدهای مخفی، خصوصی و واحدهای اطلاعاتی حیاتی ذخیره شده در پودمان‌های رمزنگاشتی باید در مقابل افشاسازی، تغییر و جایگزینی غیرمجاز محافظت گردند، همچنین کلیدهای عمومی نیز باید در مقابل تغییر و جایگزینی غیرمجاز محافظت گردند.

در مستندسازی باید انواع کلیدهای رمزنگاشتی به‌کار رفته در پودمان رمزنگاشتی و اجزا و پارامترهای آن‌ها تشریح گردد.

---

1 - Evaluation Asurance Level 4

### ۵-۷-۱ مولدهای اعداد تصادفی(RNG)[1]

مولدهای اعداد تصادفی در پودمان‌های رمزنگاشتی به طور معمول به عنوان یکی از ارکان تولید کلید مورد استفاده قرار می‌گیرند. اگر پودمان رمزنگاشتی، مولدهای مصوب و یا غیرمصوب را در یک حالت عملیاتی مصوب به کار بندد، داده‌های برونداد مولد اعداد تصادفی، باید آزمون تولید داده‌های تصادفی مداوم که در زیربند ۵-۹-۲ توصیف شده‌است را بگذراند. مولدهای اعداد تصادفی مصوب باید در معرض آزمون الگوریتم رمزنگاشتی در زیربند ۵-۹-۱ قرار بگیرند.

در صورت وجود یک مولد عدد تصادفی غیر قطعی مصوب استاندارد، می‌توان از آن برای تولید کلید یا تولید بذر[2] مولدهای عدد تصادفی قطعی مورد استفاده در تولید کلید بهره گرفت. مولدهای غیرقطعی تجاری موجود می‌تواند برای تولید بذر مولدهای عدد تصادفی قطعی مصوب مورد استفاده قرار گیرند. مولدهای عدد تصادفی غیرقطعی باید تمامی الزامات قابل اعمال برای مولدهای عدد تصادفی موجود در این استاندارد را برآورده کند.

برای تولید کلیدهای رمزنگاشتی مورد استفاده برای یک تابع امنیتی مصوب باید از مولد عدد تصادفی مصوب استفاده شود. برونداد یک مولد عدد تصادفی غیرمصوب می‌تواند ۱- به عنوان درونداد (برای مثال، بذر و کلید بذر) به یک مولد عدد تصادفی قطعی مصوب یا ۲- جهت تولید بردارهای آغازه(IV)[3] برای توابع امنیتی مصوب مورد استفاده قرار بگیرد. بذر و کلید بذر نباید دارای مقدار یکسانی باشند.

در مستندسازی باید مولدهای اعداد تصادفی (مصوب و غیر مصوب) مورد استفاده در پودمان رمزنگاشتی توصیف شوند.

### ۵-۷-۲ تولید کلید

پودمان رمزنگاشتی می‌تواند کلیدهای رمزنگاشتی را به‌صورت داخلی تولید کند. کلیدهای رمزنگاشتی تولید شده توسط پودمان رمزنگاشتی جهت استفاده در الگوریتم‌ها یا توابع امنیتی مصوب باید با استفاده از روش‌های تولید کلید مصوب تولید شوند. اگر روش تولید کلید مصوب نیازمند دریافت درونداد از یک مولد عدد تصادفی باشد، برای این منظور باید یک مولد عدد تصادفی مصوب که الزامات زیربند ۵-۷-۱ این استاندارد را برآورده می‌کند به‌کار گرفته شود.

افشاسازی روش تولید کلید (به عنوان مثال، حدس مقدار بذر برای مقدار دهی اولیه مولد عدد تصادفی قطعی) باید کمینه عملیاتی به اندازه عملیات مورد نیاز برای تعیین مقدار کلید تولید شده لازم داشته باشد

1 - Random Number Generator
2 -Seed
۳ - initialization vectors

(به عبارتی، پیچیدگی محاسباتی شکستن الگوریتم تولید کلید از جستجوی کامل کلید تولید شده، کمتر نباشد).

اگر یک بذر مرتبط با کلید، در طول فرایند تولید کلید وارد شده باشد، درونداد این بذر باید الزامات درونداد کلید در زیربند ۵-۷-۴ را رعایت کند. اگر مقادیر میانی تولید کلید قرار باشد از پودمان رمزنگاشتی خارج شوند، باید به شکل رمز شده یا با استفاده از رویه‌های تقسیم دانش خارج شوند.

مستندسازی باید هریک از شیوه‌های تولید کلید (مصوب یا غیر مصوب) به کار رفته در پودمان رمزنگاشتی را توصیف کند.

### ۵-۷-۳ استقرار کلید[1]

استقرار کلید ممکن است به *روش خودکار* (مانند استفاده از یک الگوریتم کلید عمومی)، *روش دستی* (استفاده از یک افزاره بارگذاری کلید که به صورت دستی قابل انتقال است) یا ترکیبی از روش‌های خودکار و دستی اجرا شود. اگر روش‌های برقراری کلید، توسط یک پودمان رمزنگاشتی به کار گرفته شوند، فقط روش‌های مصوب استقرار کلید باید مورد استفاده قرار گیرند.

افشاسازی امنیت روش استقرار کلید (برای مثال، افشاسازی الگوریتم مورد استفاده برای برقراری کلید) باید کمینه تعداد عملیاتی به اندازه تعداد عملیات تعیین مقدار کلید رمزنگاشتی انتقال یافته یا توافق شده نیاز داشته باشد.

اگر روش انتقال کلید[2] مورد استفاده قرار گیرد، کلید رمزنگاشتی انتقال یافته می‌باید الزامات درونداد و برونداد مطرح شده در زیربند ۵-۷-۴ را برآورده کند. اگر روش توافق کلید به‌کار رفته باشد (مانند یک کلید رمزنگاشتی که از مقادیر میانی مشترک، مشتق شده‌است)، مقادیر مشترک نیازی به رعایت الزامات درونداد/برونداد مطرح در زیربند ۵-۷-۴ ندارند.

مستندسازی باید روش‌های استقرار کلید به‌کارگرفته شده توسط پودمان رمزنگاشتی را توصیف کند.

### ۵-۷-۴ درونداد و برونداد کلید

کلیدهای رمزنگاشتی ممکن است به پودمان رمزنگاشتی وارد یا از آن خارج شوند. اگر کلیدهای رمزنگاشتی به پودمان وارد یا از آن خارج می‌شوند، درونداد و برونداد آن‌ها باید یا به صورت دستی (به طور مثال با استفاده از صفحه کلید) یا به صورت الکترونیکی (به طور مثال با کارت یا نمودافزار هوشمند یا سایر پودمان‌های الکترونیکی بارگذاری کلید) انجام شود.

---

1 - Key Establishment
2 - Key Transport

چنانچه جهت انجام عملیات تولید کلید، بذر مولد اعداد تصادفی از بیرون وارد پودمان رمزنگاشتی گردد، درونداد بذر مولد تصادفی نیز باید به روش مشابه درونداد کلیدهای رمزنگاشتی صورت پذیرد.

در حالت عملیاتی مصوب کلیدهای خصوصی و مخفی رمزشده که به پودمان رمزنگاشتی وارد یا از آن خارج می‌شوند، باید از الگوریتم‌های مصوب جهت رمزبندی این کلیدها استفاده گردد.

کلیدهایی که به روش‌های دستی وارد می‌شوند، در هنگام درونداد به پودمان رمزنگاشتی باید با استفاده از آزمون درونداد کلید دستی توصیف شده در زیربند ۵-۹-۲ مورد بررسی صحت قرار گیرند. در هنگام وارد نمودن کلید، مقدار واردشده به صورت دستی، جهت درستی‌سنجی دیداری و بالابردن دقت، ممکن است موقتی نمایش داده شود. اگر کلیدهای رمزنگاشتی یا اجزای کلید رمزشده به‌صورت دستی به پودمان رمزنگاشتی وارد شوند، در این صورت مقادیر رمز نشده آن‌ها نباید نمایش داده‌شود.

در مستندسازی باید روش‌های درونداد و برونداد کلید به کار گرفته شده در پودمان رمزنگاشتی تشریح گردد.

**۵-۷-۴-۱ درونداد و برونداد کلید برای سطوح امنیتی اول و دوم**

برای سطوح اول و دوم، کلیدهای خصوصی و محرمانه برقرارشده به روش خودکار، باید به صورت رمزشده به پودمان رمزنگاشتی وارد یا از آن خارج شوند. کلیدهای خصوصی و محرمانه برقرارشده به روش دستی، ممکن است به صورت متن آشکار، به پودمان رمزنگاشتی وارد و یا از آن خارج شوند.

**۵-۷-۴-۲ درونداد و برونداد کلید برای سطوح امنیتی سوم و چهارم**

برای سطوح امنیتی سوم و چهارم:

- کلیدهای مخفی و کلیدهای خصوصی برقرارشده به روش خودکار باید به شکل رمزشده به پودمان رمزنگاشتی وارد یا خارج شوند.

- کلیدهای مخفی و کلیدهای خصوصی برقرارشده به روش دستی، باید یا به‌صورت رمزشده یا با استفاده از رویه‌های تقسیم دانش (یعنی به صورت دو یا چند جزء کلید رمزنگاشتی متن آشکار) به پودمان رمزنگاشتی وارد یا خارج شوند.

اگر رویه‌های تقسیم دانش به کار گرفته‌شود:

- پودمان رمزنگاشتی باید کاربر وارد کننده یا خارج کننده هر جزء کلید را به‌صورت جداگانه احراز هویت کند.

- اجزای کلیدهای رمزنگاشتی متن آشکار باید به‌صورت مستقیم (برای مثال، با استفاده از یک مسیر مطمئن یا یک کابل مستقیم متصل) و بدون دخالت یا واسطه هیچ‌گونه سامانه‌ای به پودمان رمزنگاشتی وارد یا خارج شوند (به ۵-۲ مراجعه شود).

- کمینه دو جزء کلید باید برای بازسازی مجدد کلید رمزنگاشتی اصلی لازم باشد.
- مستندسازی باید ثابت کند که اگر دانستنn جزء از کلید برای بازسازی مجدد کلید مورد نیاز باشد، دانستن n-1 جزء از کلید هیچ اطلاعاتی در مورد کلید اصلی به‌جز طول آن فراهم نکند.
- مستندسازی باید رویه‌های تقسیم دانش به‌کار رفته توسط پودمان رمزنگاشتی را توصیف کند.

### ۵-۷-۵ ذخیره‌سازی کلید

کلیدهای رمزنگاشتی ممکن است به‌صورت رمزبندی شده یا به‌صورت رمز نشده در پودمان رمزنگاشتی ذخیره شوند. کلیدهای مخفی و خصوصی رمز نشده نباید از بیرون پودمان رمزنگاشتی توسط متصدیانی غیر مجاز قابل دسترس باشند.

پودمان رمزنگاشتی باید کلیدهای رمزنگاشتی (مخفی، خصوصی یا عمومی) ذخیره شده در پودمان را با موجودیت صحیح (به عنوان مثال، شخص، گروه یا فرایند) که کلیدها به وی تخصیص داده شده‌اند، مرتبط سازد.

در مستندسازی باید روش‌های به‌کار رفته توسط پودمان رمزنگاشتی برای ذخیره‌سازی کلید تشریح گردد.

### ۵-۷-۶ امحای کلید

یک پودمان رمزنگاشتی باید روشی را جهت امحاء کلیدهای رمزنگاشتی خصوصی و مخفی و سایر واحدهای اطلاعاتی حیاتی رمز نشده موجود در پودمان فراهم کند. امحای کلیدهای رمزنگاشتی یا واحدهای اطلاعاتی حیاتی که رمز شده هستند یا به طور منطقی یا فیزیکی در درون یک پودمان معتبر تعبیه شده محافظت می‌شوند (مطابق با الزامات این استاندارد) نیاز نیست.

در مستندات باید روش‌های به کارگرفته شده در پودمان رمزنگاشتی جهت امحای کلیدهای رمزنگاشتی تشریح گردد.

## ۵-۸ تداخل/ سازگاری الکترومغناطیسی

پودمان رمزنگار باید الزامات زیر را برای تداخل الکترومغناطیسی(EMI) و سازگاری الکترومغناطیسی(EMC) برآورده کند.
مستندات باید در بردارنده اثبات رعایت الزامات EMI/EMC باشند.

### ۵-۸-۱ سطوح امنیتی اول و دوم

برای سطوح امنیتی اول و دوم، یک پودمان رمزنگاشتی باید کمینه با الزامات EMI/EMC توصیف شده در بند ۱۵، زیر بخش B، کلاس A از استاندارد FCC، مطابقت داشته باشد.

### ۵-۸-۲ سطوح امنیتی سوم وچهارم

برای سطوح امنیتی سوم و چهارم، یک پودمان رمزنگاشتی باید کمینه با الزامات EMI/EMC توصیف شده در بند ۱۵، زیر بخش B، کلاس B از استاندارد FCC، مطابقت داشته باشد.

## ۵-۹ خودآزمایی

یک پودمان امنیتی جهت اطمینان از آن‌که به درستی کار می‌کند، باید *خودآزمایی‌های آغازین*[1] و نیز *آزمون‌های شرطی*[2] را انجام دهد. خودآزمایی‌های آغازین، باید به محض روشن‌شدن پودمان رمزنگاشتی انجام شوند. خودآزمایی‌های شرطی در زمانی‌که یک تابع یا یک عملیات امنیتی کاربردی فراخوانده می‌شوند، ( به عبارتی، توابع امنیتی که نیاز به خودآزمایی دارند) باید اجرا شوند. یک پودمان رمزنگاشتی ممکن است علاوه بر آزمون‌های توصیف شده در این استاندارد، خودآزمایی‌های آغازین یا شرطی دیگری را نیز انجام دهد.

اگر پودمان رمزنگاشتی در یکی از خودآزمایی‌ها شکست بخورد، باید وارد یک حالت خطا شده و یک علامت نشانگر خطا را در واسط وضعیت برونداد نمایان سازد و تا زمانی که در حالت خطا قرار دارد نباید هیچ نوع عملیات رمزنگاشتی را اجرا کند و یا برونداد در واسط برونداد داده داشته باشد.

در مستندسازی باید موارد ذیل مشخص گردد:

- خودآزمایی‌های اجرا شده توسط پودمان رمزنگاشتی شامل خودآزمایی‌های آغازین و شرطی؛
- حالت‌های خطایی که پودمان رمزنگاشتی در صورت مواجه با شکست در خودآزمایی، می‌تواند وارد این حالت‌ها شود؛
- شرایط و عملیاتی که جهت برونداد از حالت خطا و بازگشت پودمان رمزنگاشتی به حالت عادی مورد نیاز و ضروری می‌باشند (به عنوان مثال این شرایط و عملیات ممکن است شامل تعمیر و نگهداری پودمان رمزنگاشتی یا بهره‌برداری آن به سازنده جهت اشکال‌زدایی و آماده‌سازی مجدد باشد).

### ۵-۹-۱ آزمون‌های آغازین

خودآزمایی آغازین جهت اطمینان از درستی عملکرد پودمان رمزنگاشتی در هر بار استفاده از پودمان رمزنگاشتی، پس از تغذیه[3] پودمان رمزنگاشتی به‌صورت خودکار و بدون دخالت کاربر اعمال می‌گردد. اگر انجام عملیات خودآزمایی آغازین همراه با خطا صورت گیرد، پودمان رمزنگاشتی باید وارد حالت خطا گردد. در حالت خطا پودمان رمزنگاشتی نباید قادر به انجام هیچ‌یک از عملیات رمزنگاشتی و امنیتی باشد. علاوه بر انجام آزمون آغازین، به منظور فراهم آوردن امکان آزمون دوره‌ای، این امکان باید فراهم شود که با درخواست کاربر در زمان‌هایی دیگری نظیر راه‌اندازی مجدد، آزمون‌های مرتبط با آزمون آغازین صورت پذیرد.

---

1 - Power-Up Self Test
2 - Conditional Self Test
3 - Power up

خودآزمایی در پودمان‌های رمزنگاشتی کمینه باید شامل آزمون‌های ذیل باشد:

۱- آزمون الگوریتم رمزنگاشتی

آزمون الگوریتم‌های رمزنگاشتی ممکن است به دو صورت آزمون برونداد با جواب مشخص[1] و آزمون سازگاری دوگانه[2] صورت گیرد. جهت آزمایش صحت عملکرد الگوریتم‌های غیر تصادفی از آزمون برونداد با جواب مشخص استفاده می‌شود، بدین ترتیب که برونداد جدید یک الگوریتم رمزنگاشتی با برونداد از قبل تولید شده مقایسه می‌شود، در صورت عدم برابری این مقادیر، آزمون مذکور با شکست مواجه خواهد شد. جهت آزمایش صحت عملکرد الگوریتم‌های تصادفی از آزمون عملکرد الگوریتم به روش دوگانه استفاده می‌شود؛ بدین ترتیب که صحت عملکرد هر الگوریتم با توجه به ماهیت دوگانه آن آزمون تعیین می‌گردد؛ به عنوان مثال جهت آزمون یک الگوریتم رمزبندی تصادفی، یک داده آزمون با استفاده از الگوریتم مذکور رمزبندی شده و داده رمزشده با استفاده از الگوریتم رمزگشایی متناظر، رمزگشایی گشته و مقدار اطلاعات رمزگشایی شده با داده آزمون اولیه مقایسه می‌گردد؛ چنانچه این دو مقدار با هم برابر نباشند، آزمون مذکور با شکست مواجه می‌شود.

اگر در یک پودمان رمزنگاشتی دو روش پیاده‌سازی مستقل برای یک الگوریتم رمزنگاشتی وجود داشته باشد، در این‌صورت:

- آزمون برونداد با جواب مشخص ممکن است حذف شود.
- بروندادهای دو روش پیاده‌سازی باید به طور مداوم با یکدیگر مقایسه گردند؛
- اگر بروندادهای دو روش پیاده‌سازی با هم برابر نبودند، آزمون الگوریتم رمزنگاشتی باید رد شود.

۲- آزمون یکپارچگی نرم‌افزار/ثابت‌افزار

در هنگام روشن شدن پودمان رمزنگاشتی، آزمون یکپارچگی ثابت‌افزار/ نرم‌افزار پودمان رمزنگاشتی باید با استفاده از کد تشخیص خطا یا یک سازوکار احراز هویت مصوب (نظیر یک کد تشخیص احراز هویت پیام یا امضای رقمی مصوب) به کلیه اجزای نرم‌افزاری و ثابت‌افزار پودمان رمزنگاشتی اعمال شود. اگر نتیجه محاسبه شده در این آزمون با مقدار قبلی برابر نبود، آزمون یکپارچگی با شکست مواجه خواهد شد. آزمون یکپارچگی مذکور برای اجزایی از نرم‌افزار و ثابت‌افزار پودمان رمزنگاشتی که از الزامات این استاندارد مستثنی هستند (به زیربند ۵-۱ مراجعه شود)، لازم نمی‌باشد.

در صورتی که از کد تشخیص خطا استفاده شود، طول این کد باید کمینه ۱۶ بیت باشد.

۳- آزمون توابع حیاتی

1 - known-answer test
2 - pair-wise consistency test

سایر توابع امنیتی حیاتی پودمان رمزنگاشتی، باید در هنگام راه‌اندازی پودمان به عنوان قسمتی از آزمون‌های آغازین آزمایش شوند. سایر توابع حیاتی اجراشده در شرایط خاص باید به عنوان آزمون‌های شرطی آزموده شوند.
مستندات باید کلیه توابع امنیتی حیاتی لازم جهت انجام عملیات امنیتی در یک پودمان رمزنگاشتی را توصیف کنند. همچنین کلیه آزمون‌های آغازین و شرطی کاربرد پذیر اجراشده توسط پودمان را باید تعیین کند.

### ۵-۹-۲ آزمون‌های شرطی

آزمون‌های شرطی، وقتی که شرایط توصیف شده برای آزمون‌های سازگاری زوج‌کلیدها، بارگذاری نرم‌افزار یا ثابت‌افزار، درونداد دستی کلید[1]، تولید مداوم اعداد تصادفی و نیز آزمون کنارگذار، واقع شوند، باید توسط یک پودمان رمزنگاشتی اجرا شوند.

#### ۵-۹-۲-۱ آزمون سازگاری دو به دو (برای کلیدهای عمومی و خصوصی)

اگر یک پودمان کلیدهای خصوصی و عمومی را تولید کرد، در این صورت آزمون‌های سازگاری دو به دو زیر باید برروی آن‌ها انجام شود:

۱- اگر کلیدها جهت اجرای یک روش انتقال کلید مصوب استفاده شوند، آنگاه کلید عمومی باید یک مقدار رمز نشده را رمز کند. مقدار رمزشده حاصل باید با مقدار رمز نشده اولیه مقایسه شود. در صورتی که هر دو مقدار برابر باشند، آزمون باید با شکست مواجه شود. در صورتی که دو مقدار با هم متفاوت باشند، کلید خصوصی باید جهت رمزگشایی مقدار رمزشده مورد استفاده قرار گیرد و مقدار رمزگشایی شده با مقدار رمز نشده اولیه مقایسه شود. در صورتی که مقادیر با هم برابر نباشند، آزمون باید با شکست مواجه شود.

۲- اگر کلیدها جهت انجام محاسبه و درستی‌سنجی امضای رقمی، استفاده شده‌اند، آنگاه سازگاری کلیدهای خصوصی و عمومی باید با محاسبه و درستی‌سنجی امضای رقمی آزمایش می‌شود. در صورت عدم درستی‌سنجی امضای رقمی، آزمون باید با شکست مواجه شود.

#### ۵-۹-۲-۲ آزمون بارگذاری ثابت‌افزار یا نرم‌افزار

اگر اجزای نرم‌افزاری یا ثابت‌افزاری بتوانند از بیرون در پودمان رمزنگاشتی بارگذاری شوند، آزمون‌های زیر باید انجام شود:

۱- در صورتی که نرم‌افزار و اجزای ثابت‌افزار از بیرون در پودمان رمزنگاشتی بارگذاری شده باشند، یک روش احراز هویت مصوب (مانند یک کد احراز هویت پیام ، امضای رقمی و یا کد احراز هویت پیام چکیده(HMAC)[2]) باید به تمام اجزای نرم‌افزار یا ثابت افزار اعمال شود.

---

1 - Manual Key Entry

۲ - hash message authentication code

۲- نتیجه محاسبه شده باید با نتیجه تولید شده قبلی مقایسه شود. اگر نتیجه محاسبه شده با نتیجه قبلی برابر نباشد، این آزمون باید با شکست مواجه شود.

### ۵-۹-۲-۳ آزمون درونداد دستی کلید

اگر کلیدهای رمزنگاشتی یا اجزای کلید به‌صورت دستی وارد شوند، این آزمون‌ها باید انجام شود:

۱- کلید رمزنگاشتی یا اجزای کلید، باید یک EDC را به کار گرفته باشند و یا از تکرار درونداد استفاده کرده باشند.

۲- اگر یک EDC استفاده شده باشد، باید طول آن کمینه ۱۶ بیت باشد.

۳- در صورتی که EDC نتواند درستی‌سنجی شود یا تکرار درونداد‌ها با هم مطابقت نداشته باشد، آزمون با شکست مواجه می‌شود.

### ۵-۹-۲-۴ آزمون تولید مداوم اعداد تصادفی

اگر یک پودمان رمزنگاشتی، مولدهای اعداد تصادفی مصوب یا غیر مصوب را در یک شیوه عملکرد مصوب به‌کار بگیرد، باید آزمون‌های زیر را برای هر مولد انجام دهد:

۱- اگر هر فراخوانی از یک مولد عدد تصادفی، بلوک‌هایی n بیتی (n>15) را تولید کند ، اولین بلوک n بیتی تولیدشده بعد از روشن شدن، آماده‌سازی یا راه‌اندازی مجدد پودمان رمزنگاشتی، نباید مورد استفاده قرار گیرد؛ اما باید برای مقایسه با بلوکn بیتی بعدی که تولید می‌شود، ذخیره شود. هر بلوک n بیتی جدید تولید شده باید با بلوک n بیتی قبلی خود مقایسه شود. در صورتی که با هم برابر باشند، آزمون با شکست مواجه شده‌است.

۲- اگر هر فراخوانی از یک مولد عدد تصادفی، کمتر از ۱۶ بیت فراهم کند، اولین n بیتی تولید شده بعد از راه‌اندازی، آماده‌سازی یا راه‌اندازی مجدد (به ازای n>15) نباید به کارگرفته‌شود. اما باید برای مقایسه با مقدار n بیتی تولیدشده بعدی ذخیره شود. هر دنباله n بیتی جدید تولید شده، باید با دنباله n بیتی قبلی خود مقایسه شود. در صورتی که با هم برابر باشند، آزمون با شکست مواجه شده‌است.

### ۵-۹-۲-۵ آزمون کنارگذار

اگر یک پودمان رمزنگاشتی آن جایی که خدمات بتوانند بدون نیاز به پردازش رمزنگاشتی ارائه شوند (مانند انتقال داده‌های آشکار در درون پودمان)، توانایی کنارگذار را پیاده‌کرده باشد، آزمون‌های زیر جهت اطمینان از اینکه هیچ روزنه‌ای جهت برونداد غیر عمدی داده‌های متن آشکار وجود ندارد، انجام می‌شود:

۱- در هنگامی که بین یک خدمت کنارگذار انحصاری و یک خدمت رمزنگاشتی انحصاری عمل سودهی کردن صورت می‌گیرد، پودمان رمزنگاشتی باید صحت عملکرد خدمت‌های نیازمند به فرایند رمزنگاشتی را آزمایش کند.

۲- اگر یک پودمان رمزنگاشتی بتواند به‌صورت خودکار بین یک خدمت کنارگذار و یک خدمت رمزنگاشتی سودهی کند، در صورت اصلاح سازوکارهای سودهی کردن، باید درستی این سازوکارها آزمایش و بررسی شود.

مستندات باید سازوکار یا منطق کنترل کردن رویه سودهی را توصیف کنند.

### ۵-۱۰ تضمین طراحی

تضمین طراحی عبارت است از: به‌کارگیری تجربه‌های برتر سازنده پودمان رمزنگاشتی در طول طراحی، توسعه و عملکرد پودمان، دادن تضمین اینکه پودمان رمزنگاشتی منطبق با الزامات این استاندارد، به درستی آزمایش، پیکربندی، توسعه و عرضه شده‌است و اینکه مستندات راهنمای استفاده از پودمان رمزنگاشتی به‌طور مناسبی فراهم شده است. در ادامه الزامات امنیتی مدیریت پیکربندی، تحویل و به‌کارگیری، توسعه و مستندات راهنمای پودمان رمزنگاشتی تشریح می‌شود.

#### ۵-۱۰-۱ مدیریت پیکربندی

*مدیریت پیکربندی توصیف کننده* الزامات امنیتی سامانه مدیریت پیکربندی است که توسط سازنده پودمان رمزنگاشتی پیاده‌سازی می‌شود. مدیریت پیکربندی تضمین می‌کند که کلیه الزامات و ویژگی‌های عملیاتی در پیاده‌سازی پودمان تحقق یافته‌اند.

یک سامانه مدیریت پیکربندی باید برای پودمان رمزنگاشتی و کلیه اجزای درون محدوده رمزنگاری آن و همچنین مستندات آن پیاده‌سازی شود. هر نسخه اقلام پیکربندی (مانند خود پودمان، اجزای پودمان، راهنمای کاربری، خط‌مشی‌های امنیتی و سامانه‌عامل) که شامل پودمان و مستندات مربوطه هستند، باید یک شماره شناسایی منحصر به فرد گرفته و به آن برچسب شود.

#### ۵-۱۰-۲ به کارگیری و بهره‌برداری[1]

*به کارگیری و بهره‌برداری* توصیف کننده الزامات امنیتی برای بهره‌برداری، نصب و شروع به کار امن پودمان رمزنگاشتی را توصیف کرده و تضمین می‌کند که پودمان به‌صورت امن به کاربر مجاز بهره‌برداری و در شرایط صحیح و امن نصب و آماده‌سازی اولیه شده‌است.

۱- سطح امنیتی اول

رویه نصب، راه‌اندازی و شروع به کار امن پودمان رمزنگاشتی باید در مستندات تشریح گردد.

1 - Deployment and Operation

۲- سطوح امنیتی دوم، سوم و چهارم

علاوه بر الزامات سطوح اول، رویه‌های لازم جهت حفظ امنیت در حین توزیع و بهره‌برداری نسخه‌های پودمان به کاربر مجاز نیز باید در مستندات تشریح گردد.

### ۵-۱۰-۳ توسعه

*توسعه*، الزامات امنیتی جهت نمایش و ارائه قابلیت‌های امنیتی پودمان رمزنگاشتی در سطوح مختلف را توصیف می‌کند. توسعه، تضمین می‌کند که پیاده‌سازی پودمان رمزنگاشتی، متناظر با خط‌مشی امنیتی و ویژگی‌های عملیاتی آن می باشد.

*ویژگی‌های عملیاتی*، به توصیف سطح بالای درگاه‌ها و واسط‌های قابل دیدن برای کاربر و توصیف سطح بالای رفتار پودمان رمزنگاشتی اتلاق می‌شود.

۱- سطح امنیتی اول

الزامات زیر باید در سطح امنیتی اول لحاظ شود:

- مستندات باید تناظر و ارتباط طراحی اجزای سخت‌افزاری، نرم‌افزار و ثابت‌افزار پودمان رمزنگاشتی را با خط‌مشی امنیتی پودمان توصیف کنند؛
- اگر پودمان رمزنگاشتی دارای اجزای نرم‌افزاری یا ثابت افزاری باشد، در مستندات باید کد منبع این اجزای نرم‌افزاری و ثابت‌افزاری به همراه توضحیات متناظر با هر بخش کد که ارتباط بین اجزای طراحی و الزامات اعمال شده را تشریح می‌کند، آورده شود؛
- اگر پودمان رمزنگاشتی دارای اجزای سخت افزاری باشد، در مستندات باید الگوها و/یا زبان توصیف سخت‌افزار(HDL)[1] برای اجزی سخت افزاری توصیف شود.

۲- سطح امنیتی دوم

در این سطح علاوه بر الزامات قید شده در سطح اول، الزامات ذیل نیز باید اعمال گردد:

- در مستندات باید یک توصیف کارکردی از پودمان ارائه شود که در آن پودمان رمزنگاشتی، درگاه‌ها و واسط‌های خارجی پودمان و هدف این واسط‌ها به طور غیر رسمی توصیف می‌شود.

۳- سطح امنیتی سوم

در این سطح علاوه بر الزامات قید شده در سطوح اول و دوم، الزامات زیر نیز باید اعمال شود:

1 - Hardware Description Language

- تمامی اجزای نرم‌افزاری و ثابت‌افزاری پودمان رمزنگاشتی باید با استفاده از یک زبان سطح بالا پیاده‌سازی گردند. البته در موراد محدود، استفاده از زبان‌های سطح پایین نظیر اسمبلی یا ریزکد جهت بالابردن کارآیی در پودمان رمزنگاشتی یا زمانی که کد سطح بالا در اختیار نیست، مجاز است.

- اگر از زبان توصیف سخت‌افزار استفاده شده‌است، کلیه اجزای سخت‌افزاری درون پودمان رمزنگاشتی باید با استفاده از یک زبان توصیف سطح بالا پیاده‌سازی شوند.

۴- سطح امنیتی چهارم

علاوه بر سطوح امنیتی اول، دوم و سوم، در سطح چهارم الزامات زیر باید اعمال شود:

- مستندات باید یک مدل رسمی را ارائه کنند که نقش‌ها و خصوصیات خط‌مشی امنیتی پودمان رمزنگاشتی را تشریح می‌کند. این مدل رسمی باید با استفاده از یک زبان رسمی توصیف شود که از یک نمادگذاری مبتنی بر ریاضیات از قبیل منطق مرتبه اول یا نظریه مجموعه‌ها بهره می‌گیرد.

- مستندات باید توضیحاتی ارائه کنند که سازگاری و جامعیت مدل رسمی را با توجه به خط‌مشی امنیتی پودمان رمزنگاشتی نشان دهد.

- مستندات باید یک اثبات غیر رسمی به منظور نشان دادن تناظر بین مدل رسمی و توصیف کارکردی، ارائه دهند.

- برای هر جزء سخت‌افزاری، نرم‌افزاری و ثابت‌افزار پودمان رمزنگاشتی، کد منبع باید با توضیحات کاملی تشریح شوند که توصیف کننده این موارد هستند: ۱- پیش‌شرط‌های لازم برای درونداد به اجزای پودمان، توابع یا رویه‌ها به منظور اجرای صحیح و ۲- پس‌شرط‌هایی که نشان دهنده عملکرد درست اجزای پودمان، توابع یا رویه‌ها هستند. پیش‌شرط‌ها و پس‌شرط‌ها می‌توانند با استفاده از هر نمادگذاری توصیف شوند که با جزئیات کامل و بدون ابهام رفتار اجزای پودمان، توابع یا رویه‌ها را توضیح می‌دهند.

- مستندات باید یک اثبات غیر رسمی از تناظر بین طراحی پودمان رمزنگاشتی و توصیف کارکردی را توصیف کنند.

### ۴-۱۰-۵ مستندات راهنما

*راهنمای متصدی رمز* در رابطه با پیکربندی صحیح، نگهداری و مدیریت پودمان رمزنگاشتی می باشد. *راهنمای کاربر*، توابع امنیتی پودمان را به همراه دستورالعمل‌ها، راهنماها و اخطارها به منظور استفاده امن از پودمان، شرح می‌دهد. اگر پودمان رمزنگاشتی نقش تعمیر و نگهداری را پشتیبانی کند، راهنمای کاربر نهایی/متصدی رمز، خدمت‌های تعمیر و نگهداری فیزیکی و/یا منطقی را برای متصدیانی که نقش تعمیر و نگهداری را بر عهده می‌گیرند، توصیف می‌کند.

در مستندات راهنمای استفاده از پودمان رمزنگاشتی که برای نقش متصدی رمز تدوین می‌گردد باید موارد زیر توصیف شود:

- توابع و عملیات مدیریتی ، پیشامدهای امنیتی، پارامترهای امنیتی، درگاه‌های فیزیکی و واسط‌های منطقی پودمان رمزنگاشتی که توسط متصدی رمز قابل دسترس هستند؛
- رویه‌های اعمال مدیریت پودمان‌های رمزنگاشتی به روش امن
- پیش‌فرض‌هایی در خصوص رفتار کاربر که مربوط به عملکرد امن پودمان رمزنگاشتی هستند.

در مستند راهنمای استفاده پودمان رمزنگاشتی که برای نقش کاربر نهایی تدوین می‌گردد باید موارد زیر توصیف شود:

- توابع امنیتی مصوب، درگاه‌های فیزیکی و واسط‌های منطقی پودمان رمزنگاشتی که توسط کاربر نهایی قابل دسترس هستند؛
- کلیه مسؤولیت‌های کاربر نهایی که جهت حفظ امنیت پودمان رمزنگاشتی و عمکرد آن به‌صورت امن، مورد نیاز هستند.

### ۱۱-۵ اقدامات کاهش‌دهنده آسیب در برابر سایر حملات

پودمان‌های رمزنگاشتی ممکن است در مقابل حملات دیگری نیز آسیب‌پذیر باشند که در زمان انتشار این نسخه از استاندارد، الزامات امنیتی آزمون‌پذیر برای آن‌ها در دسترس نمی‌باشد (مانند حملاتی نظیر تحلیل توان[1]، تحلیل زمانی[2] و ایجاد خطا[3] ) و یا حملاتی که خارج از قلمرو این استاندارد هستند (مانند نفوذ از طریق بررسی تشعشعات[4]). در این نوع حملات، شخص مهاجم سعی می‌کند تا از طریق حمله، اطلاعاتی در ارتباط با کلیدهای رمزنگاشتی و اطلاعات محرمانه دیگری که در پودمان رمزنگاشتی ذخیره می‌گردند، به دست آورد. در ذیل این نوع حملات به طور خلاصه شرح داده شده‌است:

۱- **تحلیل توان:** حملات مبتنی بر تحلیل توان مصرفی به دو نوع کلی تحلیل ساده توان (SPA) [5] و تحلیل تفاضلی توان (DPA) [6] تقسیم می‌شوند. حملات SPA از طریق تحلیل مستقیم الگوهای مصرف توان الکتریکی و زمان‌سنجی‌های استخراج شده از دستورالعمل‌های خاص اجراشده توسط پودمان رمزنگاشتی در طی یک فرآیند رمزنگاشتی، اعمال می‌گردند. الگوهای مذکور از طریق پایش تغییرات مصرف توان الکتریکی پودمان رمزنگاشتی به دست آمده و با هدف آشکارسازی مولفه‌های مربوط به الگوریتم

1 - Power analysis
2 - Timing analysis
3 - Fault induction
4 - TEMPEST
5 - Simple Power Analysis
6 - Differential Power Analysis

رمزنگاشتی و اطلاعات مربوط به کلیدهای رمزنگاشتی مورد تحلیل قرار می‌گیرند. حملات DPA با همان اهداف حملات SPA ولی با استفاده از روش‌های آماری و یا فنون دیگر، تغییرات مصرف توان الکتریکی پودمان رمزنگاشتی را تحلیل می‌نمایند.

۲- **تحلیل زمانی**: بسیاری از برنامه‌ها به طور طبیعی شامل عملیات شاخه‌ای شرطی می‌باشند. بنابراین زمان اجرای هر بار یک الگوریتم باید دارای زمانی برابر با اجرای دیگر این الگوریتم نیست. در نتیجه این اختلافات زمانی، بدست‌آوردن و بازیابی اطلاعات پردازش شده توسط الگوریتم امکان‌پذیر می‌باشد. به همین دلیل است که زمان اجرای یک الگوریتم می‌تواند یک کانال جانبی را ایجاد کرده و اطلاعاتی را درباره داده‌های پردازش شده در طی محاسبات موجود در یک الگوریتم ارائه دهد که یک اصل کلی در حملات تحلیل زمانی می‌باشد.

۳- **ایجاد خطا:** حملات ایجاد خطا از طریق اعمال عوامل خارجی (نظیر امواج ریز موج و ایجاد تغییر در حرارت و ولتاژ) در پردازش پودمان‌های رمزنگاشتی ایجاد خطا می‌نمایند. تحلیل این خطاها و الگوهای آن می‌تواند در فرآیند مهندسی معکوس پودمان رمزنگاشتی مورد استفاده قرار گرفته و مولفه‌های خاصی از الگوریتم‌های رمزنگاشتی و اطلاعات مربوط به کلیدهای رمزنگاشتی را آشکارسازی کند.

۴- **نفوذ از طریق بررسی تشعشعات:** حملات TEMPEST، با تشخیص خارجی یا از راه دور مجموعه‌ای از سیگنال‌های الکترومغناطیسی ساطع شده از یک پودمان رمزنگاشتی و تجهیزات مرتبط با آن در طول پردازش، اعمال می‌شوند. چنین حملاتی می‌تواند برای به دست‌آوردن اطلاعاتی مثل کلید فشار داده شده، پیام نمایش داده شده در صفحه نمایش و شکل‌های دیگری از اطلاعات حیاتی و امنیتی (مانند کلیدهای رمزنگاشتی)، مورد استفاده قرار گیرد. یک سازوکار به کاررفته جهت کاهش مخاطرات چنین حملاتی، استفاده از حفاظ ویژه برای کلیه اجزا است. استفاده از حفاظ[1] در بسیاری از موارد موجب خنثی‌شدن تشعشعات و عدم انتشار آن‌ها به بیرون می‌شود.

اگر یک پودمان جهت کاهش آسیب یک یا چند حمله طراحی شده باشد، باید در خط‌مشی‌های امنیتی، سازوکارهای امنیتی به کارگرفته شده جهت کاهش آسیب شرح داده‌شود.

1 - Shield

# پیوست الف
# (الزامی)
# الزامات مستندسازی

بازبینه[1] زیر خلاصه‌ای از الزامات مستندسازی این استاندارد را بیان می‌کند. کلیه مستندات باید توسط سازنده پودمان رمزنگاشتی تهیه و ارائه شود.

## الف-۱ مشخصات پودمان رمزنگاشتی

الزامات مستندسازی جهت تعیین مشخصات و ویژگی‌های لحاظ شده در اجزای مختلف پودمان رمزنگاشتی شامل سخت‌افزار، نرم‌افزار و ثابت‌افزار در ذیل آورده شده‌است. این الزامات در مورد ریزکدها و نرم‌افزارهای سامانه‌ای که کد منبع آن‌ها در دسترس سازنده نمی‌باشد و یا در مورد هر یک از اجزای پودمان رمزنگاشتی که ارتباطی با امنیت ندارند، اعمال نمی‌گردد.

- مستندسازی باید توصیف‌کننده مشخصات اجزای مختلف پودمان رمزنگاشتی شامل سخت‌افزار، نرم‌افزار و ثابت‌افزار و مشخصات مرز رمزنگاشتی احاطه کننده این اجزا باشد. پیکربندی فیزیکی پودمان رمزنگاشتی باید در مستند تشریح گردد (کلیه سطوح امنیتی)؛

- در مستندسازی باید هر بخش از سخت‌افزار، نرم‌افزار یا ثابت‌افزار پودمان رمزنگاشتی که از الزامات این استاندارد مستثنی شده با ذکر دلایل منطقی تعیین شود (کلیه سطوح امنیتی)؛

- در مستندسازی باید درگاه‌های فیزیکی، واسط‌های منطقی و کلیه مسیرهای درونداد و برونداد اطلاعات در پودمان رمزنگاشتی مشخص شود (کلیه سطوح امنیتی)؛

- در مستندسازی باید کنترل‌های دستی و یا منطقی پودمان رمزنگاشتی، نمایش‌دهنده‌های فیزیکی و منطقی وضعیت و خصوصیات کاربردی فیزیکی، منطقی و الکتریکی مشخص شوند (کلیه سطوح امنیتی)؛

- در مستندسازی باید کلیه توابع امنیتی مصوب و غیرمصوب که در پودمان رمزنگاشتی در حالت‌های عملیاتی مصوب و غیرمصوب مورد استفاده قرار می‌گیرند، فهرست شوند (کلیه سطوح امنیتی)؛

- مستندسازی باید شامل نمودار بستک[2] نمایش‌دهنده تمامی اجزای اصلی سخت‌افزاری پودمان رمزنگاشتی و اتصال‌متقابل‌های اجزا، شامل تمامی پردازنده‌ها، میانگیرهای درونداد و برونداد، میانگیرهای متن آشکار/متن رمزی، میانگیرهای کنترلی، مخزن کلید، حافظه کاری و حافظه برنامه باشد. همچنین طرح فنی سخت‌افزار، نرم‌افزار و ثابت‌افزار باید در این مستند به زبان‌های سطح بالا توصیف گردد (کلیه سطوح امنیتی)؛

---

۱ - Checklist

۲ - Block Diagram

- مستندات باید توصیفی از طراحی سخت‌افزار، نرم‌افزار و اجزای ثابت‌افزار پودمان رمزنگاشتی را ارائه دهند (کلیه سطوح امنیتی)؛

- در مستندسازی باید کلیه اطلاعات مرتبط با امنیت شامل کلیدهای رمزنگاشتی مخفی و خصوصی (هم به صورت متن آشکار و هم رمزشده)، اطلاعات احراز هویت (مثل اسم‌رمزها یا PIN)، واحدهای اطلاعاتی حیاتی و اطلاعات محافظت شده دیگر (مانند رویدادها و داده‌های بازرسی) که آشکارشدن یا ایجاد تغییر در آن‌ها ممکن است امنیت پودمان رمزنگاشتی را به خطر اندازد، توصیف شود (کلیه سطوح امنیتی)؛

- مستندسازی باید دربردارنده خط‌مشی‌امنیتی پودمان رمزنگاشتی باشد. این خط‌مشی امنیتی باید شامل قواعد و رویه‌های مشتق شده از الزامات بیان شده در این استاندارد و قواعد مشتق شده از الزامات تکمیلی در نظر گرفته شده توسط سازنده باشد (کلیه سطوح امنیتی)؛

**الف-۲ درگاه‌ها و واسط‌ها**

در مستندسازی باید درگاه‌های فیزیکی و واسط‌های منطقی پودمان رمزنگاشتی و کلیه مسیرهای درونداد و برونداد توصیف گردد (کلیه سطوح امنیتی).

**الف-۳ نقش‌ها، خدمات و احراز هویت**

توصیف کلیه نقش‌های مجاز پشتیبانی شده توسط پودمان رمزنگاشتی. (کلیه سطوح امنیتی)
توصیف خدمات، عملیات یا توابع فراهم شده توسط پودمان رمزنگاشتی، هم مصوب و هم غیر مصوب. برای هر خدمت، توصیف دروندادهای خدمت، برونداد‌های خدمت متناظر و نقش(های) مجازی که این خدمت می‌تواند اجرا کند. (کلیه سطوح امنیتی)

توصیف هر خدمت فراهم شده توسط پودمان رمزنگاشتی که برای آن‌ها کاربر نهایی نیازی به برعهده گرفتن یک نقش مجاز ندارد و توصیف اینکه چگونه این خدمت‌ها کلیدهای رمزنگاشتی یا واحدهای اطلاعاتی حیاتی را دچار تغییر، افشا یا جابجایی نمی‌کنند یا در غیر اینصورت توصیف تاثیر آن‌ها بر امنیت پودمان.

توصیف سازوکار احراز هویت پشتیبانی شده توسط پودمان رمزنگاشتی، انواع داده احراز هویت مورد نیاز برای پیاده‌سازی سازوکار احراز هویت پشتیبانی شده، روش‌های مجاز مورد استفاده برای کنترل دسترسی به پودمان در سازوکار احراز هویت اولین بار و راه اندازی اولیه و مقاومت این سازوکارهای احراز هویت پشتیبانی شده توسط پودمان. (کلیه سطوح امنیتی)

**الف-۴ مدل‌های حالت متناهی**

در مستندسازی باید مدل‌های حالت تعریف شده برای پودمان رمزنگاشتی از طریق نمودارها و/یا جداولی که سطوح دسترسی برای هر حالت و چگونگی گذر از یک حالت به حالت دیگر، رخدادهای درونداد (شامل

داده‌های درونداد و کنترل‌های برونداد)، رویدادهای برونداد (شامل شرایط داخلی پودمان ، برونـدادهای داده و برونـدادهای وضعیت) که باعث گذر از یک حالت به حالت دیگر می‌شوند را به طـور کامـل توصـیف مـی‌کننـد، تشریح گردد (کلیه سطوح امنیتی).

**الف-۵ امنیت فیزیکی**

- توصیف پیکره فیزیکی پودمان و سطح امنیتی که سازوکارهای امنیت فیزیکـی پودمـان رمزنگاشـتی بـرای حصول آن پیاده‌سازی شده‌اند. توصیف سازوکار امنیت فیزیکی به کار گرفته شـده توسـط پودمـان. (کلیـه سطوح امنیتی)

- در صورتی که پودمان رمزنگاشتی دارای نقش تعمیر و نگهداری باشد کـه نیازمنـد دسترسـی فیزیکـی بـه محتویات پودمان است یا طراحی پودمـان بـه گونـه‌ای اسـت کـه دسترسـی فیزیکـی بـه آن در شـرایطی امکان‌پذیر است، توصیف واسـط دسترسـی تعمیـر و نگهـداری و چگـونگی امحـای کلیـدهای رمزنگاشـتی خصوصی و مخفی و واحدهای اطلاعاتی حیاتی در هنگام دسترسی به واسط دسترسـی تعمیـر و نگهـداری. (کلیه سطوح امنیتی)

- توصیف بازه‌های عملیاتی عادی پودمان رمزنگاشتی. توصـیف مشخصـات محافظـت در برابـر شکسـت‌هـای محیطی مورد استفاده توسط پودمان یا توصیف آزمون‌های شکست محیطی انجام شده روی پودمان. (فقـط در سطح چهارم)

**الف-۶ محیط عملیاتی**

توصیف محیط عملیاتی پودمان رمزنگاشتی. (کلیه سطوح امنیتی)

تعیین سامانه‌عامل به کار رفته توسط پودمان رمزنگاشتی، رخنمون‌های امنیتی قابل کـاربرد و سـطح تضـمین CC های به کاررفته (سطوح امنیتی دو، سه و چهار).

**الف-۷ مدیریت کلید رمزنگاشتی**

- توصیف کلیه کلیدهای رمزنگاشتی، اجزای کلید رمزنگاشتی و واحدهای اطلاعاتی حیاتی به‌کار رفته توسـط پودمان رمزنگاشتی.

- توصیف مولدهای اعداد تصادفی (مصوب یا غیر مصوب) به‌کار رفته توسط پودمان رمزنگاشتی. (کلیه سطوح امنیتی)

- توصیف شیوه‌های تولید کلید (مصوب یا غیر مصوب) به‌کار رفته توسط پودمان رمزنگاشتی. (کلیـه سـطوح امنیتی)

- توصیف روش‌های برقراری کلید به‌کار رفته توسط پودمان رمزنگاشتی. (کلیه سطوح امنیتی)
- توصیف روش‌های درونداد و برونداد کلید به‌کار رفته توسط پودمان رمزنگاشتی. (کلیه سطوح امنیتی)
- توصیف روش‌های ذخیره کلید به‌کار رفته توسط پودمان رمزنگاشتی. (کلیه سطوح امنیتی)
- توصیف روش‌های امحای کلید (مصوب و غیرمصوب) به کاررفته توسط پودمان رمزنگاشتی. (کلیه سطوح امنیتی)
- اگر رویه‌های تقسیم دانش استفاده شده، اثبات این‌که اگر دانستنn جزء کلید برای بازسازی کلید اصلی مورد نیاز باشد، آنگاه دانستن هر n-1 جزء از کلید هیچ اطلاعاتی از کلید اصلی به جز طول آن در اختیار نمی‌گذارد و توصیف رویه‌های تقسیم دانش به‌کار رفته توسط پودمان رمزنگاشتی. (سطوح سوم و چهارم).

**الف-۸ تداخل/سازگاری الکترومغناطیسی**

اثبات رعایت الزامات EMI/EMC در پودمان رمزنگاشتی. (کلیه سطوح امنیتی).

**الف-۹ خودآزمایی**

در مستندسازی باید موارد ذیل مشخص گردد:
- توصیف خودآزمایی‌های قابل انجام توسط پودمان رمزنگاشتی شامل خودآزمایی‌های آغازین و آزمون‌های شرطی (کلیه سطوح امنیتی)؛
- توصیف حالت‌های خطایی که پودمان رمزنگاشتی در صورت مواجه با شکست در خودآزمایی، وارد این حالت‌ها می‌شود و نیز شرایط و عملیاتی که جهت برونداد از حالت خطا و بازگشت پودمان رمزنگاشتی به حالت عادی مورد نیاز و ضروری هستند (کلیه سطوح امنیتی)؛
- توصیف کلیه توابع امنیتی حیاتی لازم جهت انجام عملیات امن در پودمان رمزنگاشتی و شناسایی آزمون‌های کاربردی آغازین و شرطی اجرا شده توسط پودمان (کلیه سطوح امنیتی)؛
- در صورتی که پودمان رمزنگاشتی یک قابلیت کنارگذار را پیاده کند، سازوکار یا منطق کنترل سودهی‌کردن به این حالت باید توصیف شود (کلیه سطوح امنیتی)؛

**الف-۱۰ ضمانت طراحی**

- توصیف رویه‌های نصب، تولید و شروع به کار امن پودمان رمزنگاشتی. (کلیه سطوح امنیتی)

- توصیف رویه‌های حفظ امنیت پودمان رمزنگاشتی حین توزیع و تحویل پودمان رمزنگاشتی به کاربران نهایی مجاز. (کلیه سطوح امنیتی)
- توصیف تناظر بین طرح سخت‌افزار، نرم‌افزار و اجزای ثابت‌افزار پودمان رمزنگاشتی با خط‌مشی امنیتی پودمان. (کلیه سطوح امنیتی)
- اگر پودمان رمزنگاشتی شامل اجزای نرم‌افزاری یا ثابت افزاری است، توصیف کد منبع نرم‌افزار و ثابت‌افزار پودمان رمزنگاشتی به همراه توضیحات کافی و علامت‌گذاری شده که به روشنی تناظر بین این اجزا با طرح پودمان را نشان می‌دهد. (کلیه سطوح امنیتی)
- اگر پودمان رمزنگاشتی شامل اجزای سخت افزاری است، توصیف طرح‌واره[1] و/یا زبان توصیف سخت‌افزار برای این اجزای سخت افزاری. (کلیه سطوح امنیتی)توصیف عملکردی که پودمان رمزنگاشتی، درگاه‌ها و واسط‌های خارجی پودمان و هدف این واسط‌ها را به‌صورت غیر رسمی تشریح می‌کند. (برای سطوح ۲ و ۳ و ۴)
- توصیف یک مدل رسمی که نقش‌ها و خصوصیات خط‌مشی امنیتی را با استفاده از یک زبان توصیفی رسمی که یک نمادگذاری مبتنی بر ریاضیات است، شرح دهد. (سطح ۴)
- توصیف دلایلی که استحکام و یکپارچگی مدل رسمی را با توجه به خط‌مشی امنیتی پودمان رمزنگاشتی، نمایش دهد. (سطح ۴)
- توصیف اثبات غیر رسمی تناظر بین مدل رسمی و توصیف عملکردی. (سطح ۴)
- برای هر بخش سخت‌افزار، نرم‌افزار و ثابت‌افزار پودمان رمزنگاشتی، تفسیر کد منبع با توضیحات کاملی که توصیف کننده این موارد باشند: ۱. پیش‌شرط‌های لازم جهت درونداد به اجزای پودمان، توابع و رویه‌ها به منظور اجرای درست و ۲. پس‌شرط‌هایی که نشان دهنده عملکرد درست اجزای پودمان، توابع یارویه‌ها هستند. پیش‌شرط‌ها و پس‌شرط‌ها باید به طور کامل و بدون ابهام توضیح داده‌شوند (سطح ۴).
- توصیف یک اثبات غیر رسمی از تناظر بین طرح پودمان رمزنگاشتی و توصیف عملیاتی. (سطح ۴).
- در مستند راهنمای استفاده از پودمان رمزنگاشتی که برای نقش متصدی رمز تدوین می‌گردد، توصیف کننده موراد زیر است:
  - توابع مدیریتی، وقایع امنیتی، پارامترهای امنیتی، درگاه‌های فیزیکی و واسط‌های منطقی قابل دسترس توسط متصدی رمز (کلیه سطوح امنیتی)،
  - رویه‌های اعمال مدیریت پودمان رمزنگاشتی به روش امن (کلیه سطوح امنیتی) و
  - فرضیاتی در مورد رفتار کاربر که به عملکرد امن پودمان رمزنگاشتی مربوط است. (کلیه سطوح امنیتی)
- مستندات راهنمای کاربر نهایی توصیف کننده موارد زیر است:
  - توابع امنیتی مصوب، درگاه‌های فیزیکی و واسط‌های منطقی قابل دسترس توسط کاربران نهایی پودمان رمزنگاشتی (کلیه سطوح امنیتی) و

---

۱ - Scheme

- کلیه مسؤولیت‌های کاربر که جهت حفظ امنیت پودمان رمزنگاشتی و عمکرد آن به‌صورت امن، مورد نیاز می‌باشد. (کلیه سطوح امنیتی)

**الف-۱۱ اقدامات کاهش‌دهنده آسیب در برابر سایر حملات**

در صورتی که پودمان برای مقابله و کاهش آسیب یک یا چند حمله طراحی شده‌است، باید در خط‌مشی امنیتی پودمان، سازوکار به کارگرفته شده توسط پودمان رمزنگاشتی به منظور کاهش آسیب حمله(ها) توصیف شود(کلیه سطوح امنیتی).

## پیوست ب
## (الزامی)
## الزامات خط‌مشی امنیتی پودمان رمزنگاشتی

خط‌مشی امنیتی یک پودمان امنیتی باید در مستندات تهیه شده توسط سازنده پودمان وجود داشته باشد. در ذیل یک نمایه کلی از محتوای مورد نیاز خط‌مشی امنیتی ارائه می‌شود.

### ب-۱ تعریف خط‌مشی امنیتی پودمان رمزنگاشتی

یک خط‌مشی امنیتی پودمان رمزنگاشتی باید شامل موارد زیر باشد:

- توصیفی از قوانین امنیتی که پودمان رمزنگاشتی باید تحت آن‌ها عمل کند. این قوانین امنیتی از الزامات مطرح شده در این استاندارد و سایر قوانین امنیتی لحاظ شده توسط سازنده استخراج می‌شوند.

توصیفی که در مورد بالا بیان شد باید به اندازه کافی جامع و کامل باشد که بتواند به سوالات زیر پاسخ دهد:

- کاربر X، هنگام اجرای خدمت Y در نقش Z دارای بخش W داده مربوط به امنیت، به ازای هر نقش، خدمت و بخش داده مربوط به امنیت مجود در پودمان رمزنگاشتی چه دسترسی‌هایی دارد؟

- چه سازوکارهای امنیت فیزیکی‌ای جهت حفاظت از پودمان در نظر گرفته شده و برای تضمین ماندگاری امنیت فیزیکی -پودمان چه اقداماتی لازم است؟

- جهت کاهش آسیب حملاتی که در این استاندارد الزامات آنها تعریف نشده است، در پودمان رمزنگاشتی چه سازوکارهای امنیت فیزیکی پیاده‌سازی شده است؟

### ب-۲ هدف خط‌مشی امنیتی پودمان رمزنگاشتی

دو دلیل عمده برای توسعه و پیگیری دقیق خط‌مشی امنیتی پودمان رمزنگاشتی وجود دارد:

- جهت فراهم‌کردن توصیفی از امنیت رمزنگاشتی که به افراد و سازمان‌ها اجازه می‌دهد تعیین کنند که آیا پودمان رمزنگاشتی به همان صورتی که در خط و مشی امنیتی آن تصریح شده، پیاده‌سازی شده است.

- با تشریح توانایی‌ها، حفاظت‌ها و حقوق دسترسی فراهم شده توسط پودمان رمزنگاشتی، به افراد و سازمان‌ها اجازه می‌دهد تا ارزیابی کنند که آیا پودمان به اندازه کافی نیازهای امنیتی آن‌ها را برطرف می‌کند.

### ب-۳ توصیف خط‌مشی امنیتی پودمان رمزنگاشتی

خط‌مشی امنیتی پودمان رمزنگاشتی باید بر حسب نقش‌ها، خدمت‌ها، کلیدها و واحدهای اطلاعاتی حیاتی بیان شود. در خط و مشی امنیتی پودمان رمزنگاشتی باید کمینه موارد زیر را توصیف شود:

- خط‌مشی شناسایی و احراز هویت،
- خط‌مشی کنترل دسترسی،

- خط‌مشی امنیت فیزیکی و
- خط‌مشی کاهش آسیب در برابر سایر حمله‌ها.

### ب-۳ خط‌مشی شناسایی و احراز هویت

خط‌مشی شناسایی و احراز هویت باید موارد زیر را دربرگیرد:

- کلیه نقش‌ها (مانند کاربر، متصدی رمز و حفظ و نگهداری ) و انواع احراز هویت متناظر با آن‌ها (مانند احراز هویت «هویت‌محور»، «نقش‌محور» یا هیچ‌کدام)س

- داده‌های احراز هویت مورد نیاز برای هر نقش یا کاربر (مانند اسم‌رمز و یا داده‌های زیست شناسی) و مقاومت سازوکار احراز هویت متناظر با آن‌ها.

### ب-۴ خط‌مشی کنترل دسترسی

خط‌مشی امنیتی پودمان رمزنگاشتی باید خط و مشی کنترل دسترسی به پودمان را توصیف کند. این توصیف باید با جزییات کافی از کلیدهای رمزنگاشتی و واحدهای اطلاعاتی حیاطی که متصدیان در طول اجرای یک خدمت به آن‌ها دسترسی دارند بوده و نیز پارامترهای هر نوع دسترسی را ارائه دهد.

خط‌مشی امنیتی باید موارد زیر را توصیف کند:

- کلیه نقش‌های پشتیبانی شده توسط پودمان رمزنگاشتی،

- کلیه خدماتی فراهم شده توسط پودمان رمزنگاشتی،

- کلیه کلیدهای رمزنگاشتی و واحدهای اطلاعاتی حیاطی به کارگرفته شده توسط پودمان رمزنگاشتی که شامل:

  - کلیدهای خصوصی، عمومی و مخفی (چه به‌صورت رمزشده و چه به‌صورت متن آشکار)
  - داده‌های احراز هویت مانند اسم‌رمز و یا پین‌کد و
  - سایر اطلاعات مرتبط با امنیت (مانند رخدادها و داده‌های ممیزی)

- برای هر نقش، خدماتی که کاربر مجاز به اجرای آن در قالب آن نقش است و

- برای هر خدمت در قالب هر نقش، نوع دسترسی به کلیدها و واحدهای اطلاعاتی حیاتی.

### ب-۵ خط‌مشی امنیت فیزیکی پودمان رمزنگاشتی

خط و مشی امنیتی پودمان رمزنگاشتی باید یک خط‌مشی امنیت فیزیکی شامل موارد زیر توصیف کند:

- سازوکار امنیت فیزیکی که در پودمان پیاده‌سازی شده‌است (مانند برچسب آشکارساز نفوذ، قفل‌ها، سوده‌های تشخیص نفوذ و امحاءکننده و هشدار دهنده‌ها).

- رفتارهای که لازم است توسط کاربر انجام گیرد تا از حفظ امنیت فیزیکی پودمان اطمینان حاصل شود (برای مثال، بازرسی دوره‌ای از برچسب آشکارساز نفوذ و یا آزمایش سودهی تشخیص نفوذ و امحاءکننده).

### ب-۶ خط‌مشی کاهش آسیب در برابر سایر حملات

خط و مشی امنیتی پودمان رمزنگاشتی باید یک خط و مشی امنیتی جهت کاهش آسیب در برابر سایر حملات توصیف کند که شامل سازوکارهای امنیتی پیاده‌سازی شده به منظور کاهش این حملات است.

### ب-۷ جدول‌های بازبینه خط‌مشی امنیتی

جدول‌های زیر به عنوان یک راهنما جهت اطمینان از اینکه خط و مشی امنیتی کامل بوده و در بر دارنده جزئیات مناسب است، می‌تواند مورد استفاده قرار گیرد:

**جدول ۲- نقش‌ها و شناسایی و احراز هویت مورد نیاز**

| نقش | نوع احراز هویت | داده‌های – احراز هویت |
|---|---|---|
| ... | ... | ... |
| ... | ... | ... |

**جدول ۳- مقاومت سازوکارهای احراز هویت**

| سازوکار احراز هویت | استحکام سازوکار |
|---|---|
| ... | ... |
| ... | ... |

**جدول ۴- خدماتی مجاز برای نقش‌ها**

| نقش | خدماتی مجاز |
|---|---|
| ... | ... |
| ... | ... |

**جدول ۵- حقوق دسترسی در قالب هر خدمت**

| خدمات | کلید رمزنگاشتی و واحدهای اطلاعاتی حیاتی | نوع دسترسی (برای مثال، خواندن، نوشتن) |
|---|---|---|
| ... | ... | ... |
| ... | ... | ... |

**جدول ۶- بازرسی/ آزمایش سازوکار امنیت فیزیکی**

| سازوکارهای امنیت فیزیکی | تناوب آزمایش و بازرسی | جزییات بازرسی یا آزمایش |
|---|---|---|
| ... | ... | ... |
| ... | ... | ... |

**جدول ۷- کاهش آسیب سایر حمله‌ها**

| سایر حمله‌ها | سازوکار کاهش آسیب | شرح محدودیت‌ها |
|---|---|---|
| ... | ... | ... |
| ... | ... | ... |

## پیوست پ
## (اطلاعاتی)
## واژه‌نامه فارسی به انگلیسی

| | واژه فارسی | معادل لاتین |
|---|---|---|
| ۱. | اتصال‌های سیمی | Wiring runs |
| ۲. | اثرناپذیری | Passivation |
| ۳. | احراز هویت | Authentication |
| ۴. | احراز هویت کردن | Authenticate |
| ۵. | احراز هویت «هویت‌محور» | Identity-based Authentication |
| ۶. | احراز هویت «نقش‌محور» | Role-based Authentication |
| ۷. | اطلاعات کلید تقطیع شده | Split key information |
| ۸. | اعتبارسنجی | Validation |
| ۹. | افشا | Disclosure |
| ۱۰. | افشاسازی | Compromise |
| ۱۱. | ریزموج | Microwave |
| ۱۲. | اندود پلاستیکی | Epoxy |
| ۱۳. | آزمون خطای محیطی | Environmental failure testing (EFT) |
| ۱۴. | آزمون شکست‌های محیطی | Environmental Failure Testing (EFT) |
| ۱۵. | صدور گواهی | Certificate |
| ۱۶. | آشکارساز نفوذ | Tamper-evident |
| ۱۷. | بارکننده کلید | Key loader |
| ۱۸. | باله | Fin |
| ۱۹. | باید | Shall |
| ۲۰. | باید | Must |
| ۲۱. | بذر | Seed |
| ۲۲. | پرچم | Flag |
| ۲۳. | رخنمون‌های حفاظتی | Protection Profiles |
| ۲۴. | بازخورد | Feedback |
| ۲۵. | پشتیبان | Backup |
| ۲۶. | پوسته | Enclosure |
| ۲۷. | پوسته | Envelope |
| ۲۸. | پوشاندن یکنواخت | Conformal coating |
| ۲۹. | پوشش | Coat |
| ۳۰. | پوشش مهر و موم کننده | Sealing coat |

| | واژه فارسی | معادل لاتین |
|---|---|---|
| ۳۱. | تجدید کلید بی‌سیم | Over-The-Air Rekeying |
| ۳۲. | تجسم ظاهری | Physical embodiment |
| ۳۳. | تراشه | Chip |
| ۳۴. | تضمین | Assurance |
| ۳۵. | تعمیر و نگهداری | Maintenance |
| ۳۶. | تغییر | Modification |
| ۳۷. | تک-تراشه‌ای | Single-chip |
| ۳۸. | یکپارچگی | Integrity |
| ۳۹. | تنظیم مجدد | Resetting |
| ۴۰. | تهویه | Ventilation |
| ۴۱. | ثابت‌افزار | Firmware |
| ۴۲. | جابه‌جایی | Substitution |
| ۴۳. | جدول گذر حالت | State transition table |
| ۴۴. | تابع درهم‌سازی | Hash |
| ۴۵. | چند-تراشه‌ای تعبیه شده | Multi-chip embedded |
| ۴۶. | چند-تراشه‌ای خودکفا | Multi-chip standalone |
| ۴۷. | پاسخ‌گویی | Accounting |
| ۴۸. | حفاظت در برابر خطای محیطی | Environmental failure protection (EFP) |
| ۴۹. | حفاظت در برابر شکست‌های محیطی | Environmental Failure Protection (EFP) |
| ۵۰. | حل شدن | Solvency |
| ۵۱. | خاموش شدن | Power off |
| ۵۲. | خدمت | Service |
| ۵۳. | خط مشی | Policy |
| ۵۴. | خط‌مشی امنیتی | Security Policy |
| ۵۵. | خطای سخت | Hard error |
| ۵۶. | خطای نرم | Soft error |
| ۵۷. | خودآزمایی | Self test |
| ۵۸. | درپوش | Cover |
| ۵۹. | درجه-تجاری | Commercial grade |
| ۶۰. | درجه-تولیدی | Production-grade |
| ۶۱. | درگاه | Port |
| ۶۲. | نفوذ | Tamper |
| ۶۳. | پایش | Monitor |
| ۶۴. | راه اندازی اولیه | Initialization |

| | واژه فارسی | معادل لاتین |
|---|---|---|
| ۶۵. | راه‌اندازی رمزنگاشتی | Cryptographic initialization |
| ۶۶. | رد شدن | Fail |
| ۶۷. | رسمی | Formal |
| ۶۸. | رصد کردن | Observation |
| ۶۹. | رمز نشده (متن اصلی) | Plaintext |
| ۷۰. | رمزبندی | Encryption |
| ۷۱. | رمزگشایی | Decryption |
| ۷۲. | رمزنگاری | Cryptography |
| ۷۳. | روشن شدن | Power on |
| ۷۴. | رویدادنگار | Log |
| ۷۵. | ریزکد | Microcode |
| ۷۶. | ریز سوده‌ها | Micro switches |
| ۷۷. | زیست‌سنجشی | Biometric |
| ۷۸. | سازوکار | Mechanism |
| ۷۹. | سبک | Mode |
| ۸۰. | سطح تضمین ارزیابی | Evaluation Assurance Level (EAL) |
| ۸۱. | سوده‌های پوششی | Cover switches |
| ۸۲. | ریزسوده‌ها | Micro switches |
| ۸۳. | طیف نور مریی | Visible spectrum |
| ۸۴. | عرضه‌کننده | Vendor |
| ۸۵. | غیر رسمی | Informal |
| ۸۶. | غیر مجاز | Unauthorized |
| ۸۷. | غیر مصوب | Non-approved |
| ۸۸. | فراصوتی | Ultrasonic |
| ۸۹. | القا شده | Induced |
| ۹۰. | قطعه نیمه‌هادی | Die |
| ۹۱. | کاهش | Mitigation |
| ۹۲. | کاهش دهنده صدمات فیزیکی | Passivation |
| ۹۳. | متصدی | Operator |
| ۹۴. | کاربر نهایی | User |
| ۹۵. | پروب گذاری | Probing |
| ۹۶. | کد احراز هویت پیام | Message authentication code |
| ۹۷. | کد تشخیص خطا | Error detection code |
| ۹۸. | کلید بذر | Seed key |

| | واژه فارسی | معادل لاتین |
|---|---|---|
| ۹۹. | کلید مخفی | Secret key |
| ۱۰۰. | کنارگذر | Bypass |
| ۱۰۱. | کنترل دسترسی صلاحدیدی | Discretionary access control |
| ۱۰۲. | گذر حالت | State transition |
| ۱۰۳. | الگوریتم امضای رقمی | Digital Signature Algorithm (DSA) |
| ۱۰۴. | مادون قرمز | Infrared |
| ۱۰۵. | پودمان رمزنگاشتی ارتباطات رادیویی | Radio communications cryptographic module |
| ۱۰۶. | متصدی رمز | Crypto officer |
| ۱۰۷. | متصل‌کننده‌ها | Connector |
| ۱۰۸. | متن رمز شده | Ciphertext |
| ۱۰۹. | متولد شدن | Spawn |
| ۱۱۰. | مجاز | Authorized |
| ۱۱۱. | مجازشناسی | Authorization |
| ۱۱۲. | محرک‌های مغناطیسی دائم | Permanent magnetic actuators |
| ۱۱۳. | مخفی | Secret |
| ۱۱۴. | مدار مجتمع | Integrated circuit (IC) |
| ۱۱۵. | مدل حالت متناهی | Finite state model |
| ۱۱۶. | مدیریت پیکربندی | Configuration Management (CM) |
| ۱۱۷. | مسیر معتمد | Trusted path |
| ۱۱۸. | مسیریابی | Routing |
| ۱۱۹. | مصوب | Approved |
| ۱۲۰. | معاوضه‌گر گرما | Heat exchanger |
| ۱۲۱. | مقاوم در برابر برداشتن | Removal-resistant |
| ۱۲۲. | ممیزی | Audit |
| ۱۲۳. | مولد اعداد تصادفی | Random Number Generator |
| ۱۲۴. | مولد اعداد تصادفی متوالی | Continuous random number generator |
| ۱۲۵. | مؤلفه | Component |
| ۱۲۶. | نشانگر | Indicator |
| ۱۲۷. | نشست | Session |
| ۱۲۸. | نصب | Installation |
| ۱۲۹. | نصب کردن | Install |
| ۱۳۰. | پایانه‌ها | Terminals |
| ۱۳۱. | نقش | Role |
| ۱۳۲. | نگاشت | Mapping |

| | واژه فارسی | معادل لاتین |
|---|---|---|
| ۱۳۳. | نمودار بستکی | Block diagram |
| ۱۳۴. | نمودار گذر حالت | State transition diagram |
| ۱۳۵. | پارامترهای اطلاعاتی حیاتی | Critical Security Parameters (CSP) |
| ۱۳۶. | دروندادهای تکراری | Duplicate entries |
| ۱۳۷. | واسط | Interface |
| ۱۳۸. | واسط برنامه‌نویسی کاربردی | Application Programming Interface (API) |
| ۱۳۹. | ورق پلاستیکی منعطف | Flexible mylar printed circuit |
| ۱۴۰. | وظایف پایه‌ها | Pin assignment |
| ۱۴۱. | یکپارچگی | Integrity |
| ۱۴۲. | یک‌دست | Uniform |

## پیوست ت
## (الزامی)
## واژه‌نامه انگلیسی به فارسی

| | واژه فارسی | معادل لاتین |
|---|---|---|
| ۱. | پاسخ‌گویی | Accounting |
| ۲. | واسط برنامه‌نویسی برنامه‌کاربردی | Application Programming Interface (API) |
| ۳. | مصوب | Approved |
| ۴. | تضمین | Assurance |
| ۵. | ممیزی | Audit |
| ۶. | احراز هویت کردن | Authenticate |
| ۷. | احراز هویت | Authentication |
| ۸. | مجازشناسی | Authorization |
| ۹. | مجاز | Authorized |
| ۱۰. | پشتیبان | Backup |
| ۱۱. | زیست‌سنجشی | Biometric |
| ۱۲. | نمودار بستک | Block diagram |
| ۱۳. | کنارگذر | Bypass |
| ۱۴. | صدور گواهی | Certificate |
| ۱۵. | تراشه | Chip |
| ۱۶. | متن رمز شده | Ciphertext |
| ۱۷. | پوشش | Coat |
| ۱۸. | درجه-تجاری | Commercial grade |
| ۱۹. | مؤلفه | Component |
| ۲۰. | افشاسازی | Compromise |
| ۲۱. | مدیریت پیکربندی | Configuration Management (CM) |
| ۲۲. | پوشاندن یکنواخت | Conformal coating |
| ۲۳. | متصل‌کننده‌ها | Connector |
| ۲۴. | مولد اعداد تصادفی متوالی | Continuous random number generator |
| ۲۵. | درپوش | Cover |
| ۲۶. | سوده‌های پوششی | Cover switches |
| ۲۷. | پارامترهای اطلاعاتی حیاتی | Critical Sevurity Parameters (CSP) |
| ۲۸. | متصدی رمز | Crypto officer |
| ۲۹. | راه‌اندازی رمزنگاشتی | Cryptographic initialization |
| ۳۰. | رمزنگاری | Cryptography |

| | واژه فارسی | معادل لاتین |
|---|---|---|
| ۳۱. | رمزگشایی | Decryption |
| ۳۲. | قطعه نیمه‌هادی | Die |
| ۳۳. | الگوریتم امضای رقمی | Digital Signature Algorithm (DSA) |
| ۳۴. | افشا | Disclosure |
| ۳۵. | کنترل دسترسی صلاحدیدی | Discretionary access control |
| ۳۶. | دروندادهای تکراری | Duplicate entries |
| ۳۷. | پوسته | Enclosure |
| ۳۸. | رمزبندی | Encryption |
| ۳۹. | پوسته | Envelope |
| ۴۰. | حفاظت در برابر خطای محیطی | Environmental failure protection (EFP) |
| ۴۱. | حفاظت در برابر شکست‌های محیطی | Environmental Failure Protection (EFP) |
| ۴۲. | آزمون خطای محیطی | Environmental failure testing (EFT) |
| ۴۳. | آزمون شکست‌های محیطی | Environmental Failure Testing (EFT) |
| ۴۴. | اندود پلاستیکی | Epoxy |
| ۴۵. | کد تشخیص خطا | Error detection code |
| ۴۶. | سطح تضمین ارزیابی | Evaluation Assurance Level (EAL) |
| ۴۷. | رد شدن | Fail |
| ۴۸. | بازخورد | Feedback |
| ۴۹. | باله | Fin |
| ۵۰. | مدل حالت متناهی | Finite state model |
| ۵۱. | ثابت‌افزار | Firmware |
| ۵۲. | پرچم | Flag |
| ۵۳. | ورق پلاستیکی منعطف | Flexible mylar printed circuit |
| ۵۴. | رسمی | Formal |
| ۵۵. | خطای سخت | Hard error |
| ۵۶. | چکیده‌سازی | Hash |
| ۵۷. | معاوضه‌گر گرما | Heat exchanger |
| ۵۸. | احراز هویت «هویت‌محور» | Identity-based Authentication |
| ۵۹. | نشانگر | Indicator |
| ۶۰. | القا شده | Induced |
| ۶۱. | غیر رسمی | Informal |
| ۶۲. | مادون قرمز | Infrared |
| ۶۳. | راه‌اندازی | Initialization |
| ۶۴. | نصب کردن | Install |

| | واژه فارسی | معادل لاتین |
|---|---|---|
| ۶۵. | نصب | Installation |
| ۶۶. | مدار مجتمع | Integrated circuit (IC) |
| ۶۷. | یکپارچگی و یکپارچگی | Integrity |
| ۶۸. | واسط | Interface |
| ۶۹. | بارکننده کلید | Key loader |
| ۷۰. | رویدادنگار | Log |
| ۷۱. | تعمیر و نگهداری | Maintenance |
| ۷۲. | نگاشت | Mapping |
| ۷۳. | سازوکار | Mechanism |
| ۷۴. | کد احراز هویت پیام | Message authentication code |
| ۷۵. | ریزسوده‌ها | Micro switches |
| ۷۶. | سوده‌های مغناطیسی اثر هال | Micro switches |
| ۷۷. | ریزکد | Microcode |
| ۷۸. | ریزموج‌ها | Microwave |
| ۷۹. | کاهش | Mitigation |
| ۸۰. | سبک | Mode |
| ۸۱. | تغییر | Modification |
| ۸۲. | پایش | Monitor |
| ۸۳. | چند-تراشه‌ای تعبیه شده | Multi-chip embedded |
| ۸۴. | چند-تراشه‌ای خودکفا | Multi-chip standalone |
| ۸۵. | باید | Must |
| ۸۶. | غیر مصوب | Non-approved |
| ۸۷. | رصد کردن | Observation |
| ۸۸. | کاربر | Operator |
| ۸۹. | تجدید کلید بی‌سیم | Over-The-Air Rekeying |
| ۹۰. | اثرناپذیری | Passivation |
| ۹۱. | کاهش دهنده صدمات فیزیکی | Passivation |
| ۹۲. | محرک‌های مغناطیسی دائم | Permanent magnetic actuators |
| ۹۳. | تجسم ظاهری | Physical embodiment |
| ۹۴. | وظایف پایه‌ها | Pin assignment |
| ۹۵. | رمز نشده (متن اصلی) | Plaintext |
| ۹۶. | خط مشی | Policy |
| ۹۷. | درگاه | Port |
| ۹۸. | خاموش شدن | Power off |

| | واژه فارسی | معادل لاتین |
|---|---|---|
| ۹۹. | روشن شدن | Power on |
| ۱۰۰. | کاوش | Probing |
| ۱۰۱. | درجه-تولیدی | Production-grade |
| ۱۰۲. | رخنمون‌های حفاظتی | Protection Profiles |
| ۱۰۳. | پودمان رمزنگاشتی ارتباطات رادیویی | Radio communications cryptographic module |
| ۱۰۴. | مولد اعداد تصادفی | Random Number Generator |
| ۱۰۵. | مقاوم در برابر برداشتن | Removal-resistant |
| ۱۰۶. | تنظیم مجدد | Resetting |
| ۱۰۷. | نقش | Role |
| ۱۰۸. | احراز هویت «نقش‌محور» | Role-based Authentication |
| ۱۰۹. | مسیریابی | Routing |
| ۱۱۰. | پوشش مهر و موم کننده | Sealing coat |
| ۱۱۱. | مخفی | Secret |
| ۱۱۲. | کلید مخفی | Secret key |
| ۱۱۳. | خط و مشی امنیتی | Security Policy |
| ۱۱۴. | بذر | Seed |
| ۱۱۵. | کلید بذر | Seed key |
| ۱۱۶. | آزمون | Self test |
| ۱۱۷. | خدمت | Service |
| ۱۱۸. | نشست | Session |
| ۱۱۹. | باید | Shall |
| ۱۲۰. | تک-تراشه‌ای | Single-chip |
| ۱۲۱. | خطای نرم | Soft error |
| ۱۲۲. | حل شدن | Solvency |
| ۱۲۳. | متولد شدن | Spawn |
| ۱۲۴. | اطلاعات کلید تقطیع شده | Split key information |
| ۱۲۵. | گذر حالت | State transition |
| ۱۲۶. | نمودار گذر حالت | State transition diagram |
| ۱۲۷. | جدول گذر حالت | State transition table |
| ۱۲۸. | جابه‌جایی | Substitution |
| ۱۲۹. | نفوذ | Tamper |
| ۱۳۰. | آشکارساز نفوذ | Tamper-evident |
| ۱۳۱. | پایانه‌ها | Terminals |
| ۱۳۲. | مسیر معتمد | Trusted path |

| | واژه فارسی | معادل لاتین |
|---|---|---|
| ۱۳۳. | فراصوتی | Ultrasonic |
| ۱۳۴. | غیر مجاز | Unauthorized |
| ۱۳۵. | یک‌دست | Uniform |
| ۱۳۶. | کاربر نهایی | User |
| ۱۳۷. | اعتبارسنجی | Validation |
| ۱۳۸. | عرضه‌کننده | Vendor |
| ۱۳۹. | تهویه | Ventilation |
| ۱۴۰. | طیف نور مریی | Visible spectrum |
| ۱۴۱. | اتصال‌های سیمی | Wiring runs |

# کتابنامه

**[1]** ISO/IEC 7816-4: 1995, Information Technology — Identification Cards — Integrated Circuit(s) with Contacts — Part 4: Interindustry Commands for Interchange.

**[2]** SEIGN Workshop – Expert Group, Version 1.04:2001, Secure Signature Creation Device Protection Profile, Type2, [SSCD]