INSO
18721
1st. Edition
2014

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

استاندارد ملی ایران
۱۸۷۲۱
چاپ اول
۱۳۹۳

فناوری اطلاعات- فنون امنیت- الزامات امنیت برای پودمان‌های رمزنگاری

Information technology – Security techniques – Security requirements for cryptographic modules

ICS: 35.040

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 حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود 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، سازمان های دولتی و غیر دولتی حاصل می شود . پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به‌عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب ، به‌عنوان استاندارد ملی ایران چاپ و منتشر می شود . 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 به‌عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5]در کشور فعالیت می کند . در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی ، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند 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 می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور ، اجرای استاندارد کالاهای صادراتی و درجه‌بندی 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 سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی ، آزمایشگاه ها 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 می کند و در صورت احراز شرایط لازم ، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند . ترویج دستگاه بین المللی 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 .

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
«فناوری اطلاعات- فنون امنیت- الزامات امنیت برای پودمان‌های رمزنگاری»

رئیس:	**سمت و / یا نمایندگی**
مشرف، بهنوش (فوق لیسانس مهندسی فناوری اطلاعات- شبکه‌های کامپیوتری)	کارشناس استاندارد – کارشناس پایگاه‌داده شرکت برق منطقه‌ای هرمزگان
دبیر:	
ترابی ، مهرنوش (فوق لیسانس مهندسی فناوری اطلاعات – تجارت الکترونیک)	کارشناس استاندارد- کارشناس تجزیه و تحلیل سیستم شرکت برق منطقه‌ای هرمزگان
اعضاء: (اسامی به ترتیب حروف الفبا)	
احمدی، محمد (فوق لیسانس مهندسی برق- مخابرات)	کارشناس استاندارد- کارشناس فیبرنوری شرکت برق منطقه‌ای هرمزگان
ایزدپناه، سحرسادات (فوق لیسانس مهندسی فناوری اطلاعات – سیستم‌های اطلاعاتی)	سرپرست اداره استاندارد سازمان فناوری اطلاعات ایران
ذاکری، صفورا (فوق لیسانس مهندسی کامپیوتر- نرم‌افزار)	عضو هیات علمی دانشگاه آزاد اسلامی بندرعباس
زمانی ، کرشنا (فوق لیسانس مهندسی فناوری اطلاعات – تجارت الکترونیک)	کارشناس مرکز رایانه دانشگاه مازندران
شایسته، محمد (فوق لیسانس مهندسی کامپیوتر- نرم‌افزار)	عضو هیات علمی دانشگاه آزاد اسلامی بندرعباس
قاسمی‌زاده، صدیقه (لیسانس مهندسی کامپیوتر- نرم‌افزار)	کارشناس شبکه برق منطقه‌ای هرمزگان
موجبی، محمود (فوق لیسانس مخابرات – رمز)	کارشناس استاندارد- کارشناس خدمات ارزش افزوده سازمان فناوری اطلاعات
مومنی، حمیدرضا (فوق لیسانس مهندسی کامپیوتر- هوش مصنوعی)	عضو هیات علمی دانشگاه تنکابن

فهرست مندرجات

عنوان **صفحه**

ادامه فهرست مندرجات

ادامه فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیت- الزامات امنیت برای پودمان‌های رمزنگاری» که پیش نویس آن در کمیسیون فنی مربوط، توسط سازمان ملی استاندارد ایران، تهیه و تدوین شده و در سیصدوچهل‌وهشتمین اجلاسیه کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۹۳/۸/۱۹ 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 به‌عنوان استاندارد ملی منتشر می شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهند شد و هر گونه 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 تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که در تهیه این استاندارد مورد استفاده قرار گرفته است به شرح زیر است:

ISO/IEC 19790:2012, Information technology – Security techniques – Security requirements for cryptographic modules

فناوری اطلاعات- فنون امنیت- الزامات امنیت برای پودمان‌های رمزنگاری

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین الزامات امنیت برای پودمان رمزنگاری است که در داخل یک سامانه امنیت مورد استفاده قرارگرفته‌است که از اطلاعات حساس در رایانه و سامانه‌های مخابرات محافظت‌می‌کند. این استاندارد چهار سطح امنیت را برای پودمان‌های رمزنگاری تعریف‌می‌کند تا برای طیف گسترده‌ای از حساسیت داده (به‌عنوان مثال، داده‌های اداری کم ارزش، نقل و انتقال سرمایه‌های میلیون دلاری، داده محافظت از عمر، اطلاعات هویت شخصی و اطلاعات حساس که توسط دولت به‌کار برده‌شده‌است) و تنوعی از محیط‌های کاربردی (به‌عنوان مثال یک امکان محافظت، یک اداره، رسانه جداشدنی، و یک محل کاملاً محافظت‌نشده) فراهم‌شود. این استاندارد چهار سطح امنیت را برای هر یک از ۱۱ ناحیه موردنیاز مشخص‌می‌کند که هر سطح امنیت، امنیت را بر روی سطح قبلی افزایش‌می‌دهد.

این استاندارد الزامات امنیت را مشخص‌می‌کند. این الزامات مشخص‌شده، برای حفظ امنیت ارائه شده توسط پودمان رمزنگاری، در نظر گرفته‌شده‌است و برای اطمینان از این‌که یک پودمان خاص امن است یا این‌که امنیت فراهم‌شده با این پودمان کافی است و برای صاحب اطلاعاتی که محافظت می‌شود قابل‌قبول است، سازگاری با این استاندارد کافی نمی‌باشد.

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 ملی ایران محسوب می‌شود. در صورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجعی که در پیوست‌های «پ»، «ت»، «ث» و «ج» آمده است، برای این استاندارد الزامی است.

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می‌رود:

۳-۱ فهرست کنترل دسترسی (ACL)[1]

فهرست مجوزها برای اعطا دسترسی به یک شی می‌باشد.

1 - Access Control List

۳-۲ راهنمای مدیر[1]

اصول نوشته‌شده که توسط مدیر رمزنگاری و/ یا سایر نقش‌های مدیریتی برای پیکربندی صحیح، نگهداری و اداره پودمان رمزنگاری استفاده‌می‌شود.

۳-۳ خودکارشده[2]

بدون مداخله یا ورودی دستی (به‌عنوان مثال، ابزارهای الکترونیکی از جمله از طریق یک شبکه رایانه‌ای) است.

۳-۴ متولی تایید[3]

هر متولی/ سازمان ملی یا بین‌المللی تحت قیمومت برای تایید و / یا ارزیابی توابع امنیتی است.

یادآوری- در مفهوم این تعریف یک متولی تایید، توابع امنیتی را بر اساس مزیت‌های رمزنگاری یا ریاضی ارزیابی و تاییدمی‌کند اما هستار آزمونی نمی‌باشد که برای انطباق با این استاندارد آزمون می‌شود.

۳-۵ روش اصالت‌سنجی داده‌های تاییدشده[4]

روش تاییدشده‌ای است که ممکن است شامل استفاده از امضا دیجیتال، کد اصالت‌سنجی پیام یا درهم‌سازی کلیدی باشد (برای مثال HMAC).

۳-۶ روش یکپارچگی تاییدشده[5]

درهم‌سازی تاییدشده، کد اصالت‌سنجی پیام یا یک الگوریتم امضا دیجیتالی است.

۳-۷ حالت تاییدشده عملیات[6]

مجموعه خدماتی که حداقل شامل یک خدمت است که از یک تابع امنیتی تاییدشده یا فرآیند استفاده‌می‌کند و می‌تواند شامل خدمات وابسته غیر ـ امنیتی باشد.

یادآوری ۱- با یک حالت خاصی از یک تابع امنیتی تاییدشده سردرگم نشوید، برای مثال، مد زنجیره‌ای بلوک رمز (CBC)[7].

یادآوری ۲- توابع امنیتی یا فرآیندهای تاییدنشده مستثنی هستند.

۳-۸ تابع امنیتی تاییدشده[8]

تابع امنیتی (برای مثال، الگوریتم رمزنگاری) که در پیوست «پ» ارجاع می‌شود.

1 - Administrator Guidance
2 - Automated
3 - Approval Authority
4 - Approved Data Authentication Technique
5 - Approved Integrity Technique
6 - Approved Mode of Operation
7 - Cipher Block Chaining
8 - Approved Security Function

۳-۹ روش رمزنگاری نامتقارن[1]

روش رمزنگاری که از دو تبدیل مرتبط استفاده‌می‌کند: یک تبدیل عمومی (با کلید عمومی تعریف‌شده‌است) و یک تبدیل خصوصی (با کلید خصوصی تعریف‌شده‌است).

یادآوری- دو تبدیل دارای خصوصیتی هستند که با توجه به تبدیل عمومی، استخراج تبدیل خصوصی در زمان محدود معین و با منابع محاسباتی معین از نظر محاسباتی غیرممکن است.

۳-۱۰ زیست‌سنجشی[2]

مشخصه قابل‌اندازه‌گیری و فیزیکی یا ویژگی رفتاری فردی برای تشخیص هویت یا بررسی هویت ادعا شده از یک اپراتور می‌باشد.

۳-۱۱ توانایی کنارگذار[3]

توانایی یک خدمت برای گمراه‌سازی جزئی یا کلی یک تابع رمزنگاری است.

۳-۱۲ گواهی‌نامه[4]

هستار داده غیرقابل‌جعل با کلید محرمانه یا خصوصی از یک متولی گواهی‌نامه است.

یادآوری- با یک گواهی اعتبارسنجی پودمان‌ها که توسط یک متولی اعتبارسنجی صادرشده‌است، اشتباه نکنید.

۳-۱۳ مصالحه[5]

افشا، اصلاح، جانشینی یا استفاده غیرمجاز از پارامترهای امنیت بحرانی یا اصلاح یا جانشینی غیرمجاز پارامترهای امنیت عمومی.

۳-۱۴ خودآزمایی شرطی[6]

آزمون انجام‌شده با یک پودمان رمزنگاری در هنگامی است که شرایط برای وقوع آزمون تعیین‌شده‌باشد.

۳-۱۵ محرمانگی[7]

خصوصیتی که اطلاعات با هویت‌های غیرمجاز در دسترس قرارنمی‌گیرد یا افشا نمی‌شود.

۳-۱۶ سامانه مدیریت پیکربندی (CMS)[8]

مدیریت ویژگی‌های امنیت و بیمه‌ها از طریق کنترل تغییرات ایجادشده در سخت‌افزار، نرم‌افزار و مستندسازی یک پودمان رمزنگاری می‌باشد.

۳-۱۷ اطلاعات کنترل[9]

اطلاعاتی است که برای هدایت اهداف عملیات پودمان وارد یک پودمان رمزنگاری می‌شود.

---

1 - Asymmetric Cryptographic Technique
2 - Biometric
3 - Bypass Capability
4 - Certificate
5 - Compromise
6 - Conditional Self-test
7 - Confidentiality
8 - Configuration Management System
9 - Control Information

۳-۱۸ پارامتر امنیت بحرانی (CSP)[1]

اطلاعات مرتبط با امنیت که افشا یا اصلاح آن می‌تواند امنیت یک پودمان رمزنگاری را به‌خطر بیاندازد.

مثال: کلیدهای رمزنگاری محرمانه و خصوصی، داده‌های اصالت‌سنجی از قبیل اسم رمز، PINs، گواهینامه‌ها یا سایر مهارهای اعتماد.

یادآوری- یک CSP می‌تواند متن‌ساده[2] و یا متن رمزشده باشد.

۳-۱۹ مسوول رمز[3]

نقش پذیرفته‌شده توسط یک فرد یا یک فرآیند (برای مثال موضوع) می‌باشد که به نمایندگی فردی عمل‌می‌کند که به یک پودمان رمزنگاری دسترسی دارد تا مقداردهی اولیه رمزنگاری را انجام‌دهد و یا توابع مدیریتی یک پودمان رمزنگاری را انجام‌دهد.

۳-۲۰ الگوریتم رمزنگاری[4]

رویه محاسبه خوش‌تعریفی است که ورودی‌های متغیر را می‌گیرد، که این ورودی‌ها ممکن است شامل کلیدهای رمزنگاری باشد و یک خروجی را تولیدکند.

۳-۲۱ حد و مرز رمزنگاری[5]

محیط پیوسته تعریف‌شده صریحی است که حدود فیزیکی و / یا منطقی یک پودمان رمزنگاری را ایجادمی‌کند و شامل تمام مولفه‌های سخت‌افزاری، نرم‌افزاری و یا ثابت‌افزار یک پودمان رمزنگاری می‌باشد.

۳-۲۲ تابع درهم‌سازی رمزنگاری[6]

تابع کارآمد محاسباتی است که رشته‌های دودویی با طول اختیاری را به رشته‌های دودویی با طول ثابت می‌نگارند به‌طوری‌که در محاسبات نمی‌توان دو مقدار جدا را پیداکرد که به یک مقدار مشترک، درهم‌شوند.

۳-۲۳ کلید رمزنگاری[7]

کلید

ترتیب نمادهایی که عملیات یک تبدیلات رمزنگاری را کنترل‌می‌کند.

مثال: یک تبدیل رمزنگاری می‌تواند شامل به‌رمزدرآوردن، کشف رمز، محاسبه تابع بررسی رمزنگاری، تولید امضا یا تطبیق امضا شود ولی به این موارد محدودنمی‌شود.

---

1 - Critical Security Parameter
2 - Plaintext
3 - Crypto Officer
4 - Cryptographic Algorithm
5 - Cryptographic Boundary
6 - Cryptographic Hash Function
7 - Cryptographic Key

۲۴-۳ مولفه کلید رمزنگاری[1]

مولفه کلید

پارامتر به‌کاربرده‌شده در اتصال با مولفه‌های کلید دیگر در یک تابع امنیتی تاییدشده برای شکل‌دادن به یک متن‌ساده CSP یا انجام یک تابع رمزنگاری می‌باشد.

۲۵-۳ پودمان رمزنگاری[2]

پودمان

مجموعه سخت‌افزار، نرم‌افزار و یا ثابت‌افزار که توابع امنیت را اجرامی‌کنند و در داخل حد و مرز رمزنگاری قرارمی‌گیرند.

۲۶-۳ خط‌مشی امنیت پودمان رمزنگاری[3]

خط‌مشی امنیت

ویژگی دقیق قواعد امنیت است که در آن یک پودمان رمزنگاری باید به‌کارانداخته‌شود و شامل قواعد حاصل شده از الزامات این استاندارد و قواعد اضافی وضع‌شده توسط پودمان یا متولی اعتبارسنجی می‌باشد.

یادآوری- به پیوست «ب» مراجعه شود.

۲۷-۳ مسیر داده[4]

مسیر فیزیکی یا منطقی است که بر روی آن داده عبور می‌کند.

یادآوری- یک مسیر داده فیزیکی را می‌توان توسط چند مسیر داده منطقی به اشتراک گذاشت.

۲۸-۳ عملیات کاهیده[5]

عملیاتی است که در آن یک زیرمجموعه از کل مجموعه الگوریتم‌ها، توابع امنیت، خدمات و یا فرآیندها در دسترس هستند و / یا به‌عنوان یک نتیجه از پیکربندی دوباره از حالت خطا، قابل پیکربندی هستند.

۲۹-۳ تحلیل توان تفاضلی (DPA)[6]

تحلیل تغییرات مصرف برق یک پودمان رمزنگاری، به‌منظور استخراج اطلاعات مربوط به عملیات رمزنگاری.

۳۰-۳ امضا دیجیتال[7]

داده‌های الحاق‌شده[8] ، یا یک تبدیل رمزنگاری یک واحد داده که به دریافت‌کننده واحد داده اجازه می‌دهد تا تا مبدأ و یکپارچگی واحد داده را اثبات‌کند و در مقابل جعل محافظت‌کند (برای مثال، توسط گیرنده).

---

1 - Cryptographic Key Component
2 - Cryptographic Module
3 - Cryptographic Module Security Policy
4 - Data Path
5 - Degraded Operation
6 - Differential Power Analysis
7 - Digital Signature
8 - Append

۳-۳۱ ورودی مستقیم[1]

ورودی یک SSP یا مولفه کلیدی در داخل یک پودمان رمزنگاری، با استفاده از افزاره‌ای از قبیل صفحه کلید می‌باشد.

۳-۳۲ امضا گسسته[2]

یک یا چند امضا که با هم یک مجموعه کامل کد را نشان‌می‌دهند.

۳-۳۳ صدورهای الکترومغناطیسی (EME)[3]

علامت آستانه تحمل هوشمند، که اگر قطع‌شود و مورد تحلیل قرارگیرد، ممکن است اطلاعاتی را افشاکند که ارسال، دریافت و مدیریت‌می‌شود یا در غیر این‌صورت با تجهیزات پردازشگر ـ اطلاعات پردازش‌می‌شود.

۳-۳۴ ورودی الکترونیکی[4]

ورودی SSPها یا مولفه‌های کلید در داخل یک پودمان رمزنگاری با استفاده از روش‌های الکترونیکی می‌باشد.

یادآوری- عملگر کلید می‌تواند هیچ دانشی از مقدار کلیدی که واردمی‌شود نداشته‌باشد.

۳-۳۵ امضا فراگیر[5]

امضایی واحد که برای تمام مجموعه کدها است.

۳-۳۶ کلید رمزشده[6]

کلید رمزنگاری است که با استفاده از یک تابع امنیتی تاییدشده با یک کلید رمزنگاری کلید، رمزگذاری‌شده است.

یادآوری- محافظت‌شده درنظرگرفته‌می‌شود.

۳-۳۷ هستار[7]

شخص، گروه، افزاره یا فرآیند می‌باشد.

۳-۳۸ انتروپی[8]

سنجش اختلال، تصادفی‌بودن یا تغییرپذیری در یک سامانه بسته می‌باشد.

یادآوری- انتروپی یک متغیر تصادفی X، یک سنجش ریاضی از مقدار اطلاعاتی است که با یک مشاهده X تهیه‌شده‌است.

1 - Direct Entry
2 - Disjoint Signature
3 - Electromagnetic Emanations
4 - Electronic Entry
5 - Encompassing Signature
6 - Encrypted Key
7 - Entity
8 - Entropy

۳-۳۹ حفاظت خرابی محیطی (EFP)[1]

استفاده از ویژگی‌ها برای حفاظت در مقابل خطر امنیت پودمان رمزنگاری به‌دلیل شرایط محیطی خارج از گستره عملیات عادی پودمان می‌باشد.

۳-۴۰ آزمون خرابی محیطی (EFT)[2]

استفاده از روش‌های خاصی است که برای فراهم‌کردن اطمینان معقولی که امنیت یک پودمان رمزنگاری توسط شرایط محیطی خارج از گستره عملیات عادی پودمان به‌خطرنخواهدافتاد.

۳-۴۱ کد تشخیص خطا (EDC)[3]

مقدار محاسبه‌شده از داده است که شامل بیت‌های اضافی اطلاعات طراحی‌شده برای تشخیص (نه برای تصحیح) تغییرات غیرعمدی در داده می‌باشد.

۳-۴۲ شکل قابل‌اجرا[4]

شکل کدی که در آن نرم‌افزار یا ثابت‌افزار کاملاً توسط محیط عملیاتی پودمان مدیریت و کنترل‌می‌شود و نیازی به کامپایل[5] یا گردآوری ندارد (برای مثال، بدون کد منبع، کد شی، یا کد کامپایل‌شده فقط-در-زمان). زمان).

۳-۴۳ استنتاج خطا[6]

روش استنتاج تغییرات رفتار عملیاتی در سخت‌افزار با کاربرد روش‌های ولتاژهای ناپایدار، تابش، روش‌های لیزر یا اریب ساعت می‌باشد.

۳-۴۴ مدل وضعیت محدود (FSM)[7]

مدل ریاضی یک ماشین ترتیبی که شامل موارد زیر است:
مجموعه محدود رخدادهای ورودی، مجموعه محدود رخدادهای خروجی، مجموعه محدود وضعیت‌ها، تابعی که وضعیت‌ها و ورودی را به خروجی نگاشت‌می‌کند، تابعی که وضعیت‌ها و ورودی‌ها را به وضعیت‌ها (یک تابع انتقال وضعیت) نگاشت‌می‌کند و یک ویژگی که وضعیت اولیه را شرح‌می‌دهد.

۳-۴۵ ثابت‌افزار[8]

کد قابل‌اجرای یک پودمان رمزنگاری که در داخل سخت‌افزار در حد و مرز رمزنگاری ذخیره‌می‌شود و نمی‌تواند به‌طور پویا در طی اجرا نوشته یا اصلاح‌شود درحالی‌که در یک محیط عملیاتی غیرقابل‌اصلاح یا محدود به‌کارمی‌افتد.

---

1 - Environmental Failure Protection
2 - Environmental Failure Testing
3 - Error Detection Code
4 - Executable Form
5 - Compile
6 - Fault Induction
7 - Finite State Model
8 - Firmware

مثال: سخت‌افزار ذخیره‌سازی می‌تواند شامل PROM، EEPROM، FLASH، حافظه وضعیت سخت، درایوهای سخت و غیره باشد ولی به اینها محدودنمی‌شود.

۳-۴۶ پودمان ثابت‌افزار[1]

پودمانی که تنها شامل ثابت‌افزار می‌باشد.

۳-۴۷ ویژگی کارکردی[2]

درگاه‌ها و سخت‌افزارهای واسط برای پودمان رمزنگاری، تعریف وظایف و کارکرد هر واسط و پودمان رمزنگاری را بیان می‌کند.

۳-۴۸ آزمون کارکردی[3]

آزمون کارکرد پودمان رمزنگاری همان‌طور که توسط ویژگی کارکردی تعریف‌شده‌است.

۳-۴۹ سخت/ سختی[4]

مقاومت نسبی یک فلز یا ماده دیگر در مقابل دندانه‌دار شدن، خراش یا خمیدگی؛ به‌طور فیزیکی سخت‌شده‌است؛ ثابت و قوی است و بادوام می‌باشد.

یادآوری- مقاومت نسبی ماده‌ای که توسط شی دیگری نفوذ پیدامی‌کند.

۳-۵۰ سخت‌افزار[5]

تجهیزات/ مولفه‌های فیزیکی که در داخل حد و مرز رمزنگاری که برای پردازش برنامه‌ها و داده‌ها استفاده‌شده‌اند.

۳-۵۱ پودمان سخت‌افزار[6]

پودمانی که اصولاً از سخت‌افزار تشکیل‌می‌شود که ممکن است شامل ثابت‌افزار هم باشد.

۳-۵۲ واسط پودمان سخت‌افزار (HML)[7]

مجموعه کاملی از فرمان‌های به‌کاربرده‌شده برای درخواست خدمات از پودمان سخت‌افزار، از جمله پارامترهایی که به‌عنوان بخشی از خدمت درخواست‌شده وارد حد و مرز رمزنگاری پودمان یا از آن خارج‌می‌شوند.

۳-۵۳ ارزش درهم[8]

خروجی یک تابع درهم‌سازی رمزنگاری است.

۳-۵۴ پودمان ترکیبی[9]

---

1 - Firmware Module
2 - Functional Specification
3 - Functional Testing
4 - Hard/Hardness
5 - Hardware
6 - Hardware Module
7 - Hardware Module Interface
8 - Hash Value
9 - Hybrid Module

پودمانی که حد و مرز رمزنگاری آن، ترکیب یک نرم‌افزار یا ثابت‌افزار، مولفه و یک مولفه سخت‌افزار گسسته را تعیین‌می‌کند.

۳-۵۵ واسط پودمان ثابت‌افزار ترکیبی (HFMI)[1]

مجموعه کامل فرمان‌های به‌کاربرده‌شده برای درخواست خدمات از پودمان ثابت‌افزار ترکیبی، از جمله پارامترهایی که به‌عنوان بخشی از خدمت درخواست‌شده وارد حد و مرز رمزنگاری پودمان یا از آن خارج‌می‌شوند.

۳-۵۶ واسط پودمان نرم‌افزار ترکیبی (HSMI)[2]

مجموعه کامل فرمان‌های به‌کاربرده‌شده برای درخواست خدمات از پودمان نرم‌افزاری ترکیبی، از جمله پارامترهایی که به‌عنوان بخشی از خدمت درخواست‌شده وارد حد و مرز رمزنگاری پودمان یا از آن خارج‌می‌شوند.

۳-۵۷ داده‌های ورودی[3]

اطلاعاتی که وارد یک پودمان رمزنگاری می‌شود و ممکن است برای اهداف تبدیل یا محاسبه با یک تابع امنیتی تاییدشده استفاده‌شود.

۳-۵۸ یکپارچگی[4]

خصوصیتی که داده به یک روش غیرمجاز و کشف‌نشده، اصلاح یا حذف‌نشده‌است.

۳-۵۹ واسط[5]

ورودی منطقی یا نقطه خروج یک پودمان رمزنگاری که دسترسی به پودمان را برای گردش‌های اطلاعات منطقی فراهم‌می‌کند.

۳-۶۰ مورد پذیرش استاندارد ISO/IEC[6]

تابع امنیتی که

- در یک استاندارد ISO/IEC تعیین می‌شود یا
- در یک استاندارد ISO/IEC پذیرش / توصیه می‌شود و در یک پیوست از استاندارد ISO/IEC یا در یک مدرکی تعیین می‌شود که توسط استاندارد ISO/IEC ارجاع‌شده‌است.

۳-۶۱ موافقت کلید[7]

رویه برقراری SSP که در آنجا کلید برآیند، یک کارکردی از اطلاعات توسط دو یا چند شریک می‌باشد. به‌طوری‌که هیچ شریک یا گروهی نمی‌تواند مقدار کلید را آزادانه از سهم شریک یا گروه دیگر با استفاده از روش‌های خودکار، از پیش تعیین‌کند.

---

1 - Hybrid Firmware Module Interface
2 - Hybrid Software Module Interface
3 - Input Data
4 - Integrity
5 - Interface
6 - ISO/IEC Adopted
7 - Key Agreement

۳-۶۲ کلید رمزنگاری کلید (KEK)[1]

کلید رمزنگاری که برای رمزدارکردن یا کشف رمز کلیدهای دیگر استفاده‌می‌شود.

۳-۶۳ بارگذاری‌کننده کلید[2]

افزاره مستقل که قابلیت ذخیره‌کردن حداقل یک متن‌ساده یا SSP رمزشده یا مولفه کلید را دارد که می‌تواند با درخواست به داخل یک پودمان رمزنگاری منتقل‌شود.

یادآوری- کاربرد یک بارگذاری‌کننده کلید نیاز به تدبیر انسان دارد.

۳-۶۴ مدیریت کلید[3]

اداره و استفاده از تولید، ثبت، گواهی، حذف ثبت، توزیع، نصب، ذخیره‌سازی، بایگانی، لغو، اشتقاق و تخریب مواد کلیدی مطابق با یک خط‌مشی امنیت می‌باشد.

۳-۶۵ انتقال کلید[4]

فرآیند انتقال یک کلید از یک هستار به هستار دیگر با استفاده از روش‌های خودکار می‌باشد.

۳-۶۶ محیط عملیاتی محدود[5]

محیط عملیاتی که طراحی‌می‌شود تا تنها تغییرات ثابت‌افزار کنترل‌شده را بپذیرد که با موفقیت از آزمون بارگذاری نرم‌افزار / ثابت‌افزار عبور می‌کند.

۳-۶۷ آزمون سطح ـ پایین[6]

آزمون مولفه‌های شخصی یا گروه مولفه‌های پودمان رمزنگاری و درگاه‌های فیزیکی و واسط‌های منطقی می‌باشد.

۳-۶۸ نقش نگهداری[7]

نقش فرضی برای انجام نگهداری فیزیکی و / یا خدمات نگهداری منطقی.

مثال: خدمات نگهداری می‌توانند شامل تشخیص‌های سخت‌افزاری و / یا ثابت‌افزار باشند ولی به اینها محدود نیستند.

۳-۶۹ راهنمای دستی[8]

مستلزم دست‌کاری عملگر انسانی است.

---

1 - Key Encryption Key
2 - Key Loader
3 - Key Management
4 - Key Transport
5 - Limited Operational Environment
6 - Low-level Testing
7 - Maintenance Role
8 - Manual

۳-۷۰ کد اصالت‌سنجی پیام (MAC)[1]

مجموع مقابله‌ای[2] رمزنگاری بر روی داده‌هایی که از یک کلید متقارن استفاده‌می‌کنند تا اصلاحات تصادفی و و عمدی داده‌ها را کشف‌کنند.

مثال: یک کد اصالت‌سنجی پیام مبتنی بر درهم‌سازی.

۳-۷۱ ریزکد[3]

دستورالعمل‌های پردازنده که مطابق با یک دستورالعمل برنامه قابل‌اجرا می‌باشد.

مثال: کد هم‌گذار[4].

۳-۷۲ کمینه انتروپی[5]

حد پایین‌تر انتروپی که در تعیین یک تخمین بدترین حالت از انتروپی نمونه، مفید می‌باشد.

۳-۷۳ محیط عملیاتی اصلاح‌پذیر[6]

محیط عملیاتی که طراحی‌می‌شود تا تغییرات کارکردی را که ممکن است شامل نرم‌افزار بدون کنترل (برای مثال، غیرقابل‌اعتماد) باشد، بپذیرد.

۳-۷۴ اصالت‌سنجی چندعاملی[7]

اصالت‌سنجی با حداقل دو عامل اصالت‌سنجی مستقل.

یادآوری ۱- یک عامل اصالت‌سنجی، تکه‌ای از اطلاعات و فرآیند است که برای اصالت‌سنجی یا بررسی هستار استفاده‌می‌شود.

یادآوری ۲- طبقه‌های عامل اصالت‌سنجی مستقل عبارتند از: چیزی که شما می‌دانید، چیزی که شما دارید و چیزی که شما هستید.

۳-۷۵ پودمان رمزنگاری تعبیه‌شده چندتراشه‌ای[8]

نمایش کیفیت فیزیکی که در آن دو یا چند تراشه مدار مجتمع به‌هم متصل‌هستند و در داخل یک محفظه یا یک محصول تعبیه‌می‌شوند که ممکن است به‌طور فیزیکی محافظت‌نشود.

مثال: تطبیق‌دهنده‌ها[9] و بردهای گسترشی[10]

---

1 - Message Authentication Code
2 - Checksum
3 - Microcode
4 - Assembler
5 - Minimum Entropy
6 - Modifiable Operational Environment
7 - Multi-factor Authentication
8 - Multiple-chip Embedded Cryptographic Module
9 - Adapters
10 - Expansion Boards

۳-۷۶ پودمان رمزنگاری مستقل چندتراشه‌ای[1]

نمایش کیفیت فیزیکی که در آن دو یا چند تراشه مدار مجتمع به‌هم متصل‌هستند و محفظه کامل به‌طور فیزیکی محافظت و نگهداری‌می‌شود.

مثال: مسیریاب‌های رمزنگاری یا رادیوهای امن.

۳-۷۷ راهنمایی غیرمدیر[2]

مطالبی که توسط کاربر و / یا سایر نقش‌های غیرمدیریتی برای کار با پودمان رمزنگاری در یک حالت تاییدشده عملیات استفاده‌می‌شود.

یادآوری- راهنمای غیرمدیر توابع امنیت پودمان رمزنگاری را شرح‌می‌دهد و شامل اطلاعات و رویه‌هایی برای کاربرد امن پودمان رمزنگاری می‌باشد، که شامل دستورالعمل‌ها، رهنمودها و هشدارها می‌باشد.

۳-۷۸ حمله غیرتهاجمی[3]

حمله‌ای که می‌تواند بر روی یک پودمان رمزنگاری بدون تماس فیزیکی مستقیم با مولفه‌ها در حد و مرز رمزنگاری پودمان اجراشود.

یادآوری- حمله‌ای که وضعیت پودمان رمزنگاری را تغییرنمی‌دهد.

۳-۷۹ محیط عملیاتی تغییرناپذیر[4]

محیط عملیاتی که طراحی‌می‌شود تا تغییرات ثابت‌افزار را نپذیرد.

۳-۸۰ نامرتبط با امنیت[5]

الزاماتی که در دامنه کاربرد این استاندارد به آنها پرداخته نمی‌شود و شامل مراجع در توابع یا فرآیندهای امنیت تاییدشده یا تاییدنشده نمی‌باشد.

۳-۸۱ عملیاتی عادی[6]

عملیاتی که در آن مجموعه کامل الگوریتم‌ها، توابع امنیت، خدمات یا فرآیندها دردسترس و / یا قابل‌پیکربندی می‌باشند.

۳-۸۲ کِدِر[7]

غیرقابل‌نفوذ با نور (برای مثال، نوری درون طیف مرئی با طول موج در محدوده ۴۰۰nm تا ۷۵۰nm)، که در طیف مرئی شفاف و نیم‌شفاف نمی‌باشد.

---

1 - Multiple-chip Standalone Cryptographic Module
2 - Non-administrator Guidance
3 - Non-invasive Attack
4 - Non-modifiable Operational Environment
5 - Non-security Relevant
6 - Normal Operation
7 - Opaque

۳-۸۳ محیط عملیاتی[1]

مجموعه‌ای از تمام نرم‌افزار و سخت‌افزارهایی که شامل یک سامانه عملیاتی و بستر[2] سخت‌افزاری می‌باشند که برای عملیات امن پودمان لازم است.

۳-۸۴ وضعیت عملیاتی[3]

وضعیتی که در آن خدمات یا توابع را می‌توان توسط یک عملگر درخواست‌کرد و نتایج این داده‌ها، خروجی از واسط خروجی داده پودمان رمزنگاری هستند.

۳-۸۵ عملگر[4]

فرد یا فرآیندی (موضوع) که از طرف فرد عمل‌می‌کند، مجاز است که یک یا چند نقش را برعهده بگیرد.

۳-۸۶ داده‌های خروجی[5]

اطلاعات یا نتایج محاسبه‌شده که توسط یک پودمان رمزنگاری تولیدشده‌اند.

۳-۸۷ غیرفعال‌سازی[6]

اثر یک فرآیند واکنشی در اتصالات نیمه‌رسانا، سطوح یا مولفه‌ها و مدارهای مجتمع ساخته‌شده که شامل ابزارهای کشف و نگهداری‌می‌باشد.

مثال: دی‌اکسید سیلیکون یا شیشه فسفر.

یادآوری- غیرفعال‌سازی می‌تواند وضع مدار را اصلاح‌کند. مواد کم‌اثرپذیرسازی به تکنولوژی وابسته است.

۳-۸۸ اسم رمز[7]

رشته‌ای از نویسه‌ها که برای اصالت‌سنجی یک هستار و یا برای بررسی اجازه دسترسی استفاده‌شده‌است.

مثال: حروف، اعداد و نمادهای دیگر.

۳-۸۹ شماره شناسانه شخصی (PIN)[8]

کد عددی که برای اصالت‌سنجی یک هستار استفاده‌می‌شود.

۳-۹۰ محافظت فیزیکی[9]

نگهداری و حفاظت از یک پودمان رمزنگاری، SCPها و PSPها با استفاده از وسایل فیزیکی می‌باشد.

---

1 - Operational Environment
2 - Platform
3 - Operational State
4 - Operator
5 - Output Data
6 - Passivation
7 - Password
8 - Personal Identification Number
9 - Physical Protection

۳-۹۱ کلید متن‌ساده[1]

کلید رمزنگاری رمزنشده یا یک کلید رمزنگاری تیره‌شده توسط روش‌های تاییدنشده که بدون محافظ است.

۳-۹۲ درگاه[2]

نقطه ورودی یا خروجی فیزیکی/ منطقی یک پودمان رمزنگاری که دسترسی به پودمان را فراهم‌می‌کند.

۳-۹۳ خودآزمایی پیش‌عملیاتی[3]

آزمون انجام‌شده توسط یک پودمان رمزنگاری بین زمانی‌که یک پودمان رمزنگاری فعال یا نصب‌می‌شود (پس از این‌که خاموش[4]، تنظیم مجدد [5]، راه‌اندازی‌مجدد[6]، شروع‌سرد[7]، قطع برق[8] و غیره می‌شود) و به وضعیت وضعیت عملیاتی انتقال‌می‌یابد.

۳-۹۴ کلید خصوصی[9]

کلید یک جفت کلید نامتقارن هستار، که تنها باید توسط آن هستار استفاده‌شود.

یادآوری- در حالت یک سامانه امضا نامتقارن، کلید خصوصی تبدیل امضا را تعریف‌می‌کند. در حالت یک سامانه رمزنگاری نامتقارن، کلید خصوصی تبدیل کشف رمز را تعریف‌می‌کند.

۳-۹۵ رتبه تولید[10]

محصول، مولفه یا نرم‌افزاری که آزموده‌شده‌است تا مطابق با ویژگی‌های عملیاتی باشد.

۳-۹۶ کلید عمومی[11]

کلید یک جفت کلید نامتقارن هستار که می‌تواند عمومی ساخته‌شود.

یادآوری ۱- در حالت سامانه امضا نامتقارن، کلید عمومی تبدیل تطبیقی را تعریف‌می‌کند. در حالت سامانه رمزنگاری نامتقارن، کلید عمومی تبدیل رمزنگاری را تعریف‌می‌کند. کلیدی که «عمومی شناخته‌شده‌است» به‌طورلزوم به‌صورت سراسری در دسترس نمی‌باشد. این کلید تنها در اختیار تمام اعضای یک گروه از پیش تعیین‌شده می‌باشد.

یادآوری ۲- برای اهداف این استاندارد، کلیدهای عمومی، CSP در نظرگرفته‌نمی‌شوند.

---

1 - Plaintext Key
2 - Port
3 - Pre-operational Self-test
4 - Power Off
5 - Reset
6 - Reboot
7 - Cold-start
8 - Power Interruption
9 - Private Key
10 - Production-grade
11 - Public Key

۳-۹۷ گواهی کلید عمومی[1]

اطلاعات کلید عمومی یک هستار که توسط متولی مناسب گواهی، امضا شده‌است و به موجب آن غیرقابل‌جعل ارائه شده‌است.

۳-۹۸ الگوریتم رمزنگاری (نامتقارن) کلید عمومی[2]

الگوریتم رمزنگاری که از دو کلید وابسته، یک کلید عمومی و یک کلید خصوصی استفاده‌می‌کند.

یادآوری- دو کلید خصوصیتی دارند که استخراج کلید خصوصی از کلید عمومی به‌طورمحاسباتی غیرممکن است.

۳-۹۹ پارامتر امنیت عمومی (PSP)[3]

اطلاعات عمومی وابسته به امنیت که اصلاح آن می‌تواند امنیت یک پودمان رمزنگاری را به‌خطراندازد.

مثال: کلیدهای رمزنگاری عمومی، گواهی‌های کلید عمومی، گواهی‌های خودامضاشده، مهارهای اعتماد، اسم رمزهای یک بارمصرف مربوط به یک شمارشگر که به‌صورت داخلی تاریخ و زمان نگهداری می‌شود.

یادآوری- یک PSP اگر نتواند اصلاح‌شود یا اگر اصلاح آن را بتوان با پودمان تعیین‌کرد، حفاظت‌شده درنظرگرفته‌می‌شود.

۳-۱۰۰ تولید بیت تصادفی[4]

افزاره یا الگوریتمی که ترتیبی از بیت‌ها را خارج‌می‌کند که از لحاظ آماری مستقل و بدون تبعیض می‌باشد.

۳-۱۰۱ پوشش جداشدنی[5]

وسایل فیزیکی که اجازه طراحی عمومی را برای دسترسی به محتواهای فیزیکی یک پودمان رمزنگاری را بدون خسارت می‌دهند.

۳-۱۰۲ نقش[6]

خصیصه امنیت مربوط به یک کاربر که حقوق یا محدودیت‌های دسترسی کاربر به خدمات یک پودمان رمزنگاری را تعریف‌می‌کند.

یادآوری- یک یا چند خدمت می توانند به یک نقش مربوط شوند. یک نقش را می‌توان به یک یا چند کاربر مرتبط‌کرد و یک کاربر می‌تواند یک یا چند نقش را برعهده‌داشته‌باشد.

۳-۱۰۳ کنترل دسترسی نقش‌محور (RBAC)[7]

مجوزهای مربوط به یک نقش که برای دسترسی به شی اعطا می‌شود.

---

1 - Public Key Certificate
2 - Public Key (Asymmetric) Cryptographic Algorithm
3 - Public Security Parameter
4 - Random Bit Generator
5 - Removable Cover
6 - Role
7 - Role-based Access Control

۳-۱۰۴ محیط زمان‌اجرا[1]

وضعیت ماشین مجازی که خدمات نرم‌افزاری را برای فرآیندها یا برنامه‌ها در زمان‌اجرای یک رایانه فراهم‌می‌کند.

۳-۱۰۵ کلید محرمانه[2]

کلید رمزنگاری، که با یک الگوریتم رمزنگاری کلید محرمانه استفاده‌شده‌است به‌طور انحصاری به یک یا چند هستار مربوط‌می‌شود و نباید عمومی‌شود.

۳-۱۰۶ تابع امنیتی[3]

الگوریتم‌های رمزنگاری همراه با حالت‌های عملیات، از قبیل رمزهای بلوکی، رمزهای رشته‌ای، الگوریتم‌های کلید متقارن یا نامتقارن، کدهای اصالت‌سنجی پیام، توابع درهم‌سازی یا سایر توابع امنیت، مولدهای بیت تصادفی، اصالت‌سنجی هستار و تولید و استقرار SSP که همه اینها توسط استاندارد ISO/IEC یا یک متولی تایید، تأیید شدند.

یادآوری- به پیوست «پ» مراجعه شود.

۳-۱۰۷ کلید شروع[4]

مقدار محرمانه‌ای که برای مقداردهی اولیه به یک مولد بیت تصادفی استفاده‌می‌شود.

۳-۱۰۸ خودآزمون‌ها[5]

مجموعه‌ای از خودآزمون‌های پیش‌عملیاتی و شرطی که به درخواست عملگر یا به‌طور دوره‌ای پس از یک حداکثر زمان عملیاتی و تحت شرایط مشخص‌شده در خط‌مشی امنیت، اجرامی‌شود.

۳-۱۰۹ داده‌های حساس[6]

داده‌ای که از نظر کاربر، نیاز به محافظت دارد.

۳-۱۱۰ پارامترهای امنیت حساس (SSP)[7]

پارامترهای امنیت بحرانی (CSP) و پارامترهای امنیت عمومی (PSP).

۳-۱۱۱ خدمت[8]

هر عملگر خارجی که یک عملیات و / یا تابعی را فراخوانی‌کرده‌است که می‌تواند توسط یک پودمان رمزنگاری انجام‌شود.

---

1 - Runtime Environment
2 - Secret Key
3 - Security Function
4 - Seed Key
5 - Self-tests
6 - Sensitive Data
7 - Sensitive Security Parameters
8 - Service

۳-۱۱۲ ورودی خدمت[1]

تمام داده یا اطلاعات کنترل که توسط پودمان رمزنگاری استفاده‌می‌شود و مقداردهی اولیه می‌کند و یا عملیات‌ها یا توابع خاصی را به‌دست‌می‌آورد.

۳-۱۱۳ خروجی خدمت[2]

تمام داده و اطلاعات وضعیت که از عملیات‌ها یا توابعی حاصل‌می‌شود که مقداردهی اولیه شده‌است و یا توسط ورودی خدمت به‌دست‌آمده‌است.

۳-۱۱۴ تحلیل توان ساده (SPA)[3]

تحلیل مستقیم (به‌طور اصولی دیداری) الگوهای اجزای دستورالعمل (یا اجرای دستورالعمل‌های فردی) در رابطه با مصرف توان الکتریکی یک پودمان رمزنگاری، با هدف استخراج اطلاعات مربوط به یک عملیات رمزنگاری.

۳-۱۱۵ پودمان رمزنگاری تک‌تراشه‌ای[4]

نمایش کیفیت فیزیکی که در آن یک تراشه مدار مجتمع منفرد (IC)[5] ممکن است به‌عنوان یک افزاره مستقل استفاده‌شود و یا ممکن است درون یک محفظه یا محصول تعبیه‌شود که ممکن است به‌طور فیزیکی محافظت‌نشود.

مثال: تراشه‌های IC منفرد یا کارت‌های هوشمند با یک تراشه IC منفرد.

۳-۱۱۶ نرم‌افزار[6]

کد قابل‌اجرای یک پودمان رمزنگاری که در رسانه پاک‌شدنی ذخیره‌می‌شود که ممکن است به‌طور پویا نوشته شود و در طی اجرا زمانی‌که در یک محیط عملیاتی تغییرپذیر عمل‌می‌کنند، اصلاح‌شود.

مثال: رسانه پاک‌شدنی می‌تواند شامل حافظه وضعیت جامد، درایوهای سخت و غیره باشد ولی به این‌ها محدودنمی‌شود.

۳-۱۱۷ پودمان نرم‌افزار[7]

پودمانی که تنها از نرم‌افزار تشکیل می‌شود.

۳-۱۱۸ آزمون بار نرم‌افزار / ثابت‌افزار[8]

مجموعه آزمون‌های اجراشده بر روی نرم‌افزار یا ثابت‌افزار که قبل از این‌که بتواند با یک پودمان رمزنگاری اجراشود باید با موفقیت گذرانده‌شود.

---

1 - Service Input
2 - Service Output
3 - Simple Power Analysis
4 - Single-chip Cryptographic Module
5 - Integrated Circuit
6 - Software
7 - Software Module
8 - Software/Firmware Load Test

یادآوری- اگر نرم‌افزار یا ثابت‌افزار جایگزین تصویر کامل باشد و تنها پس از گردش توان پودمان اجراشود، کاربردپذیرنمی‌باشد.

۳-۱۱۹ واسط پودمان نرم‌افزار/ ثابت‌افزار (SFMI)[1]

مجموعه‌ای از فرمان‌های به‌کاربرده‌شده برای درخواست خدمات پودمان نرم‌افزار یا ثابت‌افزار که شامل پارامترهایی است که به‌عنوان قسمتی از خدمت درخواست‌شده به یک حد و مرز رمزنگاری پودمان وارد یا از آن خارج می‌شوند.

۳-۱۲۰ تقسیم دانش[2]

فرآیندی که با آن یک کلید رمزنگاری به چند مولفه کلید تقسیم‌می‌شود، به‌طور اختصاصی هیچ دانشی از کلید اصلی را تقسیم‌نمی‌کند. این کلید اصلی، می‌تواند پس از آن توسط هستارهای جدا، به داخل یک پودمان رمزگردانی وارد شود و یا از آن خارج شود و ترکیب‌شود تا کلید رمزنگاری اصلی را از نو ایجاد کند.

یادآوری- برای عمل ترکیب، همه یا زیرمجموعه‌ای از مولفه‌ها می‌توانند لازم باشند.

۳-۱۲۱ استقرار SSP[3]

فرآیند دردسترس‌قراردادن یک SSP مشترک در یک یا چند هستار.

یادآوری- استقرار SSP شامل توافق SSP، انتقال SSP و ورودی یا خروجی SSP می‌باشد.

۳-۱۲۲ اطلاعات وضعیت[4]

اطلاعاتی که خروجی از یک پودمان رمزنگاری است و برای اهدافی می‌باشد که مشخصه‌های عملیاتی خاص یا وضعیت‌های پودمان را نشان‌می‌دهد.

۳-۱۲۳ قوی[5]

به راحتی مغلوب نمی‌شود، مقاومت یا توانی بیشتر از میانگین یا مقدار مورد انتظار دارد، می‌تواند حمله را تحمل‌کند یا محکم ساخته شده باشد.

۳-۱۲۴ روش رمزنگاری متقارن[6]

روش رمزنگاری که از کلید رمز مشابه برای رمزدارکردن و کشف رمز تبدیل‌ها استفاده‌می‌کند.

۳-۱۲۵ کشف مداخله[7]

تعیین خودکار این‌که یک سوءقصد صورت‌گرفته‌است تا امنیت پودمان به‌خطر افتد و این کار توسط پودمان رمزنگاری انجام‌می‌شود.

---

1 - Software/Firmware Module Interface
2 - Split Knowledge
3 - SSP Establishment
4 - Status Information
5 - Strong
6 - Symmetric Cryptographic Technique
7 - Tamper Detection

۳-۱۲۶ شاهد مداخله[1]

نشانه یا علامت قابل ملاحظه‌ای که یک سوءقصد صورت‌گرفته‌است تا امنیت پودمان رمزگشایی را به‌خطراندازد.

۳-۱۲۷ پاسخ مداخله[2]

عمل خودکاری که توسط یک پودمان رمزگشایی زمانی‌که کشف سوء قصد رخ‌داده‌است، اتخاذمی‌شود.

۳-۱۲۸ پایداری اعتماد[3]

اطلاعات معتبر، که شامل یک الگوریتم کلید عمومی، مقدار کلید عمومی، یک نام صادرکننده و سایر پارامترها (به‌طور اختیاری) می‌باشد.

مثال: پارامترهای دیگر می‌توانند شامل شوند اما به یک دوره اعتبار محدود نیستند.

یادآوری- یک مهار اعتماد را می‌توان به‌صورت یک گواهی خودامضا شده فراهم‌کرد.

۳-۱۲۹ کانال قابل‌اعتماد[4]

پیوند ارتباطات قابل‌اعتماد و امن که بین پودمان رمزنگاری و یک فرستنده یا گیرنده برقرارشده‌است تا CSPهای متن‌ساده حفاظت‌نشده، مولفه‌های کلید و داده اصالت‌سنجی را با امنیت ارتباط‌دهند.

یادآوری- یک کانال قابل‌اعتماد، در مقابل استراق سمع و همچنین مداخله فیزیکی یا منطقی توسط هستارها / متصدیان، فرآیندها یا سایر افزاره‌های ناخواسته محافظت‌می‌کند. کانال اعتماد بین درگاه‌های ورودی یا خروجی تعریف‌شده پودمان و در امتداد پیوند ارتباط با نقطه پایانی درنظرگرفته‌شده می‌باشد.

۳-۱۳۰ کاربر[5]

نقش اتخاذشده توسط یک فرد یا فرآیندی (برای مثال، موضوع) که به نمایندگی از یک فرد عمل‌می‌کند و به یک پودمان رمزنگاری دسترسی‌دارد تا خدمات رمزنگاری را به‌دست آورد.

۳-۱۳۱ صحه‌گذاری‌شده[6]

اطمینان از مطابقت آزموده‌شده توسط یک مقام متولی صحه‌گذاری.

۳-۱۳۲ متولی صحه‌گذاری[7]

هستاری که به نتایج آزمون برای مطابقت با این استاندارد صحه می‌گذارد.

۳-۱۳۳ ارائه‌دهنده[8]

هستار، گروه یا انجمنی که پودمان رمزنگاری را برای آزمون و صحه‌گذاری ارائه‌می‌دهد.

---

1 - Tamper Evidence
2 - Tamper Response
3 - Trust Anchor
4 - Trusted Channel
5 - User
6 - Validated
7 - Validation authority
8 - Vendor

یادآوری- ارائه‌دهنده صرف‌نظر از این‌که پودمان رمزنگاری را طراحی‌کرده‌اند یا طراحی‌نکرده‌اند و یا توسعه‌می‌دهند یا توسعه‌نمی‌دهند، به تمام مستندات و شاهد طراحی مربوطه دسترسی‌دارد.

۳-۱۳۴ صفرکردن[1]

روش تخریب داده ذخیره‌شده و SSPهای محافظت‌نشده برای جلوگیری از بازیابی و استفاده مجدد می‌باشد.

۴ اصطلاحات اختصاری

API	Application Program Interface	واسط برنامه کاربردی
CBC	Cipher Block Chaining	زنجیره‌ای‌کردن بلوک رمز
CCM	Counter with Cipher block chaining-Message authentication code	مواجهه با کد اصالت‌سنجی پیام زنجیره‌ای‌کردن بلوک رمز
ECB	Electronic Codebook	کتاب کد الکترونیکی
HDL	Hardware Description Language	زبان توصیف سخت‌افزار
IC	Integrated Circuit	مدار مجتمع
PROM	Programmable Read-Only Memory	حافظه فقط‌خواندنی قابل‌برنامه‌ریزی
RAM	Random Access Memory	حافظه با دسترسی تصادفی
URL	Uniform Resource Locator	جایگزین‌شونده منبع یکسان

۵ سطوح امنیت پودمان رمزنگاری

زیربندهای زیر مرور کلی بر چهار سطح امنیتی می‌باشد. مثال‌های متداول ارائه‌شدند تا چگونگی رعایت الزامات را شرح‌دهند و این‌که قرار نیست این مثال‌ها محدودکننده یا تحلیل‌برنده[2] باشند. در این مدرک، ارجاعات به یک پودمان باید به‌عنوان یک پودمان رمزنگاری تفسیرشوند. روش‌های رمزنگاری در چهار سطح امنیتی یکسان هستند. هر وضع سطح امنیتی، سطوح الزامات امنیتی را برای حفاظت از خود پودمان افزایش‌می‌دهد (برای مثال، دسترسی و دانش مولفه‌های داخلی و عملیات) و شامل SSPها هستند و در

1 - Zeroisation
2 - Exhaustive

داخل پودمان کنترل‌می‌شوند. هر الزام امنیت توسط یک Shall [xx.yy] شناسایی‌می‌شود که xx نشان‌دهنده بند و yy یک شاخص عددی در داخل بند می‌باشد.

۵-۱ سطح امنیتی ۱

سطح امنیتی ۱، سطح پایه[1] امنیت را فراهم‌می‌کند. الزامات امنیتی پایه، برای یک پودمان رمزنگاری تعیین‌می‌شوند (برای مثال، حداقل یک تابع امنیتی تاییدشده یا یک روش استقرار پارامتر امنیت حساس تاییدشده باید به‌کاربرده‌شود). پودمان‌های نرم‌افزار یا ثابت‌افزار ممکن است در یک محیط عملیاتی تغییرناپذیر، محدود یا تغییرپذیر عمل‌کنند. در یک پودمان رمزنگاری سخت‌افزار سطح امنیتی ۱، هیچ سازوکاری از امنیت فیزیکی ویژه، بیشتر از الزام پایه برای مولفه‌های رتبه تولید لازم نمی‌باشد. روش‌های کاهش غیرتهاجمی یا کاهش سایر حملات که اجرامی‌شوند مستندمی‌شوند. مثال‌های یک پودمان رمزنگاری سطح امنیتی ۱، یک تخته رمزنگاری سخت‌افزار[2] می‌باشد که در رایانه شخصی (PC)[3] یا ابزار رمزنگاری یافت‌می‌شود و در یک افزاره دستی یا رایانه همه منظوره اجرامی‌شود.

به‌طور ایده‌آل، این پیاده‌سازی‌ها برای کاربردهای امنیتی مناسب هستند که در آنجا کنترل‌ها، از قبیل امنیت فیزیکی، امنیت شبکه و روش‌های مدیریتی، خارج از پودمان تهیه‌می‌شوند اما در داخل محیطی هستند که گسترش‌می‌یابند. برای مثال، پیاده‌سازی پودمان رمزنگاری سطح امنیتی ۱ ممکن است در چنین محیط‌هایی سودمندتر(از نظر هزینه) از پودمان‌های متناظر در سطوح اطمینان بالاتر باشد که این پودمان‌های سطح بالاتر، امنیت بیشتری از SSPهای پودمان‌ها را فراهم‌می‌کنند. همچنین پیاده‌سازی پودمان رمزنگاری سطح امنیتی ۱، سازمان‌ها را توانمند می‌کند تا راه‌حل‌های رمزنگاری دیگری را انتخاب‌کنند تا مطابق با الزامات امنیتی باشد که توجه به محیطی که پودمان عمل‌می‌کند در فراهم‌کردن امنیت کلی، تعیین‌کننده می‌باشد.

۵-۲ سطح امنیتی ۲

سطح امنیتی ۲ سازوکارهای امنیت فیزیکی سطح امنیتی ۱ را با افزودن الزام برای شواهد مداخله افزایش‌می‌دهد که شامل کاربرد پوشش‌های شواهد مداخله یا پوشش‌های پلاستیکی یا قفل‌های مقاوم در برابر جداسازی، بر روی پوشش‌ها یا درهای جداشدنی می‌باشد.

پوشش‌های شواهد مداخله یا پوشش‌های پلاستیکی روی یک پودمان قرار می گیرند به‌طوری‌که پوشش یا مهر باید شکسته‌شود تا دسترسی فیزیکی به SSPهای درون پودمان حاصل‌شود. پوشش‌های شواهد مداخله یا قفل‌های مقاوم دربرابر جداسازی روی پوشش‌ها یا درها قرارمی‌گیرند تا در مقابل دسترسی فیزیکی غیرمجاز محافظت‌کنند.

سطح امنیتی ۲ نیاز به اصالت‌سنجی نقش‌محور دارد که در آن پودمان رمزنگاری به اصالت‌سنجی یک عملگر صحه‌می‌گذارد تا یک نقش ویژه را برعهده بگیرد و یک مجموعه متناظری از خدمات را انجام‌دهد.

سطح امنیتی ۲ به پودمان رمزنگاری نرم‌افزار اجازه‌می‌دهد تا در محیط تغییرپذیری اجراشود که کنترل‌های دسترسی نقش‌محور را پیاده‌سازی‌می‌کند یا حداقل، یک کنترل دسترسی اختیاری و نامحدود با سازوکار قوی

1 - Baseline
2 - Hardware Encryption Board
3 - Personal Computer

و نیرومند دارد تا گروه‌های جدید را تعریف‌کند و مجوزهای محدودکننده را از طریق فهرست‌های کنترل دسترسی واگذارکند (برای مثال، ACLها) و بتواند برای هر کاربر بیش از یک گروه را اختصاص‌دهد و از آن در مقابل‌اجرا، اصلاح و خواندن غیرمجاز نرم‌افزار رمزنگاری محافظت‌کند.

۵-۳ سطح امنیتی ۳

علاوه بر سازوکارهای امنیت فیزیکی شواهد مداخله که در سطح امنیتی ۲ لازم است، سطح امنیتی ۳ الزامات اضافی را فراهم‌می‌کند تا دسترسی غیرمجاز به SSPها را در داخل پودمان رمزنگاری کاهش‌دهد. سازوکارهای امنیت فیزیکی لازم در سطح امنیتی ۳، به احتمال زیاد سوءقصدها را در دسترسی فیزیکی مستقیم، استفاده یا اصلاح پودمان رمزنگاری و کاوش میان حفره‌ها یا شکاف‌های تهویه را کشف و پاسخ‌می‌دهد. سازوکارهای امنیت فیزیکی ممکن است شامل استفاده از محفظه‌های قوی و مدارهای کشف / پاسخ مداخله‌کننده باشند که تمام CSPها را زمانی‌که پوشش‌ها/ درهای جداشدنی پودمان رمزنگاری باز هستند، صفرمی‌کند.

سطح امنیتی ۳ نیاز به سازوکارهای اصالت‌سنجی هستارمحور[1] دارد که امنیت فراهم‌شده با سازوکارهای اصالت‌سنجی نقش‌محوری را فراهم‌می‌کند که برای سطح امنیتی ۲ تعیین‌شده‌است. یک پودمان رمزنگاری، هستار یک عملگر را اصالت‌سنجی‌می‌کند و بررسی‌می‌کند که عملگر شناسایی‌شده مجاز است که نقش مشخص‌شده را برعهده بگیرد و یک مجموعه خدمات متناظر را انجام‌دهد.

سطح امنیتی ۳ به CSPهای متن‌ساده برقرارشده دستی نیازدارد که رمزنگاری‌شود، از یک کانال قابل‌اعتماد استفاده‌کند یا از یک رویه دانش تقسیم‌شده برای هر ورودی یا خروجی استفاده‌کند.

سطح امنیتی ۳ نیز از پودمان رمزنگاری در مقابل خطر کشف امنیت حفاظت‌می‌کند که به دلیل شرایط محیطی خارج از گستره‌های عملیاتی عادی پودمان برای ولتاژ و دما است. گشت‌وگذارهای عمدی بیش از حوزه‌های عملیاتی عادی ممکن است توسط یک مهاجم استفاده‌شود تا دفاع‌های یک پودمان رمزنگاری را خنثی کند. یک پودمان رمزنگاری موردنیاز است تا شامل ویژگی‌های حفاظت محیطی ویژه باشد و به این دلیل طراحی‌شده‌است تا هنگامی‌که ولتاژ و حدود دما افزایش‌می‌یابد و CSPها صفرمی‌شود را کشف کند. همچنین رمزنگاری لازم است تا در آزمون خرابی محیطی سخت قرارگیرد تا اطمینان قابل‌قبولی را فراهم‌کند که پودمان هنگامی‌که خارج از محدوده عملیاتی عادی به شیوه‌ای که می‌تواند امنیت پودمان را به‌خطراندازد، تحت تأثیر قرارنمی‌گیرد.

روش‌های کاهش غیرتهاجمی تعیین‌شده در زیربند۷-۸ که در پودمان پیاده‌سازی‌می‌شوند در اندازه‌های[2] سطح امنیتی ۳ آزمایش می‌شوند.

در تمام بندهای این استاندارد برای پودمان‌های رمزنگاری نرم‌افزار، سطح امنیتی ۳ ارائه‌نمی‌شود، بنابراین بیشترین سطح امنیتی کلی قابل‌دستیابی توسط پودمان رمزنگاری نرم‌افزاری در سطح امنیتی ۲ محدود است.

1 - Identity-based
2 - Metrics

پودمان‌های سطح امنیتی ۳ به تضمین‌های چرخه- عمر اضافی از قبیل مدیریت پیکربندی خودکار، طراحی دقیق، آزمون سطح پایین و اصالت‌سنجی عملگر با استفاده از اطلاعات اصالت‌سنجی فراهم‌شده توسط ارائه‌دهنده[1]، نیاز دارند.

۴-۵ سطح امنیتی ۴

سطح امنیتی ۴، بالاترین سطح امنیتی را فراهم‌می‌کند که در این استاندارد تعریف‌شده‌است. این سطح شامل تمام ویژگی‌های امنیت مناسب سطوح پایین‌تر و همچنین ویژگی‌های توسعه‌یافته می‌باشد.

در سطح امنیتی ۴، سازوکارهای امنیت فیزیکی یک پوشش کاملی از حفاظت را در پودمان رمزنگاری با نیت کشف و پاسخ به تمام سوءقصدهای غیرمجاز در دسترسی فیزیکی فراهم‌می‌کند و این کار زمانی انجام‌می‌شود که SSPها در پودمان قرار می‌گیرند، خواه توان خارجی به‌کاربرده‌شود یا نشود. نفوذ محفظه پودمان رمزنگاری از هر جهت احتمال بسیار زیاد کشف‌شدن را دارد که منجر به صفرشدن فوری تمام SSPهای حفاظت‌نشده می‌شود. پودمان‌های رمزنگاری سطح امنیتی ۴ برای عملیات در محیط‌های حفاظت‌نشده فیزیکی مفید هستند.

سطح امنیتی ۴ لزوم اصالت‌سنجی چندعاملی را برای اصالت‌سنجی عملگر معرفی‌می‌کند و حداقل به دو خصیصه از سه خصیصه زیر نیاز دارد:

- چیزی که شناخته‌شده، از قبیل اسم رمز مخفیانه
- چیزی که مالکیتش را دارا می‌باشد، از قبیل کلید فیزیکی یا نشانه
- یک خصوصیت فیزیکی، از قبیل زیست‌سنجشی

در سطح امنیتی ۴، پودمان رمزنگاری لازم است که شامل ویژگی‌های حفاظت محیطی باشد که برای کشف ولتاژ و محدوده‌های دما طراحی‌شده‌است. پودمان رمزنگاری همچنین لازم است کهCSPها را صفر کند تا اطمینان قابل‌قبولی را فراهم‌کند که این پودمان تحت تأثیر قرارنمی‌گیرد زمانی‌که خارج از گستره عملیاتی عادی به شیوه‌ای که می‌تواند امنیت پودمان را به‌خطراندازد.

روش‌های کاهش غیرتهاجمی تعیین‌شده در زیربند ۸-۷ که در پودمان پیاده‌سازی‌می‌شوند در اندازه‌های سطح امنیتی ۴ آزموده می‌شوند.

سطح امنیتی ۴ در تمام بندهای این استاندارد برای پودمان‌های رمزنگاری نرم‌افزاری ارائه‌نمی‌شود. بنابراین حداکثر سطح امنیتی کلی قابل‌دستیابی با پودمان‌های رمزنگاری در سطح امنیتی ۲ محدود است.

طراحی یک پودمان سطح امنیتی ۴، با مطابقت بین شرایط پیش- وضعیت و پس- وضعیت و مشخصات کارکردی بررسی‌می‌شود.

1 - Vendor-provided

۶ اهداف امنیت کارکردی

الزامات امنیتی تعیین‌شده در این استاندارد به طراحی و پیاده‌سازی امن یک پودمان رمزنگاری مربوط‌می‌شود. الزامات امنیتی با یک سطح پایه اهداف امنیت با افزایش سطوح اهداف امنیت شروع می‌شود. الزامات از اهداف امنیت کارکردی سطح بالا (که در زیر آمده‌است) برای پودمان رمزنگاری حاصل‌می‌شوند تا:

- توابع امنیتی تاییدشده را برای حفظ اطلاعات حساس به درستی پیاده‌سازی‌کنند و به‌کارگیرند.
- از یک پودمان رمزنگاری در برابر عملیات یا کاربرد غیرمجاز محافظت‌کنند.
- از افشای غیرمجاز مضمون‌های پودمان رمزنگاری، از جمله CSPها جلوگیری‌کنند.
- از اصلاح غیرمجاز و تشخیص‌داده‌نشده پودمان رمزنگاری و الگوریتم‌های رمزنگاری جلوگیری‌کنند، از جمله اصلاح، جانشینی، درج و حذف SSPهای غیرمجاز.
- نشانه‌هایی از وضعیت عملیاتی پودمان رمزنگاری را فراهم‌کنند.
- اطمینان‌دهند که پودمان رمزنگاری زمانی‌که در یک حالت تاییدشده عملیات عمل‌می‌کند، کارش را به‌درستی انجام‌می‌دهد.
- خطاها را در عملیات پودمان کشف‌کنند و از مصالحه SSPها که ناشی از این خطاهاست جلوگیری‌کنند و
- از طراحی، توزیع و پیاده‌سازی مناسب پودمان رمزنگاری اطمینان‌دهند.

۷ الزامات امنیتی

۷-۱ کلیات

این بند الزامات امنیتی را مشخص می‌کند که [01.01] shall باید توسط پودمان رمزنگاری مطابق با این استاندارد، برآورده‌شود. الزامات امنیتی، نواحی مرتبط با طراحی و پیاده‌سازی یک پودمان رمزنگاری را پوشش‌می‌دهد. این نواحی شامل موارد زیر می‌باشد: ویژگی‌های پودمان رمزنگاری، واسط‌های پودمان رمزنگاری، نقش‌ها، خدمات و اصالت‌سنجی، امنیت نرم‌افزار/ ثابت‌افزار، محیط عملیاتی، امنیت فیزیکی، امنیت غیرتهاجمی، مدیریت پارامتر امنیت حساس، خودآزمون‌ها، تضمین چرخه عمر و کاهش حملات دیگر می‌باشد.

جدول ۱ الزامات امنیتی را در هر یک از این نواحی خلاصه می‌کند.

یک پودمان رمزنگاری [01.02] shall باید در مقابل الزامات هر ناحیه آدرس‌دهی در این بند آزموده‌شود. پودمان رمزنگاری [01.03] shall باید به‌طور مستقل، در هر ناحیه درجه‌بندی‌شود. چندین ناحیه فراهم‌می‌شود تا برای هر سطح امنیتی، سطوح امنیت با الزامات امنیتی جمعی افزایش‌یابد. در این نواحی، پودمان رمزنگاری درجه‌بندیی را دریافت‌می‌کند که بالاترین سطح امنیتی را منعکس‌می‌کند که برای آن، پودمان تمام الزامات آن ناحیه را برآورده‌می‌کند. در نواحی که برای سطوح مختلف امنیت فراهم‌نمی‌شود (برای مثال، مجموعه استاندارد الزامات)، پودمان رمزنگاری درجه‌بندی را متناسب با درجه‌بندی کلی دریافت‌می‌کند.

علاوه بر دریافت درجه‌بندی مستقل برای هر یک از نواحی امنیت، پودمان رمزنگاری درجه‌بندی امنیت کلی را دریافت‌خواهدکرد. درجه‌بندی امنیت کلی نشان‌دهنده حداقل سطح درجه‌بندی‌های مستقل می‌باشد که در این نواحی دریافت‌شده‌اند.

بسیاری از الزامات امنیتی این استاندارد شامل الزامات مستندسازی ویژه می‌باشد که در پیوست‌های «الف» و «ب» خلاصه می‌شود. تمام مستندسازی، از جمله کپی‌های راهنماهای کاربر و نصب، ویژگی‌های طراحی، مستندسازی چرخه عمر [01.04] shall باید برای یک پودمان رمزنگاری تهیه‌شود که تحت برنامه بررسی یا ارزیابی مستقل قرارمی‌گیرند.

پیوست‌های «پ»، «ت»، «ث» و «ج» مراجعی را برای موارد زیر ارائه‌می‌کنند: توابع امنیت تاییدشده، روش‌های استقرار پارامتر امنیت حساس تاییدشده، سازوکارهای اصالت‌سنجی و روش‌های آزمون کاهش حمله غیرتهاجمی تاییدشده.

جدول ۱- خلاصه الزامات امنیتی

	سطح امنیتی ۱	سطح امنیتی ۲	سطح امنیتی ۳	سطح امنیتی ۴
ویژگی‌های پودمان رمزنگاری	ویژگی پودمان رمزنگاری، حد و مرز رمزنگاری، توابع امنیت تاییدشده و حالت‌های عادی و تخریب عملیات. توصیف پودمان رمزنگاری از جمله تمام مولفه‌های سخت‌افزار، نرم‌افزار و ثابت‌افزار. تمام خدمات، اطلاعات وضعیت را فراهم‌می‌کنند تا نشان‌دهند چه زمانی خدمت از یک الگوریتم رمزنگاری تاییدشده، تابع یا فرآیند امنیت در یک روش تاییدشده استفاده‌می‌کند.			
واسط‌های پودمان رمزنگاری	واسط‌های لازم و اختیاری. ویژگی تمام واسط‌ها و تمام مسیرهای داده ورودی و خروجی.		کانال قابل اطمینان.	
نقش‌ها، خدمات و اصالت‌سنجی	جداسازی منطقی نقش‌ها و خدمات لازم و اختیاری	اصالت‌سنجی عملگر نقش‌محور یا هستارمحور.	اصالت‌سنجی عملگر هستارمحور.	اصالت‌سنجی چندعاملی
امنیت نرم‌افزار / ثابت‌افزار	روش یکپارچگی تاییدشده، SFMI، HFMI و HSMI تعریف‌شده. کد قابل‌اجرا	امضا دیجیتالی تاییدشده یا آزمون یکپارچگی مبتنی بر کد اصالت‌سنجی پیام کلیددارشده		آزمون یکپارچگی مبتنی بر امضا دیجیتال تاییدشده.
محیط عملیاتی	غیرقابل اصلاح، محدود یا قابل‌اصلاح. کنترل SSPها	قابل‌اصلاح. کنترل دسترسی اختیاری یا نقش‌محور. سازوکار حسابرسی		
امنیت فیزیکی	مولفه‌های رتبه تولید	شواهد مداخله پوشش یا محفظه کدر	کشف و پاسخ مداخله برای پوشش‌ها و درها. پوشش یا محفظه قوی. حفاظت از کاوش مستقیم. EFP یا EFT	کشف و پوشش پاسخ مداخله. EFP. کاهش تزریق اشکال.
امنیت غیرتهاجمی	پودمان طراحی‌می‌شود تا حملات غیرتهاجمی تعیین‌شده در پیوست «ج» کاهش‌دهد.			
	مستندسازی و اثربخشی روش‌های کاهش تعیین‌شده در پیوست «ج».		آزمون کاهش	آزمون کاهش
مدیریت پارامتر امنیت حساس	مولدهای بیت تصادفی، تولید، استقرار، ورودی و خروجی، ذخیره‌سازی و صفرکردن SSP			
	انتقال SSP خودکار یا موافقت SSP با استفاده از روش‌های تاییدشده			
	SSPهای به‌طوردستی استقراریافته ممکن است به شکل متن‌ساده وارد یا خارج‌شوند.		SSPهای به‌طوردستی استقراریافته ممکن است به شکل رمزدار از طریق یک کانال قابل‌اعتماد یا استفاده از رویه‌های دانش جداشده وارد یا خارج‌شوند.	

جدول ۱- ادامه

		سطح امنیتی ۱	سطح امنیتی ۲	سطح امنیتی ۳	سطح امنیتی ۴
خودآزمایی‌ها		پیش‌عملیاتی: یکپارچگی نرم‌افزار/ ثابت‌افزار، کنارگذار و آزمون کارکردهای بحرانی.			
		شرطی: الگوریتم رمزنگاری، بارگذاری نرم‌افزار/ ثابت‌افزار، سازگاری جفت‌به‌جفت، ورودی دستی، کنارگذار شرطی و آزمون کارکردهای بحرانی.			
تضمین چرخه عمر	**مدیریت پیکربندی**		سامانه مدیریت پیکربندی برای پودمان رمزنگاری، مولفه‌ها و مستندسازی. هر چرخه عمر کلی دنبال‌شده و به‌طور انحصاری شناسایی‌شده	سامانه مدیریت پیکربندی خودکار	
	طراحی	پودمان طراحی‌شده که آزمون همه خدمات مرتبط با امنیت فراهم‌شده را اجازه دهد.			
	FSM	مدل وضعیت محدود			
	توسعه	کد منبع علامت‌گذاری‌شده، طرح کلی یا HDL	زبان سطح بالای نرم‌افزار. زبان توصیف سخت‌افزار.		مستندسازی علامت‌گذاری‌شده با پیش‌شرایط در ورودی درون مولفه‌های پودمان و پس-شرایط صحیح زمانی‌که مولفه‌ها کامل است.
	آزمون	آزمون کارکردی		آزمون سطح پایین	
	تحویل و عملیات	رویه‌های مقداردهی اولیه	رویه‌های تحویل		اطلاعات اصالت‌سنجی تهیه‌شده
	راهنمایی	راهنمای مدیر و غیرمدیر			
کاهش سایر حملات		ویژگی کاهش حملات که برای آن هیچ الزمات قابل‌آزمونی در حال حاضر در دسترس نمی‌باشد.			ویژگی کاهش حملات با الزامات قابل آزمون.

۷-۲ ویژگی پودمان رمزنگاری

۷-۲-۱ الزامات کلی ویژگی پودمان رمزنگاری

یک پودمان رمزنگاری باید shall [02.01] مجموعه‌ای از سخت‌افزار، نرم‌افزار، ثابت‌افزار یا چند ترکیب از آن باشد که حداقل، یک خدمت رمزنگاری تعریف‌شده را پیاده‌سازی‌می‌کند که از یک الگوریتم رمزنگاری تاییدشده، تابع امنیتی یا فرآیند امنیت استفاده‌می‌کند و در یک حد و مرز رمزنگاری تعریف‌شده قرارمی‌گیرد. الزامات مستندسازی مشخص‌شده در بند پیوست الف-۲-۲ shall [02.02] باید تهیه‌شود.

۷-۲-۲ انواع پودمان‌های رمزنگاری

یک پودمان رمزنگاری shall [02.03] باید به‌عنوان یکی از انواع پودمان‌های زیر تعریف‌شود:

- ***پودمان سخت‌افزار*** پودمانی است که حد و مرز رمزنگاری آن در یک محیط سخت‌افزاری تعیین می‌شود. ثابت‌افزار و / یا نرم‌افزار که ممکن است شامل یک سامانه عملیاتی باشد، ممکن است در این حد و مرز رمزنگاری سخت‌افزاری قرارگیرد.
- ***پودمان نرم‌افزار*** پودمانی است که حد و مرز رمزنگاری آن حدود مولفه‌های انحصاری نرم‌افزار را تعیین‌می‌کند (ممکن است یک یا چند مولفه نرم‌افزاری باشد) که در یک محیط عملیاتی قابل تغییر اجرامی‌شود. بستر محاسبه و سامانه عملیاتی محیط عملیاتی که نرم‌افزار اجرامی‌کند، خارج از حد و مرز پودمان نرم‌افزار تعریف‌می‌شود.
- ***پودمان ثابت‌افزار*** پودمانی است که حد و مرز رمزنگاری آن حدود مولفه‌های انحصاری ثابت‌افزار را تعیین‌می‌کند که در یک محیط عملیاتی محدود یا غیرقابل‌تغییر اجرامی‌شود. بستر عملیاتی و سامانه عملیاتی محیط عملیاتی که ثابت‌افزار اجرامی‌کند خارج از حد و مرز پودمان رمزنگاری تعریف‌شده هستند اما به‌طور صریح در پودمان ثابت‌افزار محدود هستند.
- ***پودمان نرم‌افزار ترکیبی*** پودمانی است که حد و مرز رمزنگاری آن حدود ترکیب یک مولفه نرم‌افزاری و یک مولفه سخت‌افزاری گسسته را تعیین‌می‌کند (یعنی مولفه نرم‌افزاری در داخل حد و مرز پودمان سخت‌افزاری نمی‌باشد). بستر محاسبه و سامانه عملیاتی محیط عملیاتی که نرم‌افزار اجرامی‌کند خارج از حد پودمان نرم‌افزار ترکیبی هستند.
- ***پودمان ثابت‌افزار ترکیبی*** پودمانی است که حد و مرز رمزنگاری آن حدود ترکیب یک مولفه ثابت‌افزار و یک مولفه سخت‌افزار گسسته را تعیین‌می‌کند (یعنی مولفه ثابت‌افزار در داخل حد و مرز پودمان سخت‌افزار قرارنمی‌گیرد). بستر محاسبه و سامانه عملیاتی محیط عملیاتی که ثابت‌افزار اجرامی‌کند خارج از حد پودمان ثابت‌افزار ترکیبی تعریف‌شده هستند اما به‌طور صریح در پودمان ثابت‌افزار ترکیبی محدود هستند.

برای پودمان‌های نرم‌افزاری که در یک محیط تغییرپذیر اجرا می‌شوند، امنیت فیزیکی و الزامات امنیتی غیرتهاجمی در زیربندهای ۷-۷ و ۷-۸ اختیاری هستند.

برای پودمان‌های سخت افزار و ثابت‌افزار، امنیت فیزیکی و الزامات امنیتی غیرتهاجمی و زیربندهای ۷-۷ و ۷-۸ shall [02.04] باید به‌کاربرده‌شوند.

برای پودمان‌های ترکیبی، مولفه‌های نرم‌افزار و ثابت‌افزار shall [02.05] باید مطابق با تمام الزامات کاربردی زیربندهای ۷-۵ و ۷-۶ باشند. مولفه‌های سخت‌افزاری shall [02.06] باید مطابق با تمام الزامات کاربردپذیر زیربندهای ۷-۷ و ۷-۸ باشند.

۷-۲-۳ حد و مرز رمزنگاری

۷-۲-۳-۱ الزامات کلی حد و مرز رمزنگاری

یک حد و مرز رمزنگاری shall [02.07] باید شامل محیط تعریف‌شده صریح باشد (یعنی مجموعه مولفه‌های سخت‌افزار، نرم‌افزار یا ثابت‌افزار) که حد و مرز تمام مولفه‌های پودمان رمزنگاری را برقرار می‌کند. الزامات این استاندارد shall [02.08] باید در تمام الگوریتم‌ها، توابع امنیت، فرآیندها و مولفه‌های درون حد و مرز رمزنگاری پودمان به‌کاربرده‌شود. حد و مرز رمزنگاری shall [02.09] حداقل باید شامل تمام الگوریتم‌های مربوط به امنیت، توابع امنیت، فرآیند و مولفه‌های یک پودمان رمزنگاری باشد (یعنی امنیت مناسب در دامنه کاربرد این استاندارد). الگوریتم‌های مربوط به عدم امنیت، توابع امنیت، فرآیندها یا مولفه‌ها ممکن است در محدوده رمزنگاری باشند. الگوریتم‌های مربوط به عدم امنیت، توابع امنیت، فرآیندها یا مولفه‌ها ممکن است در یک حالت تاییدشده عملیات استفاده‌شود. الگوریتم‌های مربوط به عدم امنیت، توابع امنیت، فرآیندها یا مولفه‌هایی که می‌توانند در یک حالت تاییدشده عملیات استفاده‌شوند shall [02.10] باید در حالتی پیاده‌سازی‌شوند که تداخل نکنند و یا عملیات تاییدشده پودمان رمزنگاری را به‌خطر نیاندازند.

نام تعریف‌شده یک پودمان رمزنگاری shall [02.11] باید بیانگر ترکیب مولفه‌ها در داخل حد و مرز رمزنگاری باشد و بیانگر ترکیب یا محصول بزرگ‌تر نباشد. پودمان رمزنگاری shall [02.12] باید حداقل، اطلاعات نسخه ویژه را داشته‌باشد که نشان‌دهنده سخت‌افزار فردی جدا، مولفه‌های نرم‌افزار و / یا ثابت‌افزار می‌باشد.

مولفه‌های سخت‌افزار، نرم‌افزار و ثابت‌افزار در درون حد و مرز رمزنگاری ممکن است از الزامات این استاندارد مستثنی باشند. مولفه‌های سخت‌افزار، نرم‌افزار یا ثابت‌افزار مستثنی‌شده shall [02.13] باید در حالتی پیاده‌سازی‌شوند که تداخل‌نکنند و یا عملیات امنیت تاییدشده پودمانی رمزنگاری را به‌خطر نیازندازند.

سخت‌افزار، نرم‌افزار یا ثابت‌افزار مستثنی‌شده shall [02.14] باید معین شود (به پیوست «الف» مراجعه شود).

۷-۲-۳-۲ تعریفات حد و مرز رمزنگاری

حد و مرز رمزنگاری یک **پودمان رمزنگاری سخت‌افزار** shall [02.15] باید تعیین و مشخص‌شود:

- مجموعه مولفه‌های سخت‌افزاری که ممکن است شامل:
  - ساختارهای فیزیکی باشد از جمله، برد مدارها، لایه‌ها یا سطوح برجسته دیگری که اتصال فیزیکی به‌هم‌متصل را بین مولفه‌ها فراهم‌می‌کنند.
  - مولفه‌های الکتریکی فعال از قبیل مدارهای نیمه‌مجتمع[1]، سفارشی‌مجتمع[2] یا مشترک‌مجتمع[3]، پردازنده‌ها، حافظه، منبع‌های تغذیه، مبدل‌ها و غیره.

1 - Semi-integrated
2 - Custom-integrated
3 - Common-integrated

- ساختارهای فیزیکی، از قبیل محفظه‌ها، مواد ظرف یا محفظه، رابط‌ها و واسط‌ها.
- ثابت‌افزار، که ممکن است شامل یک سامانه عملیاتی باشد.
- سایر انواع مولفه‌ها در بالا فهرست نشدند.

حد و مرز رمزنگاری **پودمان رمزنگاری نرم‌افزار** [02.16] shall باید معین و شناسایی‌شود:

- مجموعه پرونده[1] یا پرونده‌های قابل‌اجرا که پودمان رمزنگاری را تشکیل می‌دهند و
- ایجاد نمونه پودمان رمزنگاری ذخیره‌شده در حافظه و اجراشده با یک یا چند پردازنده.

حد و مرز رمزنگاری یک **پودمان رمزنگاری ثابت‌افزار** [02.17] shall باید تعیین و شناسایی‌شود:

- مجموعه پرونده یا پرونده‌های قابل‌اجرا که پودمان رمزنگاری را تشکیل‌می‌دهند و
- ایجاد نمونه پودمان رمزنگاری ذخیره‌شده در حافظه و اجراشده با یک یا چند پردازنده

حد و مرز رمزنگاری یک **پودمان رمزنگاری ترکیبی** باید [02.18] shall:

- ترکیبی از حد و مرز مولفه سخت‌افزار پودمان و حد و مرز مولفه(های) نرم‌افزار یا ثابت‌افزار گسسته باشد و
- شامل مجموعه تمام درگاه‌ها و واسط‌ها از هر مولفه باشد.

علاوه بر مولفه(های) نرم‌افزار و یا ثابت‌افزار گسسته، مولفه سخت‌افزار نیز ممکن است شامل نرم‌افزار یا ثابت‌افزار جاسازی‌شده[2] باشد.

۷-۲-۴ حالت‌های عملیات

۷-۲-۴-۱ حالت‌های الزامات کلی عملیات‌ها

عملگر [02.19] shall باید بتواند پودمان را در یک حالت تاییدشده عملیات به‌کار بیاندازد. یک حالت تاییدشده عملیات [02.20] shall باید به‌عنوان مجموعه خدماتی تعریف‌شود که حداقل شامل یک خدمت است که از یک الگوریتم رمزنگاری تاییدشده، تابع یا فرآیند امنیت و خدمات یا فرآیندهای مشخص‌شده در زیربند ۷-۴-۳ استفاده‌می‌کند.

الگوریتم‌های رمزنگاری تاییدنشده، توابع امنیت و فرآیندها یا سایر خدمات تعیین‌نشده در زیربند ۷-۴-۳ نباید [02.21] shall توسط عملگر در حالت تاییدشده عملیات استفاده شود مگر این‌که الگوریتم رمزنگاری تاییدنشده یا تابع امنیتی، بخشی از یک فرآیند تاییدشده باشد و عملیات تاییدشده، مرتبط با امنیت نباشد (برای مثال، یک الگوریتم رمزنگاری تاییدنشده یا کلید تولیدی تاییدنشده که ممکن است برای مبهم‌کردن داده یا CSPها استفاده‌شود اما نتیجه آن متن‌ساده حفاظت‌نشده فرض‌می‌شود و هیچ تابع مرتبط با امنیت را تأمین نمی‌کند تا این‌که با یک الگوریتم رمزنگاری تاییدنشده حفاظت‌شود).

۷-۲-۴-۲ عملیات عادی

عملیات عادی جایی است که کل مجموعه الگوریتم‌ها، توابع امنیت، خدمات یا فرآیندها در دسترس و / یا قابل‌پیکربندی هستند.

---

1 - File
2 - Embedded

CSPها shall [02.22] باید بین خدمات تاییدشده و تاییدنشده و حالت‌های عملیاتی، انحصاری باشند (برای مثال تقسیم‌شده یا دسترسی‌شده نباشند). خروجی یک مولد بیت تصادفی (RBG)[1] تاییدشده ممکن است در یک الگوریتم تاییدنشده، تابع امنیتی یا فرآیند بدون صفرشدن شروع اولیه تصادفی RBG فراهم‌شود، در طی زمانی‌که این شروع اولیه تصادفی را نمی‌توان در حالت تاییدنشده در دسترس قرار داد.

خط‌مشی امنیت پودمان shall [02.23] باید مجموعه کامل خدماتی را تعریف‌کند که برای هر حالت تعریف‌شده عملیات تهیه‌می‌شوند (تاییدشده و تاییدنشده).

هنگامی‌که خدمات از یک الگوریتم رمزنگاری تاییدشده، تابع امنیتی یا فرآیند در یک حالت تاییدشده و خدمات یا فرآیندهای تعیین‌شده در زیربند ۷-۴-۳ استفاده‌می‌کنند، shall [02.24] باید شاخصی[2] را فراهم‌کنند.

۷-۲-۴-۳ عملیات تخریب

یک پودمان رمزنگاری ممکن است طراحی‌شود تا اگر پودمان وارد وضعیت خطا شود، از کارکردی‌شدن تخریب پشتیبانی‌کند. برای عمل پودمان رمزنگاری در عملیات تخریب، موارد زیر shall [02.25] باید به‌کاربرده‌شود:

- عملیات تخریب[02.26] shall باید تنها پس از خروج وضعیت خطا واردشود.
- پودمان shall [02.27] باید اطلاعات وضعیت را زمانی تهیه‌کند که بازپیکربندی‌شود و عملیات تخریب واردشود.
- سازوکار یا تابعی که ردشده shall [02.28] باید جداشود.
- همه خودآزمایی‌های الگوریتم شرطی shall [02.29] باید قبل از اولین استفاده عملیاتی الگوریتم رمزنگاری پس از ورود به عملیات تخریب انجام‌شود و
- اگر برای استفاده از یک الگوریتم غیرعملیاتی، تابع امنیتی و فرآیند سوءقصدهایی شود، خدمات shall [02.30] باید شاخصی را تهیه‌کنند.

پودمان رمزنگاری shall [02.31] باید در عملیات تخریب بماند تا زمانی‌که پودمان رمزنگاری بدون خرابی تمام خودآزمایی‌های شرطی و پیش‌عملیاتی موفق تاییدشود. اگر پودمان رمزنگاری در خودآزمایی‌های پیش‌شرطی ناموفق باشد، پودمان نباید shall not[02.32] وارد عملیات تخریب شود.

۷-۳ واسط‌های پودمان رمزنگاری

۷-۳-۱ الزامات کلی واسط‌های پودمان رمزنگاری

یک پودمان رمزنگاری shall [03.01] باید همه گردش اطلاعات منطقی را تنها به نقاط دسترسی فیزیکی و واسط‌های منطقی محدودکند که به‌عنوان نقاط ورودی و خروجی و از حد و مرز رمزنگاری پودمان شناسایی‌می‌شوند. واسط‌های منطقی پودمان رمزنگاری shall [03.02] باید جدا از یکدیگر باشند اگرچه آنها یک درگاه فیزیکی مشترک دارند (برای مثال، داده‌های ورودی و داده‌های خروجی ممکن است از طریق یک

1 - Random Bit Generator
2 - Indicator

درگاه وارد و خارج‌شوند) یا ممکن است بر روی یک یا چند درگاه فیزیکی توزیع شوند (برای مثال داده ورودی ممکن است از طریق هم درگاه سری و هم درگاه موازی واردشود). یک API مولفه نرم‌افزاری از یک پودمان رمزنگاری ممکن است به‌عنوان یک یا چند واسط منطقی تعریف‌شود.
الزامات مستندسازی تعیین‌شده در زیربند پیوست الف-۲-۳ [03.03] shall باید تهیه‌شوند.

۷-۳-۲ انواع واسط‌ها

- *واسط پودمان سخت‌افزار (HMI)*[1]: مجموعه کل واسط‌های به‌کاررفته برای درخواست خدمات پودمان سخت‌افزار، از جمله پارامترهایی که از حد و مرز رمزنگاری پودمان به‌عنوان بخشی از خدمت درخواستی وارد یا خارج‌می‌شوند.
- *واسط پودمان نرم‌افزار یا ثابت‌افزار (SFMI)*[2]: مجموعه کلی واسط‌های به‌کاربرده‌شده برای درخواست خدمات نرم‌افزار یا پودمان ثابت‌افزار، از جمله پارامترهایی که به‌عنوان بخشی از خدمت درخواستی از حد و مرز رمزنگاری پودمان وارد یا خارج‌می‌شوند.
- *واسط پودمان نرم‌افزار ترکیبی یا ثابت‌افزار ترکیبی (HFMI یا HSMI)*[3]: مجموعه کل واسط‌های به‌کاربرده‌شده برای درخواست خدمات پودمان نرم‌افزار ترکیبی یا ثابت‌افزار ترکیبی، از جمله پارامترهایی که به‌عنوان بخشی از خدمات درخواستی از حد و مرز رمزنگاری پودمان وارد یا خارج‌می‌شوند.

۷-۳-۳ تعریف واسط‌ها

یک پودمان رمزنگاری [03.04] shall باید واسط‌های زیر را داشته‌باشد («ورودی» و «خروجی» از دیدگاه پودمان نشان‌داده‌می‌شوند):

۱. *واسط ورودی داده*. تمام داده‌ای (به جز داده کنترل که از طریق کنترل واسط ورودی واردمی‌شود) که وارد می‌شود و با پودمان رمزنگاری پردازش می‌شود (از جمله داده متن‌ساده، داده متن رمز، SSPها و اطلاعات وضعیت از پودمان دیگر) [03.05] shall باید از طریق واسط «ورودی داده» وارد شود. در حین‌این‌که پودمان، خودآزمایی‌ها را انجام می‌دهد، داده ممکن است توسط پودمان از طریق واسط ورودی داده پذیرفته شود (به زیر بند ۷-۱۰ مراجعه شود).

۲. *واسط خروجی داده*. تمام داده‌ای (به جز داده وضعیت که از طریق واسط خروجی وضعیت و داده کنترل که از طریق واسط خروجی کنترل، خارج‌می‌شود) که خروجی از پودمان رمزنگاری است (از جمله داده متن‌ساده، داده متن رمز، و SSPها) [03.06] shall باید از طریق واسط «خروجی داده» خارج‌شود. در حین‌این‌که ورودی دستی، خودآزمایی‌های پیش‌عملیاتی، بارگیری نرم‌افزار/ ثابت‌افزار و صفرشدن را انجام‌می‌دهد و یا زمانی‌که پودمان رمزنگاری در یک وضعیت خطا می‌باشد، تمام خروجی داده از طریق واسط «خروجی داده» [03.07] shall باید جلوگیری‌شود.

1 - Hardware Module Interface
2 - Software or Firmware Module Interface
3 - Hybrid Software or Hybrid Firmware Module Interface

۳. *واسط ورودی کنترل*. تمام فرمان‌های ورودی، علائم (برای مثال، ورودی ساعت) و داده کنترل (شامل فراخوانی تابع و کنترل‌های دستی از قبیل سوئیچ‌ها، دکمه‌ها، صفحه کلیدها) که برای کنترل عملیات یک پودمان رمزنگاری استفاده‌می‌شوند [03.08] shall باید از طریق واسط «ورودی کنترل» وارد شوند.

۴. *واسط خروجی کنترل*. تمام فرمان‌های خروجی، علامت‌ها و داده‌های کنترل (برای مثال، فرمان‌های کنترل به پودمان دیگر) که برای کنترل یا نشان‌دادن وضعیت عملیات یک پودمان رمزنگاری استفاده‌می‌شوند [03.09] shall باید از طریق واسط «خروجی کنترل» خارج‌شوند. زمانی‌که پودمان رمزنگاری در یک وضعیت خطا است، تمام خروجی کنترل از طریق واسط «خروجی کنترل» [03.10] shall باید جلوگیری‌شود مگر این‌که استثناها در خط‌مشی امنیت تعیین‌شوند و با سند اثبات‌شوند.

۵. *واسط خروجی وضعیت*. تمام علائم خروجی، نشانه‌ها (برای مثال، علامت خطا) و داده وضعیت (از جمله کدهای برگشتی و نشانه‌های فیزیکی از قبیل بصری (صفحه نمایش، لامپ‌های علامت)، صوتی (زنگ‌اخبار[1]، صدای زنگ[2]، آهنگ[3]) و مکانیکی (ارتعاش)) که برای نشان دادن وضعیت یک پودمان رمزنگاری استفاده‌می‌شوند [03.11] shall باید از طریق واسط «خروجی وضعیت» خارج‌شوند. خروجی وضعیت ممکن است ضمنی یا صریح باشد.

به جز برای پودمان رمزنگاری نرم‌افزار، تمام پودمان‌ها [03.12] shall باید واسط زیر را داشته باشند:

- *واسط توان*. تمام توان الکتریکی خارجی که ورودی به پودمان رمزنگاری است [03.13] shall باید از طریق یک واسط توان واردشود. زمانی‌که تمام توان فراهم‌می‌شود یا در داخل حد و مرز رمزنگاری پودمان رمزنگاری حفاظت‌شود، واسط توان لازم نیست (مثال، یک باطری داخلی).

پودمان رمزنگاری [03.14] shall باید بین داده، اطلاعات کنترل و توان ورودی و داده، اطلاعات کنترل و وضعیت خروجی تمایز قائل شود.

ویژگی پودمان رمزنگاری [03.15] shall باید، قالب داده ورودی و اطلاعات کنترل را بدون ابهام، تعیین‌کند که شامل محدودیت‌های طول برای تمام ورودی‌های طول متغیر می‌باشد.

۷-۳-۴ کانال قابل‌اعتماد

کانال قابل‌اعتماد، پیوند برقرارشده بین پودمان رمزنگاری و یک فرستنده یا گیرنده برای ارتباط امن CSPهای متن‌ساده حفاظت‌نشده، مولفه‌های کلید و داده‌های اصالت‌سنجی می‌باشد.

یک کانال قابل‌اعتماد در مقابل استراق‌سمع و همچنین مداخله فیزیکی یا منطقی توسط عملگرها/هستارهای ناخواسته محافظت‌می‌کند. همچنین از فرآیندها یا افزاره های دیگر بین درگاه‌های ورودی یا خروجی تعریف‌شده پودمان و در پیوند رابطه با نقطه پایانی فرستنده یا گیرنده مورد انتظار محافظت‌می‌کند.

---

1 - Buzzer
2 - Tone
3 - Ring

سطوح امنیت ۱ و ۲

برای سطوح امنیت ۱ و ۲، هیچ الزاماتی برای کانال مورد اعتماد وجود ندارد.

سطح امنیتی ۳

برای سطح امنیتی ۳،

- برای انتقال CSPهای متن‌ساده حفاظت‌نشده، مولفه‌های کلید و داده اصالت‌سنجی بین پودمان رمزنگاری و نقطه پایانی فرستنده یا گیرنده‌ها، پودمان رمزنگاری shall [03.16] باید یک کانال قابل‌اعتماد را پیاده‌سازی کند.
- کانال قابل‌اعتماد shall [03.17] باید از اصلاح غیرمجاز، جانشینی و آشکارسازی در پیوند ارتباطی جلوگیری کند.
- درگاه‌های فیزیکی برای کانال قابل‌اعتماد shall [03.18] باید به‌طور فیزیکی از تمام درگاه‌های دیگر جداشود یا واسط‌های منطقی به‌کاربرده‌شده برای کانال قابل‌اعتماد shall [03.19] باید به‌طور منطقی از تمام واسط‌های دیگر جداشود.
- اصالت‌سنجی هستارمحور shall [03.20] باید برای تمام خدماتی به‌کاررود که از کانال قابل‌اعتماد استفاده‌می‌کنند و
- یک علامت وضعیت shall [03.21] باید هنگامی‌که کانال قابل‌اعتماد استفاده‌می‌شود، فراهم‌شود.

سطح امنیتی ۴

علاوه بر الزامات سطح امنیتی ۳، برای سطح امنیتی ۴، اصالت‌سنجی هستارمحور چندعاملی shall [03.22] باید برای تمام خدماتی که از کانال قابل‌اعتماد استفاده‌می‌کنند، به‌کاربرده شود.

۷-۴ نقش‌ها، خدمات و اصالت‌سنجی

۷-۴-۱ نقش‌ها، خدمات و الزامات کلی اصالت‌سنجی

یک پودمان رمزنگاری shall [04.01] باید از نقش‌های مجاز برای عملگرها و خدمات متناظر با هر نقش پشتیبانی‌کند. یک عملگر ممکن است چند نقش را برعهده‌بگیرد. اگر یک پودمان رمزنگاری از عملگرهای هم‌زمان پشتیبانی‌کند، پودمان shall [04.02] باید جداسازی نقش‌های برعهده‌گرفته توسط هر عملگر و خدمات متناظر را به‌صورت‌داخلی حفاظت‌کند. یک عملگر لازم نیست که یک نقش مجاز را برای انجام خدماتی برعهده‌گیرد که در آن CSPها و PSPها اصلاح، آشکار یا جایگزین‌نمی‌شوند (برای مثال، نمایش وضعیت‌ها، خودآزمایی‌ها یا خدمات دیگری که بر امنیت پودمان اثر نمی‌گذارند).

سازوکارهای اصالت‌سنجی ممکن است در یک پودمان رمزنگاری لازم باشد تا به یک عملگر اصالت‌دهد که به پودمان دسترسی‌دارد و بررسی‌کند که مجاز است نقش درخواستی را برعهده‌گیرد و خدمات را در آن نقش انجام‌دهد.

الزامات مستندسازی که در زیربند پیوست الف-۲-۴ تعیین‌شده‌اند shall [04.03] باید فراهم‌شوند.

۷-۴-۲ نقش‌ها

پودمان رمزنگاری shall [04.04] باید **حداقل**، از یک نقش Crypto officer پشتیبانی‌کند. نقش Crypto officer shall [04.05] باید عهده‌دار مقداردهی اولیه رمزنگاری یا توابع مدیریت و خدمات امنیت کلی باشد (برای مثال، مقداردهی اولیه پودمان، مدیریت CSPها، PSPها و توابع بازرسی).

یک پودمان رمزنگاری ممکن است از نقش User پشتیبانی نکند. اگر پودمان رمزنگاری از نقش User پشتیبانی‌کند، نقشUser، shall [04.06] باید عهده‌دار خدمات امنیت کلی از جمله عملیات رمزنگاری و سایر توابع امنیت تاییدشده باشد.

پودمان رمزنگاری ممکن است از یک نقش Maintenance پشتیبانی‌کند. نقش Maintenance نقشی است که در طی خدمات نگهداری فیزیکی و / یا منطقی عهده‌دار می‌شود (برای مثال، پوشش‌های خدمات باز، تشخیص عیب‌های خاص از قبیل خودآزمایی جاسازی‌شده (BIST)[1]). تمام SSPهای حفاظت‌نشده shall [04.07] باید هنگامی‌که به نقش Maintenance وارد یا خارج‌می‌شوند، صفرشوند. پودمان رمزنگاری ممکن است از نقش‌های دیگر علاوه بر نقش‌های تعیین‌شده بالا پشتیبانی‌کند.

۷-۴-۳ خدمات

۷-۴-۳-۱ الزامات کلی خدمات

خدمات shall [04.08] باید به تمام خدمات، عملیات‌ها یا توابعی اشاره‌کند که می‌توانند توسط یک پودمان انجام‌شوند. ورودی‌های خدمت shall [04.09] باید شامل تمام داده یا ورودی‌های کنترل در پودمانی باشند که مقداردهی اولیه می‌کنند و یا خدمات ویژه، عملیات یا توابعی را به‌دست‌می‌آورند. خروجی‌های خدمات shall [04.10] باید شامل تمام داده‌ها و وضعیت خروجی باشند که منتج از خدمات عملیات‌ها و یا توابعی هستند که مقداردهی اولیه شده‌اند و یا توسط ورودی‌های خدمت به‌دست‌آمده‌اند. هر ورودی خدمت shall [04.11] باید منتج به یک خروجی خدمت شود.

پودمان رمزنگاری shall [04.12] باید خدمات زیر را برای عملگرها فراهم‌کند:

۱. *نمایش اطلاعات نسخه‌بندی پودمان*. پودمان رمزنگاری shall [04.13] باید نام یا شناسه پودمان و اطلاعات نسخه‌بندی *که* می‌تواند به یک سابقه یا سابقه صحه‌گذاری مربوط‌شود، را خروجی‌کند. (برای مثال، اطلاعات نسخه‌بندی سخت‌افزار، نرم‌افزار و/ یا ثابت‌افزار).
۲. *نمایش وضعیت*. پودمان رمزنگاری shall [04.14] باید وضعیت فعلی را خروجی‌کند. این ممکن است شامل خروجی علامت‌های وضعیت در پاسخ به یک درخواست خدمت باشد.
۳. *انجام خودآزمایی‌ها*. پودمان رمزنگاری shall [04.15] باید راه‌اندازی‌شود و خودآزمایی‌های پیش‌عملیاتی که در زیربند ۷-۱۰-۲ تعیین‌شده‌اند، را اجراکند.
۴. *انجام توابع امنیت تاییدشده*. پودمان رمزنگاری shall [04.16] باید حداقل یک تابع امنیتی تاییدشده را اجراکند که در یک حالت تاییدشده عملیات استفاده‌می‌شود همان‌طور که در زیربند ۷-۲ تعیین‌شده‌است.

1 - Buit In Self-Test

۵. *انجام صفرشدن.* پودمان رمزنگاری shall [04.17] باید صفرشدن پارامترها را مطابق با زیربند ۷-۹-۷ انجام‌دهد.

یک پودمان رمزنگاری ممکن است خدمات دیگر، عملیات‌ها و توابع تاییدشده و تاییدنشده را علاوه بر خدمات تعیین‌شده بالا انجام‌دهد. خدمات ویژه ممکن است در بیش از یک نقش ارائه‌شوند (برای مثال، خدمات ورودی کلید که ممکن است در نقش کاربر و نقش مسوول رمز تهیه‌شوند).

۷-۴-۳-۲ توانایی کنارگذار

توانایی کنارگذار توانایی یک خدمت است که به‌طور جزئی یا کلی یک تابع یا فرآیند رمزنگاری را دور می‌زند. اگر پودمان بتواند یک داده ویژه یا وضعیت خاصی از عنصر را به شکل حفاظت‌شده رمزنگاری خارج‌کند یا (در نتیجه پیکربندی پودمان یا دخالت عملگر) بتواند عنصری را به شکل حفاظت‌نشده خارج‌کند، توانایی کنارگذار shall [04.18] باید تعریف‌شود.

اگر یک پودمان رمزنگاری توانایی کنارگذار را پیاده‌سازی‌کند، سپس:

- عملگر shall [04.19] باید یک نقش مجاز را قبل از پیکربندی توانایی کنارگذار برعهده‌گیرد.
- دو عمل داخلی مستقل shall [04.20] باید لازم باشد تا توانایی جلوگیری کنارگذار غیرعمدی داده متن‌ساده به دلیل یک خطای ساده را فعال‌کند. دو عمل داخلی مستقل shall [04.21] باید وضعیت نرم‌افزار و / یا سخت‌افزار را اصلاح‌کنند که برای میانجی‌گری توانایی کنارگذار اختصاص‌داده‌می‌شود (برای مثال، دو پرچم نرم‌افزار یا سخت‌افزار مختلف تنظیم‌می‌شوند، یکی از آنها ممکن است کاربر-راه‌انداز باشد) و
- پودمان shall [04.22] باید وضعیتی را نشان‌دهد که معلوم‌می‌کند که آیا توانایی کنارگذار:

۱. فعال‌نمی‌شود و پودمان به‌طور انحصاری خدمات را با پردازش رمزنگاری تهیه‌می‌کند (برای مثال، داده متن‌ساده رمز می‌شود) یا
۲. فعال‌می‌شود و پودمان به‌طور انحصاری خدماتی را بدون پردازش رمزنگاری تهیه‌می‌کند (برای مثال، داده متن‌ساده رمزدار نمی‌شود) یا
۳. به‌طور متناوب فعال و غیرفعال‌می‌شود و پودمان چندین خدمت را با پردازش رمزنگاری و چندین خدمت را بدون پردازش رمزنگاری فراهم‌می‌کند (برای مثال، برای پودمان‌هایی با کانال‌های ارتباطی چندگانه، داده متن‌ساده رمزدار می‌شود یا رمزدار نمی‌شود و این به پیکربندی هر کانال بستگی‌دارد).

۷-۴-۳-۳ توانایی خروجی رمزنگاری خود- راه‌اندازی‌شده

توانایی خروجی رمزنگاری خود- راه‌اندازی‌شده، توانایی پودمان در انجام عملیات‌های رمزنگاری و سایر توابع امنیت تاییدشده یا روش‌های مدیریت SSP بدون درخواست عملگر خارجی می‌باشد. توانایی خروجی رمزنگاری خود- راه‌اندازی‌شده shall [04.23] باید توسط Crypto officer پیکربندی‌شود و این پیکربندی ممکن است بر روی تنظیم مجدد، راه‌اندازی مجدد یا چرخه توان پودمان حفاظت‌شود.

اگر یک پودمان رمزنگاری توانایی خروجی رمزنگاری خود- راه‌اندازی‌شده را پیاده‌سازی‌کند، سپس:

- دو عمل داخلی مستقل shall [04.24] باید لازم باشد تا توانایی جلوگیری از خروجی غیرعمدی به دلیل یک خطای ساده را فعال‌کند. دو عمل داخلی مستقل shall [04.25] باید وضعیت نرم‌افزار و / یا سخت‌افزار را اصلاح‌کنند که برای میانجی‌گری توانایی اختصاص‌داده‌می‌شود (برای مثال، دو پرچم نرم‌افزار یا سخت‌افزار مختلف تنظیم‌می‌شوند، یکی از آنها ممکن است کاربر- راه‌انداز باشد) و
- پودمان shall [04.26] باید وضعیتی را نشان‌دهد تا تعیین‌کند آیا توانایی خروجی رمزنگاری راه‌اندازی‌شده، کاربر- راه‌انداز است.

۷-۴-۳-۴ بارگذاری نرم‌افزار/ ثابت‌افزار

اگر یک پودمان رمزنگاری توانایی بارگذاری نرم‌افزار یا ثابت‌افزار را از یک منبع خارجی داشته‌باشد، الزامات زیر shall [04.27] باید به‌کاربرده‌شوند:

- نرم‌افزار یا ثابت‌افزار بارگذاری‌شده shall [04.28] باید توسط یک مقام ذیصلاح قبل از بارگذاری صحه‌گذاری شود تا صحه‌گذاری را حفظ‌کند.
- تمام خروجی داده از طریق واسط خروجی داده shall [04.29] باید جلوگیری‌شود تا این‌که بارگذاری نرم‌افزار/ ثابت‌افزار و آزمون بار با موفقیت کامل‌شود.
- آزمون بارگذاری نرم‌افزار/ ثابت‌افزار تعیین‌شده در زیربند ۷-۱۰-۳-۴ shall [04.30] باید قبل از اجرای کد بارگذاری‌شده، انجام‌شود.
- پودمان رمزنگاری shall [04.31] باید مانع اجرای همه توابع امنیت تاییدشده بارگذاری‌شده یا اصلاح شده، شود تا این‌که پس از خودآزمون‌های پیش‌عملیاتی تعیین‌شده در زیربند۷-۱۰-۲ با موفقیت اجراشود و
- اطلاعات نسخه‌ای پودمان shall [04.32] باید اصلاح‌شود تا افزودن و / یا به‌روزرسانی نرم‌افزار یا ثابت‌افزار جدید بارگذاری‌شده را نشان‌دهند (زیربند ۷-۴-۳).

اگر بارگذاری نرم‌افزار یا ثابت‌افزار جدید، جایگزینی تصویر کامل باشد، باید shall [04.33] یک پودمان کاملا جدید را تشکیل‌دهد که توسط مرجع صحه‌گذاری برای نگهداری صحه‌گذاری، نیاز به صحه‌گذاری دارد. تصویر نرم‌افزار یا ثابت‌افزار جدید shall [04.34] باید فقط بعد از انتقال پودمان از طریق روشن‌کردن با راه‌اندای مجدد[1]، اجراشود. همه SSPها shall [04.35] باید قبل از اجرای تصویر جدید، صفرشوند.

۷-۴-۴ اصالت‌سنجی

سازوکارهای اصالت‌سنجی ممکن است در یک پودمان رمزنگاری لازم باشد تا به یک عملگر اصالت بدهد که به پودمان دسترسی داشته‌باشد و بررسی‌کند که این عملگر مجاز است که نقش درخواستی را برعهده‌گیرد و خدمات آن نقش را انجام‌دهد. انواع سازوکارهای زیر استفاده‌می‌شوند تا دسترسی به پودمان رمزنگاری را کنترل‌کنند:

اصالت‌سنجی نقش‌محور: اگر سازوکارهای اصالت‌سنجی نقش‌محور توسط پودمان رمزنگاری پشتیبانی شوند، پودمان shall [04.36] باید نیازداشته‌باشد که یک یا چند نقش به‌طور ضمنی یا

1 - Power-on Reset

صریح توسط عملگر انتخاب‌شود و [04.37] shall باید برعهده‌گیری نقش (یا مجموعه نقش‌های) انتخابی را اصالت‌سنجی کند. پودمان رمزنگاری برای اصالت‌سنجی هستار فردی عملگر لازم نمی‌باشد. انتخاب نقش‌ها و اصالت‌سنجی برعهده‌گیری نقش‌های انتخابی ممکن است ترکیب‌شوند. اگر پودمان رمزنگاری به یک عملگر اجازه‌دهد تا نقش‌ها را تغییردهد، پودمان [04.38] shall باید برعهده‌گیری هر نقشی را که از قبل برای آن عملگر اصالت‌سنجی نشده بود، اصالت‌سنجی کند.

اصالت‌سنجی هستارمحور: اگر سازوکارهای اصالت‌سنجی هستارمحور توسط پودمان رمزنگاری برعهده‌گرفته‌شود، پودمان [04.39] shall باید نیازداشته‌باشد که عملگری به‌طور فردی یا انحصاری شناسایی‌شود، [04.40] shall باید نیازداشته‌باشد که یک یا چند نقش به‌طور ضمنی یا صریح توسط عملگر انتخاب‌شود و [04.41] shall باید هستار عملگر و اصالت‌سنجی عملگر را برای برعهده‌گیری نقش انتخابی یا مجموعه نقش‌ها، اصالت‌سنجی کند. اصالت‌سنجی هستار عملگر، انتخاب نقش‌ها و اصالت‌سنجی برعهده‌گیری نقش‌های انتخابی ممکن است ترکیب‌شوند. اگر پودمان رمزنگاری به یک عملگر اجازه‌دهد تا نقش‌ها را تغییردهد، پودمان [04.42] shall باید اصالت‌سنجی عملگر شناسایی‌شده را برای برعهده‌گیری هر نقشی که قبلاً اصالت‌سنجی نشده‌بود، بررسی کند.

پودمان رمزنگاری ممکن است به یک عملگر اصالت‌سنجی‌شده اجازه‌دهد تا تمام خدمات مجاز را در یک نقش مجاز انجام‌دهد و یا ممکن است برای هر خدمت یا برای مجموعه‌های مختلف خدمات، به اصالت‌سنجی جدا نیازداشته‌باشد. هنگامی‌که یک پودمان رمزنگاری تنظیم مجدد ، راه‌اندازی مجدد ، خاموش و سپس روشن می‌شود، پودمان [04.43] shall باید به عملگر نیاز داشته‌باشد تا اصالت‌سنجی شود.

انواع مختلف داده اصالت‌سنجی ممکن است توسط یک پودمان رمزنگاری لازم باشد تا سازوکارهای اصالت‌سنجی حفاظت‌شده را پیاده‌سازی کند، که شامل (اما نه محدود) دانش یا مالکیت یک اسم رمز، PIN، کلید رمزنگاری یا معادل؛ مالکیت یک کلید فیزیکی، نشانه یا معادل؛ یا تطبیق مشخصات فردی (برای مثال، زیست‌سنجشی‌ها) می‌باشد. داده‌های اصالت‌سنجی در پودمان رمزنگاری [04.44] shall باید در مقابل کاربرد، آشکارسازی، اصلاح و جایگزینی غیرمجاز، حفاظت‌شوند. توابع امنیت تاییدشده ممکن است به‌عنوان بخشی از سازوکار اصالت‌سنجی استفاده‌شوند.

مقداردهی اولیه سازوکارهای اصالت‌سنجی ممکن است عملیات ویژه را تضمین‌کند. اگر پودمان رمزنگاری شامل داده اصالت‌سنجی لازم برای اصالت‌سنجی عملگر نباشد، پودمان برای اولین بار در دسترس می‌باشد، سپس روش‌های مجاز دیگر (برای مثال، کنترل‌های رویه‌ای یا استفاده از داده کارخانه-تنظیم‌شده یا داده اصالت‌سنجی پیش‌فرض) [04.45] shall باید استفاده‌شود تا دسترسی به پودمان را کنترل‌کند و به سازوکارهای اصالت‌سنجی مقدار اولیه دهد. اگر داده اصالت‌سنجی پیش‌فرض برای کنترل دسترسی به پودمان استفاده‌شود، داده اصالت‌سنجی پیش‌فرض [04.46] shall باید جایگزین اولین اصالت‌سنجی شود. این داده اصالت‌سنجی پیش‌فرض نیازی به تطبیق‌دادن الزامات صفرشدن ندارد (به زیربند ۷-۹-۷ مراجعه شود).

سازوکار اصالت‌سنجی ممکن است گروهی از سازوکارهای خصوصیت‌های اصالت‌سنجی مختلف باشد که به‌طور مشترک مطابق با الزامات این بند هستند. اگر پودمان رمزنگاری از توابع امنیت استفاده‌کند تا عملگر را اصالت‌سنجی کند، توابع امنیت [04.47] shall باید توابع امنیت تاییدشده باشند.

- پودمان [04.48] shall باید سازوکار اصالت‌سنجی تاییدشده را پیاده‌سازی‌کند که در پیوست «ث» تعیین‌شده‌است.
- توانایی سازوکار اصالت‌سنجی تاییدشده [04.49] shall باید در خط‌مشی امنیت تعیین‌شود (به پیوست «ب» مراجعه شود).
- برای هر سوءقصد در استفاده از سازوکار اصالت‌سنجی تاییدشده، پودمان [04.50] shall باید مطابق با توانایی هدف اصالت‌سنجی باشد. برای سوءقصدهای چندگانه در استفاده از سازوکار اصالت‌سنجی تاییدشده در طی یک دوره یک دقیقه‌ای، پودمان [04.51] shall باید مطابق با توانایی هدف اصالت‌سنجی باشد.
- سازوکار اصالت‌سنجی تاییدشده [04.52] shall باید مطابق با پیاده‌سازی پودمان باشد و به کنترل‌های رویه‌ای یا قواعد امنیت مستند، وابسته نباشد.
- برای پودمان رمزنگاری نرم‌افزاری در سطح امنیتی ۲، سامانه عامل ممکن است سازوکار اصالت‌سنجی را پیاده‌سازی‌کند. اگر سامانه عامل سازوکار اصالت‌سنجی را پیاده‌سازی‌کند، سازوکار اصالت‌سنجی [04.53] shall باید مطابق با الزامات این بند باشد.
- بازخورد داده‌های اصالت‌سنجی به یک عملگر [04.54] shall باید در طی فرآیند اصالت‌سنجی محوشود (برای مثال، هنگام ورود اسم رمز، نویسه‌ها قابل‌دیدن نیست). نویسه‌های غیرمهم ممکن است در محل داده اصالت‌سنجی واقعی نمایش‌داده‌شوند.
- بازخورد تهیه‌شده برای عملگر در طی یک اصالت‌سنجی ناتمام [04.55] shall باید از ضعیف‌شدن توانایی سازوکار اصالت‌سنجی، بیشتر از توانایی اصالت‌سنجی موردنیاز، جلوگیری‌کند.

سطح امنیتی ۱

برای سطح امنیتی ۱، نیازی نیست تا پودمان رمزنگاری برای دسترسی کنترل پودمان، سازوکارهای اصالت‌سنجی به‌کاربرد. اگر پودمان، سازوکارهای اصالت‌سنجی را پشتیبانی‌نکند پودمان [04.56] shall باید نیازداشته‌باشد به عملگری که به‌طور صریح یا ضمنی، یک یا چند نقش را انتخاب‌کند.

سطح امنیتی ۲

برای سطح امنیتی ۲، پودمان رمزنگاری [04.57] shall باید حداقل، اصالت‌سنجی نقش‌محور را برای کنترل دسترسی به پودمان به‌کاربرد.

سطح امنیتی ۳

برای سطح امنیتی ۳، پودمان رمزنگاری [04.58] shall باید از سازوکارهای اصالت‌سنجی هسترامحور استفاده‌کند تا دسترسی به پودمان را کنترل‌نماید.

سطح امنیتی ۴

برای سطح امنیتی ۴، پودمان رمزنگاری [04.59] shall باید از سازوکارهای اصالت‌سنجی هسترامحور چندعاملی، استفاده‌کند تا دسترسی به پودمان را کنترل‌کند.

۷-۵ امنیت نرم‌افزار/ثابت‌افزار

یک پودمان رمزنگاری به‌عنوان یک پودمان سخت‌افزار، ثابت‌افزار یا ترکیبی تعریف می‌شود (به زیربند ۷-۲-۲ مراجعه شود). الزامات این بند [05.01] shall باید در مولفه‌های نرم‌افزار و ثابت‌افزار پودمان رمزنگاری استفاده‌شوند.

پودمان رمزنگاری که به‌طور کامل در سخت‌افزار پیاده‌سازی‌می‌شود هدف الزامات امنیتی نرم‌افزار/ ثابت‌افزار این استاندارد نمی‌باشد.

کلید بررسی عمومی یا کلید اصالت‌سنجی پیام کلیدی ممکن است در کد پودمان قرار گیرد و یک SSP درنظرگرفته نمی‌شود.

الزامات مستندسازی تعیین‌شده در زیربند پیوست الف-۲-۵ [05.02] shall باید تهیه‌شوند.

سطح امنیتی ۱

الزامات زیر [05.03] shall باید در مولفه‌های نرم‌افزار و ثابت‌افزار یک پودمان رمزنگاری برای سطح امنیتی ۱ استفاده‌شوند:

- همه نرم‌افزار و ثابت‌افزار [05.04] shall باید در یک شکلی باشند که مطابق با الزامات این استاندارد بدون اصلاح قبل از نصب باشند (به زیربند ۷-۱۱-۷ مراجعه شود).
- یک سازوکار رمزنگاری با استفاده از یک روش یکپارچگی تاییدشده [05.05] shall باید در تمام مولفه‌های نرم‌افزاری و ثابت‌افزار در حد و مرز رمزنگاری تعریف‌شده پودمان، در یکی از روش‌های زیر به‌کار برده شود:
  - توسط خود پودمان رمزنگاری، یا
  - توسط دیگر پودمان رمزنگاری معتبر که در یک حالت تاییدشده عملیات عمل‌می‌کند.
- اگر آزمون یکپارچگی ناموفق باشد، پودمان [05.06] shall باید وارد وضعیت خطا شود. روش یکپارچگی تاییدشده ممکن است شامل یک کد یا امضای اصالت‌سنجی پیام احاطه‌شده یا چند کد یا امضای اصالت‌سنجی جدا باشد که از آن خرابی هر کد یا امضا اصالت‌سنجی جدا [05.07] shall باید سبب ورود به وضعیت خطای پودمان شود. خروجی ارجاع‌شده مورد انتظار از سازوکار روش یکپارچگی ممکن است داده در نظرگرفته‌شود و خودش هدف روش یکپارچگی نباشد. مقدار (مقادیر) موقتی که در طی آزمون یکپارچگی نرم‌افزار یا سخت‌افزار پودمان، تولیدشده‌است [05.08] shall باید از پودمان به‌محض تکمیل آزمون یکپارچگی، صفرشود.
- یک عملگر [05.09] shall باید بتواند روش یکپارچگی تاییدشده را بر روی تقاضا از طریق خدمت HMI، SFMI، HSMI، یا HFMI انجام‌دهد (به زیربند ۷-۳-۲ مراجعه شود).
- تمام ورودی‌های داده و کنترل و خروجی‌های داده، کنترل و وضعیت (به زیربند ۷-۳-۳ مراجعه شود) از پودمان رمزنگاری و خدمات (به زیربند ۷-۴-۳ مراجعه شود) [05.10] shall باید در جهت HMI، SFMI، HFMI یا HSMI تعریف‌شده باشند.

- برای یک پودمان نرم‌افزار یا ثابت‌افزار، اگر تصویر نرم‌افزار یا ثابت‌افزار بارگذاری‌شده، یک جایگزین کامل یا جایگذاشت تصویر پودمان صحه‌گذاری‌شده باشد، آزمون بار نرم‌افزار/ ثابت‌افزار، کاربردی نمی‌باشد (NA)[1] هنگامی‌که جایگزینی یا جایگذاشت، یک پودمان جدیدی را تشکیل می‌دهد.
اگر نرم‌افزار یا ثابت‌افزاری که بارگذاری می‌شود وابسته یا محدود باشد، اصلاح‌کند یا یک لازمه قابل‌اجرای پودمان صحه‌گذاری‌شده باشد اما یک جایگزین کامل یا جایگذاشت پودمان صحه‌گذاری‌شده نباشد، آزمون بار نرم‌افزار/ ثابت‌افزار، کاربردی است و [05.11] shall باید توسط پودمان صحه‌گذاری‌شده انجام‌شود.

سطح امنیتی ۲

علاوه بر الزامات سطح امنیتی ۱، الزامات زیر [05.12] shall باید در مولفه‌های نرم‌افزار و ثابت‌افراز یک پودمان رمزنگاری برای سطح امنیتی ۲ به‌کاربرده شوند:

- مولفه‌های نرم‌افزار و ثابت‌افزار یک پودمان رمزنگاری [05.13] shall باید تنها شامل کدی باشد که به شکل قابل‌اجرا است (برای مثال، نه کد منبع، کد شی یا کد کامپایل‌شده به‌موقع).
- [05.14] shall باید هیچ خدماتی یا تنظیمات کنترل از طریق واسط HMI، SFMI، HFMI یا HSMI وجودنداشته‌باشد تا عملگر بتواند شروع به‌کارکند و یا روش‌های اشکال‌زدایی را انجام‌دهد.
- امضا دیجیتال تاییدشده یا کد اصالت‌سنجی پیام کلیدی [05.15] shall باید در تمام نرم‌افزار و ثابت‌افزار درون حد و مرز رمزنگاری تعریف‌شده پودمان، به‌کاربرده‌شود. اگر نتیجه محاسبه‌شده، معادل نتیجه تولیدشده قبلی نباشد، این آزمون ناموفق است و پودمان [05.16] shall باید وارد وضعیت خطا شود.

سطح امنیتی ۳ و ۴

علاوه بر الزامات سطوح امنیت ۱ و ۲، الزامات زیر [05.17] shall باید در مولفه‌های نرم‌افزار و ثابت‌افزار یک پودمان رمزنگاری برای سطوح امنیت ۳ و ۴ به‌کاربرده‌شوند. یک سازوکار رمزنگاری با استفاده از یک امضا دیجیتال تاییدشده [05.18] shall باید در تمام مولفه‌های نرم‌افزار و ثابت‌افزار در حد و مرز رمزنگاری تعریف‌شده پودمان، به‌کاربرده‌شود.

اگر نتیجه محاسبه‌شده، معادل نتیجه تولیدشده قبلی نباشد این آزمون ناموفق است و پودمان [05.19] shall باید وارد وضعیت خطا شود.

روش امضا دیجیتال ممکن است شامل فقط یک امضا احاطه‌شده یا چند امضا جدا باشد که خرابی هر امضا جدا [05.20] shall باید باعث شود تا پودمان وارد وضعیت خطا شود. کلید امضا خصوصی [05.21] shall باید خارج از پودمان قرار گیرد.

1 - Not Applicable

۷-۶ محیط عملیاتی

۷-۶-۱ الزامات کلی محیط عملیاتی

محیط عملیاتی یک پودمان رمزنگاری به مدیریت نرم‌افزار، ثابت‌افزار و / یا سخت‌افزار موردنیاز برای عمل‌کردن پودمان اشاره‌می‌کند. محیط عملیاتی یک نرم‌افزار، ثابت‌افزار یا پودمان ترکیبی، حداقل شامل مولفه‌های پودمان، بستر محاسبه و سامانه عامل می‌باشد که کنترل می‌کند و یا اجازه اجرای نرم‌افزار یا ثابت‌افزار را در بستر محاسبه می‌دهد. یک پودمان سخت‌افزار ممکن است یک محیط عملیاتی در پودمان داشته‌باشد که شامل یک سامانه عامل است که اجازه اجرای نرم‌افزار یا ثابت‌افزار درونی را می‌دهد. سامانه عامل هنگامی‌که کاربردپذیراست، شامل ماشین (های) مجازی (سامانه و / یا فرآیند) و محیط زمان‌اجرا (برای مثال، محیط زمان‌اجرای جاوا(JRE)[1]) می‌باشد.

یک *محیط عملیاتی همه‌منظوره* به کاربرد سامانه عامل همه‌منظوره دسترس‌پذیر تجاری اشاره‌می‌کند(برای مثال، مدیر منبع) که مولفه‌های نرم‌افزار و ثابت‌افزار را مدیریت‌می‌کند و همچنین فرآیندها / ریسمان(های) سامانه و عملگر(ها) را مدیریت‌می‌کند که شامل نرم‌افزار کاربردی همه‌منظوره از قبیل پردازنده‌های کلمه می‌باشد.

محیط عملیاتی می‌تواند تغییرناپذیر، *محدود* یا *تغییرپذیر* باشد.

بند زیر سه محیط عملیاتی ویژه را تعیین‌می‌کند.

۱. ***محیط عملیاتی تغییرناپذیر*** به روشی طراحی یا پیکربندی‌می‌شود که از تغییر یا اصلاح توسط یک عملگر یا فرآیند در مولفه‌های پودمان، بستر محاسبه یا سامانه عامل جلوگیری‌کند. این محیط ممکن است شامل یک پودمان ثابت‌افزار باشد که در یک بستر محاسبه غیرقابل برنامه‌نویسی یا پودمان سخت‌افزاری کارمی‌کند که از بارگذاری هر نرم‌افزار یا ثابت‌افزار اضافی جلوگیری‌می‌کند.

۲. ***محیط عملیاتی محدود*** به روشی طراحی یا پیکربندی‌می‌شود که اجازه تغییر و اصلاح کنترل‌شده را توسط یک عملگر یا فرآیند در مولفه‌های پودمان، بستر محاسبه یا سامانه عامل می‌دهد. این محیط ممکن است عملیات ثابت‌افزار در یک پودمان سخت‌افزار قابل‌برنامه‌نویسی باشد که بارگذاری ثابت‌افزار اضافی مطابق با الزامات بارگذاری ثابت‌افزار می‌باشد که در زیربند ۷-۴-۳-۴ تعیین‌شده‌است.

۳. ***محیط عملیاتی تغییرپذیر*** به یک محیط عملیاتی اشاره‌می‌کند که ممکن است پیکربندی مجدد شود تا کارکرد را اضافه / حذف / اصلاح کند و / یا ممکن است شامل امکانات سامانه عامل همه‌منظوره باشد (برای مثال، استفاده از یک سامانه عامل رایانه، سامانه عامل کارت هوشمند قابل‌پیکربندی، یا نرم‌افزار قابل‌برنامه‌نویسی). سامانه‌های عامل محیط‌های عملیاتی تغییرپذیر هستند اگر مولفه‌های نرم‌افزاری بتواند توسط یک عملگر یا فرآیند اصلاح‌شود و / یا یک عملگر یا فرآیند بتواند نرم‌افزار را بارگذاری و اجرا کند (برای مثال، یک پردازنده کلمه) که این نرم‌افزار بخشی از نرم‌افزار، ثابت‌افزار یا پودمان ترکیبی تعریف‌شده نمی‌باشد.

---

1 - Java Runtime Environment

یک محیط عملیاتی تغییرپذیر مشخصات زیر را دارد:
توابع ممکن است در محیط عملیاتی اضافه یا اصلاح شوند. آن توابع به‌طورلزوم قابل‌اعتماد نیستند تا با عملیات پودمان رمزنگاری تداخل کنند مگر این‌که این تداخل‌ها یا محیط عملیاتی ممنوع شود.
در چنین محیطی لازم است که هیچ تابعی در محیط عملیاتی عمل نکند. این محیط عملیاتی، به بخش قابل‌اعتماد محیط عملیاتی که به SSPها دسترسی دارد تعلق ندارد مگر این‌که از طریق واسط‌های تعریف‌شده پودمان رمزنگاری باشد.
بنابراین لازم است که محیط عملیاتی توانایی را فراهم‌کند تا پودمان رمزنگاری را در طی عملیات از توابع دیگر در محیط عملیاتی جدا کنند به‌طوری‌که آن توابع نمی‌توانند اطلاعاتی را از پودمان رمزنگاری مربوط به CSPها به دست آورند و نمی‌توانند CSPها، PSPها یا گردش اجرای پودمان رمزنگاری را اصلاح‌کنند که بیشتر از طریق واسط‌هایی است که با خود پودمان رمزنگاری تهیه‌شده‌است.
یک پیکربندی خاص محیط عملیاتی ممکن است لازم باشد تا حفاظت کافی پودمان رمزنگاری با کد و داده آن به‌دست‌آورد (برای مثال، ممنوع‌کردن نوع خاصی از ارتباط درون‌فرآیندی برای پودمان رمزنگاری، تعیین حقوق دسترسی محدودکننده در پرونده‌هایی که SSPها یا کد پودمان رمزنگاری دارند).

چند مثال از محیط‌های عملیاتی در جدول زیر فراهم‌شده‌است.

جدول ۲- مثال‌هایی از محیط‌های عملیاتی

محیط عملیاتی	مثال‌های پیکربندی
غیرقابل‌اصلاح	یک بستر محاسبه که اجازه بارگیری کد را نمی‌دهد و به عملگر اجازه اصلاح پیکربندی بستر محاسبه، سامانه عملیاتی یا پودمان رمزنگاری را نمی‌دهد.
محدود	یک بستر محاسبه شامل سامانه عملیاتی است که اجازه بارگیری کد اضافی را می‌دهد که اصالت‌سنجی‌می‌شود و مطابق با تمام الزامات کاربردی این استاندارد می‌باشد.
قابل‌اصلاح	یک بستر محاسبه که اجازه بارگیری کد را می‌دهد بدون این‌که مطابق با الزامات بارگیری نرم‌افزار یا ثابت‌افزار این استاندارد باشد.
قابل‌اصلاح	یک بستر عملیاتی شامل کدی است که سامانه عملیاتی آن توسط عملگر قابل‌پیکربندی است و اجازه رفع حفاظت‌های امنیت را می‌دهد.

برای یک محیط *تغییرناپذیر* یا محدود، مولفه‌های کنترل که شامل محیط تغییرناپذیر یا محدود می‌باشد ممکن است شامل خصیصه‌هایی از بسترمحاسبه، سامانه عامل یا حدود پودمان رمزنگاری یا تمام موارد بالا باشد.

کدی که در محیط تغییرناپذیر یا محدود اجرامی‌شود، در این استاندارد به‌عنوان ثابت‌افزار اشاره می‌شود.

کدی که در یک محیط تغییرپذیر اجرامی‌شود، در این استاندارد به‌عنوان نرم‌افزار اشاره می‌شود.

اگر محیط عملیاتی تغییرناپذیر باشد یا محیط عملیاتی محدود باشد، تنها الزامات سامانه عامل در زیربند ۷-۶-۲ shall [06.01] باید به‌کاربرده‌شود.

اگر محیط عملیاتی، یک محیط عملیاتی تغییرپذیر باشد، الزامات سامانه عامل در زیربند ۷-۶-۳ shall [06.02] باید به‌کاربرده‌شود.

الزامات مستندسازی تعیین‌شده در زیربندالف-۲-۶ shall [06.03] باید فراهم‌شود.

۷-۶-۲ الزامات سامانه عامل برای محیط‌های عملیاتی محدود یا تغییرناپذیر

سطح امنیتی ۱

اگر پودمان، سطح امنیتی ۱ در زیربند ۷-۷ باشد، الزامات سطح امنیتی ۱ در زیربند ۷-۶-۳ shall [06.04] باید کاربردپذیر باشد.

سطوح امنیت ۲، ۳ و ۴

الزامات اضافی وجود ندارد.

۷-۶-۳ الزامات سامانه عامل برای محیط‌های عملیاتی تغییرپذیر

سطح امنیتی ۱

الزامات زیر در سامانه‌های عامل برای سطح امنیتی ۱ به‌کاربرده‌می‌شود.

- هر نمونه از پودمان رمزنگاری shall [06.05] باید بر روی SSPهای خودش کنترل داشته‌باشد.
- محیط عملیاتی shall [06.06] باید امکان جداسازی فرآیندهای کاربرد فردی را از یکدیگر با جلوگیری از دسترسی کنترل‌نشده به CSPها و اصلاحات کنترل‌نشده SSPها فراهم‌کند صرف‌نظر از این‌که آیا این داده در حافظه فرآیند است و یا بر روی حافظه ذخیره دائمی در محیط عملیاتی ذخیره‌شده‌است. این اطمینان می‌دهد که دسترسی مستقیم به CSPها و SSPها در پودمان رمزنگاری و بخش‌های قابل‌اعتماد محیط عملیاتی محدود است. محدودیت‌ها در پیکربندی محیط‌های عملیاتی shall [06.07] باید در خط‌مشی امنیت پودمان رمزنگاری مستندسازی شوند.
- فرآیندهایی که توسط پودمان رمزنگاری ایجاد می‌شوند shall [06.08] باید توسط پودمان تصاحب شوند و توسط فرآیندها / عملگرهای خارجی تصاحب‌نشوند.

یادآوری- این الزامات را نمی‌توان با مستندات مدیریتی و روش‌های مدیریتی اجراکرد اما باید توسط خود پودمان رمزنگاری اجراشوند.

سطح امنیتی ۲

علاوه بر الزامات سطح امنیتی ۱، برای سطح امنیتی ۲، یک محیط عملیاتی shall [06.09] باید مطابق با الزامات زیر باشد و یا توسط مقام ذیصلاح صحه‌گذاری تاییدشود.

- همه نرم‌افزار رمزنگاری، SSPها و اطلاعات کنترل و وضعیت shall [06.10] باید تحت کنترل یک سامانه عامل باشند که کنترل‌های دسترسی نقش‌محور را پیاده‌سازی‌می‌کند و یا حداقل یک کنترل دسترسی اختیاری را با سازوکار قوی برای تعریف گروه‌های جدید و تخصیص مجوزهای محدودکننده اجرامی‌کند؛ برای مثال از طریق فهرست‌های کنترل دسترسی (ACLها)[1] و با امکان یا توانایی تخصیص هر کاربر در بیش از یک گروه. سامانه عامل shall [06.11] باید پیکربندی‌شود تا در مقابل‌اجرا، اصلاح و تغییر، و خواندن غیرمجاز SSPها، داده کنترل و وضعیت، حفاظت‌کند.
- برای حفظ داده متن‌ساده، نرم‌افزار رمزنگاری، SSPها و داده اصالت‌سنجی، سازوکارهای کنترل دسترسی سامانه عامل:
  - shall [06.12] باید پیکربندی شوند تا مجموعه نقش‌ها یا گروه‌ها و مجوزهای محدودکننده مرتبط را تعریف و اعمال‌کنند که این مجوزها حقوق انحصاری برای اجرای نرم‌افزار رمزنگاری ذخیره‌شده را دارند.
  - shall [06.13] باید پیکربندی‌شود تا مجموعه نقش‌ها یا گروه‌ها و مجوزهای محدودکننده مرتبط با آن‌ها را تعریف و اعمال‌کنند که این مجوزها حقوق انحصاری برای *اصلاح* (برای مثال، نوشتن، جایگزینی و حذف) نرم‌افزار پودمان رمزنگاری مقابل می‌باشد که درحد و مرز رمزنگاری ذخیره‌شده است: برنامه‌های رمزنگاری، داده رمزنگاری (برای مثال، داده بازرسی رمزنگاری)، SSPها و داده متن‌ساده را دارا می‌باشند.
  - shall [06.14] باید پیکربندی‌شود تا مجموعه نقش‌ها یا گروه‌ها و مجوزهای محدود کننده مرتبط با آن‌ها را تعریف و اعمال‌کنند که این مجوزها حقوق انحصاری برای خواندن داده‌ها رمزنگاری (برای مثال، داده بازرسی رمزنگاری)، CSPها و داده متن‌ساده دارند.
  - shall [06.15] باید پیکربندی‌شود تا مجموعه نقش‌ها یا گروه‌ها و مجوزهای محدودکننده مرتبط را تعریف و اعمال کنند که این مجوزها حقوق انحصاری برای *واردکردن* SSPها دارند.

و

- مشخصه‌های زیر shall [06.16] باید مطابق با نقش‌ها یا حقوق گروه‌های اختصاص‌یافته و خدماتی باشند که در خط‌مشی امنیت تعریف‌شده‌اند:
  - هنگامی‌که نقش Maintenance را پشتیبانی نمی‌کنند، سامانه عامل shall [06.17] باید از تمام عملگرها و فرآیندهای اجرایی برای *اصلاح* فرآیندهای رمزنگاری اجرایی (برای مثال، تصاویر برنامه رمزنگاری بارگذاری‌شده و درحال‌اجرا) جلوگیری‌کند. در این حالت،

1 - Access Control List

فرآیندهای درحال‌اجرا به تمام فرآیندها، رمزنگاری‌شده یا رمزنگاری‌نشده اشاره‌می‌کند که توسط سامانه عامل تصاحب‌نشده و یا راه‌اندازی‌نشده است (یعنی عملگر- راه‌اندازی‌شده).

- سامانه عامل [06.18] shall باید فرآیندهای کاربر را از دستیابی خواندن یا نوشتن به SSPهای تصاحب‌شده توسط سایر فرآیندها و SSPهای سامانه جلوگیری‌کند.
- پیکربندی سامانه عامل که مطابق با الزامات بالا می‌باشد [06.19] shall باید در راهنمای مدیر تعیین‌شود. راهنمای مدیر [06.20] shall باید بیان‌کند که سامانه عامل باید پیکربندی‌شود همان‌طور که برای محتوای پودمان مشخص‌شده که باید حفاظت‌شود.

سازوکار شناسایی و اصالت‌سنجی در سامانه عامل [06.21] shall باید مطابق با الزامات زیربند ۷-۴-۳ باشد و باید در خط‌مشی امنیت پودمان تعیین‌شود:

همه نرم‌افزار رمزنگاری، SSPها، اطلاعات کنترل و وضعیت [06.22] shall باید تحت کنترل:

- یک سامانه عامل باشند که [06.23] shall باید حداقل خصیصه‌های زیر را داشته باشند:

- سامانه عامل [06.24] shall باید یک سازوکار بازرسی را با تاریخ و زمان هر رویداد بازرسی‌شده فراهم‌کند. پودمان رمزنگاری [06.25] shall نباید شامل SSPها به‌عنوان بخشی از هر سابقه بازرسی باشد.
- پودمان رمزنگاری [06.26] shall باید رخدادهای زیر را فراهم‌کند که با سازوکار بازرسی سامانه عامل ثبت‌می‌شود:
  - اصلاحات، دسترسی‌ها، حذف‌ها و افزایش داده‌های رمزنگاری و SSPها.
  - سوءقصدها در تهیه ورودی نامعتبر برای کارکردهای Crypto Officer.
  - افزایش یا حذف یک عملگر به و از یک نقش Crypto Officer (اگرآن نقش‌ها توسط پودمان رمزنگاری مدیریت‌شوند).
  - استفاده از یک کارکرد Crypto Officer مربوط به امنیت.
  - تقاضاها برای دسترسی به داده‌های اصالت‌سنجی مربوط به پودمان رمزنگاری.
  - استفاده از یک سازوکار اصالت‌سنجی (برای مثال، login) مربوط به پودمان رمزنگاری و
  - تقاضاهای صریح برای برعهده‌گیری یک نقش Crypto Officer.
- سازوکار بازرسی سامانه عامل [06.27] shall باید توانایی بازرسی رخدادهای مربوط به سامانه عامل زیر را داشته‌باشد:
  - دسترسی خواندن یا نوشتن تمام عملگرها به داده‌های بازرسی ذخیره‌شده در مسیر بازرسی.
  - دسترسی به پرونده‌های استفاده‌شده توسط پودمان رمزنگاری برای ذخیره‌کردن داده‌های رمزنگاری یا SSPها.
  - افزایش یا حذف یک عملگر به و از یک نقش Crypto Officer (اگر آن نقش‌ها توسط محیط عملیاتی مدیریت‌شوند).

- تقاضاها برای استفاده از سازوکارهای مدیریت داده اصالت‌سنجی.
- سوءقصدها برای استفاده از کارکرد کانال قابل‌اعتماد و این‌که آیا این تقاضا هنگامی‌که کانال قابل‌اعتماد در این سطح امنیتی پشتیبانی می‌شود واگذارشده‌است و
- شناسایی آغازگر و هدف یک کانال قابل‌اعتماد، هنگامی‌که کانال قابل‌اعتماد در این سطح امنیتی پشتیبانی می‌شود.

- سامانه عامل [06.28] shall باید پیکربندی‌شود تا از عملگرها (غیر از عملگرهایی با امتیازات شناسایی‌شده در خط‌مشی امنیت) در برابر اصلاح نرم‌افزار پودمان رمزنگاری و داده‌های بازرسی ذخیره‌شده در محیط عملیاتی پودمان رمزنگاری جلوگیری‌کند.

فقط سامانه‌های عامل که پیکربندی می‌شوند تا مطابق با الزامات امنیتی بالا باشند [06.29] shall باید در این سطح امنیتی مجاز باشند، آیا پودمان رمزنگاری در یک حالت تاییدشده عملیات عمل‌می‌کند یا نه. توصیه می‌شود سابقه بازرسی در مقابل اصلاح غیرمجاز از طریق استفاده از یک تابع امنیتی تاییدشده محافظت‌شود.

۷-۷ امنیت فیزیکی

۷-۷-۱ نمایش تضمین‌های امنیت فیزیکی

یک پودمان رمزنگاری [07.01] shall باید از سازوکارهای امنیت فیزیکی استفاده‌کند تا هنگامی‌که نصب‌می‌شود، دسترسی فیزیکی غیرمجاز به محتوای پودمان را محدودکند و مانع استفاده یا اصلاح غیرمجاز پودمان شود (از جمله جایگزینی کل پودمان). تمام مولفه‌های داده سخت‌افزار، نرم‌افزار و ثابت‌افزار و SSPها در حد و مرز رمزنگاری [07.02] shall باید حفاظت‌شوند.

یک پودمان رمزنگاری که کاملاً در نرم‌افزار پیاده‌سازی‌می‌شود به‌طوری‌که امنیت فیزیکی تنها توسط بستر محاسبه فراهم‌می‌شود، در الزامات امنیتی فیزیکی این استاندارد قرارنمی‌گیرد.

الزامات این بند [07.03] shall باید در پودمان‌های سخت‌افزار و ثابت‌افزار و در مولفه‌های سخت‌افزار و ثابت‌افزار پودمان‌های ترکیبی کاربردپذیر باشند.

الزامات این بند [07.04] shall باید در حد و مرز فیزیکی تعریف‌شده پودمان کاربردپذیر باشند. الزامات امنیتی فیزیکی برای سه نمایش کیفیت فیزیکی تعریف‌شده از یک پودمان رمزنگاری تعیین می‌شوند.

۱. **پودمان‌های رمزنگاری تک تراشه‌ای** نمایش کیفیت‌های فیزیکی هستند که در آن یک تراشه IC تک به‌عنوان یک افزاره مستقل استفاده‌می‌شود و یا ممکن است در یک محفظه یا محصول جاسازی‌شود که ممکن است به‌طور فیزیکی حفاظت‌نشود. مثال‌های پودمان‌های رمزنگاری تک تراشه‌ای شامل تراشه‌های IC تک یا کارت‌های هوشمند با یک تراشه IC تک می‌باشد.
۲. **پودمان‌های رمزنگاری تعبیه‌شده چند تراشه‌ای** نمایش کیفیت‌های فیزیکی هستند که در آن دو یا چند تراشه IC به‌هم متصل هستند و در یک محفظه یا محصول جاسازی می‌شوند که ممکن است به‌طور فیزیکی محافظت‌نشوند. مثال‌های پودمان‌های رمزنگاری جاسازی‌شده چند تراشه‌ای شامل تطبیق‌دهنده‌ها و بردهای توسعه می‌باشند.

۳. **پودمان‌های رمزنگاری مستقل چند تراشه‌ای** نمایش کیفیت‌های فیزیکی هستند که در آن دو یا چند تراشه IC به‌هم متصل هستند و کل محفظه به‌طور فیزیکی محافظت‌شده‌است. مثال‌های پودمان‌های چند تراشه‌های، پودمان‌های رمزنگاری مستقل شامل مسیریاب‌های رمزنگاری، رادیوهای امن یا نشانه‌های[1] USB می‌باشند.

با توجه به سازوکارهای امنیت فیزیکی یک پودمان رمزنگاری، سوءقصدهای غیرمجاز در دسترسی فیزیکی، استفاده یا اصلاح shall [07.05] باید احتمال زیاد کشف‌شدن را داشته باشند:

- پس از یک سوءقصد با گذاشتن علائم قابل‌دیدن(یعنی شواهد مداخله).

و / یا

- در طی یک سوءقصد دسترسی.

و عمل‌های فوری و مناسب shall [07.06] باید توسط پودمان رمزنگاری در نظرگرفته‌شوند تا از SSPها حفاظت‌کنند.

جدول ۳ الزامات امنیتی فیزیکی را در نمایش کیفیت‌های کلی و سه نمایش کیفیت خاص برای هر چهار سطح امنیتی خلاصه می‌کند. الزامات امنیتی فیزیکی خاص- نمایش کیفیت در هر سطح امنیتی، الزامات کلی را در همان سطح افزایش می‌دهد و الزامات خاص- نمایش کیفیت سطح قبلی را نیز افزایش‌می‌دهد.

1 - Tokens

جدول ۳- خلاصه الزامات امنیتی فیزیکی برای پودمان‌های رمزنگاری

	الزامات کلی برای تمام نمایش کیفیت‌ها	تک تراشه‌ای	چندتراشه‌ای جاسازی‌شده	چندتراشه‌ای مستقل
سطح امنیتی ۱	مولفه‌های رتبه تولید. کم‌اثرسازی‌کردن استاندارد. صفرکردن به‌صورت رویه یا خودکار، هنگام دسترسی به واسط دسترسی نگهداری	بدون الزامات اضافی	محفظه رتبه تولید یا پوشش جدایی‌پذیر	محفظه رتبه تولید یا پوشش جدایی‌پذیر
سطح امنیتی ۲	شواهد مداخله ، ابهام یا نیم‌شفافی در طیف مرئی. جلوگیری از مشاهده مستقیم درون حفره‌ها یا شکاف‌ها	پوشش شواهد مداخله بر روی تراشه یا محفظه	مواد در محفظه‌قرارداده‌شده شواهد مداخله - یا محصورشده با مهرو موم‌های شواهد مداخله یا قفل‌های مقاوم برای برداشتن درها یا پوشش‌های جداشدنی	مواد در محفظه‌قرارداده‌شده شواهد مداخله - یا محصورشده با مهرو موم‌های شواهد مداخله یا قفل‌های مقاوم برای برداشتن درها یا پوشش‌های جداشدنی
سطح امنیتی ۳	مدار پاسخ مداخله و صفرکردن. صفرکردن خودکار هنگام دسترسی به واسط دسترسی نگهداری. جلوگیری از کاوش در حفره‌ها و شکاف‌ها. EFP یا EFT برای دما و ولتاژ	پوشش شواهد مداخله سخت بر روی تراشه یا محفظه بسیار مقاوم برای نفوذ و حذف	محفظه‌قرارداده‌شده شواهد مداخله سخت یا محفظه قوی	محفظه‌قرارداده‌شده شواهد مداخله سخت یا محفظه قوی
سطح امنیتی ۴	کشف مداخله و پوشش پاسخ. EFP برای دما و ولتاژ. حفاظت از القا اشتباه	پوشش بسیار مقاوم در برابر حذف بر روی تراشه	کشف مداخله و پوشش پاسخ با امکان صفرکردن	کشف مداخله و پوشش پاسخ با امکان صفرکردن

به‌طور کلی، سطح امنیتی ۱ یک مجموعه اصلی الزامات را فراهم‌می‌کند. سطح امنیتی ۲ به افزایش سازوکارهای شواهد مداخله و ناتوانی در جمع‌آوری اطلاعات در مورد عملیات‌های داخلی از نواحی بحرانی پودمان (ناشفافی) نیاز دارد. سطح امنیتی ۳ برای استفاده محفظه‌های تطبیقی و غیرتطبیقی قوی یا سخت با کشف مداخله و سازوکارهای پاسخ برای پوشش‌ها و درهای جداشدنی و مقاومت در کاوش‌های مستقیم از طریق نقاط باز یا ورودی، الزاماتی را می‌افزاید. EFP یا EFT در سطح امنیتی ۳ لازم است. سطح امنیتی ۴ برای استفاده محفظه‌های تطبیقی و غیر تطبیقی قوی یا سخت با کشف مداخله و سازوکارهای پاسخ برای

کل محفظه یا آسیب زیاد، الزاماتی را می‌افزاید. حفاظت از خرابی محیطی و حفاظت از حملات القاشده اشتباه، در سطح امنیتی ۴ لازم هستند.
هنگامی‌که یک پودمان رمزنگاری طراحی‌می‌شود تا اجازه دسترسی فیزیکی را بدهد، الزامات امنیتی برای یک واسط دسترسی نگهداری تعیین‌می‌شود. (برای مثال، توسط ارائه‌دهنده پودمان یا افراد مجاز دیگر).
الزامات مستندسازی تعیین‌شده در پیوست الف-۲-۷ shall [07.07] باید فراهم‌شوند.

۷-۷-۲ الزامات کلی امنیت فیزیکی

الزامات زیر shall [07.08] باید در تمام نمایش کیفیت‌های فیزیکی به‌کاربرده شوند.

- مستندسازی shall [07.09] باید نمایش کیفیت فیزیکی و سطح امنیتی را تعیین‌کند که برای آن، سازوکارهای امنیت فیزیکی یک پودمان رمزنگاری پیاده‌سازی‌می‌شود.
- هنگامی‌که صفرشدن برای اهداف امنیت فیزیکی انجام‌می‌شود، صفرشدن shall [07.10] باید در یک مدت زمان با اندازه کافی کوچک رخ‌دهد تا از بازیافت داده‌های حساس بین زمان کشف و صفرشدن واقعی جلوگیری‌شود.
- اگر پودمان شامل نقش Maintenance باشد که به دسترسی به محتوای پودمان نیاز دارد یا اگر پودمان طراحی‌می‌شود تا به دسترسی فیزیکی اجازه‌دهد (برای مثال، توسط ارائه‌دهنده پودمان یا افراد مجاز دیگر):
  - یک واسط دسترسی نگهداری shall [07.11] باید تعریف‌شود.
  - یک واسط دسترسی نگهداری shall [07.12] باید شامل تمام مسیرهای دسترسی فیزیکی در مرکز پودمان رمزنگاری باشد که شامل همه پوشش‌ها یا درهای جداشدنی باشد.
  - همه پوشش‌ها یا درهای جداشدنی در این واسط دسترسی نگهداری shall [07.13] باید با استفاده از سازوکارهای امنیت فیزیکی مناسب، حفاظت‌شود.

سطح امنیتی ۱

الزامات زیر shall [07.14] باید در تمام پودمان رمزنگاری برای سطح امنیتی ۱ به‌کاربرده شوند:

- پودمان رمزنگاری shall [07.15] باید شامل مولفه‌های رتبه تولید باشد که شامل روش‌های غیرفعال‌سازی استاندارد می‌باشد (برای مثال، پوشش تطبیقی یا یک پوشش محکم بر روی مدارهای پودمان به‌کاربرده شود تا در مقابل آسیب محیطی یا فیزیکی دیگر محافظت‌کند).
- هنگامی‌که نگهداری فیزیکی انجام‌می‌شود، صفرشدن shall [07.16] باید طبق رویه‌ای توسط عملگر یا به‌طور خودکار توسط پودمان رمزنگاری انجام‌گیرد.

سطح امنیتی ۲

علاوه بر الزامات کلی برای سطح امنیتی ۱، الزامات زیر shall [07.17] باید در تمام پودمان‌های رمزنگاری برای سطح امنیتی ۲ به‌کاربرده شوند:

- پودمان رمزنگاری shall [07.18] باید هنگامی‌که سوءقصد برای دسترسی فیزیکی به پودمان می‌شود، شواهد مداخله را فراهم‌کند (برای مثال، روی پوشش، محفظه و مهر).

- مواد ، پوشش یا محفظه شواهد مداخله [07.19] shall باید شفاف یا نیم‌شفاف در طیف مرئی باشد (یعنی نور با طول موج با دامنه ۴۰۰nm تا ۷۵۰nm) تا از جمع‌شدن اطلاعات در مورد عملیات‌های داخلی از نواحی بحرانی پودمان جلوگیری‌کند.
- اگر پودمان رمزنگاری شامل حفره‌ها یا شکاف‌هایی باشد، پودمان [07.20] shall باید طوری ساخته‌شود که از جمع‌شدن اطلاعات ساختار داخلی پودمان یا مولفه‌ها توسط مشاهده بصری مستقیم با استفاده از منابع نور مصنوعی در طیف بصری ساختار داخلی یا مولفه‌های پودمان جلوگیری‌کند.

سطح امنیتی ۳

علاوه بر الزامات کلی برای سطح امنیتی ۱ و ۲، الزامات زیر [07.21] shall باید در تمام پودمان‌های رمزنگاری برای سطح امنیتی ۳ به‌کاربرده شوند:

- اگر پودمان رمزنگاری شامل همه درها یا پوشش‌های جداشدنی باشد یا اگر یک واسط دسترسی نگهداری تعریف‌شود، پودمان [07.22] shall باید شامل پاسخ مداخله و امکان صفرشدن باشد. پاسخ مداخله و توانایی صفرشدن [07.23] shall باید هنگامی‌که در باز می‌شود یا یک پوشش خارج می‌شود یا واسط دسترسی نگهداری مورد دسترسی قرارمی‌گیرد، بلافاصله تمام SSPهای حفاظت‌نشده را صفرکند. پاسخ مداخله و توانایی صفرشدن [07.24] shall باید هنگامی‌که SSPهای حفاظت‌نشده در پودمان رمزنگاری قرار می‌گیرند، به‌صورت عملیاتی باقی‌بماند.
- اگر پودمان رمزنگاری شامل حفره‌ها یا شکاف‌های تهویه باشد، پودمان [07.25] shall باید طوری ساخته‌شود که از کاوش فیزیکی کشف‌نشده داخل محفظه جلوگیری‌کند (برای مثال، جلوگیری از افشا توسط یک افشاکننده چندقسمتی منفرد تک).
- پوشش‌ها، محفظه‌ها یا ظرف‌های مواد تطبیقی یا غیرتطبیقی قوی و سخت [07.26] shall باید مشخصات مقاومت و سختی را بر روی محدوده دمای مورد انتظار پودمان‌ها از عملیات، ذخیره‌سازی و توزیع حفظ‌کند.
- اگر مهرهای شواهد مداخله به‌کاربرده شوند، آنها [07.27] shall باید به‌طور انحصاری شمارش‌شوند و یا جداگانه قابل‌شناسایی باشند (برای مثال، نوار شاهد به‌طورانحصاری شمارش‌شده یا مهرهای تصویر لیزری قابل‌شناسایی).
- پودمان [07.28] shall باید شامل ویژگی‌های EFP یا تحت EFT باشد.

سطح امنیتی ۴

علاوه بر الزامات کلی برای سطوح امنیت ۱، ۲ و ۳، الزامات زیر [07.29] shall باید در تمام پودمان‌های رمزنگاری برای سطح امنیتی ۴ به‌کاربرده شوند:

- پودمان رمزنگاری [07.30] shall باید توسط یک پوشش جداشدنی‌مقاوم نیم‌شفاف سخت یا توسط یک پوشش کشف مداخله با توانایی پاسخ مداخله و صفرشدن، حفاظت‌شود.
- پودمان [07.31] shall باید شامل ویژگی‌های EFP باشد.

- پودمان رمزنگاری shall [07.32] باید حفاظت از القا اشتباه را فراهم‌کند. روش‌های کاهش القا اشتباه و اندازه‌های کاهش به‌کاربرده‌شده shall [07.33] باید طبق پیوست «ب» مستندسازی شود.

۷-۷-۳ الزامات امنیتی فیزیکی برای هر نمایش کیفیت امنیت فیزیکی

۷-۷-۳-۱ پودمان‌های رمزنگاری تک تراشه‌ای

علاوه بر الزامات امنیتی فیزیکی کلی مشخص‌شده در زیربند ۷-۷-۲، الزامات زیر در پودمان‌های رمزنگاری تک تراشه‌ای مشخص‌شده‌اند.

سطح امنیتی ۱

هیچ الزامات اضافی از سطح امنیتی ۱ برای پودمان‌های رمزنگاری تک تراشه‌ای وجود ندارد.

سطح امنیتی ۲

علاوه بر الزامات برای سطح امنیتی ۱، الزامات زیر shall [07.34] باید در پودمان‌های رمزنگاری تک تراشه‌ای برای سطح امنیتی ۲ استفاده‌شوند:

- پودمان رمزنگاری shall [07.35] باید با یک پوشش شواهد مداخله پوشانده‌شود (برای مثال، ماده کم‌اثرسازی شواهد مداخله یا مواد شواهد مداخله که کم‌اثرسازی را پوشش‌می‌دهد) یا در یک محفظه شواهد مداخله قرارگیرد تا مانع مشاهده مستقیم، کاوش یا دستکاری پودمان شود و شاهد سوءقصدها را فراهم‌کند تا با آن مداخله کند یا پودمان را حذف‌کند.

سطح امنیتی ۳

علاوه بر الزامات برای سطوح امنیت ۱ و ۲، الزامات زیر shall [07.36] باید در پودمان‌های رمزنگاری تک تراشه‌ای برای سطح امنیتی ۳ به‌کاربرده شوند.

- پودمان shall [07.37] باید با یک پوشش شواهد مداخله کدر سخت پوشانده شود (برای مثال، یک اندود پلاستیکی[1] کدر سخت که بی‌اثرسازی را پوشش‌می‌دهد).

یا

- محفظه shall [07.38] باید طوری پیاده‌سازی شود که سوءقصدها در حذف یا نفوذ محفظه shall [07.39] باید احتمال زیاد علت آسیب‌رسانی جدی در پودمان رمزنگاری داشته باشند (یعنی پودمان کار نمی‌کند).

سطح امنیتی ۴

علاوه بر الزامات برای سطوح امنیت ۱، ۲ و ۳، الزامات زیر shall [07.40] باید در پودمان‌های رمزنگاری تک تراشه‌ای برای سطح امنیتی ۴ استفاده‌شوند:

- پودمان رمزنگاری shall [07.41] باید با یک پوشش جداشدنی- مقاوم، کدر و سخت با مشخصات چسبندگی و سختی پوشانده‌شود به‌طوری‌که تلاش برای جداکردن پوشش یا کاوش از پودمان، احتمال زیاد منتج به آسیب جدی در پودمان دارد (یعنی پودمان عمل نمی‌کند).

1 - Epoxy

- پوشش جداشدنی- مقاوم [07.42] shall باید مشخصات قدرت تحلیل‌بردنی را داشته‌باشد به‌طوری‌که انحلال پوشش، احتمال زیاد انحلال یا آسیب جدی پودمان را دارد (یعنی پودمان عمل نمی‌کند).

۷-۷-۳-۲ پودمان‌های رمزنگاری جاسازی‌شده چند تراشه‌ای

علاوه بر الزامات امنیتی کلی تعیین‌شده در زیربند ۷-۷-۲، الزامات زیر مخصوص پودمان‌های رمزنگاری جاسازی‌شده چند تراشه‌ای هستند.

سطح امنیتی ۱

اگر پودمان رمزنگاری در یک محفظه یا پوشش جداشدنی باشد، یک محفظه رتبه تولید یا پوشش جداشدنی [07.43] shall باید استفاده‌شود.

سطح امنیتی ۲

علاوه بر الزامات برای سطح امنیتی ۱، الزامات زیر [07.44] shall باید در پودمان‌های رمزنگاری جاسازی‌شده چند تراشه‌ای برای سطح امنیتی ۲ به‌کاربرده شوند:

- مولفه‌های پودمان [07.45] shall باید با یک پوشش شواهد مداخله یا مواد ظرفی (برای مثال، پوشش‌های ضدخش یا نشت‌رنگ) پوشانده شوند تا مانع مشاهده مستقیم شوند و شاهد سوءقصدها را پیدا کنند که با مولفه‌های پودمان مداخله یا جدا می‌شوند.

یا

- پودمان [07.46] shall باید کاملاً در یک فلز یا محفظه رتبه تولید پلاستیک سخت قرار گیرد که ممکن است شامل درها یا پوشش‌های جداشدنی باشد.

و

- محفظه شامل همه درها یا پوشش‌های جداشدنی باشد، سپس هریک از درها یا پوشش‌ها [07.47] shall باید با قفل‌های مکانیکی برداشتن- مقاوم قفل شود که از کلیدهای فیزیکی یا منطقی استفاده‌می‌کند یا [07.48] shall باید با مهرهای شواهد مداخله حفاظت‌شود (برای مثال، نوار شاهد یا مهرهای تصویر لیزری).

سطح امنیتی ۳

علاوه الزامات برای سطوح امنیت ۱ و ۲، الزامات زیر [07.49] shall باید در پودمان‌های رمزنگاری جاسازی‌شده چند تراشه‌ای برای سطح امنیتی ۳ به‌کاربرده شوند.

- نمایش کیفیت چند تراشه‌ای مدارات در پودمان رمزنگاری [07.50] shall باید با یک پوشش سخت یا ماده ظرفی پوشانده شود (برای مثال، یک ماده اندود پلاستیکی سخت).

یا

- پودمان [07.51] shall باید در داخل یک محفظه قوی قرار گیرد.

به‌طوری‌که سوءقصدها در حذف یا نفوذ محفظه، یک احتمال زیاد علت آسیب جدی به پودمان را دارند (یعنی پودمان عمل نمی‌کند).

سطح امنیتی ۴

علاوه بر الزامات برای سطوح امنیت ۱، ۲ و ۳ الزامات زیر [07.52] shall باید در پودمان‌های رمزنگاری جاسازی‌شده چند تراشه‌ای برای سطح امنیتی ۴ به‌کاربرده شوند:

- مولفه‌های پودمان [07.53] shall باید در یک محفظه تطبیقی یا غیرتطبیقی قوی یا سخت باشد.
- محفظه [07.54] shall باید توسط یک پوشش کشف مداخله پوشانده‌شود (برای مثال، یک مدار چاپی مایلار[1] انعطاف‌پذیر با یک الگوی هندسی مارپیچی رسانا یا یک بسته سیم‌پیچ با یک مدار شکننده و انعطاف‌ناپذیر یا یک محفظه قوی) که [07.55] shall باید مداخله را با وسایلی چون برش‌کاری، مته، فرزکاری، تیزکنی، سوزاندن، ذوب یا حل‌کردن مواد ظرف یا محفظه، در یک حدی که برای دسترسی SSPها کافی است، پیداکنند.
- پودمان [07.56] shall باید شامل مدارات پاسخ مداخله و صفرکردن باشد که [07.57] shall باید به‌طور پیوسته پوشش کشف مداخله را نظارت کند و با کشف مداخله، [07.58] shall باید بی‌معطلی تمام SSPهای حفاظت‌نشده را صفر کند. هنگامی‌که SSPهای حفاظت‌نشده در پودمان رمزنگاری قرار می‌گیرند، مدارات پاسخ مداخله [07.59] shall باید عملیاتی بمانند.

۷-۷-۳-۳ پودمان‌های رمزنگاری مستقل چند تراشه‌ای

علاوه بر الزامات امنیتی کلی تعیین‌شده در زیربند ۷-۷-۲، الزامات زیر مخصوص پودمان‌های رمزنگاری مستقل چند تراشه‌ای هستند.

سطح امنیتی ۱

پودمان رمزنگاری [07.60] shall باید به‌طور کامل در یک محفظه رتبه تولید پلاستیکی سخت یا فلزی قرار گیرد که ممکن است شامل درها یا پوشش‌های جداشدنی باشد.

سطح امنیتی ۲

علاوه بر الزامات برای سطح امنیتی ۱، الزامات زیر [07.61] shall باید در پودمان‌های رمزنگاری مستقل چند تراشه‌ای برای سطح امنیتی ۲ به‌کاربرده شوند.

- اگر محفظه پودمان رمزنگاری شامل هر یک از درها یا پوشش‌های جداشدنی باشد، سپس درها یا پوشش‌ها [07.62] shall باید با قفل‌های مکانیکی برداشتن- مقاوم قفل‌شوند که از کلیدهای منطقی یا فیزیکی استفاده‌می‌کند یا [07.63] shall باید با مهرهای شواهد مداخله حفاظت‌شوند (مثال نوار شاهد یا مهرهای تصویر لیزری).

سطح امنیتی ۳

علاوه بر الزامات برای سطوح امنیت ۱ و ۲، الزامات زیر [07.64] shall باید در پودمان‌های رمزنگاری مستقل چند تراشه‌ای برای سطح امنیتی ۳ به‌کاربرده شوند:

- پودمان [07.65] shall باید در یک محفظه قوی قرارگیرد به‌طوری‌که سوءقصدها در خروج یا نفوذ محفظه، یک احتمال زیاد علت آسیب جدی را در پودمان دارند (یعنی پودمان عمل نمی‌کند).

1 - Mylar

سطح امنیتی ۴

علاوه بر ملزومات برای سطوح امنیت ۱، ۲ و ۳، ملزومات زیر [07.66] shall باید در پودمان‌های رمزنگاری مستقل چند تراشه‌ای برای سطح امنیتی ۴ استفاده‌شوند:

- محفظه پودمان رمزنگاری [07.67] shall باید شامل یک پوشش کشف مداخله باشد که از سازوکارهای کشف مداخله استفاده‌می‌کند از قبیل سوئیچ‌های پوشش (برای مثال، سوئیچ‌های میکرو، سوئیچ‌های اثر هال مغناطیسی[1]، محرک‌های مغناطیسی دائمی و غیره)، آشکارسازهای حرکت (مثال فراصوت، مادون قرمز یا ریزموج) یا سازوکارهای کشف مداخله همان‌طور که در سطح امنیتی ۴ در زیربند ۷-۷-۳-۲ شرح داده شده‌است. سازوکارهای کشف مداخله [07.68] shall باید به حملات پاسخ دهند از قبیل برش‌کاری، مته، فرزکاری، تراشیدن، سوزاندن، ذوب یا انحلال در یک حدی که برای دسترسی SSPها کافی است.
- پودمان رمزنگاری [07.69] shall باید شامل پاسخ مداخله و توانایی صفرکردن باشد که [07.70] shall باید به‌طور پیوسته پوشش کشف مداخله را نظارت‌کند و کشف مداخله، [07.71] shall باید بی‌معطلی تمام SSPهای حفاظت‌نشده را صفرکند. هنگامی‌که SSPها در پودمان رمزنگاری قرارمی‌گیرند پاسخ مداخله و توانایی صفرکردن [07.72] shall باید به‌طور عملیاتی حفظ‌شود.

۷-۷-۴ حفاظت / آزمون خرابی محیطی

۷-۷-۴-۱ الزامات کلی حفاظت / آزمون خرابی محیطی

افزاره‌های الکتریکی و مدارها طراحی‌می‌شوند تا در گستره خاصی از شرایط محیطی عمل‌کنند. گردش‌های عمدی یا تصادفی خارج از گستره‌های عملیاتی عادی ولتاژ و دما می‌توانند باعث عملیات نامنظم یا خرابی افزاره‌های الکتریکی یا مدار حرکت شوند که می‌توانند امنیت پودمان رمزنگاری را به‌خطراندازند. اطمینان قابل‌قبول که امنیت یک پودمان رمزنگاری نمی‌تواند با شرایط محیطی حدی به‌خطربیافتد می‌تواند با داشتن پودمانی فراهم‌شود که از ویژگی‌های EFP استفاده‌می‌کنند و یا تحت EFT قرار می‌دهند.

برای سطوح امنیت ۱ و ۲، پودمان لازم نیست از ویژگی‌های EFP استفاده کند یا تحت EFT قرار گیرد. در سطح امنیتی ۳، پودمان [07.73] shall باید از ویژگی‌های EFP استفاده کند یا تحت EFT قرار گیرد. در سطح امنیتی ۴، پودمان [07.74] shall باید از ویژگی‌های EFP استفاده کند.

۷-۷-۴-۲ ویژگی‌های حفاظت خرابی محیطی

ویژگی‌های حفاظت خرابی محیطی (EFP) [07.75] shall باید از پودمان رمزنگاری در مقابل شرایط محیطی غیرعادی حفاظت‌کند (تصادفی یا تحمیل‌شده) هنگامی‌که خارج از گستره عملیاتی عادی پودمان است که می‌تواند امنیت پودمان را به‌خطر اندازد.

هنگامی‌که دمای عملیاتی و ولتاژ خارج از گستره‌های عملیاتی عادی تعیین‌شده هستند، پودمان رمزنگاری [07.76] shall باید نظارت‌کند و به‌درستی پاسخ‌دهد.

---

1 - Magnetic Hall Effect

اگر دما یا ولتاژ بیرون از گستره عملیاتی عادی پودمان رمزنگاری بیافتد، توانایی حفاظت shall [07.77] باید:

- پودمان را خاموش‌کند تا از عملیات بیشتر جلوگیری‌کند.

یا

- بی‌معطلی تمام SSPهای حفاظت‌نشده را صفرکند.

۷-۷-۴-۳ رویه‌های آزمون خرابی محیطی

آزمون خرابی محیطی (EFT) shall [07.78] باید شامل ترکیب تجزیه‌وتحلیل، شبیه‌سازی و آزمون پودمان رمزنگاری باشد تا اطمینان قابل‌قبول را فراهم‌کند که شرایط محیطی (تصادفی یا تحمیل‌شده) هنگامی‌که خارج از محدوده‌های عملیاتی عادی پودمان برای دما و ولتاژ است، امنیت پودمان را به‌خطر نمی‌اندازند.

EFT shall [07.79] باید اثبات‌کند که اگر دمای عملیاتی یا ولتاژ خارج از محدوده عملیاتی عادی پودمان منتج‌به خرابی‌شود، shall [07.80] باید امنیت پودمان رمزنگاری هیچ‌گاه به‌خطر نیافتد.

محدوده دمایی که آزموده‌می‌شود shall [07.81] باید از دمایی در داخل محدوده دمای عملیاتی عادی تا پایین‌ترین دما (یعنی سردترین) باشد که یا (۱) پودمان را خاموش‌می‌کند تا از عملیات بیشتر جلوگیری‌کند یا (۲) بی‌معطلی تمام SSPهای حفاظت‌نشده را صفرمی‌کند و از دمایی در محدوده دمای عملیاتی عادی تا بالاترین (یعنی گرم‌ترین) دما باشد که (۱) خاموش‌می‌کند یا وارد وضعیت خطا می‌شود یا (۲) SSPهای حفاظت‌نشده را صفرمی‌کند. گستره دمایی که آزمون‌می‌شود shall [07.82] باید از ۱۰۰°C- تا ۲۰۰°C+ (۱۵۰°F- تا ۴۰۰°F+) باشد؛ بنابراین این آزمون shall [07.83] باید متوقف‌شود به محض این‌که (۱) پودمان خاموش‌می‌شود تا از عملیات بیشتری جلوگیری‌کند، (۲) تمام SSPهای حفاظت‌نشده بی‌معطلی صفرمی‌شوند یا (۳) پودمان وارد یک وضعیت خرابی می‌شود. دما shall [07.84] باید نه فقط در حد و مرز فیزیکی پودمان، بلکه در داخل مولفه‌های حساس و افزاره‌های بحرانی هم نظارت شود.

محدوده ولتاژ آزمون‌شده shall [07.85] باید به‌تدریج از ولتاژی در محدوده ولتاژ عملیات عادی تا یک ولتاژ پایین‌تر کم‌شود که یا (۱) پودمان را خاموش‌می‌کند تا از عملیات بیشتری جلوگیری‌کند یا (۲) بی‌معطلی تمام SSPهای حفاظت‌نشده را صفرمی‌کند و shall [07.86] باید به‌تدریج از یک ولتاژ در داخل محدوده ولتاژ عملیاتی عادی تا یک ولتاژ بالاتر افزایش‌یابد که یا (۱) پودمان را خاموش‌می‌کند تا از عملیات بیشتری جلوگیری‌کند یا (۲) بی‌معطلی تمام SSPهای حفاظت‌نشده را صفرمی‌کند.

۸-۷ امنیت غیرتهاجمی

حملات غیرتهاجمی تلاش‌می‌کند تا پودمان رمزنگاری را با دستیابی به دانش CSPهای پودمان بدون این‌که پودمان را تغییر فیزیکی دهد یا موردتجاوز قراردهد، به‌خطر اندازد. پودمان‌ها ممکن است روش‌های مختلفی را پیاده‌سازی‌کنند تا از شدت این نوع حملات بکاهند. اندازه‌های آزمون برای کاهش حملات غیرتهاجمی برای هر یک از توابع امنیت مرتبط آدرس‌دهی‌شده با این استاندارد، در پیوست «ج» اشاره‌می‌شوند.

این زیربند کاربردپذیر نمی‌باشد اگر پودمان رمزنگاری، روش‌های کاهش حمله غیرتهاجمی را پیاده‌سازی‌نکند تا SSPهای حفاظت‌نشده پودمان را از حملات غیرتهاجمی حفاظت‌کند که در پیوست «ج» اشاره‌شده‌اند.

روش‌های کاهش حمله غیرتهاجمی پیاده‌سازی‌شده توسط پودمان رمزنگاری برای حفاظت از SSPهای پودمان که در پیوست «ج» اشاره‌نمی‌شوند shall [08.01] باید مطابق با الزامات زیربند ۷-۱۲ باشند.

روش‌های کاهش حمله غیرتهاجمی پیاده‌سازی‌شده توسط پودمان رمزنگاری برای حفاظت از SSPهای پودمان که در پیوست «ج» اشاره‌می‌شوند [08.02] shall باید مطابق با الزامات زیر باشند.
الزامات مستندسازی تعیین‌شده در زیربند پیوست الف-۲-۸ [08.03] shall باید فراهم‌شوند.

سطوح امنیت ۱ و ۲

برای سطوح امنیت ۱ و ۲، مستندسازی [08.04] shall باید تمام روش‌های کاهش را تعیین‌کند که برای محافظت از CSPهای پودمان از روش‌های کاهش حمله غیرتهاجمی ارجاع‌شده در پیوست «ج»، به‌کاررفته‌اند. مستندسازی [08.05] shall باید شامل دلیل اثربخشی هر یک از روش‌های کاهش حمله باشد.

سطح امنیتی ۳

علاوه بر الزامات برای سطوح امنیت ۱ و ۲، برای سطح امنیتی ۳، پودمان رمزنگاری [08.06] shall باید آزمون‌شود تا مطابق با اندازه‌های آزمایش کاهش حمله غیرتهاجمی تاییدشده برای سطح امنیتی ۳ باشد همان‌طور که در پیوست «ج» مراجعه‌شده‌است.

سطح امنیتی ۴

علاوه بر الزامات برای سطوح امنیت ۱ و ۲، برای سطح امنیتی ۴، پودمان رمزنگاری [08.07] shall باید آزمون‌شود تا مطابق با اندازه‌های آزمایش کاهش حمله غیرتهاجمی تاییدشده برای سطح امنیتی ۴ باشد همان‌طور که در پیوست «ج» مراجعه‌شده‌است.

۷-۹ مدیریت پارامتر امنیت حساس

۷-۹-۱ الزامات کلی مدیریت پارامتر امنیت حساس

پارامترهای امنیت حساس (SSPها) شامل پارامترهای امنیت بحرانی (CSPها) و پارامترهای امنیت عمومی (PSPها) می‌باشد. الزامات امنیتی برای مدیریت SSP شامل کل چرخه عمر SSPها می‌باشد که با پودمان به‌کاربرده‌شده‌اند. مدیریت SSP شامل RBGها، تولید SSP، استقرار SSP، ورودی/ خروجی SSP، ذخیره‌سازی SSP و صفرکردن SSP حفاظت‌نشده می‌باشد.
CSPهای رمزشده به CSPهایی اشاره‌می‌کند که با استفاده از یک تابع امنیتی تاییدشده رمزنگاری‌می‌شوند. CSPهای رمزنگاری‌شده یا تیره‌شده با استفاده از توابع امنیت تاییدنشده که در دامنه کاربرد این استاندارد است، متن‌ساده حفاظت‌نشده درنظرگرفته می‌شوند.
CSPها [09.01] shall باید در پودمان از دسترسی، استفاده، آشکارسازی، اصلاح و جایگزینی غیرمجاز محافظت شوند.
PSPها [09.02] shall باید در داخل پودمان در مقابل اصلاح و جانشینی غیرمجاز محافظت شوند.
پودمان [09.03] shall باید SSP تولیدشده، داخل‌شده به و خارج‌شده از پودمان را به یک هستار (برای مثال، شخص، گروه، نقش یا فرآیند) که SSP به آن اختصاص یافته، مرتبط سازد.
مقادیر درهم‌سازی اسم رمزها، اطلاعات وضعیت RBG و مقادیر تولید کلید واسط [09.04] shall باید CSPهای حفاظت‌شده درنظرگرفته شوند.
الزامات مستندسازی تعیین‌شده در زیربند پیوست الف-۲-۹ [09.05] shall باید فراهم‌شوند.

۷-۹-۲ مولدهای بیت تصادفی

یک پودمان رمزنگاری ممکن است شامل مولدهای بیت تصادفی (RBGها)، زنجیره‌ای از RBGها باشد یا ممکن است تنها شامل یک RBG باشد. RBGهای تاییدشده در پیوست «پ» فهرست می‌شوند.

اگر یک تابع امنیتی تاییدشده، تولید SSP یا روش استقرار SSP به مقادیر تصادفی نیاز داشته باشند، یک RBG تاییدشده shall [09.06] باید استفاده‌شود تا این مقادیر را فراهم‌کند.

اگر انتروپی، از بیرون حد و مرز رمزنگاری جمع‌آوری‌شود، جریان داده تولیدشده با استفاده از این ورودی انتروپی shall [09.07] باید یک CSP درنظرگرفته شود.

۷-۹-۳ تولید پارامتر امنیت حساس

یک پودمان ممکن است پارامترهای امنیت حساس (SSPها) را در داخل تولیدکند و یا آنها ممکن است از SSPهایی حاصل‌شوند که وارد پودمان شده‌اند.

به‌خطرافتادن امنیت روش تولید SSP که از خروجی یک RGB تاییدشده استفاده‌می‌کند (برای مثال، حدس‌زدن مقدار شروع تولید اعداد تصادفی برای مقداردهی اولیه به RGB قطعی) shall [09.08] باید حداقل بسیاری از عملیات‌ها مانند تعیین مقدار SSP تولیدشده را لازم داشته‌باشد.

SSPهایی که توسط پودمان از خروجی یک RBG تاییدشده یا مشتق‌شده از یک SSP واردشده به پودمان و به‌کاربرده شده توسط تابع امنیتی تاییدشده یا روش استقرار SSP، تولیدمی‌شوند shall [09.09] باید با استفاده از یک روش تولید SSP تاییدشده تولیدشود که در پیوست «ت» فهرست‌شده‌اند.

۷-۹-۴ استقرار پارامتر امنیت حساس

استقرار SSP ممکن است شامل:

- انتقال SSP *خودکار* یا روش‌های موافقت SSP یا
- ورود یا خروج SSP *دستی* از طریق روش‌های مستقیم یا الکترونیکی باشد.

استقرار SSP خودکار shall [09.10] باید از یک روش تاییدشده‌ای استفاده‌کند که در پیوست «ت» فهرست‌شده‌است. استقرار SSP دستی shall [09.11] باید مطابق با الزامات زیربند ۷-۹-۵ باشد.

۷-۹-۵ ورود و خروج پارامتر امنیت حساس

SSPها ممکن است به‌طور دستی وارد پودمان شوند و یا به‌طورمستقیم (برای مثال، واردشده از طریق صفحه‌کلید یا صفحه شماره یا خروجی از طریق صفحه نمایش بصری) یا به‌صورت الکترونیکی (برای مثال، از طریق یک کارت / نشانه‌های هوشمند، کارت PC، سایر افزاره‌های بارگذاری کلید الکترونیکی یا سامانه عامل پودمان) از پودمان خارج شوند. اگر SSPها به‌طوردستی وارد پودمان شوند و یا از آن خارج شوند، ورودی یا خروجی shall [09.12] باید وارد واسط‌های HMI، SFMI، HFMI یا HSMI تعریف‌شده شود.

تمام SSPهای حفاظت‌شده از طریق رمزنگاری، که وارد یک پودمان شده‌اند و یا از آن خارج شده‌اند shall [09.13] باید با استفاده از یک تابع امنیتی تاییدشده رمزنگاری شوند.

برای SSPهای به‌طورمستقیم وارده‌شده، مقادیر واردشده ممکن است به‌طور موقتی نمایش‌داده‌شوند تا بررسی بصری امکان‌پذیر باشد و دقت بهبود یابد. اگر SSPهای رمزنگاری‌شده مستقیماً وارد پودمان شوند،

مقادیر متن‌ساده SSPها shall not [09.14] نباید نمایش داده شوند. SSPهای به‌طورمستقیم وارده‌شده (متن‌ساده یا رمزنگاری شده) shall [09.15] باید در طی ورود به پودمان برای درستی با استفاده از آزمون ورودی دستی شرطی بررسی شود که در زیربند ۷-۱۰-۳-۵ تعیین‌شده‌است.

برای جلوگیری از خروج غیرعمدی اطلاعات حساس، دو عمل داخلی مستقل shall [09.16] باید نیاز باشد تا هر CSP متن‌ساده را خارج‌کند. این دو عمل داخلی مستقل shall [09.17] باید برای میانجی‌گری خروجی CSPها اختصاص‌داده‌شوند.

برای ورود یا خروج الکترونیکی از طریق یک اتصال بی‌سیم؛ CSPها، مولفه‌های کلید و داده‌های اصالت‌سنجی shall [09.18] باید رمزنگاری شوند.

PSPهای واردشده به‌طور دستی، نیازی نیست که با رمزنگاری، اصالت‌سنجی شوند.

سطوح امنیت ۱ و ۲

CSPهای متن‌ساده، مولفه‌های کلید و داده‌های اصالت‌سنجی ممکن است از طریق درگاه‌ها و واسط‌های منطقی مشترک با دیگر درگاه‌های فیزیکی و واسط‌های منطقی پودمان رمزنگاری واردشوند.

برای پودمان‌های نرم‌افزاری یا مولفه‌های نرم‌افزاری یک پودمان نرم‌افزار ترکیبی، CSPها، مولفه‌های کلید و داده‌های اصالت‌سنجی ممکن است به شکل متن‌ساده یا رمزنگاری‌شده وارد یا خارج‌شوند مشروط بر این‌که CSPها، مولفه‌های کلید و داده‌های اصالت‌سنجی shall [09.19] باید در داخل محیط عملیاتی نگهداری‌شوند و مطابق با الزامات زیربند ۷-۶-۳ باشند.

سطح امنیتی ۳

علاوه بر سطوح امنیت ۱ و ۲، برای سطح امنیتی ۳، CSPها، مولفه‌های کلید و داده‌های اصالت‌سنجی shall [09.20] باید وارد به یا خارج از پودمانی شوند که با کانال قابل‌اطمینان رمزنگاری‌شده‌است.

CSPهایی که کلیدهای رمزنگاری خصوصی و محرمانه متن‌ساده می‌باشند shall [09.21] باید وارد به یا خارج از پودمان با استفاده از روش‌های دانش تقسیمی که از کانال قابل‌اعتماد استفاده‌می‌کنند، شوند.

اگر پودمان از روش‌های دانش تقسیمی استفاده‌کند، پودمان shall [09.22] باید از اصالت‌سنجی عملگر هستارمحور جدا برای واردکردن یا خارج‌کردن هر مولفه کلید استفاده‌کند و حداقل دو مولفه کلید shall [09.23] باید لازم باشند تا کلید رمزنگاری اصلی را بازسازی‌کنند.

سطح امنیتی ۴

علاوه بر سطح امنیتی ۳، برای سطح امنیتی ۴، پودمان shall [09.24] باید از اصالت‌سنجی عملگر هستارمحور جدا و چند عاملی برای واردکردن یا خارج‌کردن هر مولفه کلید استفاده‌کند.

۷-۹-۶ ذخیره‌سازی پارامتر امنیت حساس

پارامترهای امنیت حساس (SSPهای) ذخیره‌شده در پودمان ممکن است به شکل متن‌ساده یا رمزشده ذخیره‌شوند. یک پودمان shall [09.25] باید هر SSP ذخیره‌شده را به پودمانی مرتبط سازد که آن پودمان همراه با هستاری (برای مثال، عملگر، نقش یا فرآیند) است که به آن SSP تخصیص می‌یابد.

دسترسی به CSPهای متن‌ساده توسط عملگرهای غیرمجاز shall [09.26] باید ممنوع‌شود. اصلاح PSPها توسط عملگرهای غیرمجاز shall [09.27] باید ممنوع‌شود.

۷-۹-۷ صفرکردن پارامتر امنیت حساس

پودمان shall [09.28] باید روشی را فراهم‌کند تا تمام SSPهای حفاظت‌نشده و مولفه‌های کلید را در پودمان صفرکند. SSPهای ذخیره‌شده به‌طور موقتی و سایر مقادیر ذخیره‌شده با مالکیت پودمان باید زمانی صفرشوند که آنها دیگر برای استفاده آینده لازم نیستند.

SSP صفرشده shall not [09.29] نباید قابل‌ارزیابی یا قابل‌استفاده مجدد باشد.

صفرکردن PSPهای حفاظت‌شده، CSPهای رمزشده، یا دیگر CSPهایی که به‌طور فیزیکی یا منطقی در پودمان معتبر جاسازی‌شده اضافی حفاظت‌می‌شوند (مطابق با الزامات این استاندارد) لازم نمی‌باشد.

اگر SSPها به‌طور انحصاری استفاده‌شوند تا داده متن‌ساده را در فرآیندهایی آشکارکنند که پروکسی‌های اصالت‌سنجی می‌باشند، نباید مطابق با این الزامات صفرکردن باشند (برای مثال، CSPیی که کلید مقداردهی اولیه پودمان می‌باشد).

پارامترهایی که فقط برای اهداف خودآزمایی در زیربند ۷-۱۰ استفاده شده‌اند نیازی نیست که مطابق با الزامات صفرکردن باشند.

سطح امنیتی ۱

صفرکردن SSPهای حفاظت‌نشده ممکن است طبق روش توسط عملگر پودمان انجام‌شود و مستقل از کنترل پودمان باشد (برای مثال، قالب‌بندی مجدد دیسک سخت، تخریب جوی پودمان در طی ورودی مجدد و غیره).

سطح امنیتی ۲ و ۳

پودمان رمزنگاری shall [09.30] باید صفرکردن SSPهای حفاظت‌نشده را انجام‌دهد (برای مثال، رونویسی با داده تمام صفر یا تمام یک یا داده تصادفی). صفرکردن shall [09.31] باید رونویسی یک SSP حفاظت‌نشده را با دیگر SSP حفاظت‌نشده، مستثنی کند. SSPهای موقتی هنگامی‌که دیگر لازم نیستند shall [09.32] باید صفرشوند. هنگامی‌که صفرشدن کامل‌شد، پودمان shall [09.33] باید یک نشانه وضعیت خروجی را فراهم‌می‌کند.

سطح امنیتی ۴

علاوه بر الزامات سطوح امنیت ۲ و ۳، الزامات زیر shall [09.34] باید برآورده شود:

- صفرکردن shall [09.35] باید فوری و بی‌وقفه باشد و shall [09.36] باید در یک مدت زمان کافی بسیار کوچک روی‌دهد برای این‌که از بازیافت داده‌های حساس بین زمان شروع به صفرشدن و زمان واقعی صفرشدن، جلوگیری‌کند.
- تمام SSPهای حفاظت‌نشده shall [09.37] باید صفرشوند، چه متن‌ساده و چه حفاظت‌شده از طریق رمزنگاری، به‌طوری‌که پودمان به وضعیت کارخانه‌ای برگردد.

۷-۱۰ خودآزمایی‌ها

۷-۱۰-۱ الزامات کلی خودآزمایی

خودآزمایی‌های شرطی و پیش‌عملیاتی پودمان رمزنگاری، اطمینان عملگر را فراهم‌می‌کنند که عیب‌ها واردنشده‌اند تا از عملیات تصحیح پودمان جلوگیری‌کنند. تمام خودآزمایی‌ها [10.01] shall باید انجام‌شوند و تعیین گذر یا خرابی [10.02] shall باید توسط پودمان انجام‌شود، بدون کنترل‌های خارجی، که به‌طورخارجی، بردارهای متن ورودی، نتایج خروجی مورد انتظار را فراهم‌کرده‌اند یا مداخله عملگر و یا این‌که آیا پودمان در یک حالت تاییدشده یا تاییدنشده عمل‌می‌کند.

قبل از این‌که پودمان هر خروجی داده را از طریق واسط خروجی داده تهیه کند، خودآزمایی‌های پیش‌عملیاتی باید [10.03] shall انجام‌شوند و با موفقیت تایید شوند.

قبل از این‌که یک تابع یا فرآیند امنیت فراخوانی شود، خودآزمایی‌های شرطی باید [10.04] shall انجام‌شوند (یعنی توابع امنیتی که برای آن خودآزمایی‌ها لازم هستند).

تمام خودآزمایی‌های شناسایی‌شده در استانداردهای الگوریتمی اساسی (پیوست‌های «پ» تا «ث») باید [10.05] shall پیاده‌سازی‌شوند هنگامی‌که در پودمان رمزنگاری کاربردپذیر می‌باشند. تمام خودآزمایی‌های شناسایی‌شده علاوه بر (یا به جای) آنهایی که در استانداردهای الگوریتمی اساسی تعیین‌شده‌اند (پیوست‌های «پ» تا «ث») باید [10.06] shall پیاده‌سازی‌شوند همان‌طور که در پیوست‌های «پ» تا «ث» برای هر تابع امنیتی تاییدشده، روش اسقرار SSP و سازوکار اصالت‌سنجی مراجعه‌شده‌اند.

یک پودمان رمزنگاری ممکن است آزمون کارکردهای بحرانی شرطی یا پیش‌عملیاتی را علاوه برآزمون‌هایی انجام‌دهد که در این استاندارد تعیین‌شده‌اند.

اگر یک پودمان رمزنگاری یک خودآزمایی را شکست دهد، پودمان باید [10.07] shall وارد وضعیت خطا شود و باید [10.08] shall یک علامت خطا خارج کند همان‌طور که در زیربند ۷-۳-۳ تعیین‌شده‌است.

پودمان رمزنگاری تا زمانی‌که در یک وضعیت خطا می‌باشد، نباید [10.09] shall not هیچ عملیات رمزنگاری یا کنترل خروجی و داده را از طریق واسط خروجی داده و کنترل انجام‌دهد. پودمان رمزنگاری نباید [10.10] shall not از هیچ تابعی استفاده کند که به یک تابع یا الگوریتمی وابسته می‌باشد که یک خودآزمایی را شکست‌داده‌است تا این‌که خودآزمایی مربوطه تکرارشده‌است و با موفقیت تاییدشود. اگر پودمان وضعیت خطا را در خرابی یک خودآزمایی پودمان خارج‌نکند، متصدی پودمان باید [10.11] shall بتواند تعیین‌کند آیا این پودمان به‌طور ضمنی از طریق یک روش بدون ابهام که در خط‌مشی امنیت مستند شده‌است (پیوست «ب») وارد یک وضعیت خطا شده است.

در سطوح امنیت ۳ و ۴، پودمان باید [10.12] shall یک سامانه ثبت خطا را حفاظت‌کند که توسط یک متصدی مجاز پودمان قابل دسترسی است. سامانه ثبت خطا باید [10.13] shall حداقل اطلاعاتی را از جدیدترین رخداد خطا فراهم‌کند (یعنی کدام خودآزمایی خراب شده است).

الزامات مستندسازی تعیین‌شده در پیوست الف-۲-۱۰ باید [10.14] shall فراهم‌شوند.

۷-۱۰-۲ خودآزمایی‌های پیش‌عملیاتی

۷-۱۰-۲-۱ الزامات کلی خودآزمایی پیش‌عملیاتی

آزمون‌های پیش‌عملیاتی توسط یک پودمان رمزنگاری بین هنگامی‌که یک پودمان رمزنگاری روشن یا معرفی می‌شود (پس از خاموش‌شدن، تنظیم مجدد، راه‌اندازی مجدد، شروع سرد، قطع برق و غیره) و قبل از انتقال‌های پودمان به وضعیت عملیاتی نباید shall not [10.15] انجام و با موفقیت تایید شود.

یک پودمان رمزنگاری باید shall [10.16] آزمون‌های پیش‌عملیاتی زیر را انجام‌دهد، هنگامی‌که کاربردپذیر است:

- آزمون یکپارچگی پیش‌عملیاتی نرم‌افزار / ثابت‌افزار
- آزمون کنارگذار پیش‌عملیاتی
- آزمون توابع بحرانی پیش‌عملیاتی

۷-۱۰-۲-۲ آزمون یکپارچگی نرم‌افزار/ ثابت‌افزار پیش‌عملیاتی

تمام مولفه‌های نرم‌افزار و ثابت‌افزار در حد و مرز رمزنگاری باید shall [10.17] با استفاده از یک روش یکپارچگی تاییدشده مطابق با الزامات تعیین‌شده در زیربند ۵-۷ بررسی‌شوند. اگر بررسی‌ها ردشوند، آزمون یکپارچگی نرم‌افزار/ ثابت‌افزار پیش‌عملیاتی باید shall [10.18] ردشود. آزمون یکپارچگی نرم‌افزار/ ثابت‌افزار پیش‌عملیاتی برای هر نرم‌افزار یا ثابت‌افزار مستثنی‌شده از الزامات امنیتی این استاندارد لازم نمی‌باشد یا برای هر کد اجرایی ذخیره‌شده در حافظه غیرقابل پیکربندی مجدد لازم نمی‌باشد.

اگر یک پودمان سخت‌افزاری شامل نرم‌افزار یا ثابت‌افزار نباشد، پودمان باید shall [10.19] حداقل یک خودآزمایی الگوریتم رمزنگاری را پیاده‌سازی‌کند همان‌طور که در زیربند ۷-۱۰-۳-۲ به‌عنوان یک خودآزمایی پیش‌عملیاتی تعیین‌شده‌است.

یک الگوریتم رمزنگاری که برای انجام روش یکپارچگی تاییدشده برای آزمون نرم‌افزار/ ثابت‌افزار پیش‌عملیاتی استفاده‌می‌شود باید shall [10.20] ابتدا خودآزمایی الگوریتم رمزنگاری را تاییدکند که در زیربند ۷-۱۰-۳-۲ تعیین‌شده‌است.

۷-۱۰-۲-۳ آزمون کنارگذار پیش‌عملیاتی

اگر پودمان رمزنگاری یک توانایی کنارگذار را پیاده‌سازی‌کند، این پودمان باید shall [10.21] اطمینان‌دهد که عملیات فعال‌سازی نظارت منطق توانایی کنارگذار توسط اعمال این منطق، صحیح می‌باشد. پودمان باید shall [10.22] مسیر داده را بررسی‌کند توسط:

- تنظیم سوئیچ کنارگذار برای این‌که پردازش رمزنگاری را فراهم‌کند و بررسی‌کند که داده‌های منتقل‌شده به درون سازوکار کنارگذار به‌طور رمزنگاری پردازش‌می‌شود و
- تنظیم سوئیچ کنارگذار برای این‌که پردازش رمزنگاری را فراهم نکند و بررسی کند که داده‌های منتقل‌شده به درون سازوکار کنارگذار به‌طور رمزنگاری پردازش نمی‌شود.

۷-۱۰-۲-۴ آزمون توابع بحرانی پیش‌عملیات

ممکن است توابع امنیت دیگری وجود داشته باشند که در عملیات امن یک پودمان رمزنگاری بحرانی هستند که باید [10.23] shall به‌عنوان یک آزمون پیش‌عملیاتی آزموده‌شوند. مستندسازی باید [10.24] shall توابع بحرانی پیش‌عملیاتی را تعیین‌کند که آزموده می‌شوند.

۷-۱۰-۳ خودآزمایی‌های شرطی

۷-۱۰-۳-۱ الزامات کلی خودآزمایی شرطی

هنگامی‌که شرایط تعیین‌شده برای آزمون‌های زیر به‌وجود می‌آید، *خودآزمایی‌های شرطی* باید [10.25] shall با یک پودمان رمزنگاری انجام‌گیرد: خودآزمایی الگوریتم رمزنگاری، آزمون سازگاری دوبه‌دو، آزمون بار نرم‌افزار/ ثابت‌افزار، آزمون ورود دستی آزمون کنارگذار شرطی و آزمون توابع بحرانی شرطی.

۷-۱۰-۳-۲ خودآزمایی الگوریتم رمزنگاری شرطی

خودآزمایی الگوریتم رمزنگاری. یک آزمون الگوریتم رمزنگاری باید [10.26] shall برای تمام توابع رمزنگاری (برای مثال، توابع امنیت، روش‌های اسقرار SSP و اصالت‌سنجی) از هر الگوریتم رمزنگاری تاییدشده که در پودمان رمزنگاری پیاده‌سازی شده است و در پیوست‌های «پ» تا «ث» مراجعه شده است، انجام‌گیرد. آزمون شرطی باید [10.27] shall قبل از اولین کاربرد عملیاتی الگوریتم رمزنگاری انجام‌گیرد.

یک خودآزمایی الگوریتم رمزنگاری ممکن است یک آزمون *پاسخ ـ معلوم*، یک آزمون *مقایسه* و یا یک آزمون *کشف خطا* باشد.

یک *آزمون پاسخ ـ معلوم* شامل مجموعه‌ای از بردارهای ورودی شناخته‌شده می‌باشد (برای مثال، داده، مطلب راهنما، یا ثابت‌ها به جای بیت‌های تصادفی) که با الگوریتم رمزنگاری انجام‌می‌شود تا نتیجه‌ای را تولیدکند. این نتیجه با نتیجه خروجی مورد انتظار معلوم مقایسه‌می‌شود. اگر خروجی محاسبه‌شده با پاسخ معلوم مساوی نباشد، خودآزمایی پاسخ معلوم الگوریتم رمزنگاری باید [10.28] shall رد شود.

یک خودآزمایی الگوریتم باید [10.29] shall حداقل از کمترین طول کلیدی تاییدشده، اندازه پودمان، DSA اول یا منحنی‌های مناسب استفاده‌کند که توسط پودمان پشتیبانی‌می‌شود.

اگر یک الگوریتم چند حالت را مشخص کند (برای مثال، ECB، CBC و غیره) حداقل یک حالت باید [10.30] shall برای خودآزمایی انتخاب شود که با پودمان پشتیبانی می‌شود و یا توسط مقام ذیصلاح صحه‌گذاری مشخص می‌شود.

مثال‌هایی از آزمون‌های پاسخ ـ معلوم:

- توابع یک‌طرفه: بردارهای آزمون ورودی، خروجی را تولید می‌کنند که باید [10.31] shall شبیه به خروجی مورد انتظار باشند (برای مثال درهم‌سازی، درهم‌های کلید، اصالت‌سنجی پیام، RBG (بردار انتروپی ثابت)، موافقت SSP).
- توابع برگشت‌پذیر: هر دو تابع مستقیم و معکوس باید [10.32] shall خودآزمایی شوند (برای مثال، رمزنگاری و رمزگشایی کلید متقارن، رمزگذاری و رمزگشایی انتقال SSP، تولید و بررسی امضا دیجیتال).

یک آزمون مقایسه، خروجی دو یا چند پیاده‌سازی الگوریتم رمزنگاری مستقل را مقایسه می‌کند، اگر خروجی‌ها برابر نباشند، خودآزمایی مقایسه الگوریتم رمزنگاری باید [10.33] shall رد شود.
یک *آزمون کشف اشکال* شامل انجام سازوکارهای کشف اشکال می‌باشد که در پیاده‌سازی الگوریتم رمزنگاری جمع‌آوری‌شده است، اگر یک اشکال کشف شود، خودآزمایی کشف اشکال الگوریتم رمزنگاری باید [10.34] shall رد شود.

۷-۱۰-۳-۳ آزمون سازگاری دو به دوی شرطی

اگر یک پودمان رمزنگاری جفت‌های کلید عمومی یا خصوصی تولید کند، یک آزمون سازگاری دو به دو باید [10.35] shall برای هر جفت کلید عمومی و خصوصی تولیدشده انجام‌شود که در پیوست «پ» تا «ث» برای الگوریتم رمزنگاری کاربردی اشاره می‌شود.

۷-۱۰-۳-۴ آزمون بار نرم‌افزار/ ثابت‌افزار شرطی

اگر یک پودمان رمزنگاری توانایی بارگذاری نرم‌افزار یا ثابت‌افزار را از یک منبع خارجی داشته‌باشد، الزامات زیر علاوه بر الزامات زیربند ۷-۴-۳-۴ باید [10.36] shall انجام‌شوند:

- پودمان رمزنگاری باید [10.37] shall یک روش اصالت‌سنجی تاییدشده را پیاده‌سازی‌کند تا صحت نرم‌افزار یا ثابت‌افزاری که بارگذاری می‌شود را بررسی کند.
- کلید اصالت‌سنجی مرجع باید [10.38] shall به‌طور مستقل در پودمان قبل از بارگذاری نرم‌افزار یا ثابت‌افزار بارگذاری شود.
- روش اصالت‌سنجی تاییدشده کاربردی باید [10.39] shall با موفقیت بررسی‌شود یا آزمون بارگذاری نرم‌افزار / ثابت‌افزار باید [10.40] shall رد شود. اگر آزمون بارگذاری نرم‌افزار / ثابت‌افزار رد شود، نرم‌افزار یا ثابت‌افزار بارگذاری‌شده نباید [10.41] shall not استفاده‌شود.

۷-۱۰-۳-۵ آزمون ورودی دستی شرطی

اگر SSPها یا مولفه‌های کلید به‌طور دستی و مستقیم وارد پودمان رمزنگاری شوند یا اگر خطا در بخش متصدی انسانی باعث ورود نادرست مقدار موردنظر شود، آزمون‌های ورودی دستی زیر [10.42] shall انجام می‌گیرد:

- SSP یا مولفه‌های کلید باید [10.43] shall یک EDC کاربردی داشته‌باشند و یا باید [10.44] shall با استفاده از ورودی‌های دو نسخه‌ای وارد شوند.

اگر یک EDC استفاده‌شود، EDC باید [10.45] shall حداقل ۱۶ بیت طول داشته‌باشد. اگر EDC نتواند بررسی‌شود و یا ورودی‌های دونسخه‌ای مطابقت نکنند، آزمون باید [10.46] shall رد شود.

۷-۱۰-۳-۶ آزمون کنارگذار شرطی

اگر یک پودمان رمزنگاری، توانایی کنارگذار را پیاده‌سازی‌کند که در آنجا خدمات ممکن است بدون پردازش رمزنگاری تهیه‌شوند (برای مثال، انتقال متن ساده از طریق پودمان) سپس مجموعه آزمون‌های کنارگذار باید [10.47] shall انجام‌گیرند تا اطمینان‌دهند که یک نقطه خرابی از مولفه‌های پودمان موجب خروجی غیرعمدی متن ساده نمی‌شود.

یک پودمان رمزنگاری باید shall [10.48] عملیات صحیح خدماتی را آزمون کند که پردازش رمزنگاری را فراهم‌می‌کنند هنگامی‌که یک سوئیچ بین یک خدمت کنارگذار انحصاری و یک خدمت رمزنگاری انحصاری روی‌می‌دهد.

اگر یک پودمان رمزنگاری بتواند به‌طور خودکار بین یک خدمت کنارگذار و یک خدمت رمزنگاری، تهیه چند خدمت با پردازش رمزنگاری و چند خدمت بدون پردازش رمزنگاری تغییر کند، سپس هنگامی‌که سازوکار نظارت روش راه‌گزینی اصلاح‌می‌شود (برای مثال، جدول مبدا/ مقصد آدرس IP) پودمان باید shall [10.49] برای عملیات صحیح خدماتی آزمون شود که پردازش رمزنگاری را فراهم‌می‌کنند.

اگر یک پودمان رمزنگاری اطلاعات داخلی را نگهداری‌کند که توانایی کنارگذار را نظارت‌می‌کند، سپس این پودمان باید shall [10.50] یکپارچگی اطلاعات نظارتی را از طریق یک روش یکپارچگی تاییدشده و قبل از اصلاح اطلاعات نظارتی بررسی‌کند و باید shall [10.51] یک مقدار یکپارچگی جدیدی را با استفاده از روش یکپارچگی تاییدشده پس از اصلاح تولیدکند.

۷-۱۰-۳-۷ آزمون توابع بحرانی شرطی

توابع امنیتی دیگری وجوددارند که ممکن است برای عملیات امن یک پودمان رمزنگاری، بحرانی باشند که باید shall [10.52] به‌عنوان یک خودآزمایی شرطی آزمون‌شوند.

۷-۱۰-۳-۸ خودآزمایی‌های دوره‌ای

سطوح امنیت ۱ و ۲

یک پودمان رمزنگاری باید shall [10.53] به متصدیان اجازه‌دهد تا خودآزمایی‌های پیش‌عملیاتی یا شرطی را طبق تقاضا برای آزمون دوره‌ای پودمان شروع‌کنند. ابزار قابل قبول برای شروع خودآزمایی‌های دوره‌ای طبق تقاضا عبارتند از: خدمت تهیه‌شده، تنظیم مجدد، راه‌اندازی مجدد یا چرخه توان.

سطوح امنیت ۳ و ۴

علاوه بر الزامات در سطوح امنیت ۱ و ۲، پودمان باید shall [10.54] به تکرار با یک دوره زمان تعریف‌شده خودکار، بدون ورودی خارجی یا کنترل، خودآزمایی‌های پیش‌عملیاتی یا شرطی را انجام‌دهد. مدت زمان و هر شرایطی که ممکن است موجب وقفه عملیات‌های پودمان در طی زمان شوند تا خودآمازیی‌های پیش‌عملیاتی یا شرطی را تکرار کنند باید shall [10.55] در خط‌مشی امنیت تعیین‌شوند (به پیوست «ب» مراجعه شود) (برای مثال، اگر پودمان، خدمات بحرانی مأموریتی را انجام‌دهد که نمی‌توانند متوقف شوند و دوره زمانی برای شروع خودآزمایی‌های پیش‌عملیاتی قبول شود، خودآزمایی‌ها پس از آنکه دوره زمانی دوباره قبول شود، ممکن است به تأخیر بیافتند).

۷-۱۱ اطمینان چرخه عمر

۷-۱۱-۱ الزامات کلی اطمینان چرخه عمر

الزامات چرخه عمر به کاربرد بهترین عمل‌ها توسط ارائه‌دهنده یک پودمان رمزنگاری اشاره‌می‌کند که در طی طراحی، توسعه، عملیات و پایان عمر یک پودمان رمزنگاری، اطمینانی را فراهم‌می‌کند که پودمان به درستی طراحی، توسعه، آزمایش، پیکربندی، ارسال و نصب می‌شود و این‌که مستندسازی راهنمای مناسب برای

متصدی تهیه‌می‌شود. الزامات امنیتی برای مدیریت پیکربندی، طراحی، مدل وضعیت محدود، توسعه، آزمون ارسال و عملیات و مستندسازی راهنما تعیین‌می‌شوند.
الزامات مستندسازی تعیین‌شده در پیوست الف-۲-۱۱ باید shall [11.01] فراهم‌شوند.

۷-۱۱-۲ مدیریت پیکربندی

مدیریت پیکربندی، الزامات را برای یک سامانه مدیریت پیکربندی تعیین‌می‌کند که با یک ارائه‌دهنده پودمان رمزنگاری انجام‌شده‌است و اطمینانی فراهم‌می‌کند که یکپارچگی پودمان رمزنگاری توسط نیاز به نظم و کنترل در فرآیندهای اصلاح و تغییر پودمان رمزنگاری و مستندسازی مربوطه محافظت‌می‌شود. یک سامانه مدیریت پیکربندی در محل گذاشته‌می‌شود تا از تغییرات و اصلاحات غیرمجاز یا تصادفی جلوگیری‌کند و قابلیت ردیابی تغییری که در پودمان رمزنگاری و مستندسازی مربوطه دنبال‌می‌شود را فراهم‌کند.

سطوح امنیت ۱ و ۲

الزامات امنیتی زیر باید shall [11.02] در پودمان‌های رمزنگاری برای سطوح امنیت ۱ و ۲ به کاربرده شوند:

- یک سامانه مدیریت پیکربندی باید shall [11.03] برای توسعه پودمان رمزنگاری و مولفه‌های پودمان در حد و مرز رمزنگاری استفاده‌شود و در مستندسازی پودمان مربوطه به‌کار آید.
- هر نسخه از هر عنصر پیکربندی (برای مثال، پودمان رمزنگاری، بخش‌های سخت‌افزار پودمان، مولفه‌های نرم‌افزار پودمان، HDL پودمان، راهنمای کاربر، خط‌مشی امنیت و غیره) که شامل پودمان و مستندسازی مربوطه است باید shall [11.04] تعیین‌شود و با یک شناسه انحصاری برچسب زده شود.
- سامانه مدیریت پیکربندی باید shall [11.05] تغییرات مربوط به شناسایی و نسخه یا نسخه مجدد هر یک از پیکربندی‌ها در تمام چرخه عمر پودمان رمزنگاری صحه‌گذاری‌شده، دنبال و نگهداری‌کند.

سطوح امنیت ۳ و ۴

علاوه بر الزامات برای سطوح امنیت ۱ و ۲، عناصر پیکربندی باید shall [11.06] با استفاده از یک سامانه مدیریت پیکربندی خودکار مدیریت‌شوند.

۷-۱۱-۳ طراحی

طراحی یک راه‌حل مهندسی است که مشخصات کارکردی را برای یک پودمان رمزنگاری مشخص‌می‌کند. طراحی اطمینان‌می‌دهد که مشخصات کارکردی یک پودمان رمزنگاری متناظر با کارکرد موردنظری می‌باشد که در خط‌مشی امنیت توصیف‌شده‌است.
پودمان‌های رمزنگاری باید shall [11.07] طراحی‌شوند تا امکان آزمون تمام خدمات مربوط به امنیت فراهم‌شده را ایجادکنند.

۷-۱۱-۴ مدل وضعیت محدود

عملیات یک پودمان رمزنگاری باید shall [11.08] با استفاده از یک مدل وضعیت محدود (یا معادل) تعیین‌شود که با یک نمودار انتقال وضعیت و یک جدول انتقال وضعیت و توضیحات وضعیت

نشان‌داده‌شده‌اند. FSM باید [11.09] shall جزئیات کافی داشته‌باشد تا اثبات‌کند که پودمان رمزنگاری مطابق با تمام الزامات این استاندارد می‌باشد.

FSM یک پودمان رمزنگاری باید [11.10] shall حداقل شامل وضعیت‌های عملیاتی یا خطای زیر باشد:

- *وضعیت روشن/ خاموش:* وضعیتی که در آن پودمان خاموش است، در حالت انتظار می‌باشد (حافظه فرّار نگهداری‌شده‌است) یا وضعیت عملیاتی در حافظه غیرفرّار نگهداری‌شده‌است (برای مثال وضعیت خاموشی موقت[1]) و در آن توان اولیه، ثانویه یا پشتیبان در پودمان به‌کاربرده می‌شود. این وضعیت ممکن است بین منابع توان تشخیص‌داده‌شود که در یک پودمان رمزنگاری به کار می‌آید. برای یک پودمان نرم‌افزاری، روشن بودن عمل ایجاد یک تصویر اجرایی از پودمان رمزنگاری می‌باشد.
- *وضعیت مقداردهی اولیه کلی:* وضعیتی که در آن پودمان رمزنگاری مقداردهی اولیه می‌شود قبل از این‌که پودمان به وضعیت تاییدشده منتقل شود.
- *وضعیت مسوول رمز:* وضعیتی که در آن خدمات مسوول رمز انجام‌می‌شود (برای مثال، مقداردهی اولیه رمزنگاری، مدیریت امن و مدیریت راهنما).
- *وضعیت ورودی CSP.* وضعیتی برای وارد کردن CSPها به داخل پودمان رمزنگاری.
- *وضعیت کاربر:* (اگر یک نقش کاربر پیاده‌سازی‌شود): وضعیتی که در آن کاربران مجاز، خدمات امنیت را به‌دست‌می‌آورند، عملیات‌های رمزنگاری را انجام می‌دهند و یا سایر کارکردهای تاییدشده را انجام می‌دهند.
- *وضعیت تاییدشده:* وضعیتی که در آن توابع امنیت تاییدشده انجام می‌شوند.
- *وضعیت خودآزمایی:* وضعیتی که در آن، پودمان رمزنگاری خودآزمایی‌ها انجام می‌دهد.
- *وضعیت خطا:* وضعیت هنگامی‌که پودمان رمزنگاری به یک شرط خطا برخورد می‌کند (برای مثال، یک خودآزمایی با شکست مواجه‌شده‌است). ممکن است یک یا چند شرط خطا در یک وضعیت خطای پودمان وجود داشته‌باشد. وضعیت‌های خطا ممکن است شامل خطاهای «سخت» باشد که یک کارکرد نادرست وسیله را نشان می‌دهند و ممکن است به نگهداری نیازداشته‌باشند و یا به خدمت یا تعمیر پودمان رمزنگاری نیازداشته‌باشند و یا به خطاهای «نرم» قابل بازیافت نیازداشته‌باشند که ممکن است نیاز به مقداردهی اولیه یا راه‌اندازی مجدد پودمان داشته‌باشد. بازیابی از وضعیت‌های خطا باید [11.11] shall امکان‌پذیر باشند، به جز برای آنهایی که با خطاهای سخت ایجادشده‌اند که نیاز به نگهداری، خدمت یا تعمیر پودمان رمزنگاری دارند.

هر خدمت پودمان رمزنگاری جدا، کاربرد تابع امنیتی، وضعیت خطا، خودآزمایی یا اصالت‌سنجی متصدی باید [11.12] shall به صورت یک وضعیت جدا به تصویر کشیده شود.

تغییر به وضعیت مسوول رمز از هر نقش دیگری غیر از نقش مسوول رمز، باید [11.13] shall ممنوع شود.

یک پودمان رمزنگاری ممکن است شامل سایر وضعیت‌های زیر باشد اما محدود به آن نیست:

1- Hibernate

وضعیت کنارگذار: وضعیتی که در آن یک خدمت، در نتیجه پیکربندی پودمان یا مداخله متصدی، سبب خروجی متن ساده از یک داده خاص یا قلم وضعیتی می‌شود که به‌طور عادی به شکل رمزشده خارج می‌شود.
وضعیت ساکن: وضعیتی که در آن پودمان رمزنگاری بی‌اثر است (برای مثال، توان کم، معلق یا خاموشی موقت).

۷-۱۱-۵ توسعه

یک فرآیند *توسعه* مناسب، اطمینانی فراهم‌می‌کند که پیاده‌سازی پودمان رمزنگاری مطابق با مشخصات کارکردی پودمان و خط‌مشی امنیتی می‌باشد که پودمان رمزنگاری قابل نگهداری است و پودمان رمزنگاری صحه‌گذاری‌شده قابل تولید مجدد است. این بند، الزامات امنیتی را برای نمایش تابع امنیتی پودمان رمزنگاری در سطوح مختلف انتزاع از مشخصات کارکردی تا نمونه اجرایی تعیین‌می‌کند.

سطح امنیتی ۱

الزامات زیر باید [11.14] shall در پودمان‌های رمزنگاری برای سطح امنیتی ۱ به‌کاربرده شوند:

- اگر پودمان رمزنگاری شامل نرم‌افزار یا ثابت‌افزار، کد منبع، مرجع زبان، مترجم، نسخه‌های مترجم و گزینه‌های مترجم، پیونددهنده و گزینه‌های پیونددهنده، کتابخانه‌های زمان اجرا و تنظیمات کتابخانه زمان اجرا، تنظیمات پیکربندی، فرآیندها و روش‌های ساخت، گزینه‌های ساخت، متغیرهای محیطی و تمام منابع دیگر کاربردی باشد که برای کامپایل و پیوند کد منبع به شکل اجرایی استفاده‌می‌شوند، باید [11.15] shall با استفاده از سامانه مدیریت پیکربندی دنبال‌شوند.
- اگر پودمان رمزنگاری شامل نرم‌افزار یا ثابت‌افزارباشد، کدهای منبع باید [11.16] shall با نظراتی اعلان‌شوند که مطابقت نرم‌افزار یا ثابت‌افزار را در طراحی پودمان به‌تصویر می‌کشند.
- اگر پودمان رمزنگاری شامل سخت‌افزار باشد، مستندسازی باید [11.17] shall قواعد معنایی و/ یا HDL را در شرایط کاربردی تعیین‌کند؛
- اگر پودمان رمزنگاری شامل سخت‌افزار باشد، HDL باید [11.18] shall با نظراتی تفسیرشود که مطابقت سخت‌افزار با طراحی پودمان را به‌تفسیر بکشد.
- برای پودمان‌های رمزنگاری نرم‌افزار و ثابت‌افزار و مولفه نرم‌افزار و ثابت‌افزار یک پودمان ترکیبی:
  - نتیجه یکپارچگی و سازوکارهای روش اصالت‌سنجی تعیین‌شده در زیربندهای ۷-۵ و ۷-۱۰ باید [11.19] shall محاسبه‌شوند و در پودمان نرم‌افزار یا ثابت‌افزار توسط ارائه‌دهنده در طی توسعه پودمان مجتمع‌شوند.
  - مستندسازی پودمان رمزنگاری باید [11.20] shall مترجم، تنظیمات پیکربندی و روش‌هایی را تعیین‌کند که کد منبع را در یک شکل اجرایی کامپایل‌می‌کند و
  - پودمان رمزنگاری باید [11.21] shall با استفاده از ابزارهای توسعه رتبه تولید توسعه یابند (برای مثال، مترجم‌ها).

سطوح امنیت ۲ و ۳

علاوه بر الزامات برای سطح امنیتی ۱، الزامات زیر باید [11.22] shall در پودمان‌های رمزنگاری برای سطوح امنیت ۲ و ۳ به‌کاربرده شوند:

- تمام نرم‌افزار یا ثابت‌افزار باید [11.23] shall با استفاده از منطق یا زبان سطح بالا، غیراختصاصی پیاده‌سازی‌شود و اگر در عملکرد پودمان لازم باشد یا هنگامی‌که یک زبان سطح بالا در دسترس نباشد، باید [11.24] shall برای استفاده از یک زبان سطح پایین تهیه‌شوند (برای مثال زبان اسمبلی یا ریزکد).
- مدارهای مجتمع سفارشی در یک پودمان رمزنگاری باید [11.25] shall با استفاده از یک HDL سطح بالا پیاده‌سازی‌شوند (مثال VHDL یا Verilog).
- پودمان‌های رمزنگاری نرم‌افزار یا ثابت‌افزار باید [11.26] shall طوری طراحی و پیاده‌سازی‌شوند که از کاربرد کد، پارامترها یا علائم غیرضروری برای کارکرد و اجرای پودمان اجتناب کنند.

سطح امنیتی ۴

علاوه بر الزامات برای سطوح امنیت ۱، ۲ و ۳، الزامات زیر باید [11.27] shall در پودمان‌های رمزنگاری برای سطح امنیتی ۴ استفاده‌شوند:

- برای هر مولفه سخت‌افزار یا نرم‌افزار پودمان رمزنگاری، مستندسازی باید [11.28] shall با نظراتی تفسیرشود که (۱) پیش‌شرایط لازم برای ورودی را در هر مولفه پودمان، تابع و رویه تعیین کنند تا به درستی اجراکنند و (۲) هنگامی‌که اجرای هر مولفه پودمان، تابع و رویه، کامل است، پس‌شرایط مورد انتظار صحیح باشد. پیش‌شرایط و پس‌شرایط ممکن است با استفاده از هر نشان‌گذاری که به‌طور کامل جز به جز تفصیل شده‌اند، مشخص‌شوند و بدون ابهام، رفتار مولفه پودمان رمزنگاری، تابع و رویه را شرح می‌دهند.

۷-۱۱-۶ آزمون ارائه‌دهنده

این بند الزاماتی را برای *آزمون ارائه‌دهنده* پودمان رمزنگاری تعیین‌می‌کند که شامل موارد زیر است:
آزمون تابع امنیتی پیاده‌سازی شده در پودمان رمزنگاری، ایجاد اطمینانی که وضعیت‌های پودمان رمزنگاری مطابق خط‌مشی امنیت پودمان و مشخصات کارکردی می‌باشند.

سطوح امنیت ۱ و ۲

برای سطوح امنیت ۱ و ۲، مستندسازی باید [11.29] shall آزمون کارکردی انجام‌شده بر روی پودمان رمزنگاری را تعیین‌کند.
برای پودمان‌های رمزنگاری نرم‌افزار یا ثابت‌افزار و مولفه نرم‌افزار یا ثابت‌افزار یک پودمان ترکیبی، ارائه‌دهنده باید [11.30] shall از ابزارهای عیب‌یابی خودکار استفاده‌کند (برای مثال، کشف سرریزی بافر).

سطوح امنیت ۳ و ۴

علاوه بر الزامات برای سطوح امنیت ۱ و ۲، مستندسازی باید [11.31] shall رویه‌هایی را برای نتایجی از آزمون سطح پایین تعیین‌کند که بر روی پودمان رمزنگاری انجام شده‌اند.

۷-۱۱-۷ تحویل و عملیات

این بند الزامات امنیتی را برای تحویل امن، نصب و راه‌اندازی یک پودمان رمزنگاری تعیین‌می‌کند که اطمینان‌می‌دهد این پودمان با اطمینان به متصدیان مجاز تحویل‌می‌شود و به روش صحیح و امن نصب و مقداردهی اولیه می‌شود.

سطح امنیتی ۱

برای سطح امنیتی ۱، مستندسازی باید [11.32] shall روش‌هایی را برای نصب امن، مقداردهی اولیه و راه‌اندازی پودمان رمزنگاری تعیین‌کند.

سطح امنیتی ۲ و ۳

علاوه بر الزامات سطح امنیتی ۱، مستندسازی باید [11.33] shall رویه‌های لازم برای حفاظت از امنیت را در طی توزیع، نصب و مقداردهی اولیه نسخه‌های یک پودمان رمزنگاری برای متصدیان مجاز تعیین‌کند. این رویه‌ها باید [11.34] shall تعیین‌کنند که چگونه مداخله را در طی تحویل، نصب و مقداردهی اولیه پودمان برای متصدیان مجاز کشف‌کنند.

سطح امنیتی ۴

علاوه بر الزامات سطوح امنیت ۱، ۲، ۳، رویه‌ها باید [11.35] shall به یک متصدی مجاز نیازداشته‌باشند تا پودمان را با استفاده از داده‌های اصالت‌سنجی‌شده، توسط ارائه‌دهنده اصالت‌سنجی‌کنند.

۷-۱۱-۸ پایان عمر

این بند الزامات امنیتی را زمانی تعیین‌می‌کند که یک پودمان رمزنگاری دیگر توسعه‌نمی‌یابد یا برای کاربرد بعدی توسط اپراتور، در نظر گرفته نمی‌شود.

سطوح امنیت ۱ و ۲

برای سطح امنیتی ۱ و ۲، مستندسازی باید [11.36] shall رویه‌هایی را برای حفاظت امن پودمان رمزنگاری تعیین‌کند. نگهداری عبارتست از فرآیند خارج‌کردن اطلاعات حساس (برای مثال، SSPها، داده کاربر و غیره) از پودمان، بنابراین ممکن است به متصدیان دیگر توزیع یا تنظیم‌شود.

سطوح امنیت ۳ و ۴

علاوه بر الزامات سطوح امنیت ۱ و ۲، مستندسازی باید [11.37] shall رویه‌های لازم را برای تخریب این پودمان تعیین کنند.

۷-۱۱-۹ اسناد راهنمایی

الزامات در این بند اطمینان‌می‌دهند که تمام هستارها با استفاده از پودمان رمزنگاری، به‌اندازه کافی، راهنما و رویه‌های دارند تا پودمان را در یک حالت تاییدشده عملیات، مدیریت‌کنند و از آن استفاده‌نمایند.

مستندسازی راهنما شامل راهنمایی مدیر و غیرمدیر می‌باشد.

راهنمای مدیر باید [11.38] shall تعیین‌کند که:

- کارکردهای مدیریتی، رخدادهای امنیت، پارامترهای امنیت (و مقادیر پارامتر، اگر مناسب باشد) درگاه‌های فیزیکی و واسط‌های منطقی پودمان رمزنگاری موجود در نقش‌های مسوول رمز و یا نقش‌های مدیریتی دیگر؛
- روش‌های لازم برای حفظ سازوکارهای اصالت‌سنجی متصدی مستقل که به‌طور کارکردی مستقل است؛
- رویه‌هایی برای این‌که پودمان رمزنگاری، در یک حالت تاییدشده چگونه عملیات را مدیریت‌می‌کند؛ و
- فرض‌های مربوط به رفتار کاربر که به عملیات امن پودمان رمزنگاری مرتبط است.

راهنمای غیرمدیر باید shall [11.39] تعیین‌کند:

- توابع امنیت تاییدشده و تاییدنشده، درگاه‌های فیزیکی و واسط‌های منطقی موجود برای کاربران یک پودمان رمزنگاری؛ و
- تمام مسئولیت‌های لازم کاربر برای حالت تاییدشده عملیات یک پودمان رمزنگاری.

۷-۱۲ کاهش حملات دیگر

قرارگرفتن یک پودمان رمزنگاری در معرض خطر حملات که در جای دیگر در این استاندارد تعریف‌نشده است، به نوع پودمان، پیاده‌سازی و محیط اجرا بستگی‌دارد. این حملات ممکن است اهمیت خاصی برای پودمان‌های رمزنگاری داشته‌باشند که در محیط‌های میزبان اجراشده‌اند (برای مثال، جایی‌که حمله‌کننده‌ها ممکن است متصدیان مجاز پودمان باشند). این حملات به‌طور کلی به تحلیل اطلاعاتی وابسته هستند که از منابعی به‌دست‌آمده‌اند که به‌طور فیزیکی خارج از پودمان می‌باشند. در تمام حالت‌ها، حملات سعی می‌کنند تا دانشی در مورد CSPهای درون پودمان رمزنگاری را تعیین کنند.

الزامات مستندسازی تعیین‌شده در پیوست الف-۲-۱۲ باید shall [12.01] فراهم‌شوند.

سطوح امنیت ۱، ۲ و ۳

اگر یک پودمان رمزنگاری طراحی‌شود تا یک یا چند حمله خاص را کاهش‌دهد که در جای دیگر این استاندارد تعریف‌نشده‌اند، آنگاه اسناد پشتیبانی پودمان باید shall [12.02] حمله (ها)یی را بشمارند که این پودمان برای کاهش طراحی‌می‌شود. هنگامی‌که الزامات و آزمون‌های مربوطه تهیه می‌شوند، وجود و کارکرد مناسب سازوکارهای امنیت که برای کاهش حملات به کار رفته‌اند صحه‌گذاری خواهدشد.

سطح امنیتی ۴

علاوه بر الزامات برای سطوح امنیت ۱، ۲، ۳، الزامات زیر باید shall [12.03] در پودمان‌های رمزنگاری برای سطوح امنیت ۴ به‌کاربرده شوند:

- اگر کاهش حملات خاص که در جای دیگری از این استاندارد تعریف‌نشده‌اند درخواست‌شود، مستندسازی باید shall [12.04] روش‌هایی را تعیین‌کند که حملات را کاهش‌دهد و روش‌هایی را نیز برای تعیین اثربخشی روش‌های کاهش حملات، آزمون‌کند.

پیوست الف
(الزامی)
الزامات مستندسازی

الف-۱ هدف

این پیوست حداقل مستندسازی را مشخص‌می‌کند که باید shall [A.01] برای یک پودمان رمزنگاری لازم باشد که در یک طرح تحقیق مستقل قرارمی‌گیرد.

الف-۲ اقلام

الف-۲-۱ کلیات

هیچ الزامات مستندات کلی مشخص‌نشده‌است.

الف-۲-۲- ویژگی‌های پودمان رمزنگاری

- ویژگی نوع پودمان (سخت‌افزار، نرم‌افزار، ثابت‌افزار، پودمان نرم‌افزار ترکیبی یا ثابت‌افزار ترکیبی). (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی حد و مرز پودمان (سطوح امنیت ۱، ۲، ۳ و ۴)
- ویژگی مولفه‌های سخت‌افزار، نرم‌افزار و ثابت‌افزار پودمان رمزنگاری و شرح پیکربندی فیزیکی پودمان (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی مولفه‌های سخت‌افزار، نرم‌افزار یا ثابت‌افزار پودمان رمزنگاری که محروم از الزامات امنیتی این استاندارد و یک شرح توجیه برای استثنا، هستند (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی درگاه‌های فیزیکی و واسط‌های منطقی یک پودمان رمزنگاری (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی کنترل‌های دستی یا منطقی یک پودمان رمزنگاری، نشانه‌های وضعیت فیزیکی یا منطقی و مشخصه‌های فیزیکی، منطقی و الکتریکی کاربردپذیر (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی تمام توابع امنیت تاییدشده و تاییدنشده، که توسط یک پودمان رمزنگاری و ویژگی تمام حالت‌های عملیات تاییدشده و تاییدنشده، به‌کاربرده می‌شوند. (سطوح امنیت ۱، ۲، ۳ و ۴).
- نمودار بلوکی که تمام مولفه‌های اصلی سخت‌افزاری یک پودمان رمزنگاری و اتصال‌های درونی مولفه را به تصویر می‌کشد، که شامل تمام ریزپردازنده‌ها، بافرهای ورودی/ خروجی، بافرهای متن ساده/ متن رمزشده، بافرهای کنترل، ذخیره‌سازی کلید، حافظه کار و حافظه برنامه می‌باشد. (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی طراحی سخت‌افزار، نرم‌افزار و ثابت‌افزار یک پودمان رمزنگاری (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی تمام اطلاعات مربوط به امنیت، از جمله کلیدهای رمزنگاری خصوصی و محرمانه (هم متن ساده و هم متن رمزشده)، داده‌های اصالت‌سنجی (برای مثال، اسم رمزها، PINها)، CSPها، PSPها و اطلاعات حفاظت‌شده دیگر (برای مثال، رخدادهای بازرسی شده، داده بازرسی) که آشکارسازی یا اصلاح آنها ممکن است امنیت پودمان رمزنگاری را به‌خطر بیاندازد (سطوح امنیت ۱، ۲، ۳ و ۴).

- ویژگی چگونگی پشتیبانی یک پودمان از یک حالت تخریب‌شده عملیات (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی یک خط‌مشی امنیت پودمان رمزنگاری شامل قواعد مشتق‌شده از الزامات این استاندارد و قواعد مشتق‌شده از هر الزامات اضافی که توسط ارائه‌دهنده اعمال‌شده‌است (سطوح امنیت ۱، ۲، ۳ و ۴).

الف-۲-۳ واسط‌های پودمان رمزنگاری

- ویژگی ورودی داده، خروجی داده، ورودی کنترل، خروجی کنترل، خروجی وضعیت و واسط‌های توان، هم فیزیکی و هم منطقی (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی موارد استثنا و استدلال اگر واسط خروجی کنترل در طی وضعیت خطا ممانعت‌نشود (سطوح امنیت ۱، ۲، ۳ و ۴).

الف-۲-۴ نقش‌ها، خدمات و اصالت‌سنجی

- ویژگی تمام نقش‌های معتبر که با یک پودمان رمزنگاری پشتیبانی شده است (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی خدمات، عملیات‌ها یا توابع تهیه‌شده توسط یک پودمان رمزنگاری، تاییدشده و تاییدنشده. برای هر خدمت، مشخصه ورودی خدمت، خروجی خدمت متناظر و نقش(های) مجاز که در آن خدمت را می‌توان انجام‌داد (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی هر خدمت فراهم‌شده توسط پودمان رمزنگاری که برای آن خدمت متصدی لازم نیست تا نقش مجاز داشته‌باشد و این‌که چگونه این خدمات، کلیدهای رمزنگاری و سایر CSPها را اصلاح، آشکار یا جایگزین نمی‌کنند یا به عبارت دیگر بر امنیت پودمان اثر می‌گذارند (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی سازوکارهای اصالت‌سنجی پشتیبانی‌شده توسط یک پودمان رمزنگاری، انواع داده اصالت‌سنجی مورد نیاز برای انجام سازوکارهای اصالت‌سنجی پشتیبانی‌شده، روش‌های مجاز به‌کاربرده‌شده برای دسترسی کنترل به پودمان برای اولین بار و شروع سازوکار اصالت‌سنجی، و تقویت سازوکارهای اصالت‌سنجی پشتیبانی‌شده با پودمان، از جمله استدلالی که کاربرد چند سازوکار اصالت‌سنجی را پشتیبانی‌می‌کند (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی خدمات پودمان که اطلاعات نسخه‌ای پودمان را نشان می‌دهند، وضعیت را نشان می‌دهند، خودآزمایی‌ها را انجام می‌دهند، توابع امنیت تاییدشده و صفرکردن را انجام می‌دهند (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی سازوکارهای کنارگذار (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی سازوکارهای بارگذاری نرم‌افزار یا ثابت‌افزار (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی کنترل‌ها و واسط توانایی خروجی رمزنگاری خودراه‌انداز (سطوح امنیت ۱، ۲، ۳ و ۴).

الف-۲-۵ امنیت نرم‌افزار / ثابت‌افزار

- ویژگی روش‌های یکپارچگی تاییدشده (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی روشی برای متصدی برای انجام روش یکپارچگی تاییدشده بر روی تقاضا (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی شکل کد اجرایی (سطوح امنیت ۲، ۳ و ۴).

الف-۲-۶ محیط عملیاتی

- ویژگی محیط عملیاتی برای یک پودمان رمزنگاری، از جمله سامانه عامل به‌کارگرفته‌شده توسط پودمان رمزنگاری (اگر کاربردپذیر باشد) (سطوح امنیت ۱ و ۲).
- ویژگی قواعد امنیت، تنظیمات یا محدودیت‌ها در پیکربندی محیط عملیاتی (سطوح امنیت ۱ و ۲).
- مستندات راهنمایی مدیر برای پیکربندی سامانه عامل مطابق با الزامات ویژگی (سطح امنیتی ۲).

الف-۲-۷ امنیت فیزیکی

- ویژگی نمایش کیفیت فیزیکی و سطح امنیتی که برای آن، سازوکارهای امنیت فیزیکی یک پودمان رمزنگاری پیاده‌سازی‌می‌شوند. ویژگی سازوکارهای امنیت فیزیکی که توسط یک پودمان به‌کاربرده می‌شوند (سطوح امنیت ۱، ۲، ۳ و ۴).
- اگر یک پودمان رمزنگاری شامل نقش نگهداری باشد که به دسترسی فیزیکی محتوای پودمان نیاز دارد یا اگر پودمان طراحی شود تا اجازه دسترسی فیزیکی دهد، ویژگی واسط دسترسی نگهداری و چگونگی صفرکردن CSPها هنگامی‌که واسط دسترسی نگهداری در دسترس باشد (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی محدوده‌های عملیاتی عادی یک پودمان رمزنگاری. ویژگی مشخصات حفاظت خرابی محیطی به‌کارگرفته‌شده توسط یک پودمان رمزنگاری یا ویژگی آزمون‌های خرابی محیطی انجام‌شده (سطح امنیتی ۴).
- ویژگی روش‌های کاهش القا خرابی به‌کاربرده شده است (سطح امنیتی ۴).

الف-۲-۸ امنیت غیرتهاجمی

- ویژگی روش‌های کاهش به‌کاربرده‌شده در مقابل حملات غیرتهاجمی از جمله آنهایی که در پیوست «ج» تعیین‌شده‌اند (سطوح امنیت ۱، ۲، ۳ و ۴).
- شاهد اثربخشی هر روش کاهش حمله به‌کاربرده شده (سطوح امنیت ۱، ۲، ۳ و ۴).

الف-۲-۹ مدیریت پارامتر امنیت حساس

- ویژگی تمام CSPها و PSPهای به‌کاربرده‌شده توسط یک پودمان رمزنگاری (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی تمام RBGها و کاربرد آنها (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی حداقل انتروپی لازم توسط پودمان برای هر پارامتر ورودی انتروپی واردشده (سطوح امنیت ۱، ۲، ۳ و ۴).

- ویژگی هر RBG (تاییدشده و تاییدنشده و منابع انتروپی) که توسط یک پودمان رمزنگاری به‌کارگرفته‌شده است (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی حداقل انتروپی و روش تولید حداقل انتروپی درخواست‌شده اگر انتروپی از داخل حد و مرز رمزنگاری پودمان رمزنگاری جمع‌آوری‌شود (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی هر روش تولید SSP که از یک RBG استفاده‌می‌کند (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی تمام روش‌های برقرارشده SSP که توسط یک پودمان به‌کارگرفته‌شده است (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی هر روش تولید SSP که با یک پودمان به‌کاربرده شده است (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی هر روش تولید کلید (تاییدشده و تاییدنشده) که با یک پودمان رمزنگاری به‌کاربرده شده است (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی روش‌های اسقرار SSP که توسط یک پودمان رمزنگاری به‌کارگرفته‌شده است (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی روش‌های ورودی و خروجی SSP که توسط یک پودمان به‌کارگرفته‌شده است (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی ورودی کلید و روش‌های خروجی که توسط یک پودمان رمزنگاری به‌کارگرفته‌شده است (سطوح امنیت ۱، ۲، ۳ و ۴).
- اگر رویه‌های دانش تقسیمی استفاده‌شوند، مستندسازی فراهم‌شده برای اثبات این است که اگر دانش مولفه‌های n لازم است تا CSP اصلی را بازسازی کند، سپس دانش همه مولفه های n-1 هیچ اطلاعاتی را در مورد CSP اصلی غیر از طول فراهم نمی‌کند (سطوح امنیت ۳ و ۴).
- ویژگی رویه‌های دانش تقسیمی که توسط یک پودمان رمزنگاری به‌کارگرفته‌شده است (سطوح امنیت ۳ و ۴).
- ویژگی SSPهای ذخیره‌شده در پودمان (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی چگونه CSPها از دسترسی غیرمجاز محافظت می‌شوند، و هنگامی‌که در پودمان ذخیره می‌شوند، از استفاده، آشکارسازی، اصلاح و جایگزینی محافظت می‌شوند (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی چگونگی محافظت PSPها از اصلاح و جایگزینی غیرمجاز هنگامی‌که در داخل پودمان ذخیره‌می‌شوند (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی این‌که چگونه پودمان، یک PSP ذخیره‌شده در پودمان را با هستار (متصدی، نقش یا فرآیند)، همکاری‌می‌دهد که در آن پارامتری اختصاص‌داده‌می‌شود (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی روش(های) صفرکردن به‌کارگرفته شده توسط یک پودمان و دلیل این‌که چگونه این روش‌ها از بازیابی و استفاده مجدد مقادیر صفرشده جلوگیری‌می‌کنند (سطوح امنیت ۱، ۲، ۳ و ۴).

الف-۲-۱۰ خودآزمایی‌ها

- ویژگی خودآزمایی‌های انجام‌شده توسط یک پودمان رمزنگاری از جمله آزمون‌های پیش‌عملیاتی و شرطی (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی موفقیت خودآزمایی و نشانه وضعیت خرابی (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی وضعیت‌های خطا که یک پودمان رمزنگاری می‌تواند واردکند هنگامی‌که خودآزمایی شکست‌می‌خورد و شرایط و عمل‌های لازم برای خروج از وضعیت‌های خطا و ازسرگیری عملیات عادی یک پودمان رمزنگاری (برای مثال، این ممکن است شامل نگهداری پودمان، توان‌گیری دوباره پودمان، بازیابی پودمان خودکار، ورود به عملیات تخریب‌شده یا بازگشت پودمان به ارائه‌دهنده برای خدمات، باشد). (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی تمام توابع امنیت بحرانی در عملیات امن یک پودمان رمزنگاری و شناسایی آزمون‌های توان ـ بالای کاربردپذیر و آزمون‌های شرطی انجام‌شده با پودمان (سطوح امنیت ۱، ۲، ۳ و ۴).
- اگر پودمان رمزنگاری یک توانایی کنارگذار را پیاده‌سازی‌کند، ویژگی سازوکار یا منطقی که رویه راه‌گزینی را نظارت‌می‌کند (سطوح امنیت ۱، ۲، ۳ و ۴).

الف-۲-۱۱ اطمینان چرخه عمر

- ویژگی سامانه مدیریت پیکربندی که برای پودمان رمزنگاری، به‌کاربرده‌شده است. (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی مستندات پشتیبانی برای توسعه پودمان رمزنگاری و اسناد مربوطه که توسط سامانه مدیریت پیکربندی فراهم‌شده‌است. (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی رویه‌ها برای نصب، تولید و راه‌اندازی امن یک پودمان رمزنگاری (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی رویه‌هایی برای حفاظت از امنیت در حالی‌که نسخه‌های یک پودمان رمزنگاری به متصدیان مجاز توزیع و ارسال می‌شود.
- ویژگی مطابقت بین طراحی مولفه‌های سخت‌افزار، نرم‌افزار یا ثابت‌افزار یک پودمان رمزنگاری و خط‌مشی امنیت پودمان رمزنگاری و FSM) (سطوح امنیت ۱، ۲، ۳ و ۴).
- اگر یک پودمان رمزنگاری شامل نرم‌افزار باشد، ویژگی کد منبع برای نرم‌افزار، با توضیحاتی تفسیرمی‌شود که به‌طور واضح مطابقت نرم‌افزار را در طراحی پودمان به تصویر می‌کشد (سطوح امنیت ۱، ۲، ۳ و ۴).
- اگر یک پودمان رمزنگاری شامل سخت‌افزار باشد، ویژگی طرح کلی و / یا فهرست‌های HDL سخت‌افزاری می‌باشد (سطوح امنیت ۱، ۲، ۳ و ۴).
- ویژگی یک ویژگی کارکردی که به‌طور یکنواخت پودمان رمزنگاری، کارکرد پودمان رمزنگاری، درگاه‌های فیزیکی خارجی و واسط‌های منطقی پودمان رمزنگاری و هدف درگاه‌های فیزیکی و واسط‌های منطقی را شرح‌می‌دهد (سطوح امنیت ۲، ۳ و ۴).

- ویژگی طراحی دقیق که کارکرد داخلی مولفه‌های اصلی پودمان رمزنگاری، واسط‌های مولفه داخلی، مصرف واسط‌های مولفه و جریان اطلاعات داخلی را شرح‌می‌دهد (در حد و مرز رمزنگاری به‌طور کلی و همچنین در داخل مولفه‌های اصلی) (سطوح امنیت ۳ و ۴).
- ویژگی (از جمله پیش‌شرایط و پس‌شرایط) مطابقت بین طراحی پودمان رمزنگاری و ویژگی کارکردی (سطح امنیتی ۴).
- ویژگی FSM (یا معادل) با استفاده از یک نمودار انتقال وضعیت و جدول انتقال وضعیت که شامل موارد زیر می‌باشد (سطوح امنیت ۱، ۲، ۳ و ۴):
  - وضعیت‌های عملیاتی و خطای یک پودمان رمزنگاری
  - انطباق انتقال‌ها از یک وضعیت به وضعیت دیگر
  - رخدادهای ورودی، از جمله ورودی‌های داده و ورودی‌های کنترل، که باعث انتقال‌ها از یک وضعیت به وضعیت دیگر می‌شوند و
  - رخدادهای خروجی، از جمله شرایط پودمان داخلی، خروجی‌های داده و خروجی‌های وضعیت که از انتقال‌ها از یک وضعیت به وضعیت دیگر حاصل‌می‌شوند.
- ویژگی یک منبع برای نرم‌افزار یا ثابت‌افزار (سطوح امنیت ۱، ۲، ۳ و ۴).
- برای هر مولفه سخت‌افزار و نرم‌افزار، تفسیر کد منبع با توضیحاتی که مشخص‌می‌کند (۱) پیش‌شرایط که با ورود به مولفه پودمان، تابع یا رویه برای اجرای درست، لازم‌بوده‌است و (۲) پس‌شرایط که باید صحیح باشد هنگامی‌که اجرای مولفه پودمان، تابع یا رویه کامل است (سطح امنیتی ۴).
- برای راهنمایی مدیر، ویژگی‌های زیر (سطوح امنیت ۱، ۲، ۳ و ۴).
  - توابع مدیریتی، رخدادهای امنیت، پارامترهای امنیت (و مقادیر پارامتر، اگر مناسب است) درگاه‌های فیزیکی و واسط‌های منطقی پودمان رمزنگاری که برای مسوول رمز در دسترس است.
  - رویه‌هایی در مورد این‌که چگونه پودمان رمزنگاری به روش امن مدیریت شود و
  - فرض‌هایی که رفتار کاربر که به عملیات امن پودمان رمزنگاری مربوط‌می‌شود را درنظرمی‌گیرد.
- برای راهنمایی غیرمدیر، ویژگی‌های زیر (سطوح امنیت ۱، ۲، ۳ و ۴):
  - توابع امنیت تاییدشده، درگاه‌های فیزیکی و واسط‌های منطقی در دسترس کاربران پودمان رمزنگاری می‌باشد و
  - تمام مسئولیت‌های کاربر برای عملیات امن پودمان لازم هستند.

الف-۲-۱۲ کاهش حملات دیگر

- اگر یک پودمان رمزنگاری طراحی‌شود تا یک یا چند حمله خاص را کاهش‌دهد که در جای دیگری از این استاندارد تعریف‌نشده‌است، در مستندسازی پودمان، سازوکارهای امنیت به‌کارگرفته‌شده توسط پودمان رمزنگاری برای کاهش حملات را به‌شمارآورید. (سطوح امنیت ۱، ۲ و ۳).

- اگر یک پودمان رمزنگاری طراحی‌شود تا یک یا چند حمله خاص را کم‌کند که در جای دیگر این استاندارد تعریف‌نشده‌است، روش‌های به‌کاررفته برای کاهش حملات و روش‌های آزمون اثربخشی روش‌های کاهش را مستندکنید. (سطوح امنیت ۴).

پیوست ب
(الزامی)
خط‌مشی امنیت پودمان رمزنگاری

ب-۱ کلیات

فهرست زیر الزاماتی را خلاصه می‌کند که باید shall [B.01] در خط‌مشی امنیت غیراختصاصی تهیه‌شود. قالب خط‌مشی امنیت باید shall [B.02] به ترتیبی که در این پیوست است نشان‌داده‌شود و همان‌طور که توسط یک مقام ذیصلاح صحه‌گذاری تعیین‌شده‌است، خط‌مشی امنیت نباید shall not [B.03] با عنوان اختصاصی یا حق نسخه‌برداری بدون عبارتی مشخص‌شود که اجازه نسخه‌برداری یا توزیع را می‌دهد.

ب-۲ اقلام

ب-۲-۱ کلیات

- یک جدول، سطوح بند فردی و سطوح عمومی را نشان‌می‌دهد.

ب-۲-۲ ویژگی پودمان رمزنگاری

- هدف موردنظر یا کاربرد پودمان شامل محیط کاربرد موردنظر می‌باشد.
- نمودار توضیح‌دهنده، طرح کلی یا تصویری از پودمان. یک تصویر شامل پودمان‌های سخت‌افزار است. اگر خط‌مشی امنیت چند نسخه از پودمان را احاطه‌کند، هر نسخه به‌طور جداگانه نشان‌داده‌می‌شود یا تفسیرمی‌شود که این نمونه نمایشی، برای تمام نسخه‌ها شرح‌داده‌می‌شود. برای یک پودمان رمزنگاری نرم‌افزار یا ثابت‌افزار، خط‌مشی امنیت شامل یک نمودار بلوکی است که شرح‌می‌دهد:
  - موقعیت شی منطقی پودمان نرم‌افزار یا ثابت‌افزار با توجه به سامانه عامل، کاربردهای پشتیبانی دیگر و حد و مرز رمزنگاری به‌طوری که تمام لایه‌های منطقی و فیزیکی بین شی منطقی و حد و مرز رمزنگاری به‌طور واضح تعریف‌می‌شوند و
  - تراکنش‌های شی منطقی، پودمان نرم‌افزار یا ثابت‌افزار با سامانه عامل و کاربردهای پشتیبانی دیگر در داخل حد و مرز رمزنگاری قرارمی‌گیرد.
- توصیف پودمان(ها):
  - تهیه نسخه/ شناسایی پودمان‌ها و تمام مولفه‌ها (سخت‌افزار، نرم‌افزار یا ثابت‌افزار).
- تعیین سخت‌افزار، نرم‌افزار، ثابت‌افزار یا ترکیبی:
  - برای پودمان‌های رمزنگاری نرم‌افزار، ثابت‌افزار و ترکیبی، سامانه‌های عامل را فهرست‌کنید که این پودمان بر روی آن آزمون‌شده‌است و سامانه‌های عامل را فهرست‌کنید که ارائه‌دهنده تأیید می‌کند که می‌توان با پودمان استفاده کرد.
- درجه‌بندی امنیت کلی پودمان و سطوح امنیت نواحی فردی.
- تعریف دقیق حدود رمزنگاری و فیزیکی پودمان:

- سخت‌افزار، نرم‌افزار یا ثابت‌افزار از حدود رمزنگاری در خط‌مشی امنیت تعیین‌شده، مستثنی‌شده‌اند.

- حالت‌های عملیات و چگونگی ورود / خروج از هر حالت. خط‌مشی امنیت هر حالت تاییدشده عملیات را که در پودمان رمزنگاری اجراشده‌اند و این‌که چگونه هر حالت پیکربندی‌می‌شود را شرح‌می‌دهد.
- توصیف عملیات تخریب‌شده.
- جدول تمام توابع امنیت، با قدرت کلید معین که برای خدمات تاییدشده است و همچنین حالت‌های پیاده‌سازی‌شده عملیات (برای مثال، CBC، CCM) اگر مناسب باشد.
- نمودار بلوکی، هنگامی‌که کاربردی است.
- الزامات مقداردهی اولیه، اگر کاربردی باشد.

ب-۲-۳ واسط‌های پودمان رمزنگاری

- جدول فهرست تمام درگاه‌ها و واسط‌ها (فیزیکی و منطقی).
- تعریف اطلاعاتی که بر روی پنج واسط منطقی تاییدمی‌شوند.
- تعیین درگاه‌های فیزیکی و داده‌هایی که بر روی آنها عبور می‌کنند.
- تعیین کانال قابل‌اعتماد.
- ویژگی استثناها و منطق اگر واسط خروجی کنترل در طی وضعیت خطا منع‌نشود.

ب-۲-۴ نقش‌ها، خدمات و اصالت‌سنجی

- تعیین همه نقش‌ها
- جدول نقش‌ها، با مطابقت دستورات خدمت با ورودی و خروجی.
- تعیین هر روش اصالت‌سنجی، چه این روش هویت‌محور باشد یا نقش‌محور و این روش لازم است.
- چگونه قدرت الزامات اصالت‌سنجی برآورده‌می‌شود؟
- اگر یک توانایی کنارگذار وجود دارد، دو عمل مستقل و جدا چه هستند و چگونه وضعیت بررسی‌می‌شود؟
- اگر یک توانایی خروجی رمزنگاری خودراه‌انداز وجود دارد، دو عمل مستقل چه هستند و چگونه وضعیت نشان داده می‌شود؟
- اگر نرم‌افزار یا ثابت‌افزار خارجی بارگذاری شود، کنترل‌ها را بر روی بارگیری و جداسازی کدی تعیین کنید که دسترسی غیرمجاز و کاربرد پودمان را مانع‌شود.
- فهرست جداگانه خدمات امنیت و غیرامنیت تاییدشده و تاییدنشده.
- برای هر خدمت، نام خدمت، یک شرح دقیق هدف و/ یا استفاده خدمت (نام خدمت ممکن است در بعضی نمونه‌ها، این اطلاعات را بدهد)، فهرستی از توابع امنیت تاییدشده (الگوریتم‌ها، روش‌های مدیریت کلید یا روش اصالت‌سنجی) که از طریق فراخوانی خدمت پیاده‌سازی‌شده‌است و فهرستی از SSPهای مربوط به خدمت با توابع امنیت تاییدشده‌ای که استفاده‌می‌کند. برای هر نقش متصدی

مجاز در استفاده از اطلاعات خدمت و شرح حقوق دسترسی فردی به تمام SSPها و اطلاعات روش کاربردی را شرح‌دهید تا هر نقش را اصالت‌سنجی کند.

- شرح فرآیند تأسیسات و سازوکارهای اصالت‌سنجی رمزنگاری.

ب-۲-۵ امنیت نرم‌افزار / ثابت‌افزار

- تعیین روش‌های یکپارچگی تاییدشده که به‌کاربرده‌شده‌است.
- تعیین این‌که چگونه متصدی می‌تواند آزمون یکپارچگی را طبق تقاضا شروع‌کند.
- تعیین شکل و هر مولفه‌ای که از کد اجرایی تهیه‌شده‌است.
- اگر پودمان منبع باز باشد، مترجم‌ها و پارامترهای کنترل لازم است تا کد را در قالب اجرایی کامپایل‌کند.

ب-۲-۶ محیط عملیاتی

- شناسایی محیط عملیاتی (برای مثال، غیرقابل تغییر، محدود یا قابل تغییر)
- شناسایی سامانه‌های عامل و بسترهای آزمایش شده.
- برای هر سطح کاربردی، توضیح این‌که چگونه الزامات مورد قبول هستند.
- ارائه‌دهنده ممکن است ادعای واردشدن به سایر سامانه‌های عاملی را کند که تاکنون به‌طور مشخص صحت عملکردشان آزمون‌نشده‌است.
- ویژگی قواعد امنیت، تنظیمات یا محدودیت‌ها در پیکربندی محیط عملیاتی.
- ویژگی هر محدودیتی در پیکربندی محیط عملیاتی.

ب-۲-۷ امنیت فیزیکی

- تعیین نمایش کیفیت (تک‌تراشه‌ای، چندتراشه‌ای جاسازی‌شده یا چندتراشه‌ای مستقل).
- تعیین سازوکارهای امنیت فیزیکی که در پودمان پیاده‌سازی می‌شوند (برای مثال، شواهد مداخله، مهرها، قفل‌ها، پاسخ مداخله و سوئیچ‌های صفرکردن و هشدارها).
- تعیین عمل‌های لازم توسط متصدیان برای اطمینان از این‌که امنیت فیزیکی حفظ‌می‌شود (برای مثال، نظارت و بازبینی دوره‌ای مهرهای شواهد مداخله یا آزمون پاسخ مداخله و سوئیچ‌های صفرکردن).
  - تعیین اطلاعات زیر اگر پودمان نیاز به متصدیی دارد که از مهرهای شواهد مداخله یا وسایل امنیتی استفاده‌می‌کند که متصدی در چرخه عمر پودمان به کار می‌برد یا اصلاح می‌کند: تصویر مرجع یا شرح‌های لازم در پیوست ب-۲-۲ پودمانی را نشان می‌دهند که پیکربندی‌شده‌است یا ساخته‌شده‌است همان‌طور که تعیین‌شده‌است. تصاویر/ شرح‌های اضافی ممکن است تهیه‌شوند تا پیکربندی‌های دیگری را نشان‌دهند.
  - اگر صفحه‌های پرکننده لازم باشند تا شکاف‌ها یا دهانه‌های پرنشده را پوشش‌دهند تا الزامات تیرگی را مطابقت‌دهند، آنها در تصویر یا شرح‌ها با مهرهای مداخله‌کننده می‌مانند که در شرایط لازم تثبیت شده‌اند. صفحه‌های پرکننده در فهرست قسمت‌ها وارد می‌شوند.

- تصاویر یا شرح‌ها، موقعیت دقیق هر مهر شواهد مداخله یا وسیله امنیتی لازم را نشان‌می‌دهند تا الزامات امنیتی فیزیکی را تطبیق‌دهند.
- تعداد کل مهرهای شواهد مداخله یا وسایل امنیت که لازم هستند، نشان‌داده‌می‌شوند (برای مثال، ۵ مهر شواهد مداخله و ۲ صفحه تیرگی). تصاویر و شرح‌هایی که دستور موقعیت دقیق را می‌دهند، هر قلم شمارش شده در تصویر یا شرح را دارند و معادل تعداد کل نشان داده شده است (مهرهای شواهد مداخله واقعی یا وسایل امنیت لازم نیستند تا شمارش شوند).
- اگر مهرهای شواهد مداخله یا وسایل امنیت، قسمت‌هایی هستند که می‌توانند بار دیگر از ارائه‌دهنده پودمان مرتب‌شوند، خط‌مشی امنیت، شماره قسمت ارائه‌دهنده پودمان مهر، وسایل امنیت یا جعبه[1] امنیت کاربردی را نشان‌می‌دهد. پس از پیکربندی، متصدی پودمان ممکن است لازم باشد تا حذف‌کند و مهرهای شواهد مداخله جدید یا وسایل امنیت را وارد کند.
- تعیین نقش متصدی مسئول برای امنیت و کنترل‌داشتن همیشگی بر تمام مهرهای غیرکاربردی و کنترل مستقیم و مشاهده هر تغییری در پودمان از قبیل پیکربندی مجدد اگر مهرهای شواهد مداخله یا وسایل امنیت حذف یا نصب شوند تا امنیت پودمان حفاظت‌شده را در طی تغییرات تضمین‌کنند و پودمان به وضعیت تاییدشده FIPS برگردد.
- اگر مهرهای شواهد مداخله یا وسایل امنیت را بتوان حذف یا نصب‌کرد، با توجه به چگونگی سطح یا افزاره باید دستورات مشخصی تهیه‌شود تا از یک مهر شواهد مداخله جدید یا وسیله امنیتی استفاده‌کنند.

- تعیین روش‌های کاهش القا خرابی که پیاده‌سازی‌شده است.

ب-۲-۸ امنیت غیرتهاجمی

- تعیین تمام روش‌های کاهش غیرتهاجمی که در پیوست «ج» مراجعه‌شده‌است توسط پودمان به‌کاربرده‌شده‌است تا از CSPهای پودمان در برابر حملات غیرتهاجمی حفاظت‌کند.
- شرح اثربخشی روش‌های غیرتهاجمی مراجعه‌شده در پیوست «ج» که توسط پودمان به‌کاربرده‌شده‌است تا از CSPهای پودمان در برابر حملات غیرتهاجمی محافظت‌کند.

یادآوری- سطح شرح جزئیات که اثربخشی روش‌های کاهش غیرتهاجمی را شرح‌می‌دهد در پیوست «ج» مراجعه‌شده‌است که با پودمان استفاده‌شده‌است تا از CSPهای پودمان در برابر حملات غیرتهاجمی محافظت‌کند که باید شبیه به چیزی باشد که بر روی مستندسازی آگهی مشاهده‌می‌شود (فهرست‌های محصول).

1- Kit

ب-۲-۹ مدیریت پارامترهای امنیت حساس

- تهیه یک جدول راهنما که مشخص می‌کند: انواع کلید، توان‌ها در بیت‌ها، تابع(های) امنیت، عدد(های) گواهی تابع امنیتی که در کجا و چگونه کلیدها تولید می‌شوند، آیا کلیدها وارد یا خارج‌می‌شوند، هر تولید SSP و روش استقرار به‌کاربرده شده و شناسایی هر کلید مربوطه.
- نشان دادن جدولی از SSPها و چگونگی تولید آنها.
- تعیین مولدهای بیت تصادفی تاییدشده و تاییدنشده.
- شرح کاربردهای خروجی‌های RBG.
- تعیین منابع انتروپی RBG.
- تعیین روش(های) I/O کلید دستی و الکترونیکی.
- تعیین روش‌های ذخیره‌سازی SSP.
- تعیین روش‌های صفرکردن SSP حفاظت‌نشده و دلیل و توانایی شروع متصدی.
- تعیین دوره‌های انتقال یا قاب‌ها هنگامی‌که در آنجا یک الگوریتم یا طول کلید از تاییدشده به تاییدنشده منتقل‌می‌شود.

ب-۲-۱۰ خودآزمایی‌ها

- تهیه فهرست خودآزمایی‌های پیش‌عملیاتی و شرطی با پارامترهای تعریف‌شده و فهرست شرایطی که با آن آزمون‌ها انجام‌می‌گیرند.
- تعیین مدت زمان و خط‌مشی در رابطه با هر شرایطی که ممکن است باعث وقفه در عملیات‌های پودمان در طی مدت تکرار خودآزمایی‌ها شود.
- شرح تمام وضعیت‌های خطا و نشانه‌های وضعیت.
- شرح شروع عملیاتی، اگر کاربردی باشد.

ب-۲-۱۱ اطمینان چرخه عمر

- تعیین روش‌هایی برای نصب امن، مقداردهی اولیه، راه‌اندازی و عملیات پودمان.
- تعیین هر یک از الزامات نگهداری.
- تهیه راهنمایی مدیر و غیر ـ مدیر (ممکن است یک مستند جدا باشد).

ب-۲-۱۲ کاهش حملات دیگر

- تعیین این‌که چه چیزهایی حملات دیگر را کم‌می‌کند.
- شرح اثربخشی روش‌های کاهش فهرست‌شده.
- فهرست راهنمایی و محدودیت‌های مربوط به امنیت.

یادآوری- سطح شرح دقیق سازوکار(های) امنیت پیاده‌سازی‌شده‌است تا دیگر حملاتی را کم‌کند که باید شبیه به چیزی باشد که در مستندسازی آگهی مشاهده‌می‌شود (فهرست‌های محصول).

پیوست پ
(الزامی)
توابع امنیت تاییدشده

پ-۱ هدف

این پیوست فهرستی از استانداردهای تاییدشده ISO/IEC را فراهم‌می‌کند که توابع امنیت تاییدشده را تعیین‌می‌کند که در این استاندارد کاربردپذیر هستند. طبقه‌بندی‌ها شامل رمزهای بلوکی، رمزهای جریان، کلید نامتقارن، کدهای اصالت‌سنجی پیام، توابع درهم‌سازی، اصالت‌سنجی هستار، مدیریت کلید و تولید بیت تصادفی هستند. این فهرست جامع نیست.

این پیوست، توابع امنیت تاییدشده مقام ذیصلاح تاییدشده را ممانعت نمی‌کند.

یک مقام ذیصلاح تایید، ممکن است این پیوست را در تمامیت آن با فهرست خودش که در مورد توابع امنیت تاییدشده است، جایگزین‌کند.

پ-۱-۱ رمزهای بلوکی

a. ISO/IEC 18033-3, Encryption Algorithms — Part 3: Block Ciphers

پ-۱-۲ رمزهای جریانی

b. ISO/IEC 18033-4, Encryption Algorithms — Part 4: Stream Ciphers

پ-۱-۳ الگوریتم‌ها و روش‌های نامتقارن

a. ISO/IEC 9796-2, Information technology — Security techniques — Digital signatures with message recovery — Part 2: Integer factorisation based techniques.
b. ISO/IEC 9796-3, Information technology — Security techniques — Digital signature with message recovery — Part 3: Discrete logarithm based techniques.
c. ISO/IEC 14888 (all parts), Information technology — Security techniques — Digital Signatures with Appendix.
d. ISO/IEC 15946 (all parts), Information technology — Security techniques — Cryptographic techniques based on elliptic curves.
e. ISO/IEC 18033-2, Information technology — Security techniques — Encryption Algorithms — Part 2: Asymmetric cryptographic algorithms.

پ-۱-۴ کدهای اصالت‌سنجی پیام

a. ISO/IEC 9797-2, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function.

پ-۱-۵ توابع درهم‌سازی

a. ISO/IEC 10118-2, Information technology — Security techniques — Hash functions — Part 2: Hash functions using an n-bit block cipher.

b. ISO/IEC 10118-3, Information technology — Security techniques — Hash functions — Part 3: Dedicated hash functions.

c. ISO/IEC 10118-4, Information technology — Security techniques — Hash functions — Part 4: Hash functions using modular arithmetic.

پ-۱-۶ اصالت‌سنجی هستار

a. ISO/IEC 9798-2, Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms.

b. ISO/IEC 9798-3, Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques.

c. ISO/IEC 9798-4, Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function.

d. ISO/IEC 9798-5, Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques.

e. ISO/IEC 9798-6, Information technology — Security techniques — Entity authentication — Part 6: Mechanisms using manual data transfer.

پ-۱-۷ مدیریت کلید

a. ISO/IEC 11770-2, Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques.

b. ISO/IEC 11770-3, Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques.

c. ISO/IEC 11770-4, Information technology — Security techniques — Key management — Part 4: Key establishment mechanisms based on weak secrets.

پ-۱-۸ تولید بیت تصادفی

a. ISO/IEC 18031, Information technology — Security techniques — Random bit generation.

پیوست ت
(الزامی)
تولید و روش‌های اسقرار پارامتر امنیت حساس تاییدشده

ت-۱ هدف

این پیوست فهرستی از استانداردهای تاییدشده ISO/IEC را تهیه‌می‌کند که در مورد تولید و روش‌های اسقرار پارامتر امنیت حساس تاییدشده است و برای این استاندراد کاربردپذیر می‌باشد. از استفاده مقام ذیصلاح تایید که تولید و روش‌های اسقرار پارامتر امنیت حساس تاییدشده را تاییدکرده‌است، ممانعت‌نمی‌کند. این فهرست جامع نمی‌باشد.

این پیوست، تولید پارامتر امنیت حساس تاییدشده توسط مقام ذیصلاح تایید و روش‌های استقرار را منع‌نمی‌کند.

یک مقام ذیصلاح تایید ممکن است این پیوست را در تمامیت آن با فهرست خودش که در مورد تولید پارامتر امنیت حساس تاییدشده و روش‌های تأسیسات است، جایگزین‌کند.

ت-۱-۱ تولید پارامتر امنیت حساس

ت-۱-۲ روش‌های استقرار پارامتر امنیت حساس

a. ISO/IEC 11770-2, Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques.
b. ISO/IEC 11770-3, Information technology — Security techniques — Key Management — Part 3: Mechanisms using asymmetric techniques.
c. ISO/IEC 15946-3, Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment.

پیوست ث
(الزامی)
سازوکارهای اصالت‌سنجی تاییدشده

ث-۱ هدف

این پیوست فهرستی از سازوکارهای اصالت‌سنجی تاییدشده استانداردهای ISO/IEC را فراهم‌می‌کند که برای این استاندارد کاربردپذیر است. کاربرد سازوکارهای اصالت‌سنجی تاییدشده مقام ذیصلاح تایید را منع‌نمی‌کند. این فهرست جامع نیست.

این پیوست، کاربرد سازوکارهای اصالت‌سنجی تاییدشده مقام ذیصلاح تایید را منع‌نمی‌کند.

یک مقام ذیصلاح تایید ممکن است این پیوست را در تمامیت آن با فهرست خودش که در مورد سازوکارهای اصالت‌سنجی تاییدشده است، جایگزین‌کند.

ث-۱-۱ سازوکارهای احرازهویت

الف. در این زمان هیچ سازوکار تاییدشده‌ای تعریف‌نشده‌است.

پیوست ج
(الزامی)
اندازه‌های آزمون کاهش حمله غیرتهاجمی تاییدشده

ج-۱ هدف

این پیوست فهرستی از اندازه‌های آزمون کاهش حمله غیرتهاجمی تاییدشده استانداردهای ISO/IEC را فراهم‌می‌کند که برای این استاندارد کاربردپذیر می‌باشد. کاربرد اندازه‌های آزمون کاهش حمله غیرتهاجمی تاییدشده مقام ذیصلاح تایید را منع نمی‌کند. این فهرست جامع نیست.

این پیوست، کاربرد اندازه‌های آزمون کاهش حمله غیرتهاجمی تاییدشده مقام ذیصلاح تایید را منع‌نمی‌کند. یک مقام ذیصلاح تایید ممکن است این پیوست را در تمامیت آن با فهرست خودش که در مورد اندازه‌های آزمون کاهش حمله غیرتهاجمی است، جایگزین‌کند.

ج-۱-۱ اندازه‌های آزمون کاهش حمله غیر تهاجمی

الف. در این زمان هیچ اندازه‌ای از آزمون کاهش حمله غیرتهاجمی تاییدشده‌ای، تعریف‌نشده‌است.

کتابنامه

[1] ISO 10007:2003, Quality management systems — Guidelines for configuration management

[2] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-2, May 25, 2001 (with latest change notices)

[3] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements