به نام خدا

پروفایل حفاظتی مشترک رمزگذاری کل درایو – اکتساب مجوز

خرداد ۹۴

نسخه ۱,۰

فهرست

۱- مقدمه

این سند که در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک[۱] (CC) توسط مرکز مدیریت راهبردی افتا و سازمان فناوری اطلاعات ایران تهیه و نهایی شده است، برای بیان الزامات کارکرد امنیتی هر محصول لازم است. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی را که در این سند برای برآورده کردن الزامات ارائه شده‌اند، در محصول خود فراهم کنند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد.

این پروفایل حفاظتی مشترک (cPP[۲])، توسط انجمن فنی بین‌المللی[۳] (iTC) رمزگذاری کل درایو به همراه نمایندگانی از صنعت، کارگزاری‌های دولتی، آزمایشگاه‌های آزمون معیار مشترک و اعضای دانشگاه‌ها توسعه یافته است.

۱-۱- اهداف سند

این سند پروفایل حفاظتی مشترک معیار مشترک را معرفی می‌کند تا از این طریق الزامات کارکرد امنیتی[۴] (SFR) و الزامات تضمین امنیتی[۵] (SAR) رمزگذاری کل درایو - اکتساب مجوز[۶] (FDE-AA) را ارائه نماید[۷]. اقدامات ارزیابی که توصیف کننده اقداماتی است که توسط ارزیاب اجرا می‌شود، برای تعیین

---

[۱] Common Criteria

[۲] collaborative Protection Profile

[۳] international Technical Community

[۴] security functional requirements

[۵] security assurance requirements

[۶] Full Drive Encryption – Authorization Acquisition

[۷] این پروفایل حفاظتی مشارکتی (cPP)، توسط جامعه فنی بین‌المللی رمزنگاری (FDE iTC) به همراه نمایندگانی از صنعت، آژانس‌های دولتی، آزمایشگاه‌های تست معیار مشترک و اعضای دانشگاه‌ها توسعه یافته است.

این موضوع است که آیا یک محصول الزامات کارکرد امنیتی اتخاذ شده در این پروفایل حفاظتی مشترک را که در *سند پشتیبان (سند فنی الزامی) رمزگذاری کل درایو: اکتساب مجوز ژانویه ۲۰۱۵* توصیف شده است برآورده می‌سازد یا خیر.

راه‌حل کامل رمزگذاری کل درایو (FDE)[۸] هم به مؤلفه‌های اکتساب مجوز (AA)[۹] و هم به مؤلفه‌های موتور رمزگذاری (EE)[۱۰] نیاز دارد. محصولی ممکن است تمام راه‌حل را ارائه دهد و ادعای انطباق با این پروفایل حفاظتی مشترک و پروفایل حفاظتی مشترک موتور رمزگذاری کل درایو – موتور رمزگذاری را داشته باشد.

با این حال به دلیل اینکه پروفایل حفاظتی اکتساب مجوز یا موتور رمزگذاری در مراحل مقدماتی خود می‌باشد، امکان صدور حکمی که تمام محصولات وابسته، منطبق بر یک پروفایل حفاظتی مشترک باشد وجود ندارد. محصولات وابسته اعتبارسنجی‌نشده (به عنوان مثال موتور رمزگذاری) ممکن است به عنوان قسمت قابل قبولی از محیط عملیاتی برای محصول یا محصول اکتساب مجوز در نظر گرفته شود که به صورت مورد به مورد توسط طرح ملی مربوطه تعیین شده است.

انجمن فنی بین‌المللی (iTC) رمزگذاری کل درایو در نظر دارد تا راهنمایی‌هایی را برای توسعه‌دهندگانی ارائه دهد که محصولات آن‌ها هر دو مؤلفه اکتساب مجوز و موتور رمزگذاری را فراهم می‌کند، در نتیجه به آن‌ها در توسعه هدف امنیتی[۱۱] (ST) کمک می‌کند تا بتوانند ادعای انطباق با هر دو پروفایل حفاظتی مشترک رمزگذاری کل درایو را داشته باشد. یکی از جنبه‌های مهمی که باید نویسندگان هدف امنیتی در نظر بگیرند این است که انتخابی در خلاصه مشخصه محصول (ASE_TSS) وجود دارد که باید تکمیل شود. هرفردی به سادگی نمی‌تواند به الزامات تضمین امنیتی در این پروفایل حفاظتی مشترک ارجاع دهد.

---

[۸] Full Drive Encryption

[۹] Authorization Acquisition

[۱۰] Encryption Engine

[۱۱] Security Target

۱-۲- دامنه کاربرد سند

دامنه کاربرد پروفایل حفاظتی مشترک در فرایندهای توسعه و ارزیابی در ارزیابی امنیت فناوری اطلاعات معیار مشترک توصیف شده است. به‌طور خاص، یک پروفایل حفاظتی مشترک الزامات امنیتی فناوری اطلاعات مربوط به نوع خاصی از فناوری محصول را تعریف کرده و الزامات کارکردی و تضمین امنیتی را برای برآورده شدن توسط محصول منطبق مشخص می‌کند.

۱-۳- مخاطبان هدف

مخاطبان هدف این پروفایل حفاظتی مشترک، توسعه‌دهندگان، استفاده‌کنندگان از معیار مشترک، ایجادکنندگان سیستم، ارزیاب‌ها و طرح‌ها می‌باشند. با این حال، ممکن است پروفایل‌های حفاظتی مشترک و اسناد پشتیبان خطاهای ویرایشی جزئی داشته باشند، پروفایل‌های حفاظتی مشترک به عنوان اسناد زنده بوده و انجمن‌های فنی بین‌المللی (iTC) برای انجام به روزرسانی‌ها و بازبینی‌های مداوم منصوب شده‌اند.

۱-۴- اسناد مرتبط

پروفایل‌های حفاظتی

[FDE-EE] پروفایل حفاظتی مشترک رمزگذاری درایو کامل – موتور رمزگذاری، نسخه ۱، ۲۶ ژانویه، ۲۰۱۵

معیار مشترک[۱۲]

[CC1] معیار مشترک ارزیابی امنیت فناوری اطلاعات، قسمت ۱: معرفی و مدل عمومی؛ CCMB-2012-09-001، نسخه ۳,۱، بازبینی ۴، سپتامبر ۲۰۱۲

[۱۲] برای جزئیات بیشتر به سایت http://www.commoncriteriaportal.org/ مراجعه نمایید.

[CC2] معیار مشترک ارزیابی امنیت فناوری اطلاعات، قسمت ۲: مؤلفه‌های کارکرد امنیتی؛ CCMB-2012-09-002، نسخه ۳,۱، بازبینی 4، سپتامبر ۲۰۱۲

[CC3] معیار مشترک ارزیابی امنیت فناوری اطلاعات، قسمت ۳: مؤلفه‌های تضمین امنیت؛ CCMB-2012-09-003، نسخه ۳,۱، بازبینی 4، سپتامبر ۲۰۱۲

[CEM] متدولوژی ارزیابی مشترک امنیت فناوری اطلاعات، روش ارزیابی، CCMB-2012-09-004، نسخه ۳,۱، بازبینی 4، سپتامبر ۲۰۱۲

[SD] اسناد پشتیبانی (اسناد فنی الزامی)، رمزگذاری درایو کامل: اکتساب مجوز ژانویه ۲۰۱۵

۱-۵- معرفی کار پروفایل‌های حفاظتی مشترک رمزگذاری کل درایو

هدف از اولین مجموعه از پروفایل‌های حفاظتی مشترک (cPPها) برای رمزگذاری کل درایو (FDE): اکتساب مجوز (AA) و موتور رمزگذاری (EE)، ارائه الزاماتی برای محافظت از داده‌های غیرفعال[۱۳] برای افزاره مفقودی می‌باشد که شامل انباره است. این پروفایل‌های حفاظتی مشترک به راه‌حل‌های رمزگذاری کل درایو مبتنی بر سخت‌افزار و یا نرم‌افزار اجازه برآورده ساختن این الزامات را می‌دهد. افزاره‌های انبارش اشکال مختلفی دارند: از جمله درایوهای سخت سامانه یا درایوهای حالت جامد در سرورها، ایستگاه‌های کاری، لپ‌تاپ‌ها، افزاره‌های سیّار، تبلت‌ها و رسانه‌های بیرونی. یک راه‌حل سخت‌افزاری می‌تواند یک درایو خود رمزگذار یا دیگر راه‌حل‌های مبتنی بر سخت‌افزار باشد؛ واسطهای مورد استفاده (USB، SATA و ...) برای اتصال افزاره انبارش به ماشین میزبان، خارج از دامنه کاربرد این پروفایل حفاظتی مشترک می‌باشد.

رمزگذاری کل درایو، تمام داده‌ها (با استثنائات خاص) را در افزاره انبارش رمزگذاری می‌کند و تنها بعد از اعطای مجوز موفقیت‌آمیز اجازه دسترسی به داده‌ها را به راه‌حل رمزگذاری کل درایو می‌دهد. استثنائات شامل ضرورت عدم رمزگذاری بخشی از افزاره انبارش (اندازه ممکن است بر اساس پیاده‌سازی متفاوت باشد)

[۱۳] Data-at-Rest

برای مواردی مانند رکورد راه‌انداز اصلی[۱۴] (MBR) یا دیگر نرم‌افزارهای از پیش احراز هویت شده اکتساب مجوز یا موتور رمزگذاری است. این پروفایل‌های حفاظتی مشترک رمزگذاری کل درایو، اصطلاح "رمزگذاری کل درایو" را به نحوی تفسیر می‌کنند تا به راه‌حل‌های رمزگذاری کل درایو اجازه دهد تا بخشی از افزاره انبارش را تا زمانی‌که شامل متن خام کاربر یا داده‌های خام مجوز باشند، به صورت رمزگذاری نشده باقی بگذارند.

از آنجایی که پروفایل حفاظتی مشترک رمزگذاری کل درایو از راه‌حل‌های گوناگونی پشتیبانی می‌کند، دو پروفایل حفاظتی مشترک که الزامات مؤلفه‌های رمزگذاری کل درایو را توصیف می‌کنند در **شکل ۱** نشان داده شده است.

شکل ۱ -جزئیات مؤلفه‌های رمزگذاری کل درایو

پروفایل حفاظتی مشترک رمزگذاری کل درایو: اکتساب مجوز، الزاماتی را برای بخش اکتساب مجوز توضیح داده و الزامات امنیتی و اقدامات تضمین لازم برای تعامل با کاربر را به طور مفصل توضیح داده و در نتیجه منجر به دسترس‌پذیری مقادیر رمزگذاری مرزی[۱۵] (BEV) می‌شود.

پروفایل حفاظتی مشترک رمزگذاری کل درایو: موتور رمزگذاری، الزاماتی را برای بخش موتور رمزگذاری شرح داده و الزامات امنیتی و اقدامات تضمین لازم برای رمزگذاری یا رمزگشایی عملی داده را توسط کلید رمزگذاری داده[۱۶] (DEK) به طور مفصل توضیح می‌دهد. همچنین، هرکدام از پروفایل‌های حفاظتی مشترک شامل مجموعه‌ای از الزامات اصلی برای کارکردهای مدیریتی، ساماندهی مناسب کلیدهای رمزنگاری، به روزرسانی‌های صورت گرفته به شیوه‌ای امن، ممیزی و خودآزمایی‌ها می‌باشند.

---

[۱۴] Master Boot Record

[۱۵] Border Encryption Value

[۱۶] Data Encryption Key

توصیف محصول، دامنه کاربرد و کارکردهای اکتساب مجوز را تعریف کرده و تعریف مسئله امنیتی به توصیف مفروضات در نظر گرفته شده درباره محیط عملیاتی و تهدیدات مربوط به اکتساب مجوز که الزامات پروفایل حفاظتی مشترک را مورد توجه قرار می‌دهند، می‌پردازد.

۱-۶- پیاده‌سازی‌ها

راهکارهای رمزگذاری کل درایو با ترکیب‌های فروشندگان و روش‌های پیاده‌سازی، تنوع می‌یابند. بنابراین، فروشندگان، محصولاتی را ارزیابی خواهند کرد که هر دو مؤلفه راهکارهای رمزگذاری کل درایو (اکتساب مجوز و موتور رمزگذاری) را بر اساس هر دو پروفایل حفاظتی مشترک، ارائه می‌دهند که می‌تواند در یک ارزیابی با یک هدف امنیتی انجام شود. فروشنده‌ای که تنها یک مؤلفه رمزگذاری کل درایو را ارائه می‌دهد تنها در برابر پروفایل حفاظتی مشترک کاربردپذیر ارزیابی می‌شود. پروفایل حفاظتی مشترک رمزگذاری کل درایو به دو سند تقسیم می‌شود تا به آزمایشگاه‌ها اجازه دهد راه‌حل‌های درخور هریک از پروفایل‌های حفاظتی مشترک را به طور مستقل ارزیابی کنند. زمانیکه مشتری راهکار رمزگذاری کل درایو را کسب می‌کند، در واقع آن‌ها محصول منحصر به‌فرد فروشنده را به دست می‌آورند که پروفایل‌های حفاظتی مشترک اکتساب مجوز و یا موتور رمزگذاری را برآورده می‌سازد، یا دو محصولی که یکی از آن‌ها پروفایل حفاظتی مشترک اکتساب مجوز و دیگری پروفایل حفاظتی مشترک موتور رمزگذاری را برآورده می‌کند.

جدول زیر چندین مثال از گواهی را نشان می‌دهد:

جدول ۱ مثال‌هایی از پیاده‌سازی‌های پروفایل حفاظتی مشترک

پیاده‌سازی	پروفایل حفاظتی مشترک	شرح
میزبان	اکتساب مجوز	نرم‌افزار میزبان، واسطی برای درایو خود رمزگذار ارائه می‌دهد.
درایو خود رمزگذار[۱۷] (SED)	موتور رمزگذاری	درایو خودرمزگذار همراه با نرم‌افزار میزبان جداگانه‌ای استفاده می‌شود.
نرم‌افزار رمزگذاری کل درایو	اکتساب مجوز + موتور رمزگذاری	یک راهکار نرم‌افزاری رمزگذاری کل درایو
ترکیبی	اکتساب مجوز + موتور رمزگذاری	ترکیبی از سخت‌افزار (مثلاً سخت‌افزار موتور رمزگذاری، کمک پردازنده رمزنگاری) و نرم‌افزار منحصر به فروشنده

[۱۷] Self-Encrypting Drive

۲- فرهنگ اصطلاحات

- **عامل مجوز (Authorization Factor)**

مقداری که کاربر می‌داند یا آن را دارد یا (مانند کلمه‌عبور، نشانه و ...) به محصول ارسال شده است تا تعیین کند که کاربر جزء جامعه مجاز به استفاده از دیسک سخت است و از آن برای استخراج یا رمزگشایی مقدار رمزگذاری مرزی (BEV) و رمزگشایی احتمالی کلید رمزگذاری داده (DEK) استفاده می‌شود. قابل ذکر است که این مقادیر ممکن است برای تعیین هویت خاص کاربر استفاده نشود.

- **تضمین (Assurance)**

اساسی برای اعتماد به اینکه محصول الزامات کارکردی امنیتی را برآورده می‌سازد [CC1]

- **مقدار رمزگذاری مرزی (Border Encryption Value)**

مقداری که از اکتساب مجوز به موتور رمزگذاری گذشته و جهت اتصال زنجیره‌های کلید دو مؤلفه در نظر گرفته‌شده است.

- **پاکسازی کلید (Key Sanitization)**

روشی برای پاکسازی داده رمزگذاری شده با استفاده از بازنویسی امن کلیدی که داده را رمزگذاری کرده است.

- **کلید رمزگذاری داده ((Data Encryption Key (DEK)**

کلیدی که برای رمزگذاری داده در حال سکون استفاده می‌شود.

- **رمزگذاری کل درایو (Full Drive Encryption)**

اشاره به افزارههایی از قالب‌های منطقی داده در دسترس کاربر دارد که توسط سامانه میزبان مدیریت می‌شود و شاخص‌ها و افزاره‌ها و سیستم‌عاملی که مجوز را خواندن یا نوشتن داده را به قالب‌های این افزاره‌ها نگاشت می‌کند. به‌خاطر تعریف برنامه امنیتی (SPD) و پروفایل حفاظتی مشترک، رمزگذاری کل درایو (FDE)، رمزگذاری و مجوز را روی یک افزاره به گونه‌ای انجام می‌دهد که به‌طور مشترک توسط سیستم‌عامل و سامانه فایل پشتیبانی و تعریف شده است. محصولات رمزگذاری کل درایو، تمام داده‌ها (با استثنائات خاص) را روی افزاری از افزاره انبارش رمزگذاری می‌کنند و اجازه دسترسی به داده به راه‌حل رمزگذاری کل درایو را تنها بعد از اعطای موفق مجوز می‌دهد. استثنائات شامل ضرورت رمزگذاری نشده رها کردن افزاری از افزاره انبارش (که ممکن است اندازه آن‌ها متفاوت باشد)، برای مواردی مانند رکورد راه‌اندازی اصلی (MBR) یا دیگر نرم‌افزارهای از قبل احراز هویت شده اکتساب مجوز یا موتور رمزگذاری می‌باشد. پروفایل حفاظتی مشترک رمزگذاری کل درایو اصطلاح "رمزگذاری کل درایو" را تفسیر می‌کند تا به راه‌حل‌های رمزگذاری کل درایو اجازه دهد، افزاری از افزاره انبارش را تا زمانیکه شامل داده حفاظت نشده می‌باشند، رمزگذاری رها کند.

- **کلید میانی (Intermediate Key)**

کلیدی که در نقطه‌ای بین مجوز کاربر اولیه و کلید رمزگذاری داده استفاده می‌شود.

- **سکو میزبان (Host Platform)**

سخت‌افزار و نرم‌افزار محلی که محصول روی آن اجرا می‌شود و هیچ‌گونه دستگاه جانبی (مانند دستگاه‌های USB) که ممکن است به سخت‌افزار و نرم‌افزار محلی متصل شوند را شامل نمی‌باشد.

- **زنجیره کلید (Key Chaining)**

روش استفاده از لایه‌های متعدد کلیدهای رمزگذاری به منظور حفاظت از داده. کلید لایه بالایی، کلید لایه پایینی را رمزگذاری می‌کند که داده را رمزگذاری می‌کند. این روش می‌تواند هر تعداد لایه داشته باشد.

- **کلید رمزگذاری کلید (Key Encryption Key (KEK))**

  کلیدی که برای رمزگذاری دیگر کلیدها مانند کلیدهای رمزگذاری داده (DEK) یا انبارشی که شامل کلیدها می‌شوند، استفاده می‌شود.

- **اجزای کلید (Key Material)**

  اجزای کلید که معمولاً به عنوان داده پارامتر امنیت بحرانی (CSP) شناخته می‌شوند و همچنین شامل داده‌های مجوز، مقادیر مقطعی و فراداده‌ها می‌باشند.

- **کلید انتشار کلید (Key Release Key (KRK))**

  کلیدی که برای انتشار کلید دیگر از محل انبارش استفاده می‌شود و برای استخراج مستقیم یا رمزگشایی دیگر کلیدها استفاده نمی‌شود.

- **سیستم‌عامل (Operating System (OS))**

  نرم‌افزاری که در بالاترین سطح امتیاز قرار دارد و می‌تواند به طور مستقیم منابع سخت‌افزاری را کنترل کند.

- **حافظه غیرفرّار (Non-Volatile Memory)**

  نوعی از حافظه کامپیوتر که اطلاعات درون آن بدون برق، باقی می‌مانند.

- **حالت خاموش (Powered-Off State)**

حالتی که در آن دستگاه خاموش شده است.

- **داده حفاظت شده (Protected Data)**

به تمام داده‌های روی افزاره انبارش اشاره دارد به استثنای افراره کوچکی که به منظور عملکرد صحیح موردنیاز برای محصول است. تمام فضای روی دیسک که کاربر می‌تواند روی آن داده بنویسد و شامل سیستم‌عامل، برنامه‌های کاربردی و داده‌های کاربر می‌باشد. داده حفاظت شده شامل رکورد اصلی راه‌اندازی یا نواحی از پیش احراز هویت شده درایو نمی‌باشد – نواحی از درایو که ضرورتاً رمزگذاری نشده‌اند.

- **Submask**

رشته‌ای از بیت‌ها است که می‌تواند به روش‌های مختلفی تولید و ذخیره شوند.

- **محصول (هدف ارزیابی) (TOE)** [۱۸]

محصول مورد ارزیابی که در این سند، سامانه رمزگذاری کل درایو- اکتساب مجوز است و مجموعه‌ای است از سخت‌افزارها، میان‌افزارها و یا نرم افزارها که با دستورالعمل‌ها و راهنمایی‌هایی همراه می‌باشند.

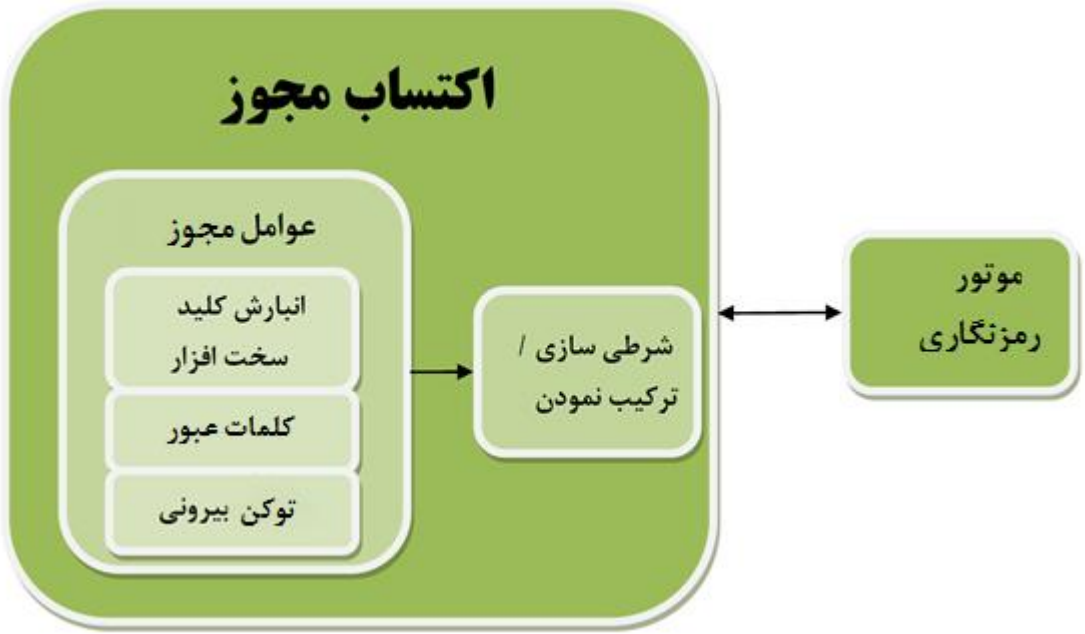
۳- شرح محصول

۳-۱- مرور کلی بر محصول

[۱۸] Target of Evaluation

محصول این پروفایل حفاظتی مشترک (اکتساب مجوز)، ممکن است راه‌حل نرم‌افزاری میزبان باشد که موتور رمزگذاری سخت‌افزاری (مثلاً درایو خودرمزنگار) را مدیریت می‌کند یا قسمتی از ارزیابی ترکیبی این پروفایل حفاظتی مشترک و پروفایل حفاظتی مشترک موتور رمزگذاری فروشنده‌ای باشد که ارائه دهنده راه‌حلی است که شامل هر دو مؤلفه می‌باشد.

بخش زیر مرور کلی از کارکردهای اکتساب مجوز رمزگذاری کل درایو و قابلیت‌های امنیتی را ارائه می‌دهد.



شکل ۲ جزئیات اکتساب مجوز

۳-۱-۱- معرفی اکتساب مجوز

اکتساب مجوز، مقدار رمزگذاری مرزی (BEV) را ارسال می‌کند که می‌تواند کلید رمزگذاری کلید[۱۹] (KEK)، کلید انتشار کلید[۲۰] (KRK) یا انواع دیگری از کلیدهای موتور رمزگذاری باشد. موتور رمزگذاری نباید به‌طور مستقیم از این مقدار به عنوان کلیدی جهت رمزگشایی یا انتشار کلید رمزگذاری داده استفاده کند. این مقدار ممکن است به‌عنوان قسمتی از طرحی استفاده شود که با استفاده از دیگر کلیدهای میانی، از کلید رمزگذاری داده محافظت می‌کند. کلید رمزگذاری کلید، کلیدهای دیگر به ویژه کلید رمزگذاری داده یا دیگر کلیدهای میانی که به کلید رمزگذاری داده متصل هستند، را می‌پوشاند. کلیدهای انتشار کلید به موتور رمزگذاری مجوز می‌دهد که هرگونه کلید رمزگذاری داده یا دیگر کلیدهای میانی را انتشار دهد که به کلید رمزگذاری داده متصل هستند. شکل ۲ مؤلفه‌های درون اکتساب مجوز و ارتباط آن با موتور رمزگذاری را نشان می‌دهد.

عوامل مجوز ممکن است برای هر کاربر یکتا باشد یا توسط گروهی از افراد استفاده شود. به‌عبارت دیگر، موتور رمزگذاری به عوامل مجوز از اکتساب مجوز نیاز دارد تا تعیین کند که مالک عامل مجوز متعلق به جامعه‌ای از کاربران مجاز به دسترسی به اطلاعات ذخیره شده بر روی افزاره انبارش می‌باشد (و به مجوز کاربر خاصی نیاز ندارد). مثال‌هایی از عوامل مجوز شامل، کلمه‌های عبور، عبارات عبور، مقادیر تولید شده تصادفی ذخیره‌شده در توکن‌های گذرگاه جهانی سریال[۲۱] (USB) یا پین برای انتشار کلید بر روی رسانه انبارش سخت‌افزاری مانند واحد سکوهای امن (TPM[۲۲]) می‌باشد.

۳-۱-۲- قابلیت‌های امنیتی اکتساب مجوز

---

[۱۹] Key Encryption Key

[۲۰] Key Releasing Key

[۲۱] Universal Serial Bus

[۲۲] Trusted Platform Module

اکتساب مجوز، عوامل مجوزی را فراهم می‌کند که موتور رمزگذاری از آن برای دستیابی به داده موجود بر روی افزاره انبارش استفاده می‌کند و کارکردهای مدیریتی متنوعی انجام می‌دهد. بسته به نوع عامل مجوز، اکتساب مجوز ممکن است شرایط بیشتری روی آن‌ها اعمال کند. به‌عنوان مثال، ممکن است تابع استخراج کلید مبتنی بر کلمه‌عبور تأیید شده[۲۳] (PBKDF2) را روی کلمه‌های عبور، اعمال کند. یک توکن بیرونی[۲۴] شامل مقادیر تولید شده تصادفی با استحکام مناسب ممکن است به شرطی‌سازی بیشتری روی عوامل مجوز نیاز نداشته باشد. اکتساب مجوز ممکن است یک یا تعدادی از عوامل مجوز را به روشی با یکدیگر ترکیب کند که استحکام هر دو عامل حفظ شود.

اکتساب مجوز به عنوان واسط اصلی مدیریت برای موتور رمزگذاری عمل می‌کند. با این حال، موتور رمزگذاری نیز ممکن است کارکردهای مدیریتی ارائه دهد. الزامات موجود در پروفایل حفاظتی مشترک موتور رمزگذاری، نحوه اداره این ویژگی‌ها را بیان می‌کند. کارکردهای مدیریتی ممکن است شامل توانایی ارسال دستورات به موتور رمزگذاری مانند تغییر کلید رمزگذاری داده، راه‌اندازی کاربران جدید، مدیریت کلیدهای رمزگذاری کلید و دیگر کلیدهای میانی و انجام پاکسازی کلید (مانند بازنویسی کلید رمزگذاری داده) باشد. همچنین ممکن است دستوراتی ارسال کند که درایو را برای استفاده همزمان چند کاربر افراز (پارتیشن‌بندی) کند. با این حال این سند مدیریت این افرازه‌ها را ارائه نمی‌دهد و فرض بر این است که مدیران سیستم و کاربران، تنها داده‌های روی کل درایوها را آماده و مدیریت می‌کنند.

۳-۱-۳- واسط / مرز

واسط و مرز میان مجوز اکتساب و موتور رمزگذاری بر اساس پیاده‌سازی متفاوت خواهد بود. اگر فروشنده‌ای تمام راه‌حل رمزگذاری کل درایو را ارائه دهد، ممکن است انتخاب کند که واسطی بین مؤلفه‌های مجوز اکتساب و موتور رمزگذاری پیاده‌سازی نکند. چنانچه فروشنده راه‌حلی برای یکی از مؤلفه‌ها ارائه دهد،

[۲۳] password-based key derivation function

[۲۴] external token

فرض زیر بیان می‌کند که کانال میان دو مؤلفه به اندازه کافی امن است. هرچند، استانداردها و مشخصاتی برای واسط بین مؤلفه‌های اکتساب مجوز و موتور رمزگذاری وجود دارد، پروفایل حفاظتی مشترک در این نسخه، فروشندگان را ملزم به تبعیت از این استانداردها نمی‌کند.

۳-۲- محصول و محیط‌های عملیاتی یا محیط‌های پیش از راه‌اندازی

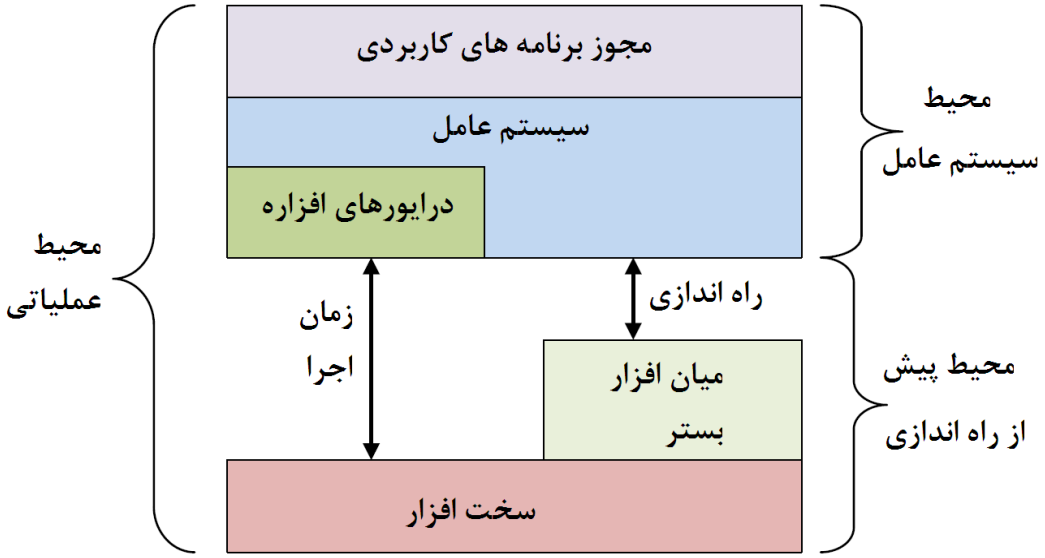
محیطی که اکتساب مجوز در آن عمل می‌کند ممکن است بسته به مرحله راه‌اندازی سکوی که در آن عمل می‌کنند، متفاوت باشد، شکل ۳ را ببینید. براساس معماری راه‌حل، جنبه‌های آماده‌سازی، مقداردهی اولیه و مجوز ممکن است در مرحله پیش از راه‌اندازی انجام شود، درحالی‌که به احتمال زیاد رمزگذاری، رمزگشایی و کارکردهای مدیریتی در محیط سیستم‌عامل اجرا می‌شود. در راه‌حل‌های غیر نرم‌افزاری، رمزگذاری یا رمزگشایی در محیط پیش از سیستم‌عامل شروع می‌شود و تا محیط حاضر سیستم‌عامل ادامه می‌یابد.

در محیط سیستم‌عامل، اکتساب مجوز دارای طیف کاملی از خدمات در دسترس سیستم‌عامل از جمله درایورهای سخت‌افزاری، کتابخانه رمزنگاری و شاید دیگر خدمات بیرون از محصول می‌باشد.

محیط پیش از راه‌اندازی با قابلیت‌های محدود شده بیشتر محدود می‌شود. این محیط حداقل تعداد دستگاه‌های جانبی را راه‌اندازی می‌کند و تنها درایورهای ضروری را جهت آوردن سکوه از یک شروع سرد[۲۵] تا اجرای سیستم‌عامل کارکردی کامل با اجرای برنامه‌های کاربردی بارگذاری می‌کند.

محصول اکتساب مجوز، شامل یا تقویت‌کننده ویژگی‌ها و توابع محیط عملیاتی می‌باشد.

[۲۵] cold start



شکل ۳ محیط عملیاتی

۳-۳- قابلیت‌های کارکردی به تعویق افتاده تا نسخه بعدی پروفایل حفاظتی مشترک

به دلیل محدودیت‌های زمانی، این پروفایل حفاظتی مشترک تعدادی از کارکردهای مهم را تا نسخه بعدی پروفایل حفاظتی مشترک به تعویق می‌اندازد. این کارکردهای مهم شامل الزامات مدیریت افزاره (پارتیشن) یا حجم، مدیریت از راه دور و مدیریت روشن بودن (الزامات محافظت از حالت روشن بودن) می‌باشد.

۳-۴- حالت استفاده محصول

حالت استفاده محصول منطبق با پروفایل‌های حفاظتی مشترک رمزگذاری کل درایو، برای محافظت از داده غیرفعالی می‌باشد که روی افزاره‌ای که گم شده یا به سرقت‌رفته‌ای قرار دارد که بدون هرگونه دسترسی قبلی توسط مهاجم، خاموش شده است. حالت استفاده‌ای که مهاجم به افزاره‌ای دسترسی دارد که در

حالت روشن می‌باشد و قادر به ایجاد تغییر محیط یا خود محصول است (مانند حملات evil maid)، در این پروفایل (رمزگذاری کل درایو- اکتساب مجوز و رمزگذاری کل درایو- موتور رمزگذاری) مورد توجه نیست.

۴-مسائل امنیتی

۴-۱- تهدیدها

این بخش توضیح می‌دهد چگونه الزامات، تهدیدات نگاشت‌شده را تضعیف می‌کنند. یک الزام ممکن است جنبه‌هایی از تهدیدات گوناگون را تضعیف کند. الزامی هم ممکن است تنها یک تهدید را به‌شکل محدودی تضعیف کند.

تهدید شامل عامل تهدید، دارایی و اقدام مضر آن عامل تهدید روی آن دارایی، می‌باشد. عوامل تهدید، موجودیت‌هایی هستند که در صورتی دارایی‌ها را در معرض خطر قرار می‌دهند که مهاجم افزاره انبارش گم‌شده یا به‌سرقت‌رفته را به‌دست آورد. تهدیدات، الزامات کارکردی محصول را عقب می‌رانند. به‌عنوان مثال یکی از تهدیدات دسترسی غیرمجاز به داده‌ها (T.UNAUTHORIZED_DATA_ACCESS) می‌باشد. عامل تهدید، متصرف (کاربر غیرمجاز) افزاره انبارش گم شده یا به‌سرقت‌رفته می‌باشد. دارایی، داده موجود بر روی افزاره انبارش می‌باشد و اقدام مضر تلاش برای به دست آوردن این داده‌ها از افزاره انبارش می‌باشد. این تهدید، باعث عقب راندن الزامات کارکردی افزاره انبارش رمزگذاری‌شده (محصول) می‌شود تا به فرد مجوز بدهد تا بتواند از محصول برای دسترسی به دیسک سخت و داده‌های رمزگذاری یا رمزگشایی استفاده کند. در اختیار داشتن کلید رمزگذاری کلید، کلید رمزگذاری داده، کلیدهای میانی، عوامل مجوز، submaskها، اعداد تصادفی یا هر مقدار دیگری که در ایجاد کلید یا عوامل مجوز مشارکت دارد می‌تواند به کاربر غیرمجاز اجازه دهد تا رمزگذاری را بشکند، این تعریف مسئله امنیتی، اجزای کلید را معادل داده با اهمیت درنظر می‌گیرد و در میان دارایی‌های دیگری که در بخش زیر به آن‌ها اشاره می‌شود، نمایان می‌شوند.

در اینجا، مهم است که مجدداً تأکید شود که پروفایل حفاظتی مشترک از محصول (محصول) انتظار ندارد که در برابر تصاحب دیسک سخت گم‌شده یا به‌سرقت‌رفته که می‌تواند کدهای مخرب یا مؤلفه‌های سخت‌افزاری قابل بهره‌برداری را به محصول یا محیط عملیاتی معرفی کند، دفاع نماید. فرض بر این است

که کاربر به صورت فیزیکی از محصول محافظت می‌کند و محیط عملیاتی حفاظت کافی در برابر حملات منطقی را ارائه می‌دهد. یکی از نواحی ویژه‌ای که محصول منطبق، برخی از اقدامات حفاظتی را ارائه می‌دهد، در ارائه به‌روز رسانی برای محصول می‌باشد. هرچند به جز این ناحیه، این پروفایل حفاظتی مشترک هیچ اقدام مقابله‌ای دیگری را الزامی نمی‌کند. به‌طور مشابه، این الزامات مسئله "گم‌شدن یا پیدا شدن" دیسک سخت را مورد توجه قرار نمی‌دهد، جاییکه مهاجم ممکن است دیسک سخت را برداشته باشد، بخش رمزگذاری‌نشده افزاره راه‌انداز (مانند رکورد راه‌انداز اصلی، افزاره راه‌انداز) را به خطر بیندازد و سپس آن را برای بازیابی توسط کاربر اصلی در دسترس قرار دهد که در نتیجه می‌توانند کد به خطر افتاده را به اجرا در بیاورند.

تهدیدات	توضیحات
تهدیدات دسترسی غیرمجاز به داده‌ها T.UNAUTHORIZED_DATA_ACCESS	تهدید اصلی، افشای غیر مجاز داده محافظت‌شده و ذخیره‌شده بر روی افزاره انبارش می‌باشد که مورد توجه پروفایل حفاظتی مشترک می‌باشد. اگر مهاجمی افزاره انبارش گم‌شده یا به‌سرقت‌رفته (به عنوان مثال افزاره انبارش موجود در یک لپ‌تاپ یا افزاره انبارش بیرونی قابل‌حمل) را به‌دست آورد، ممکن است که اقدام به اتصال افزاره انبارش مورد هدف به میزبانی کند که بر آن کنترل کامل داشته و دسترسی اولیه‌ای به افزاره انبارش (به عنوان مثال بخش مشخص شده‌ای از دیسک، قالب‌های مشخص) دارند. [FCS_AFA_EXT.1.1, FCS_KYC_EXT.1.1, FCS_KYC_EXT.1.2, FCS_PCC_EXT.1, FMT_SMF.1.1] منطق: الزام کارکرد امنیتی زنجیره‌ای‌کردن کلید (FCS_KYC_EXT.1.2)، مستلزم آن است که مقادیر رمزگذاری مرزی (BEV) جهت دسترسی به داده‌های رمزگذاری‌شده و محافظت‌شده بر روی درایو، به موتور رمزگذاری ارائه شود. یک یا چند submask [الزام کارکرد امنیتی اکتساب عامل مجوز (FCS_AFA_EXT.1.1)] ممکن است با [الزام کارکرد امنیتی ترکیب (FCS_SMC_EXT.1.1) submask] ترکیب شود و یا به [الزام امنیتی زنجیره‌ای کردن کلید (FCS_KYC_EXT.1.1)] متصل شوند تا مقدار رمزگذاری مرزی را تولید نمایند. این مجموعه از الزامات این اطمینان را می‌دهند که مقدار رمزگذاری مرزی به‌درستی تولید و محافظت می‌شود و از افشای غیرمجاز داده‌های رمزگذاری‌شده محافظت‌شده، جلوگیری می‌کند. الزام امنیتی مشخصات توابع مدیریتی (FMT_SMF.1.1) این اطمینان را می‌دهد که توابع هدف امنیتی، توابع ضروری برای مدیریت جوانب مهم هدف ارزیابی ازجمله درخواست تغییر و پاک کردن کلید رمزگذاری داده را ارائه می‌دهند.

	تصاحب هر کلید، عوامل مجوز، submaskها، اعداد تصادفی یا هر مقدار دیگری که در ایجاد کلید یا عوامل مجوزی که در ایجاد کلید یا عوامل مجوز دیگر مشارکت دارند می‌تواند به کاربر غیرمجاز اجازه دهند تا رمزگذاری را بشکنند. پروفایل حفاظتی مشترک، تصاحب اجزای کلیدزنی را با اهمیتی معادل خود داده‌ها درنظر می‌گیرد. عوامل تهدید ممکن است به دنبال اجزای کلیدزنی در بخش‌های رمزگذاری‌نشده افزاره انبارش و دیگر دستگاه‌های جانبی در محیط عملیاتی (OE) مانند پیکربندی BIOS، فلش SPI یا TPMs باشند. [FCS_PCC_EXT.1, FCS_KYC_EXT.1.1, FCS_AFA_EXT.1.1, FPT_KYP_EXT.1.1, FCS_CKM_EXT.4, FCS_CKM.4.1, FCS_CKM.1.1, FCS_VAL_EXT.1.1, FMT_SMF.1.1]
تهدید در معرض خطر قرار دادن اجزای کلید زنی T.KEYING_MATERIAL_COMPROMISE	منطق: مقدار مرزی رمزگذاری ممکن است [الزام کارکرد امنیتی زنجیره‌ای کردن کلید(FCS_KYC_EXT.1.1)] را به یک یا چندینsubmask [الزام کارکرد امنیتی اکتساب عامل مجوز (FCS_AFA_EXT.1.1)] متصل شود. این الزامات این اطمینان را می‌دهند که مقدار رمزگذاری مرزی به‌درستی تولید شده و محافظت می شود. الزام کارکرد امنیتی حفاظت از کلید و اجزای کلید (FPT_KYP_EXT.1.1) این اطمینان را می‌دهد که اجزای کلیدی که پوشانده نشده‌اند، در حافظه غیرفرّار ذخیره نشوند و الزام کارکرد امنیتی تخریب اجزای کلید و کلید رمزنگاری توسعه یافته (FCS_CKM_EXT.4) به همراه الزام کارکرد امنیتی تخریب کلید رمزنگاری (FCS_CKM.4.1) از تخریب مناسب اجزای کلید اطمینان حاصل می‌کند. این الزامات افشای اجزای کلید متن خام را به حداقل می‌رسانند. الزام کارکرد امنیتی مشخصات توابع مدیریتی (FMT_SMF.1.1) این اطمینان را می‌دهد که توابع هدف امنیتی، توابع ضروری برای مدیریت جوانب مهم هدف ارزیابی از جمله تولید و پیکربندی عوامل مجوز، را ارائه می‌دهند.
تهدید به‌روزرسانی غیرمجاز T.UNAUTHORIZED_UPDATE	عوامل تهدید ممکن است اقدام به اجرای به‌روزرسانی محصولی کنند که ویژگی‌های امنیتی هدف ارزیابی را به‌خطر می‌اندازند. انتخاب ضعیف پروتکل‌های به‌روزرسانی، الگوریتم‌های تولید و درستی‌سنجی امضا و پارامترها ممکن است به مهاجمان این اجازه را بدهد که نرم‌افزار و یا سفت‌افزاری را نصب کنند که ویژگی‌های امنیتی در نظر گرفته شده را دور می‌زنند و دسترسی غیرمجاز آن‌ها به داده‌ها را فراهم می‌کنند. [FPT_TUD_EXT.1.1, FPT_TUD_EXT.1.2, FPT_TUD_EXT.1.3, FMT_SMF.1.1]

	منطق: عناصر ۱ و ۲ و ۳ الزامات کارکرد امنیتی به روزرسانی قابل اعتماد (FPT_TUD_EXT.1.1, FPT_TUD_EXT.1.2 و FPT_TUD_EXT.1.3) به کاربران مجاز قابلیت پرس‌وجوی نسخه فعلی سفت‌افزار یا نرم‌افزار هدف ارزیابی، به‌روزرسانی‌های نخستین و بررسی به‌روزرسانی‌ها قبل را از نصب با استفاده از امضای دیجیتالی تولید کننده ارائه می‌دهد. الزام امنیتی مشخصات توابع مدیریتی (FMT_SMF.1.1) این اطمینان را می‌دهد که توابع هدف امنیتی (TSF) توابع ضروری برای مدیریت جوانب مهم هدف ارزیابی از جمله آغاز به‌روزرسانی‌های نرم‌افزار یا میان‌افزار سامانه را ارائه دهند.

۴-۲- مفروضات

مفروضاتی که برای کاهش تهدیدات باید درست باقی بمانند، در بخش زیر توضیح داده شده است:

مفروضات	توضیحات
فرض حالت اولیه درایو (A.INITIAL_DRIVE_STATE)	کاربران، رمزگذاری کل درایو را روی افزاره انبار شی که جدیداً تهیه شده یا مقداردهی اولیه شده ا ست و خالی از داده‌های محافظت‌شـــده در نواحی اســـت که مورد هدف رمزگذاری نیســـتند، فعال می‌کنند. این پروفایل حفاظتی م شترک شامل الزاماتی نمی شود که تمام نواحی بر روی افزاره‌های انبارش را جستجو کند که به طور بالقوه حاوی داده‌های محافظت شده می‌با شند. در بع ضی موارد ممکن ا ست این کار غیر ممکن با شد، برای مثال در حالتی که داده‌ها در بخش‌های "بد" گنجانده شده‌اند. درحالیکه افشای ناخواسته داده‌های موجود در بخش‌های بد یا فضاهای افراز نشـده، بعید اسـت، با این حال ممکن اسـت کسـی از ابزارهای قانونی برای بازیابی داده از چنین نواحی افزاره انبارش اسـتفاده نماید. در نتیجه، پروفایل حفاظتی مشـترک فرض می‌کند، بخش‌های بد، فضـاهای افراز نشـده و نواحی‌ای که ممکن ا ست شامل کدهای رمز نشده با شند (مانند رکورد راه‌انداز ا صلی و نرم‌افزار از قبل احراز هویت شده اکتساب مجوز یا موتور رمزگذاری) حاوی هیچ داده محافظت شده‌ای نمی‌باشند. [OE.INITIAL_DRIVE_STATE]
فرض حالت امن A.SECURE_STATE	به‌محض اتمام آماده‌ســازی مناســب، درایو تنها زمانی امن در نظر گرفته می‌شـود که در حالت خاموش باشـد و تا زمانیکه روشن شود و مجوز اولیه را دریافت کند. [OE.POWER_DOWN]

فرض کانال مطمئن A.TRUSTED_CHANNEL)	ارتباط میان و بین مؤلفه‌های محصول (اکتساب مجوز و موتور رمزگذاری) به اندازه کافی برای جلوگیری از افشای اطلاعات محافظت‌شده هستند. در مواردی که یک محصول منحصر به‌فرد هر دو پروفایل حفاظتی مشترک را برآورده می‌سازد، ارتباط بین مؤلفه‌ها فراتر از مرزهای هدف ارزیابی توسعه نمی‌یابد (به‌عبارت دیگر مسیر ارتباطی درون مرز هدف ارزیابی است). در مواردی که محصولات مستقل، الزامات اکتساب مجوز و موتور رمزگذاری را برآورده می‌سازند، نزدیکی فیزیکی دو محصول در طول عملیاتشان، بدین معنا است که عامل تهدید از شانس بسیار کمی برای مداخله در کانال بین این دو بدون توجه کاربر و انجام اقدامات مناسب، برخوردار است. [OE.TRUSTED_CHANNEL]
فرض کاربر آموزش‌دیده A.TRAINED_USER	کاربران مجاز از تمام راهنماهای کاربری ارائه شده، از جمله نگهداری از کلمه‌های عبور و یا عبارات عبور و توکن‌های بیرونی که به‌گونه‌ای امن جدا از افزاره انبارش و یا سکوه ذخیره شده‌اند، پیروی می‌کنند. [OE.PASSPHRASE_STRENGTH, OE.POWER_DOWN, OE.SINGLE_USE_ET, OE.TRAINED_USERS]
فرض حالت سکو A.PLATFORM_STATE	سکویی که افزاره انبارش در آن مقیم شده (یا افزاره انبارش بیرونی به آن و صل شده ا ست)، باید عاری از هرگونه نرم‌افزار مخربی باشد تا بتواند با عملکرد صحیح محصول ارتباط برقرار کند. [OE.PLATFORM_STATE]
فرض کاربرد واحد توکن بیرونی (A.SINGLE_USE_ET)	توکن‌های بیرونی که شـــامل عوامل مجوز می‌باشـــند، برای هدف دیگری جز انبارش عوامل مجوز توکن بیرونی استفاده نمی‌شوند. [OE.SINGLE_USE_ET]

فرض خاموش بودن A.POWER_DOWN	کاربر سکو و یا افزاره انبارش را تا زمانی‌که تمام حافظه فرّار بعد از خاموش شدن پاک شود، بدون مراقبت رها نمی‌کند، بنابراین حملات باقی مانده حافظه اجرا نشدنی می‌شوند. کاربران مجاز سکو و یا افزاره انبارش را در حالتی باقی نمی‌گذارند که اطلاعات حساس در حافظه غیر فرّار باقی مانده باشند (مانند قفل صفحه نمایش). کاربر سکو و یا انبارش را خاموش می‌کند یا در حالت روشن مدیریت شده مانند "مد هایبرنت" قرار می‌دهد. [OE.POWER_DOWN]
فرض استحکام کلمه‌عبور A.PASSWORD_STRENGTH	مدیران سیستم مجاز این اطمینان حاصل می‌کنند که عوامل مجوز کلمه‌عبور یا عبارات عبور به اندازه کافی استحکام و آنتروپی برای انعکاس حساسیت داده محافظت شده را دارند. [OE.PASSPHRASE_STRENGTH]
فرض کارکرد شناسایی و احرازهویت سکو (A.PLATFORM_I&A)	محصول در کارکردهای عادی شناسایی و احراز هویت سکو مانند ورود به سیستم‌عامل مداخله نمی‌کند یا آن را تغییر نمی‌دهد. محصول ممکن است عوامل مجوز را برای واسط ورود به سیستم‌عامل فراهم کند اما آن را تغییر نداده یا عملکرد واسط واقعی را کاهش نخواهد داد. [OE.PLATFORM_I&A]
فرض رمزنگاری قوی A.STRONG_CRYPTO	تمام رمزنگاری‌های پیاده‌سازی‌شده در محیط عملیاتی و مورد استفاده محصول، الزامات موجود در این پروفایل حفاظتی مشترک را برآورده می‌سازند. از جمله این الزامات، تولید عوامل مجوز نشانه (توکن) بیرونی توسط تولیدکننده بیت تصادفی است. [OE.STRONG_ENVIRONMENT_CRYPTO]

۴-۳- خط‌مشی‌های امنیتی سازمان

هیچ خط‌مشی امنیت سازمانی در این پروفایل حفاظتی مشترک معرفی نشده است.

۵- اهداف امنیتی

۵-۱- اهداف امنیتی محیط عملیاتی

محیط عملیاتی محصول، اقدامات فنی و رویه‌ای را برای کمک به محصول جهت ارائه درست قابلیت‌های توابع امنیتی خود، پیاده‌سازی می‌کند. این قسمت راه‌حل معقول، اهداف امنیتی محیط عملیاتی را شکل می‌دهد و شامل مجموعه‌ای از گزاره‌هایی می‌باشد که اهدافی را توصیف می‌کند که محیط عملیاتی باید به آن‌ها برسد.

هدف امنیتی محیط عملیاتی	توضیحات
هدف امنیتی کانال مطمئن OE.TRUSTED_CHANNEL	ارتباط میان و بین مؤلفه‌های محصول (یعنی اکتساب مجوز و موتور رمزنگاری)، برای جلوگیری از افشای اطلاعات به‌خوبی محافظت می‌شوند. منطق: در راهکارهایی که فرصتی برای مهاجم وجود دارد تا در کانال بین اکتساب مجوز و موتور رمزنگاری مداخله نماید، کانال امنی برای جلوگیری از سوءاستفاده باید برقرار شود. فرض کانال مطمئن [A.TRUSTED_CHANNEL] فرض را بر وجود کانالی امن بین اکتساب مجوز و موتور رمزنگاری می‌گذارد، مگر زمانی که مرزی درون آن وجود داشته باشد و در محصول رخنه نکرده باشد یا چنان نزدیک باشد که رخنه بدون آشکارسازی غیرممکن باشد.
هدف امنیتی حالت اولیه درایو OE.INITIAL_DRIVE_STATE	محیط عملیاتی، افزاره انبارشی را ارائه می‌دهد که جدیداً تهیه‌شده یا مقداردهی اولیه شده‌اند و خالی از داده‌های محافظت‌شده در نواحی است که مورد هدف رمزنگاری نیستند. منطق: ازآنجایی‌که پروفایل حفاظتی مشترک مستلزم آن است که تمام داده‌های محافظت شده رمزنگاری شوند، فرض حالت اولیه درایو (A.INITIAL_DRIVE_STATE)، فرض را بر این می‌گذارد که حالت اولیه افزاره مورد هدف رمزنگاری کل درایو، خالی از داده‌های محافظت‌شده در نواحی‌ای از درایو است که رمزنگاری، فراخوانی نخواهد شد (مانند رکورد راه‌اندازی اصلی و نرم‌افزار از قبل احراز هویت شده اکتساب مجوز یا موتور رمزنگاری). با توجه به این حالت شروع معلوم، محصول (هنگامی‌که نصب و عملیاتی شد) اطمینان حاصل می‌کند که افرازهای (پارتیشن‌های) قالب‌های منطقی داده‌های در دسترس کاربر، محافظت‌شده هستند.
هدف امنیتی استحکام کلمه عبور OE.PASSPHRASE_STRENGTH	مدیر سیستم مجاز مسئول حصول اطمینان از انطباق عوامل مجوز عبارات عبور با دستورالعمل‌های شرکت استفاده‌کننده از محصول، است. منطق: کاربران به‌درستی آموزش می‌بینند، [فرض کاربر آموزش‌دیده (A.TRAINED_USER)] تا عوامل مجوز را منطبق با دستورالعمل‌های اجرایی ایجاد نمایند.

هدف امنیتی خاموش شدن OE.POWER_DOWN	حافظه فرّار بعد از خاموش شدن پاک می‌شود، بنابراین حملات باقی‌مانده در حافظه، غیر اجرایی می‌شوند. منطق: کاربران به‌درستی آموزش می‌بینند، [فرض کاربر آموزش‌دیده (A.TRAINED_USER)] تا افزاره‌های انبارش را قبل از خاموش شدن، بدون مراقبت رها نکنند یا آن را در حالت روشن مدیریت‌شده مانند حالت خواب زمستانی قرار دهند. فرض خاموش بودن (A.POWER_DOWN) تصریح می‌کند که حملات باقی‌مانده در حافظه با قرار گرفتن افزاره در حالت خاموش یا حالت خواب زمستانی، غیرفعال می‌شوند.
هدف امنیتی کاربرد واحد نشانه (توکن) بیرونی OE.SINGLE_USE_ET	توکن‌های بیرونی که شامل عوامل مجوز می‌باشند، برای هدف دیگری به‌جز ذخیره عوامل مجوز توکن‌های بیرونی، استفاده نخواهند شد. منطق: کاربران به‌درستی آموزش می‌بینند، [فرض کاربر آموزش‌دیده (A.TRAINED_USER)] تا از عوامل مجوز توکن‌های بیرونی برای موارد در نظر گرفته‌شده و نه برای اهداف دیگری استفاده کنند.
هدف امنیتی محیط رمزنگاری قوی OE.STRONG_ENVIRONMENT_CRYPTO	محیط عملیاتی، قابلیت کارکرد رمزنگاری‌ای را ارائه خواهد داد که متناسب با الزامات و قابلیت‌های محصول و پیوست ۱ است. منطق: تمام رمزنگاری‌های اجراشده در محیط عملیاتی و مورداستفاده توسط محصول، الزامات ذکرشده در این پروفایل حفاظتی مشترک [فرض رمزنگاری قوی (A.STRONG_CRYPTO)] را برآورده می‌سازند.
هدف امنیتی کاربر آموزش‌دیده OE.TRAINED_USERS	کاربران مجاز، به‌درستی آموزش می‌بینند و از تمام راهنمایی‌ها برای امن ساختن محصول و عوامل مجوز پیروی می‌نمایند. منطق: کاربران به‌درستی آموزش می‌بینند [فرض کاربران آموزش‌دیده (A.TRAINED_USER)] تا عوامل مجوز را مطابق با راهنمایی‌ها ایجاد نمایند، عوامل مجوز توکن‌های بیرونی را با افزاره ذخیره نکرده و محصول را در مواقع موردنیاز خاموش کنند [هدف امنیتی حالت سکو (OE.PLATFORM_STATE)] سکویی که افزاره انبارش در آن مقیم است (یا یک افزاره انبارش بیرونی به آن متصل است)، عاری از نرم‌افزارهای مخربی است که می‌تواند در عملکرد صحیح محصول اختلال ایجاد نماید. سکوی عاری از نرم‌افزارهای مخرب [هدف امنیتی حالت سکو (OE.PLATFORM_STATE)] از بردار حملاتی جلوگیری می‌کند که به‌طور بالقوه می‌تواند در عملکرد صحیح محصول اختلال ایجاد کند.

هدف امنیت حالت سکو OE.PLATFORM_STATE	سکویی که افزاره انبارش در آن قرار دارد (یا یک افزاره انبارش بیرونی به آن متصل است)، عاری از نرم‌افزارهای مخرب می‌باشد که به‌طور بالقوه می‌تواند در عملکرد صحیح محصول اختلال ایجاد نماید. منطق: سکوی عاری از نرم‌افزارهای مخرب [هدف امنیتی حالت سکو (OE.PLATFORM_STATE)] از بردار حملاتی جلوگیری می‌کند که به‌طور بالقوه می‌تواند در عملکرد صحیح محصول اختلال ایجاد نماید.
هدف امنیتی کارکرد شناسایی و احرازهویت سکو OE.PLATFORM_I&A	محیط عملیاتی، ساز و کارهای شناسایی و احراز هویت کاربر فردی را ارائه خواهد داد که مستقل از عوامل مجوز استفاده شده در محصول عمل می‌کنند. منطق: با اینکه ممکن است محصول، عوامل مجوز را برای واسط ورود سیستم‌عامل ارائه دهد، با این حال نباید قابلیت‌های کارکردی واسط واقعی را کاهش دهد یا در آن تغییری ایجاد نماید. فرض کارکرد شناسایی و احرازهویت سکو (A.PLATFORM_I&A)، مستلزم آن است که محصول در کارکردهای شناسایی و احراز هویت (I&A) سکو عادی تغییری ایجاد نکند یا در آن مداخله ننماید.

۶-الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول، به صورت خلاصه در بخش زیر آورده شده است.

جدول ۲ الزامات کارکردی محصول

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**اکتساب عامل مجوز ۱**	FCS_AFA.EXT.1.1
۲	**زنجیره‌ای کردن کلید ۱**	FCS_KYC_EXT.1.1
۳	**زنجیره‌ای کردن کلید ۲**	FCS_KYC_EXT.1.2
۴	**تخریب کلید رمزنگاری و اجزای کلید ۱**	FCS_CKM_EXT.4.1
۵	**تخریب کلید رمزنگاری ۱**	FCS_CKM.4.1

۶	**مشخصات کارکرد مدیریتی ۱**	FMT_SMF.1.1
۷	**حفاظت از کلید و اجزای کلید ۱**	FPT_KYP_EXT.1.1
۸	**به‌روزرسانی امن ۱**	FPT_TUD_EXT.1.1
۹	**به‌روزرسانی امن ۲**	FPT_TUD_EXT.1.2
۱۰	**به‌روزرسانی امن ۳**	FPT_TUD_EXT.1.3

۶-۱- کلاس پشتیبانی رمزنگاری

شماره الزام	نام الزام
۱	**اکتساب عامل مجوز ۱**

توابع هدف امنیتی باید عوامل مجوز زیر را بپذیرند: [انتخاب:

- Submask استخراج شده از عامل مجوز کلمه‌عبور مشروط به‌گونه‌ای که در الزام امنیتی ساخت و شرطی‌سازی کلمه‌عبور رمزنگاری (FCS_PCC_EXT.1) تعریف شده است.
- عامل کارت هوشمند بیرونی که حداقل طول بیت برابر با کلید رمزگذاری داده را داشته باشد و از submask تولید شده توسط محصول (با استفاده از تولیدکننده بیت تصادفی توصیف‌شده در الزام امنیتی عملیات رمزنگاری (تولید بیت تصادفی) (FCS_RBG_EXT.1)) محافظت می‌کند با استفاده از الگوریتم RSA[۲۶] (اندازه کلید ۲۰۴۸ یا بیشتر) محافظت شده است.

[۲۶] Rivest Shamir Adleman Algorithm

- عامل کارت هوشمند بیرونی که حداقل طول بیت برابر با کلید رمزگذاری داده را داشته باشد و از submask تولید شده توسط سکو میزبان محافظت می‌کند، با استفاده از RSA (اندازه کلید ۲۰۴۸ یا بیشتر) محافظت شده است.
- عامل نشانه (توکن) USB بیرونی که حداقل استحکام امنیتی برابر با مقدار رمزگذاری مرزی را داشته باشد و submask تولید شده توسط محصول را با استفاده از تولیدکننده بیت تصادفی توصیف شده در الزام امنیتی عملیات رمزنگاری (تولید بیت تصادفی) (FCS_RBG_EXT.1) ارائه می‌دهد.
- عامل نشانه (توکن) USB بیرونی که حداقل استحکام امنیتی برابر با مقدار رمزگذاری مرزی را داشته باشد و submask تولید شده توسط سکو میزبان را ارائه می‌دهد.].

نکته کاربردی ۱: این الزام مشخص می‌کند که محصول کدام یک از عوامل مجوز را از کاربر می‌پذیرد. کلمه‌عبور وارد شده توسط کاربر، یکی از عوامل مجوز است که محصول همانگونه که در الزام امنیتی ساخت و شرطی‌سازی کلمه‌عبور رمزنگاری (FCS_PCC_EXT.1) ، توضیح داده شد، باید بتواند برای آن شرط بگذارد. گزینه دیگر، عامل مجوز کارت هوشمند با ویژگی متمایز کننده در نحوه تولید ارزش- یا توسط تولیدکننده بیت تصادفی محصول یا توسط سکو می‌باشد. همچنین ممکن است از نشانه USB بیرونی به همراه مقدار submask تولید شده توسط تولیدکننده بیت تصادفی محصول یا توسط سکو استفاده شود.

محصول ممکن است هر تعداد از عوامل مجوز را بپذیرد که تحت عنوان «submask"ها طبقه‌بندی می شوند. نویسنده هدف امنیتی عوامل مجوز را که پشتیبانی می‌کند انتخاب کرده و ممکن است چندین روش برای یک انتخاب وجود داشته باشد.

استفاده از عوامل مجوز متعدد ترجیح داده می شود؛ اگر بیشتر از یک عامل مجوز استفاده شده باشد، submask های تولید شده باید با استفاده از الزام امنیتی ترکیب submask (FCS_SMC_EXT.1) که در پیوست ۱ توضیح داده شده است، ترکیب شوند.

۲	**زنجیره‌ای کردن کلید ۱**

توابع هدف امنیتی باید حاوی زنجیره‌ای از کلیدها باشد: [انتخاب: یک، استفاده از submask ای به عنوان مقدار رمزگذاری مرزی؛ کلیدهای میانی صادر شده از یک یا چندین submask برای محدوده مقدار رمزگذاری مرزی که از روش‌های زیر استفاده می‌کند: [انتخاب: استخراج کلید به نحوی که در الزام امنیتی استخراج کلید رمزنگاری

(FCS_KDF_EXT.1) توصیف شده است، پوشاندن کلید به نحوی که در الزام امنیتی عملیات رمزنگاری- پوشاندن کلید ((FCS_COP.1(d)) توصیف شده است، ترکیب کلید به نحوی که در الزام امنیتی ترکیب (FCS_SMC_EXT.1) submask تو صیف شده ا ست، انتقال کلید به نحوی که در الزام امنیتی عملیات رمزنگاری- انتقال کلید ((FCS_COP.1(e)) توصیف شده است، رمزگذاری کلید به نحوی که در الزام امنیتی عملیات رمزنگاری- رمزگذاری کلید ((FCS_COP.1(g)) توصیف شده است]] درحالیکه استحکام اثربخش [انتخاب: ۱۲۸ بیت،۲۵۶ بیت] را حفظ می‌کند.	
زنجیره‌ای کردن کلید ۲	۳
الزام امنیتی زنجیره‌ای کردن کلید (FCS_KYC_EXT.1.2) توابع هدف امنیتی باید یک مقدار رمزگذاری مرزی [انتخاب: ۱۲۸ بیت، ۲۵۶ بیت] را برای موتور رمزگذاری [انتخاب: تنها بعد از اینکه توابع هدف امنیتی فرایند اعتبارسنجی را به نحوی که در الزام امنیتی اعتبارسنجی (FCS_VAL_EXT.1) توصیف شده است، بدون اعتبارسنجی در حال وقوع، با موفقیت انجام داده است]، ارائه دهد. **نکته کاربردی ۲:** زنجیره‌ای کردن کلید، روشی است که از چندین لایه کلید رمزگذاری استفاده می‌کند تا در نهایت مقدار رمزگذاری مرزی را امن سازد. تعداد کلیدهای میانی متفاوت خواهد بود - از یک (مانند در نظر گرفتن عامل مجوز کلمه‌عبور و استفاده از آن به عنوان مقدار رمزگذاری مرزی) تا بسیار. این موضوع برای تمام کلیدهایی که در پوشاندن نهایی یا استخراج مقدار رمزگذاری مرزی نقش دارند، اعمال می‌شود؛ از جمله آن‌هایی که در نواحی افزاره انبارش حفاظت شده، قرار دارند (مانند کلیدهای ذخیره شده واحد بستر قابل اعتماد، مقادیر مقایسه‌ای). تا زمانیکه تمام زنجیره‌ها، الزامات زنجیره کلید را برآورده سازند، زنجیره‌های کلید مختلف تا مقدار رمزگذاری مرزی، اجازه داده شده است. زمانیکه نویسنده هدف امنیتی رو شی را برای ایجاد زنجیره انتخاب می‌کند (چه با ا ستخراج کلید یا عدم پو شاندن آن‌ها یا کلیدهای رمزگذاری یا با ا ستفاده از انتقال کلید RSA)، الزامات مناسب را از پیوست ۲ بیرون خواهند کشید. برای یک پیاده‌سازی استفاده از هرکدام یا تمام این روش‌ها، مجاز است. برای الزام امنیتی زنجیره‌ای کردن کلید (FCS_KYC_EXT.1.2) فرایند اعتبارسنجی در پیوست ۲ از الزام امنیتی اعتبارسنجی (FCS_VAL_EXT.1)، تعریف شده است. اگر آن انتخاب توسط نویسنده هدف امنیتی انجام شود، آنگاه FCS_VAL_EXT.1 در بدنه هدف امنیتی قرار داده می‌شود.	

رو شی که هدف ارزیابی برای زنجیره کردن کلیدها و مدیریت یا حفاظت آن‌ها ا ستفاده می‌کند در شرح مدیریت کلید تو ضیح داده شده ا ست. برای اطلاعات بی‌شتر شرح مدیریت کلید را ببینید.	
تخریب کلید رمزنگاری و اجزای کلید ۱	۴
توابع هدف امنیتی باید تمام کلیدها یا اجزای کلید که دیگر موردنیاز نیستند را از بین ببرد. **نکته کاربردی ۳:** کلیدها از جمله کلیدهای میانی و اجزای کلید را که دیگر موردنیاز نیستند را باید با استفاده از روش تأییدشده تخریب کلید رمزنگاری و اجزای کلید (FCS_CKM.4.1) در حافظه فرّار از بین برد. نمونه‌هایی از کلیدها، کلیدهای میانی، sub maskها و مقادیر رمزنگاری مرزی می‌باشند. مواردی نیز وجود دارد که کلیدها یا اجزای کلید که در انبارش پایدار وجود دارند، دیگر موردنیاز نیستند و لازم است تا از بین بروند. بر اساس پیاده‌سازی، فروشندگان توضیح می‌دهند که چه زمانی کلیدهای خاصی دیگر موردنیاز نیستند. شرایط متعددی وجود دارد که در آن وجود اجزای کلید بیش از این ضرورت ندارد، مانند، یک کلید پوشانده شده که ممکن است هنگامی‌که کلمه عبور تغییر کرد، دیگر موردنیاز نباشد. بااین‌حال مواردی هم وجود دارد که کلیدها اجازه دارند در حافظه باقی بمانند، مانند کلید شناسایی افزاره.	
تخریب کلید رمزنگاری ۱	۵
توابع هدف امنیتی باید کلیدهای رمزنگاری را مطابق با شیوه پاک کردن کلید رمزنگاری مشخص‌شده پاک کنند [انتخاب: برای حافظه فرّار، پاک کردن باید توسط بازنویسی مستقیم منحصر به فرد انجام شود [انتخاب: متشکل از الگوی شبه‌تصادفی با استفاده از تولیدکننده بیت تصادفی توابع هدف امنیتی، متشکل از الگوی شبه‌تصادفی با استفاده از تولیدکننده بیت تصادفی سکو میزبان، متشکل از صفرها] که با خواندن - تأیید دنبال می‌شود. برای حافظه غیر فرّار پاک کردن باید با موارد زیر اجرا شود: یک [انتخاب: یک، سه یا دفعات بیشتری] از بازنویسی مکان انبارش داده کلید شامل [انتخاب: الگوی شبه‌تصادفی با استفاده از تولیدکننده بیت تصادفی توابع هدف امنیتی همانگونه که در الزام امنیتی عملیات رمزنگاری- تولید بیت تصادفی (FCS_RGB_EXT.1) توضیح داده شده است، الگوی شبه تصادفی با استفاده از تولیدکننده بیت تصادفی	

سکو میزبان، الگوی ثابت]، که توسط [انتخاب: خواندن- تأیید، هیچ] دنبال می‌شود. اگر خواندن – درستی‌سنجی داده‌های بازنویسی شده با شکست مواجه شود، فرایند دوباره باید تکرار شود؛] که [انتخاب: NIST SP800-88، هیچ استانداردی] را برآورده می‌سازد.

نکته کاربردی ۴: نکته کاربردی: کلیدها از جمله کلیدهای میانی یا اجزای کلید، که دیگر مورد نیاز نمی‌باشند با استفاده از یکی از این متدهای پذیرفته شده، در حافظه فرّار از بین می‌روند. در این موارد، روش تخریب با یکی از روش‌های توضیح داده شده در این الزام، مطابقت دارد. این الزام روشی را برای انجام پاک کردن رمزنگاری فراخوانی می‌کند و شرایط به خوبی تعریف شده‌ای را برای تخریب اطلاعات کلید، در نظر می‌گیرد. بعضی از راه‌حل‌ها، دسترسی نوشتن در مکان‌هایی از رسانه که کلید ذخیره شده است را پشتیبانی می‌کنند، بنابراین مجوز تخریب کلیدهای رمزنگاری از طریق بازنویسی مستقیم کلید و داده‌های اجزای کلید را نیز صادر می‌کنند. در دیگر موارد تکنیک‌های مجازی‌سازی انبارش روی سامانه و یا سطح افزاره می‌تواند منجر به نسخه‌های متعدد از داده کلید شده و یا فناوری رسانه زیرین از بازنویسی مستقیم مکان‌هایی که داده‌های کلید ذخیره شده‌اند پشتیبانی نکند. توجه داشته باشید حافظه‌هایی که یک بار قابل برنامه‌ریزی شدن هستند مستثنی هستند.

۶-۲- کلاس مدیریت امنیت

شماره الزام	نام الزام
۶	**مشخصات کارکرد مدیریتی ۱**

توابع هدف امنیتی باید قادر به انجام توابع مدیریتی زیر باشد:

[

ارسال درخواست تغییر کلید رمزگذاری داده به موتور رمزگذاری،

ارسال درخواست پاک کردن رمزنویسی کلید رمزگذاری داده به موتور رمزگذاری،

اجازه به کاربران مجاز برای تغییر عوامل مجوز یا مجموعه‌ای از عوامل مجوز استفاده شده،

آغاز به روزرسانی نرم‌افزار یا سفت‌افزار محصول

[انتخاب: هیچ تابع دیگری، [انتخاب: ایجاد عوامل مجوز با استفاده از تولیدکننده بیت تصادفی توابع هدف امنیتی، پیکربندی عوامل مجوز، پیکربندی قابلیت رمزنگاری، غیرفعال کردن قابلیت بازیابی کلید، به‌روزرسانی امن کلید عمومی مورد نیاز برای به‌روزرسانی امن، [اختصاص: دیگر توابع مدیریتی ارائه شده توسط توابع هدف امنیتی]].]

نکته کاربردی ۵: هدف از این الزام، بیان قابلیت‌های مدیریتی است که محصول در اختیار دارد. این بدان معنی است که محصول باید بتواند فهرستی از توابع را انجام دهد. مورد (ه) برای تعیین قابلیت‌هایی استفاده می‌شود که محصول ممکن است شامل آن‌ها باشد، اما نیازی نیست با این پروفایل حفاظتی مشترک مطابقت داشته باشد. پیکربندی قابلیت رمزنگاری، می‌تواند شامل توابع مدیریت کلید باشد، به عنوان مثال مقدار رمزگذاری مرزی پوشانده یا رمزگذاری خواهد شد و موتور رمزگذاری نیاز دارد تا این مقدار را رمزگشایی کند یا از حالت پوشیده خارج نماید. در مورد (ه) اگر هیچ تابع مدیریت دیگری ارائه نشود (یا ادعا نشود)، آنگاه "هیچ تابع دیگری" باید انتخاب شود.

تغییر کلید رمزگذاری داده، به داده‌هایی نیاز دارد تا با کلید رمزگذاری داده جدید دوباره رمزگذاری شـــود، اما به کاربران این اجازه را بدهد تا بتوانند کلیدهای رمزگذاری جدید را تولید کنند.

برای اهداف این سند، پاکسازی کلید به معنای از بین بردن کلید رمزگذاری داده با استفاده از یکی از روش‌های تخریب پذیرفته شده، می‌باشد. در بعضی از پیاده‌سازی‌ها، تغییر کلید رمزگذاری داده می‌تواند همان کارکردی را داشته باشد که پاک کردن رمزنگاری کلید رمزگذاری داده دارد.

۶-۳- کلاس حفاظت از توابع هدف امنیتی

شماره الزام	نام الزام
۷	**حفاظت از کلید و اجزای کلید ۱**

توابع هدف امنیتی باید تنها زمانی کلیدها را در حافظه غیر فرّار ذخیره ســـازند که مطابق موارد مشـــخص شـــده در الزام امنیتی عملیات رمزنگاری- پوشـــاندن کلید ((FCS_COP.1 (d) پو شیده شده با شد، یا مطابق با تو ضیحات الزام امنیتی عملیات رمزنگاری -رمزگذاری کلید (FCS_COP.1 (g)) یا الزام امنیتی عملیات رمزنگاری - انتقال کلید (FCS_COP.1 (e)) رمزگذاری شده باشند، مگر آنکه کلید از هرکدام از معیارهای زیر تبعیت کند [انتخاب:

کلید متن خام بخشی از زنجیره کلید نباشد، همانگونه که در الزام امنیتی زنجیره‌ای کردن کلید (FCS_KYC_EXT.1) توضیح داده شده است.

کلید متن خامی که دیگر دسترسی به داده رمزگذاری شده را بعد از آماده‌سازی اولیه، فراهم نخواهد کرد.

کلید متن خام انشعاب کلیدی است که مطابق توضیحات الزام امنیتی ترکیب submask (FCS_SMC_EXT.1) ترکیب شده است و نیمی دیگر از انشعاب کلید یکی از این موارد است[انتخاب: پو شیده شده مطابق تو ضیحات الزام امنیتی عملیات رمزنگاری - پو شاندن کلید ((FCS_COP.1 (d) یا رمزگذاری شده مطابق تو ضیحات الزام امنیتی عملیات رمزنگاری -رمزگذاری کلید (FCS_COP.1 (g)) یا الزام امنیتی عملیات رمزنگاری - انتقال کلید (FCS_COP.1 (e))) یا استخراج شده و در حافظه غیر فرّار ذخیره نشده است.]

کلید متن خام در یک افزاره انبارش بیرونی برای استفاده به عنوان یک عامل مجوز استفاده ذخیره شده است.

کلید متن خام برای [انتخاب: پوشاندن کلید مطابق توضیحات الزام امنیتی عملیات رمزنگاری - پوشاندن کلید ((FCS_COP.1 (d)) یا رمزگذاری مطابق توضیحات الزام امنیتی عملیات رمزنگاری -رمزگذاری کلید (FCS_COP.1 (g)) یا الزام امنیتی عملیات رمزنگاری - انتقال کلید (FCS_COP.1 (e))) که در حال حاضر [انتخاب: مطابق توضیحات FCS_COP.1(d)) پوشانده شده است، مطابق توضیحات FCS_COP.1(g)) یا رمزگذاری شده است]]، استفاده شده است. **نکته کاربردی ۶:** انبارش کلید متن خام در حافظه غیر فرّار به چند دلیل مجاز است. اگر کلیدهای موجود در حافظه حفاظت شده باشد که برای کاربر در محصول یا محیط عملیاتی قابل دسترسی نباشند، تنها روش‌هایی که اجازه می‌دهند، نقش امنیتی مرتبط را برای محافظت از مقدار رمزگذاری مرزی یا کلید رمزگذاری داده ایفا کنند، این است که یک انشعاب کلید یا لایه‌های افزوده‌های ارائه دهنده پوشاندن یا رمزگذاری کلید که محافظت شده‌اند وجود داشته باشد.	
به‌روزرسانی امن ۱	۸
توابع هدف امنیتی باید برای کاربران مجاز توانایی پرس‌وجوی نسخه فعلی نرم‌افزار یا سفت افزار محصول را ارائه دهد.	
به‌روزرسانی امن ۲	۹
توابع هدف امنیتی باید برای کاربران مجاز توانایی آغاز به‌روزرسانی نرم‌افزار یا میان‌افزار محصول را ارائه دهد.	
به‌روزرسانی امن ۳	۱۰
توابع هدف امنیتی باید به‌روزرسانی‌های میان‌افزار یا نرم‌افزار محصول را با استفاده از امضای دیجیتال سازنده قبل از نصب آن به‌روزرسانی‌ها، بررسی کند. **نکته کاربردی ۷:** سازوکار امضای دیجیتال که در عنصر سوم مورداشاره قرارگرفته است، یکی از موارد توصیف‌شده در الزام کارکرد امنیتی عملیات رمزنگاری درستی سنجی امضا ((FCS_COP.1(a)) در پیوست ۱ است. درحالی‌که این مؤلفه نیاز دارد تا محصول قابلیت‌های به‌روزرسانی را خود پیاده سازی کند، اعمال کنترل‌های رمزنگاری با استفاده از کارکردهای در دسترس در محیط عملیاتی، قابل‌قبول است.	

۷- الزامات تضمین امنیت

این پروفایل حفاظتی مشترک الزامات تضمین امنیتی (SAR) را شناسایی می‌کند تا میزانی که ارزیاب مستندات را برای ارزیابی کاربرد پذیر تعیین می‌کند و آزمون‌های مستقل را انجام می‌دهد بیان کند. اقدامات ارزیابی منحصر به فردی که باید انجام شود، در سند پشتیبانی کننده (سند فنی الزامی) رمزگذاری کل درایو: اکتساب مجوز ژانویه ۲۰۱۵، توضیح داده شده است

قابل توجه نویسندگان محصول: انتخابی در ASE_TSS وجود دارد که باید انجام شود. هر فرد به سادگی نمی‌تواند به الزامات تضمین امنیتی در این پروفایل حفاظتی مشترک ارجاع دهد.

مدل کلی ارزیابی هدف‌های ارزیابی بر اساس اهداف امنیتی نوشته شده‌اند تا همانگونه که در ادامه می‌آید با این پروفایل حفاظتی مشترک مطابقت داشته باشد: بعد از آنکه هدف امنیتی برای ارزیابی مورد تصویب قرار گرفت، افزارگان ارزیابی امنیت فناوری اطلاعات (ITSEF)، محصول، فناوری اطلاعات محیطی پشتیبانی کننده، (اگر نیاز باشد) و راهنمایی کاربر یا مدیرسیستم برای محصول را به دست خواهد آورد. از افزارگان ارزیابی امنیت فناوری اطلاعات انتظار می‌رود تا اقدامات الزامی شده توسط متدولوژی ارزیابی مشترک (CEM) را برای الزامات تضمین امنیت پشتیبانی چرخه حیات (ALC) و ارزیابی هدف امنیتی (ASE) اعمال کند. همچنین افزارگان ارزیابی امنیت فناوری اطلاعات، اقدامات ارزیابی همراه با اسناد پشتیبانی را انجام می‌دهد که قبلاً به عنوان تفسیری از دیگر الزامات تضمین متدولوژی ارزیابی مشترکی در نظر گرفته شده است که برای تکنولوژی خاص معرفی شده در محصول به‌کار برده می‌شود. اقدامات ارزیابی که توسط اسناد پشتیبانی اتخاذ شده است، به روشی مشخص مواردی که توسعه‌دهنده برای ارائه اثبات انطباق محصول با این پروفایل حفاظتی مشترک نیاز دارد را ارائه می‌دهد.

جدول ۳ الزامات تضمین امنیت

نام کلاس	نام الزام	توضیحات
Security Target(ASE)	ASE_CCL.1	ادعاهای انطباق

	ASE_ECD.1	تعریف مؤلفه‌های توسعه‌یافته
	ASE_INT.1	معرفی هدف امنیتی
	ASE_OBJ.1	اهداف امنیتی برای محیط عملیاتی
	ASE_REQ.1	الزامات امنیتی اعلام‌شده
	ASE_SPD.1	تعریف مسائل امنیتی
	ASE_TSS.1	خلاصه مشخصات محصول
Development(ADV)	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents(AGD)	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests(ATE)	ATE_IND.1	آزمون مستقل – انطباق
Vulnerability Assessment(AVA)	AVA_VAN.1	بررسی آسیب‌پذیری
Life cycle Support(ALC)	ALC_CMC.1	برچسب‌گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

۷-۱- ارزیابی هدف امنیتی (ASE)

هدف امنیتی به ازای هر اقدام ارزیابی هدف امنیت (ASE) تعریف شده در متدولوژی ارزیابی مشترک، ارزیابی می‌شود. علاوه بر این، ممکن است اقدامات ارزیابی مشخص شده در اسناد پشتیبانی که توضیحات ضروری را برای گنجاندن در خلاصه مشخصه محصول (TSS) که خاص نوع فناوری محصول می‌باشد فراخوانی کند.

الزامات کارکرد امنیتی در این پروفایل مشترک، به پیاده‌سازی‌های منطبق اجازه ادغام طیف گسترده‌ای از رویکردهای مدیریت کلید قابل قبول را تا زمانی که اصول اصلی برآورده شوند می‌دهد. با توجه به حیاتی بودن طرح مدیریت کلید، این پروفایل حفاظتی مشترک مستلزم آن است که توسعه دهنده شرح مفصلی از پیاده‌سازی مدیریت کلید خود را ارائه دهد. این اطلاعات می‌تواند به عنوان پیوست هدف امنیتی ارسال شود و از آنجا که انتظار نمی‌رود چنین سطحی از جزئیات در دسترس عموم قرار بگیرد به صورت اختصاصی مشخص می‌شود. در پیوست ۵ جزئیات مورد انتظار از توصیف مدیریت کلید توسعه دهنده را ببینید.

علاوه بر این اگر محصول شامل تولید اعداد تصادفی باشد، در پیوست ۴ توضیحاتی در مورد اطلاعاتی که انتظار می‌رود با توجه به کیفیت آنتروپی ارائه گردد، فراهم آمده است.

پالایش ASE_TSS.1.1C: خلاصه مشخصات محصول، باید توضیح دهد که چگونه محصول هریک از الزامات کارکرد امنیتی را برآورده می‌سازد، از جمله شرح مدیریت کلید اختصاصی (پیوست ۵) و [انتخاب: نوشتار[۲۷] آنتروپی، هیچ مستند اختصاصی مشخص شده پروفایل حفاظتی مشترک].

۷-۲- توسعه (ADV)

اطلاعات طراحی درباره محصول همچنین بخش خلاصه مشخصه محصول هدف امنیتی، و هرگونه اطلاعات اضافه مورد نیاز این پروفایل حفاظتی مشترک که نباید عمومی شود (مانند نوشتار آنتروپی) در مستندات راهنمایی در دسترس برای کاربر نهایی گنجانده شده است.

۷-۲-۱- مشخصات کارکردی اصلی (ADV_FSP.1)

مشخصات کارکردی، واسط‌های توابع هدف امنیتی را توصیف می‌کند (TSFI ها). داشتن مشخصات کامل و رسمی این واسط‌ها ضروری نمی‌باشد. علاوه بر این، به دلیل اینکه اهداف ارزیابی منطبق بر این پروفایل حفاظتی مشترک ضرورتاً واسط‌هایی برای محیط عملیاتی دارند که مستقیماً قابل فراخوانی توسط کاربران محصول نمی‌باشد، اشاره مختصری وجود دارد که مشخص کننده این است که چنین واسط‌هایی توضیح داده شده و از آن‌ها تنها آزمودن غیر مستقیم

[۲۷] Essay

چنین واسط‌هایی ممکن است امکان‌پذیر باشد. برای این پروفایل حفاظتی مشترک، اقدامات ارزیابی برای این خانواده، بر روی فهم واسط‌های ارائه شده در خلاصه مشخصه محصول در پاسخ به الزامات کارکردی و واسط‌های ارائه شده در اسناد راهنما تمرکز دارد. هیچ سند اضافه‌ای از "مشخصات کارکردی" برای برآوردن اقدامات ارزیابی مشخص شده در اسناد پشتیبانی لازم نمی‌باشد.

اقدامات ارزیابی در اسناد پشتیبانی با الزامات کارکرد امنیت کاربرد پذیر مرتبط هستند؛ از آنجایی که این اقدامات مستقیماً با الزامات کارکرد امنیتی در ارتباط هستند، ردگیری عنصر ADV_FSP.1.2D در حال حاضر به طور ضمنی انجام شده و هیچ سند اضافه‌ای لازم نمی‌باشد.

۷-۳- مستندات راهنما (AGD)

مستندات راهنما با هدف امنیتی ارائه خواهد شد. این راهنمایی‌ها باید شامل شرحی از نحوه بررسی پرسنل IT در ارتباط با ایفای نقش محیط عملیاتی برای توابع امنیتی باشد. مستندات باید در یک سبک غیر رسمی و قابل خواندن توسط پرسنل IT ارائه شود.

همانگونه که در هدف امنیتی ادعا شده است این راهنمایی‌ها باید برای هر محیط عملیاتی ارائه شود که محصول از آن پشتیبانی می‌کند. این راهنمایی شامل:

- دستورالعمل‌هایی برای نصب موفقیت آمیز توابع هدف امنیتی (TSF) در آن محیط؛ و
- دستورالعمل‌هایی برای مدیریت امنیت توابع هدف امنیتی (TSF) به عنوان یک محصول و یک مؤلفه از محیط عملیاتی بزرگ‌تر؛ و
- دستورالعمل‌هایی برای فراهم کردن قابلیت‌های اجرایی محافظت شده.

همچنین باید راهنمایی‌های مربوط به توابع امنیتی خاصی ارائه شود؛ الزامات چنین راهنمایی‌هایی در اقدامات ارزیابی مشخص شده در اسناد پشتیبانی وجود دارد.

۷-۳-۱- راهنمای کاربری (AGD_OPE.1)

راهنمای کاربری نباید در یک سند مجزا وجود داشته باشد. راهنمای کاربران، مدیران‌سیستم و توسعه‌دهندگان برنامه‌های کاربردی می‌تواند در میان اسناد یا صفحات وب منتشر شوند.

توسعه‌دهنده باید اقدامات ارزیابی موجود در اسناد پشتیبانی را مورد بازبینی قرار دهد تا جزئیات راهنمایی‌ای را که ارزیاب بررسی خواهد کرد معین کند. این کار اطلاعات ضروری را برای آماده‌سازی راهنمای قابل قبول ارائه می‌دهد.

۷-۳-۲- راهنمای آماده‌سازی (AGD_PRE.1)

با راهنمای عملیاتی، توسعه‌دهنده باید به دنبال اقدامات ارزیابی باشد تا محتوای مورد نیاز را با توجه به راهنمای آماده‌سازی تعیین کند.

۷-۴- کلاس پشتیبانی چرخه حیات (ALC)

در سطح اطمینان فراهم شده برای اهداف ارزیابی منطبق بر این پروفایل حفاظتی مشترک، پشتیبانی چرخه حیات به جوانب قابل مشاهده کاربر نهایی از چرخه حیات تا آزمایش توسعه مربوط به فروشنده محصول و فرایند مدیریت پیکربندی محدود می‌شود. این به معنای تضعیف نقش حیاتی اقدامات توسعه‌دهنده در کمک به امن بودن کلی محصول نمی‌باشد؛ بلکه بازتابی از اطلاعاتی است که باید برای ارزیابی در این سطح اطمینان در دسترس باشد.

۷-۴-۱- برچسب‌گذاری محصول (ALC_CMC.1)

این مؤلفه در شناسایی محصول مورد هدف است به طوری که بتوان آن را از دیگر محصولات یا نسخه‌های همان فروشنده متمایز کرد و زمانیکه توسط کاربر نهایی تهیه می‌شود، بتواند به آسانی مشخص شود. ارزیاب، واحدهای کار متدولوژی ارزیابی مشترک مرتبط با ALC_CMC.1 را انجام می‌دهد.

۷-۴-۲- پوشش پیکربندی محصول (ALC_CMS.1)

با توجه به دامنه محصول و الزامات شواهد ارزیابی مرتبط با آن، ارزیاب واحدهای کار متدولوژی ارزیابی مشترک را مطابق با ALC_CMS.1 انجام می‌دهد.

۷-۵- کلاس آزمون‌ها (ATE)

آزمودن برای جنبه‌های کارکردی سامانه و نیز جوانبی که از نقاط ضعف پیاده‌سازی یا طراحی منافعی می‌برند مشخص شده است. اولی از طریق خانواده ATE_IND و دومی از طریق خانواده AVA_VAN انجام شده است. برای این پروفایل حفاظتی مشترک، آزمودن بر اساس قابلیت‌های کارکردی اعلام شده و واسط‌هایی، همراه با وابستگی در دسترس بودن اطلاعات طراحی، می‌باشد. یکی از خروجی‌های اصلی فرایند ارزیابی، همانگونه که در الزامات زیر مشخص شده است. گزارش آزمون می‌باشد.

۷-۵-۱- آزمون مستقل- انطباق (ATE_IND.1)

آزمودن برای تأیید قابلیت کارکردی توصیف شده در خلاصه مشخصه محصول و نیز راهنمای عملیاتی (شامل دستورالعمل‌های "پیکربندی ارزیابی شده") انجام شده است. تمرکز این آزمون تأیید برآورده شدن الزاماتی است که در بخش ۵ مشخص شده‌اند. اقدامات ارزیابی اسناد پشتیبانی، اقدامات آزمودن خاصی را مشخص می‌کند که برای بررسی انطباق با الزامات کارکرد امنیتی ضروری می‌باشند. ارزیاب گزارش آزمون را ارائه می‌دهد که مستند کننده طرح و نتایج آزمون و نیز پوشش استدلال‌های متمرکز بر ترکیبات سکو محصول می‌باشد که ادعای انطباق با این پروفایل حفاظتی مشترک را دارند.

۷-۶- کلاس ارزیابی آسیب‌پذیری (AVA)

برای تولید اول این پروفایل حفاظتی مشترک، انتظار می‌رود که کمیته فنی بین‌المللی (iTC) به بررسی منابع باز بپردازد که آسیب‌پذیری‌های کشف شده را برای این نوع از این محصولات کشف کند و آن محتوا را برای مبحث AVA_VAN فراهم سازد. در اکثر موارد، این آسیب‌پذیری‌ها به مهارتی فراتر از مهاجم اصلی نیاز دارند. این اطلاعات در توسعه پروفایل‌های حفاظتی آینده، استفاده خواهند شد.

۷-۶-۱- بررسی آسیب‌پذیری (AVA_VAN.1)

پیوست ۱ همراه با سند پشتیبانی کننده، راهنمایی برای ارزیاب جهت انجام تحلیل آسیب‌پذیری ارائه می‌دهد.

پیوست ۱ الزامات اختیاری

همانطور که در مقدمه این پروفایل حفاظتی مشترک بیان شد، الزامات پایه (آن‌هایی که باید توسط محصول انجام شود) در بدنه این پروفایل حفاظتی مشترک وجود دارد. علاوه بر این، دو نوع دیگر از الزامات در پیوست‌های ۱ و ۲ مشخص شده‌اند.

اولین نوع (در این پیوست) الزاماتی است که می‌تواند در هدف امنیتی وجود داشته باشد اما به منظور ادعای انطباق برای محصول با این پروفایل حفاظتی مشترک ضروری نیست. نوع دوم (در پیوست ۲) الزاماتی مبتنی بر انتخاب‌هایی در بدنه پروفایل حفاظتی مشترک می‌باشد: اگر انتخاب معینی انجام شود، آنگاه الزامات اضافه‌ای در آن پیوست نیاز است تا در بدنه هدف امنیتی قرار بگیرد (مانند پروتکل‌های رمزنگاری انتخاب شده در الزامات کانال امن).

بعضی از الزامات در این بخش تکرار شداند، اما از آنجا که نویسنده هدف امنیتی در برابر ترکیب الزامات مناسب از ضمائم به بدنه هدف امنیتی آن‌ها، مسئول می‌باشد، تعداد تکرار صحیح به نویسنده هدف امنیتی واگذار می‌شود.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۱	عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار اولیه) ۱	FCS_SNI_EXT.1.1
۱۲	عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار اولیه) ۲	FCS_SNI_EXT.1.2
۱۳	عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار اولیه) ۳	FCS_SNI_EXT.1.3
۱۴	تولید کلید رمزنگاری (کلیدهای نامتقارن) ۱	FCS_CKM.1(b)
۱۵	تولید کلید رمزنگاری (کلیدهای متقارن) ۱	FCS_CKM.1(c)
۱۶	ترکیب submask ۱	FCS_SMC_EXT.1.1
۱۷	اعتبارسنجی ۱	FCS_VAL_EXT.1.1
۱۸	اعتبارسنجی ۲	FCS_VAL_EXT.1.2
۱۹	اعتبارسنجی ۳	FCS_VAL_EXT.1.3
۲۰	عملیات رمزنگاری (درستی‌سنجی امضا) ۱	FCS_COP.1(a)
۲۱	عملیات رمزنگاری (الگوریتم چکیده‌ساز) ۱	FCS_COP.1(b)
۲۲	عملیات رمزنگاری (الگوریتم چکیده‌ساز کلیدی) ۱	FCS_COP.1(c)

۱. کلاس: پشتیبانی رمزنگاری

همانطور که در بدنه این پروفایل حفاظتی مشترک مشخص شد، برای محصول قابل قبول است که یا به طور مستقیم کارکردهای رمزنگاری‌ای پیاده‌سازی نماید که از فرایند رمزگذاری رمزگشایی درایو پشتیبانی می‌کند و یا از این کارکردها در محیط عملیاتی استفاده کند (به عنوان مثال فراخوانی واسط ارائه دهنده رمزنگاری سیستم‌عامل؛ کتابخانه رمزنگاری طرف سوم؛ یا یک شتاب دهنده رمزنگاری سخت‌افزاری). الزامات این بخش، قابلیت کارکردی رمزنگاری را مشخص

می‌کند که باید در این محصول یا در محیط عملیاتی وجود داشته باشد تا محصول اهداف امنیتی را برآورده سازد. چنانچه قابلیت کارکردی در محصول ارائه شود، این الزامات توسط نویسنده هدف امنیتی به بدنه هدف امنیتی انتقال می‌یابد.

اگر قابلیت کارکردی صرفاً مورد استفاده محصول باشد و توسط محیط عملیاتی فراهم شده باشد، آنگاه توسعه دهنده توابعی را در هر محیط عملیاتی شناسایی خواهد کرد که در هدف امنیتی فهرست شده است. این شناسایی باید به گونه‌ای باشد که ارزیاب بتواند از اطلاعات مشخصات خلاصه محصول (که مستلزم آن است که روشی که توسط هرکدام از عملیات فراخوانی می‌شود، شناسایی شود) به همراه اطلاعات توابع در محیط عملیاتی استفاده کند تا اقداماتی را برای اعتباردهی هریک از محیط‌های عملیاتی فهرست شده برای محصول انجام دهد و درنتیجه بتواند الزامات این بخش را برآورده سازد. ارزیاب محیط عملیاتی را بررسی می‌کند تا اطمینان حاصل کند که محیط عملیاتی آن توابع را عرضه کرده و واسط‌هایی در مستندات محیط عملیاتی موجود است.

شماره الزام	نام الزام
۱۱	**عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار) ۱**
توابع هدف امنیتی تنها باید از salt هایی استفاده کند که توسط [انتخاب: تولید اعداد تصادفی به‌نحوی‌که در الزام کارکرد امنیتی تولید عدد تصادفی (FCS_RBG_EXT.1) توصیف‌شده است، تولید اعداد تصادفی ارائه‌شده توسط سکوی میزبان] تولیدشده است.	
۱۲	**عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار) ۲**
توابع هدف امنیتی تنها از مقدار مقطعی منحصربه‌فرد با حداقل اندازه [۶۴] بیت استفاده می‌کند.	
۱۳	**عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار) ۳**
توابع هدف امنیتی باید بردارهای اولیه را به شیوه زیر ایجاد نماید: [CBC (زنجیره قالب‌های رمز): بردارهای اولیه باید غیرتکراری باشند. CCM (کد احراز اصالت پیام زنجیره‌ای قالب‌های رمز شمارگر): مقدار مقطعی باید غیرتکراری باشند.	

XTS (قالب رمز قابل پیچاندن بلوک XEX (XOR رمزنگاری XOR) با سرقت متن رمز): بدون بردار اولیه. مقادیر تنظیم‌شده باید اعداد صحیح غیر منفی باشند که به طور متوالی اختصاص می‌یابند و با عدد صحیح غیر منفی دلخواه شروع می‌شود. GCM (سبک شمارنده گالیوس): بردار اولیه باید غیرتکراری باشد. تعداد فراخوانی‌های GCM برای کلید مخفی‌شده نباید از 2^{32} تجاوز کند.]. **نکته کاربردی ۸:** این الزام تعدادی از عامل‌های مهم را پوشش می‌دهد-salt باید تصادفی باشد اما مقادیر مقطعی (nonce ها) تنها باید یکتا باشند. FCS_SNI_EXT.1.3 مشخص می‌کند که چگونه بردار اولیه باید برای هر مد رمزگذاری ساماندهی شود. زنجیره قالب‌های رمز، قالب رمز قابل پیچاندن بلوک XEX (XOR رمز گذاری XOR و سبک شمارنده گالیوس برای رمزگذاری استاندارد رمزگذاری پیشرفته داده‌ها مجاز می‌باشند. AES-CCM یک مد مجاز برای پوشاندن کلید می‌باشد.	
تولید کلید رمزگذاری (کلیدهای نامتقارن) ۱	۱۴
توابع هدف امنیتی باید کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم تولید کلید رمزنگاری مشخص شده، تولید نمایند: [انتخاب: • طرح RSA از اندازه کلید رمزنگاری ۲۰۴۸ بیت یا بیشتر استفاده می‌کند که FIPS PUB 186-4، "استاندارد امضای الکترونیک (DSS)"، پیوست B.3 را برآورده می‌سازد. • طرح رمزگذاری خم بیضوی از "خم‌های NIST" P-256، P-384 و [انتخاب: P-521، هیچ منحنی دیگری] استفاده می‌کند که FIPS PUB 186-4، "استاندارد امضای دیجیتال (DSS)"، پیوست B.4 را برآورده می‌سازد. • طرح (رمزنگاری رشته محدود)FFC از اندازه کلید رمزنگاری ۲۰۴۸ بیت یا بیشتر استفاده می‌کند که FIPS PUB 186-4، "استاندارد امضای دیجیتال (DSS)"، پیوست B.1 را برآورده می‌سازد. **نکته کاربردی ۹:** نویسنده هدف امنیتی باید تمام طرح‌های تولید کلید را برای برقراری کلید انتخاب نماید. زمانیکه تولید کلید برای برقراری کلید استفاده می‌شود، طرح‌های موجود در الزام امنیتی تخریب کلید رمزگذاری (FCS_CKM.2.1) و پروتکل‌های رمزنگاری انتخاب شده باید با انتخاب مطابقت داشته باشد. اگر محصول به عنوان دریافت کننده در طرح برقراری کلید RSA ایفای نقش نماید، نیاز نیست محصول تولید کلید RSA را پیاده‌سازی نماید.	

برای تمامی طرح‌ها (طرح‌های RSA، طرح‌های ECC، طرح‌های FFC) تولید بیت تصـــادفی (RBG) نیاز دارد تا الف) مقادیر اولیه‌ای برای RSA تولید نماید و ب) کلیدهای خ صو صی را به طور م ستقیم برای ECC و FFC تولید نماید. بنابراین الزام امنیتی عملیات رمزنگاری -تولید بیت ت صادفی (FCS_RBG_EXT.1) به همراه الزامات کارکرد امنیتی به کار می‌روند. الگوریتم چکیده ساز نیز زمانی مورد نیاز ا ست که الگوریتم تولید زوج کلید بر ا ساس پیو ست B.3.2 یا B.3.5 از FIPS 186-4 انتخاب شده ا ست. در این موارد، الزام امنیتی عملیات رمزنگاری -پوشاندن کلید ((FCS_COP.1(d) به همراه این الزام کارکرد امنیتی استفاده می‌شود.	
تولید کلید رمزگذاری (کلیدهای متقارن) ۱	۱۵
توابع هدف امنیتی باید کلیدهای رمزنگاری متقارن را با استفاده از تولید کننده بیت تصادفی مطابق با توضیحات مشخص شده در الزام امنیتی عملیات رمزنگاری -تولید بیت تصادفی (FCS_RBG_EXT.1) و اندازه‌های کلید رمزنگاری مشخص شده [انتخاب:۱۲۸ بیت، ۲۵۶ بیت] تولید نماید که مورد زیر را برآورده می‌سازد: [هیچ استانداردی]. **نکته کاربردی ۱۰:** کلیدهای متقارن ممکن است برای تولید کلید در طول زنجیره کلید استفاده شود.	
ترکیب Submask ۱	۱۶
توابع هدف امنیتی باید submask ها را با اســـتفاده از روش [انتخاب: تابع بولی XOR، SHA-256، SHA-512] جهت تولید کلید میانی یا مقدار رمزگذاری مرزی، ترکیب کند. **نکته کاربردی ۱۱:** این الزام، رو شی را معرفی می‌کند که یک مح صول ممکن ا ست submask های مختلف را با ا ستفاده از XOR یا SHA-hash، با هم ترکیب کند. توابع چکیده ساز ت صویب شده در الزام امنیتی عملیات رمزنگاری - الگوریتم چکیده ساز ((FCS_COP.1(b) و در الزام امنیتی عملیات رمزنگاری - الگوریتم چکیده سازکلید دار ((FCS_COP.1(c) اتخاذ شده‌اند.	
اعتبارسنجی ۱	۱۷
توابع هدف امنیتی باید اعتبارسنجی [انتخاب:submask، کلید میانی، مقدار رمزگذاری مرزی] را با استفاده از این روش‌ها: [انتخاب: پوشاندن کلید مطابق توضیحات مشخص شده در الزام امنیتی عملیات رمزنگاری -پوشاندن کلید ((FCS_COP.1(d)، چکیده‌سازی [انتخاب:submask، کلید میانی، مقدار رمزگذاری مرزی] به نحوی که در [انتخاب:	

الزام امنیتی عملیات رمزنگاری - الگوریتم چکیده‌ساز ((FCS_COP.1(b)) و الزام امنیتی عملیات رمزنگاری - الگوریتم چکیده‌سازکلید دار ((FCS_COP.1(c))] مشخص شده است و مقایسه آن با مقدار چکیده‌ساز ذخیره شده [انتخاب: submask، کلید میانی، مقدار رمزگذاری مرزی]، رمزگشایی مقدار معلوم با استفاده از [انتخاب:submask، کلید میانی، مقدار رمزگذاری مرزی] همانطور که در الزام امنیتی عملیات رمزنگاری - رمزگشایی/رمزگذاری داده‌های ((FCS_COP.1(f)) AES مشخص شده است و مقایسه آن با مقدار معلوم ذخیره شده] انجام دهند.	
اعتبارسنجی ۲	۱۸
توابع هدف امنیتی باید مقدار رمزگذاری مرزی را تنها بعد از اعتبارسنجی به موتور رمزگذاری ارسال کند.	
اعتبارسنجی ۳	۱۹
توابع هدف امنیتی باید [انتخاب: صدور پاکسازی کلید مربوط به کلید رمزگذاری داده به موتور رمزگذاری بر روی تعداد قابل پیکربندی از تلاش‌های اعتبارسنجی که به طور متوالی با شکست مواجه شده‌اند، ایجاد تأخیری که تنها [اختصاص: تعداد تلاش‌های مشخص شده توسط نویسنده هدف امنیتی]، می‌تواند در یک دوره ۲۴ ساعته ایجاد شود، اعتبارسنجی را بعد از [اختصاص: تعداد تلاش‌های مشخص شده توسط نویسنده هدف امنیتی] تلاش‌های اعتبارسنجی که به طور متوالی با شکست مواجه شده است، مسدود کند. **نکته کاربردی ۱۲:** هدف از انجام اعتبارسنجی امن، افشا نکردن هر موردی می‌باشد که ممکن است submaskها را در معرض خطر قرار دهد. برای انتخاب‌های موجود در الزام امنیتی اعتبارسنجی ۱ (FCS_VAL_EXT.1.1)، در صورتیکه چندین موجودیت از یک نوع موجود باشد، نویسنده هدف امنیتی باید در شرح مدیریت کلید (KMD) به روشنی مشخص کند که به کدامیک از موجودیت‌های مشخص در این الزام کارکردی امنیتی ارجاع داده می‌شود. محصـــول، submaskها را قبل از آنکه مقدار رمزگذاری مرزی را به موتور رمزگذاری ارائه دهند، اعتبارســـنجی می‌کند (مانند عوامل مجوز). زمانیکه یک کلمه‌عبور به عنوان عامل مجوز ا ستفاده می شود، قبل از هرگونه تلاش برای اعتبار سنجی، برای آن شرط گذا شته می شود. در مواردی که، اعتبار سنجی عامل یا عوامل مجوز با شکست روبرو	

می‌شـــود، محصـــول مقدار رمزگذاری مرزی را به موتور رمزگذاری ارســـال نخواهد کرد. زمانیکه از پوشـــاندن کلید در الزام امنیتی عملیات رمزنگاری - پوشـــاندن کلید ((FCS_COP.1(d)) استفاده می‌شود، اعتبارسنجی ذاتاً انجام می‌شود. تأخیر باید توسط محصول اعمال شود، اما این الزام برای مورد توجه قرار دادن حملاتی که محصولات را دور می‌زنند در نظر گرفته نشده است (مثلاً مهاجم مقدار چکیده‌ساز یا مقدار رمزگذاری "معلوم" را به دست می‌آورد و حملات را در خارج از محصول شکل می‌دهد، مانند کراکرهای کلمه‌عبور طرف سوم). توابع رمزنگاری (مانند چکیده ساز، رمزگشـــایی) که انجام می‌شـــوند، همان‌هایی هســـتند که در الزام امنیتی عملیات رمزنگاری - الگوریتم چکیده‌ســـاز ((FCS_COP.1(b)) ، الزام امنیتی عملیات رمزنگاری - الگوریتم چکیده‌سازکلید دار ((FCS_COP.1(c)) و الزام امنیتی عملیات رمزنگاری - رمزگذاری/رمزگشایی داده‌های ((FCS_COP.1(f AES) مشخص شده‌اند. در صورتیکه چندین عامل احراز هویت استفاده شود، ممکن است نیاز باشد تا نویسنده هدف امنیتی این الزام را تکرار کند و در نتیجه یا روش‌های مختلفی برای اعتبارسنجی استفاده می‌شود یا در بعضی موارد یک یا چندین عامل احرازهویت ممکن است، اعتبارسنجی شود و یک یا چندین عامل اعتبارسنجی نشوند.	
عملیات رمزنگاری (درستی‌سنجی امضا) ۱	۲۰
توابع هدف امنیتی باید [خدمات امضای رمزنگاری (درستی‌سنجی)] را انجام دهند مطابق با [انتخاب: • الگوریتم امضای دیجیتالی RSA با اندازه کلید ۲۰۴۸ بیت یا بیشتر • الگوریتم امضای دیجیتالی خم بیضوی با اندازه کلید ۲۵۶ بیت یا بیشتر]. که موارد زیر را بر آورده می‌سازد: [انتخاب: • FIPS PUB 186-4، "اســـتاندارد امضـــای دیجیتال (DSS)". بخش ۵،۵. با اســـتفاده از PKCS#1 v2.1 طرح‌های امضـــا RSASSA-PSS و یا RSASSA-PKCS1-v1_5؛ ISO/IEC 9796-2، طرح امضای دیجیتال ۲ یا طرح امضای دیجیتال ۳ برای طرح‌های RSA. • FIPS PUB 186-4، "استاندارد امضای دیجیتال (DSS)". بخش ۶ و پیوست ۴. پیاده‌سازی "منحنی‌های NIST" p-256.p-384 و [انتخاب:p-521، هیچ منحنی دیگری]؛ISO/IEC 14888-3، بخش ۶،۴ برای طرح ECDSA.].	

نکته کاربردی ۱۳: نکته کاربردی: نویسنده هدف امنیتی باید الگوریتم پیاده سازی شده را برای انجام امضاهای دیجیتال انتخاب نماید. برای الگوریتم‌های انتخاب شده، نویسنده هدف امنیتی باید اختصاص‌ها/انتخاب‌های مناسبی برای تعیین پارامترهایی ایجاد کند که برای آن الگوریتم پیاده‌سازی شده‌اند.
۲۱ **عملیات رمزنگاری (الگوریتم چکیده‌ساز) ۱**
توابع هدف امنیتی باید [خدمات چکیده‌ساز رمزگذاری] را مطابق با [انتخاب: SHA-256،SHA-512] که [ISO/IEC 10118-3:2004] را برآورده می‌سازد، انجام دهد. **نکته کاربردی ۱۴:** انتخاب چکیده‌ساز باید مطابق با استحکام کلی الگوریتم استفاده شده برای الزام امنیتی زنجیره‌ای کردن کلید (FCS_KYC_EXT.1.2) باشد. (SHA 256 باید برای کلیدهای AES 128 بیتی و SHA 512 بیتی باید برای کلیدهای AES 256 بیتی انتخاب شود.) انتخاب استاندارد بر اساس الگوریتم انتخاب شده، صورت می‌گیرد.
۲۲ **عملیات رمزنگاری (الگوریتم چکیده‌ساز کلیدی) ۱**
توابع هدف امنیتی باید [احراز هویت پیام‌های چکیده‌ساز کلیددار] را مطابق با [انتخاب: HMAC-SHA-256،HMAC-SHA-512] و اندازه‌های کلید رمزنگاری [اختصاص: اندازه کلید (بر حسب بیت) استفاده شده در HMAC] که [ISO/IEC 9797-2:2011، بخش ۷ "الگوریتم MAC 2"] را برآورده می‌سازد، انجام دهد. **نکته کاربردی ۱۵:** اندازه کلید [k] در اختصاص محدوده بین L1 و L2 در جاییکه L2≤k≤L1 می‌باشد، قرار می‌گیرد (که در ISO/IEC 10118 برای تابع چکیده‌ساز مناسب به عنوان مثال برای SHA-256، L1=512 و L2=256 تعریف شده است).

۲. کلاس: حفاظت از توابع هدف امنیتی (FPT)

شماره الزام	نام الزام	تطابق الزام با استاندارد
۲۴	آزمودن توابع هدف امنیتی ۱	FPT_TST_EXT.1.1

شماره الزام	نام الزام
۲۳	**آزمودن توابع هدف امنیتی ۱**
توابع هدف امنیتی باید مجموعه‌ای از خود آزمایی‌ها را [انتخاب: در طول راه‌اندازی اولیه (روشن کردن)، قبل از اینکه تابع برای اولین بار فراخوانی شود] برای نشان دادن عملکرد صحیح توابع هدف امنیتی، اجرا کند. **نکته کاربردی ۱۶:** آزمون‌های مربوط به توابع رمزنگاری پیاده سازی شده در محصول می‌تواند آن قدر به تعویق بیفتد تا اینکه آزمون‌ها قبل از اینکه تابع فراخوانی شود، انجام شود. اگر الزام امنیتی عملیات رمزنگاری -تولید بیت تصادفی (FCS_RBG_EXT.1) توسط محصول و طبق NIST SP 800-90 اجرا شد، ارزیاب باید بررسی کند که خلاصه مشخصات محصول، آزمون‌های سلامت را که با بخش ۱۱,۳ از NIST SP 800-90 سازگار می‌باشند شرح دهد. اگر هر تابع عملیات رمزنگاری (FCS_COP) توسط محصول پیاده‌سازی شد، خلاصه مشخصات محصول باید خود آزمایی‌های با پاسخ معلوم را برای این توابع توضیح دهد. ارزیاب باید بررسی کند که خلاصه مشخصات محصول برای بعضی از مجموعه توابع غیر رمزنگاری که بر روی عملکرد صحیح توابع هدف امنیتی تأثیر گذارند، روشی که به وسیله آن این توابع مورد آزمون قرار می‌گیرند را توضیح می‌دهد. خلاصه مشخصات محصول، برای هرکدام از این توابع، روشی که توسط آن عملکرد صحیح تابع یا مؤلفه بررسی شده است را شرح خواهد داد. ارزیاب باید تعیین نماید که تمام توابع یا مؤلفه‌های شناسایی شده در ابتدای راه‌اندازی آزمون شده‌اند.	

پیوست ۲ الزامات مبتنی بر انتخاب

همانطور که در مقدمه این پروفایل حفاظتی مشترک بیان شد، الزامات پایه (آن‌هایی که باید توسط محصول یا سکو زیرین آن اعمال شود) در بدنه این پروفایل حفاظتی مشترک وجود دارد. در اینجا الزامات افزوده‌ای بر اساس انتخاب در بدنه پروفایل حفاظتی مشترک وجود دارد: اگر انتخاب‌های معینی صورت گیرد، آنگاه الزامات افزوده زیر نیز باید گنجانده شود.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۲۴	**عملیات رمزنگاری (پوشاندن کلید)۱**	FCS_COP.1(d)
۲۵	**عملیات رمزنگاری (انتقال کلید) ۱**	FCS_COP.1(e)
۲۶	**عملیات رمزنگاری (رمزگذاری/رمزگشایی داده‌های استاندارد رمزگذاری پیشرفته)**	FCS_COP.1(f)
۲۷	**عملیات رمزنگاری (رمزگذاری کلید) ۱**	FCS_COP.1(g)
۲۸	**استخراج کلید رمزنگاری ۱**	FCS_KDF_EXT.1.1
۲۹	**عملیات رمزنگاری (تولید بیت تصادفی) ۱**	FCS_RBG_EXT.1.1
۳۰	**عملیات رمزنگاری (تولید بیت تصادفی) ۲**	FCS_RBG_EXT.1.2
۳۱	**ساخت و شرطی‌سازی کلمه‌عبور رمزنگاری ۱**	FCS_PCC_EXT.1.1

همانطور که با الزامات موجود در پیوست ۱ توضیح داده شد، نویسنده هدف امنیتی باید اطمینان حاصل کند که به درستی با تعداد تکرار وفق داده شده‌اند، که البته به الزامات مبتنی بر انتخاب و الزامات انتخابی که در بدنه هدف امنیتی وجود دارد، بستگی دارد.

❖ حدس‌زدن عوامل مجوز (T.AUTHORIZATION_GUESSING)

عوامل تهدید ممکن است نرم‌افزار میزبان را برای عوامل مجوز حدسی تکرار شده مانند کلمات عبور و پین‌ها به کار برند. حدس زدن موفق عوامل مجوز ممکن است باعث شود تا محصول کلیدهای رمزگذاری داده را منتشر سازد یا در غیر این صورت، آن را در حالتی قرار دهد که داده حفاظت شده را برای کاربران غیرمجاز افشا سازد.

[FCS_VAL_EXT.1.1, FCS_VAL_EXT.1.2, FCS_VAL_EXT.1.3]

منطق: تنها مقدار رمزگذاری مرزی [FCS_VAL_EXT.1.1] معتبر برای موتور رمزگذاری [FCS_VAL_EXT.1.2] ارسال می‌شود. پاسخ به تلاش برای اعتبارسنجی شکست خورده [FCS_VAL_EXT.1.3] تهدید حدس زدن موفقیت آمیز عامل مجوز را کاهش می‌دهد.

۱. کلاس: پشتیبانی رمزنگاری (FCS)

شماره الزام	نام الزام
۲۴	**عملیات رمزنگاری (پوشاندن کلید)۱**
توابع هدف امنیتی باید [پوشاندن کلید] را مطابق با الگوریتم رمزنگاری مشخص [استاندارد رمزگذاری پیشرفته] در مدهای پیش رو [انتخاب: پوشاندن کلید، پوشاندن کلید با لایه‌گذاری، سبک شمارنده گالیوس، کد احراز اصالت پیام زنجیره‌ای قالب‌های رمز شمارگر] و با اندازه کلید رمزنگاری [انتخاب:۱۲۸ بیت، ۲۵۶ بیت] انجام دهد که [ISO/IEC 18033-3(AES)، [انتخاب: NIST SP 800-38F، ISO/IEC 19772]] را برآورده می‌سازد. **نکته کاربردی ۱۷:** اگر نویسنده هدف امنیتی، پوشاندن کلید را در رویکرد زنجیره‌ای کردن کلید انتخاب نماید، که در FCS_KYC_EXT.1 مشخص شده است، این الزام در بدنه هدف امنیتی استفاده می‌شود.	
۲۵	**عملیات رمزنگاری (انتقال کلید)۱**

توابع هدف امنیتی باید [انتقال کلید] را مطابق با الگوریتم رمزنگاری مشخص RSA] دنبال کننده مدهای] انتخابKTS-OAEP:، [[KTS-KEM-KWSو با اندازه کلید رمزنگاری [انتخاب:۲۰۴۸ بیت، ۳۰۷۲ بیت] انجام دهد کهNIST SP 800-56B] ، بازنگری ۱ [را برآورده می‌سازد. **نکته کاربردی ۱۸:** اگر نویسنده هدف امنیتی، انتقال کلید را در رویکرد زنجیره‌ای کردن کلید انتخاب نماید، که در FCS_KYC_EXT.1 مشخص شده است، این الزام در بدنه هدف امنیتی استفاده می‌شود.	
عملیات رمزنگاری (رمزگذاری/رمزگشایی داده استاندارد رمزگذاری پیشرفته) ۱	۲۶
توابع هدف امنیتی باید [رمزگذاری و رمزگشایی داده] را مطابق با الگوریتم رمزنگاری مشخص [استاندارد رمزگذاری پیشرفته استفاده شده در مدهای [انتخاب:زنجیره قالب‌های رمز، سبک شمارنده گالیوس، قالب رمز قابل پیچاندن بلوک XEX (XOR رمز گذاری XOR) با سرقت متن رمز (XTS)]] و با اندازه کلید رمزنگاری [انتخاب:۱۲۸ بیت، ۲۵۶ بیت] انجام دهد که [استاندارد رمزگذاری پیشرفته توصیف شده در ISO/IES 18033-3، [انتخاب: زنجیره قالب‌های رمز توصیف شده در ISO/IEC 10116، سبک شمارنده گالیوس توصیف شده در ISO/IEC 19772 و قالب رمز قابل پیچاندن بلوک XEX (XOR رمز گذاری XOR) با سرقت متن رمز (XTS) توصیف شده در IEEE 1619] را برآورده می‌سازد. **نکته کاربردی ۱۹:** هدف از این الزام در زمینه این پروفایل حفاظتی مشترک، ارائه الزامات توابع امنیتی می‌باشد که الگوریتم‌های رمزگذاری/رمزگشایی متقارن درخوری که برای استفاده در این محصول مناسب است را بیان می‌کند. اگر نویسنده هدف امنیتی، الزامات اعتبارسنجی را با یکدیگر ادغام کند (FCS_VAL_EXT.1) و گزینه‌ای را برای رمزگشایی مقدار معلوم انتخاب کند و مقایسه‌ای انجام دهد، در واقع این الزامی است که برای تعیین الگوریتم، مدها و اندازه‌های کلیدی که نویسنده هدف امنیتی می‌تواند از بین آن‌ها انتخاب کند استفاده می‌شود. یا در صورتی که نویسنده هدف امنیتی استفاده از رمزگذاری/رمزگشایی استاندارد رمزگذاری پیشرفته را برای حفاظت از کلیدها به عنوان بخشی از رویکرد زنجیره‌ای کردن کلیدی که در FCS_KYC_EXT.1 مشخص شده است را انتخاب کند، این الزام در بدنه هدف امنیتی استفاده می‌شود. همانگونه که در IEEE 1619 مشخص شده است زمانیکه مد قالب رمز قابل پیچاندن بلوک XEX (XOR رمزگذاری XOR) با سرقت متن رمز (XTS) انتخاب می‌شود، ، استفاده از کلید رمزنگاری ۲۵۶ بیتی یا ۵۱۲ بیتی مجاز است. کلید XTS-AES به دو کلید AES با اندازه مساوی تقسیم می‌شود- به عنوان مثال، زمانیکه کلید ۲۵۶ بیتی	

و مد قالب رمز قابل پیچاندن بلوک XEX (XOR رمز گذاری XOR) با سرقت متن رمز (XTS) انتخاب شده است AES-128 برای الگوریتم زیرین استفاده می‌شود، زمانیکه کلید ۵۱۲ بیتی و مد قالب رمز قابل پیچاندن بلوک XEX (XOR رمزگذاری XOR) با سرقت متن رمز (XTS) انتخاب شده است، AES-256 استفاده می‌شود.	
عملیات رمزنگاری (رمزگذاری کلید) ۱	۲۷
توابع هدف امنیتی باید [رمزگذاری و رمزگشایی کلید] را مطابق با الگوریتم رمزنگاری مشخص شده [استاندارد رمزگذاری پیشرفته استفاده شده در [انتخاب: زنجیره قالب‌های رمز، سبک شمارنده گالیوس]] و اندازه کلید رمزنگاری [انتخاب:۱۲۸ بیت، ۲۵۶ بیت] انجام دهد که [استاندارد رمزگذاری پیشرفته مشخص شده در ISO/IES 18033-3، [زنجیره قالب‌های رمز توصیف شده در ISO/IEC 10116، سبک شمارنده گالیوس توصیف شده در ISO/IEC 19772]] را برآورده می‌سازد. **نکته کاربردی ۲۰:** درصورتی‌که نویسنده هدف امنیتی استفاده از رمزگذاری/رمزگشایی استاندارد رمزگذاری پیشرفته را برای حفاظت از کلیدها به عنوان بخشی از رویکرد زنجیره‌ای کردن کلید که در FCS_KYC_EXT.1 مشخص شده است را انتخاب نماید، این الزام در بدنه هدف امنیتی استفاده می‌شود.	
استخراج کلید رمزنگاری ۱	۲۸
توابع هدف امنیتی باید [انتخاب: submask تولید شده توسط تولیدکننده اعداد تصادفی مطابق چیزی که در الزام امنیتی عملیات رمزنگاری - تولید بیت تصادفی (FCS_RBG_EXT.1) مشخص شده است، submask کلمه‌عبور شرطی‌شده، submask وارد شده] را بپذیرد تا کلیدهای میانی را همانطور که در [انتخاب: NIST SP 800-108 [انتخاب: تابع استخراج کلید در مد شمارش، تابع استخراج کلید در مد بازخورد، تابع استخراج کلید در مد تکرار خطوط عبور دوتایی]، NIST SP 800-132] تعریف شده است، با استفاده از توابع چکیده‌سازی کلیددار مشخص شده در الزام امنیتی عملیات رمزنگاری - الگوریتم چکیده‌ساز کلیددار ((FCS_COP.1(c))، استخراج کند به طوری که خروجی حداقل از نظر استحکام امنیتی (در تعداد بیت‌ها) با مقدار رمزگذاری مرزی برابری کند. **نکته کاربردی ۲۱:** درصورتی که نویسنده هدف امنیتی استفاده از استخراج کلید در رویکرد زنجیره‌ای کردن کلید که در FCS_KYC_EXT.1 مشخص شده است را انتخاب کند، این الزام در بدنه هدف امنیتی استفاده می‌شود. این الزام روش‌های قابل قبولی را برای تولید کلید تصادفی جدید یا submask موجود برای ایجاد کلید جدید در طول زنجیره‌ای کردن کلید، ایجاد می‌کند.	

۲۹	**عملیات رمزنگاری (تولید بیت تصادفی) توسعه‌یافته ۱**
توابع هدف امنیتی باید تمام خدمات مربوط به تولید بیت تصادفی قطعی را مطابق با [انتخاب: ISO/IEC 18031:2011، NIST SP 800-90A] با استفاده از [انتخاب: Hash DRBG (هرکدام) ، HMAC_DRBG (هرکدام) ، CTR_DRBG (AES)]] انجام دهد.	
۳۰	**عملیات رمزنگاری (تولید بیت تصادفی) توسعه‌یافته ۲**
تولید بیت تصادفی قطعی باید حداقل توسط یک منبع آنتروپی تولید مقدار اولیه، انجام شود که آنتروپی را از [انتخاب: [اختصاص: تعداد منابع مبتنی بر نرم‌افزار] منابع نویز مبتنی بر نرم‌افزار، [اختصاص: تعداد منابع مبتنی بر سخت‌افزار] منابع نویز مبتنی بر سخت‌افزار] با حداقل [انتخاب: ۱۲۸ بیت، ۲۵۶ بیت] از آنتروپی که حداقل با بزرگ‌ترین استحکام امنیتی برابری کند که بر اساس جدول ISO/IEC 18031:2011 C.1 "جدول استحکام امنیتی برای توابع چکیده‌ساز" از کلیدها و مقادیر چکیده‌ساز که تولید خواهد شد، تلفیق می‌کند. **نکته کاربردی ۲۲:** ISO/IEC 18031:2011 شامل روش‌های مختلفی برای تولید اعداد تصادفی می‌باشد. هرکدام از این‌ها به نوبه خود به اصول رمزنگاری زمینه‌ای (توابع چکیده‌سازی، رمزها) وابسته هستند. نویسنده هدف امنیتی، تابع مورد استفاده را انتخاب خواهد کرد و نیز اصول رمزنگاری زمینه‌ای استفاده شده در این الزام را خواهد گنجاند. درحالیکه هرکدام از توابع چکیده‌ساز معرفی شده (SHA-224،SHA-256، SHA-384،SHA-524) برای Hash-DRBG یا HMAC-DRBG مجاز هستند، تنها پیاده‌سازی مبتنی بر استاندارد رمزگذاری پیشرفته برای CTR_DRBG مجاز است. جدول C.2 در ISO/IEC 18031:2011 شناسایی‌ای از استحکام امنیتی، آنتروپی و الزامات طول نقطه آغاز تصادفی را برای AES-128 و قالب رمز ۲۵۶ ارائه می‌دهد. CTR_DRGB در ISO/IEC 18031:2011 مستلزم آن است که از تابع استخراج استفاده کند، در حالیکه NIST SP 800-90A الزامی نکرده است. هردو مدل قابل قبول هستند. در اولین انتخاب الزام امنیتی عملیات رمزنگاری تولید بیت تصادفی ۱ (FCS_RBG_EXT.1.1)، نویسنده هدف امنیتی استانداردی را انتخاب می‌کند که با آن‌ها سازگار می‌باشد.	

در اولین انتخاب الزام امنیتی عملیات رمزنگاری تولید بیت تصادفی ۲ (FCS_RBG_EXT.1.2) نویسنده هدف امنیتی توضیح می‌دهد که چه تعداد منابع آنتروپی برای هر نوع منبع آنتروپی که آن‌ها به کار می‌برند، استفاده می‌شود. لازم به ذکر است که ترکیبی از سخت‌افزار و نرم‌افزار مبتنی بر منابع نویز پذیرفتنی هستند. لازم به ذکر است که منبع آنتروپی به عنوان بخشی از تولید بیت تصادفی در نظر گرفته می‌شود و اگر تولید بیت تصادفی در محصول وجود داشته باشد، توسعه دهنده ملزم به ارائه توصیف آنتروپی مشخص شده در پیوست ۴ می‌باشد. اسناد *و آزمون‌های* مورد نیاز برای اقدام ارزیابی این عنصر ضرورتاً هرکدام از منابع نشان داده شده در FCS_RBG_EXT.1.2 را پوشش می‌دهد.

۳۱	**ساخت و شرطی‌سازی کلمه‌عبور رمزنگاری ۱**

کلمه‌عبوری که برای تولید عامل مجوز کلمه‌عبور استفاده می‌شود باید قادر به فعالسازی [اختصاص: عدد صحیح مثبت از ۶۴ یا بیشتر] نویسه‌هایی در مجموعه {نویسه‌های با حروف بزرگ، نویسه‌های با حروف کوچک، اعداد و [اختصاص: دیگر نویسه‌های خاص پشتیبانی شده]} بوده و باید [توابع استخراج کلید مبتنی بر کلمه‌عبور] را مطابق با الگوریتم رمزنگاری مشخص شده در [HMAC-[انتخاب:SHA-256،SHA-384، SHA-512]] با [اختصاص: عدد صحیح مثبت ۱۰۰۰ یا بیشتر] تکرارها، اندازه کلید رمزنگاری خروجی [انتخاب:۱۲۸، ۲۵۶] که [NIST SP 800-132] را برآورده می‌سازد، انجام دهد.

نکته کاربردی ۲۳: کلمه‌عبور بر روی ماشین میزبان به صورت توالی از نویسه‌ها نمایش داده می‌شود که رمزگذاری آن‌ها وابسته به محصول و سیستم‌عامل زیرین می‌باشد. این توالی باید به صورت رشته‌ای از بیت‌ها شرطی شود که تا submask را برای استفاده به عنوان ورودی زنجیره کلید شکل دهد. شرطی‌سازی می‌تواند با استفاده از یکی از توابع چکیده‌ساز تعیین شده یا فرایند توصیف شده در NIST SP 800-132، انجام شود. روش مورد استفاده توسط نویسنده هدف امنیتی انتخاب می‌شود. اگر شرطی‌سازی ۸۰۰-۱۳۲ مشخص شده است، نویسنده هدف امنیتی تعداد تکرارهایی که انجام شده است را پر خواهد کرد. ۸۰۰-۱۳۲ به استفاده از تابع شبه تصادفی (PRF) شامل HMAC با یک تابع چکیده‌سازی پذیرفته شده، نیاز دارد. نویسنده هدف امنیتی، تابع چکیده‌ساز مورد استفاده و همچنین الزامات مناسب HMAC را انتخاب می‌کند.

پیوست ۳ تعریف مؤلفه‌های توسعه‌یافته

این پیوست، شامل تعریف الزامات توسعه یافته از جمله موارد موجود در پیوست ۱ و ۲ می‌باشد که در این پروفایل حفاظتی مشترک استفاده شده است .

❖ پس زمینه و دامنه

این سند تعریفی برای تمام مؤلفه‌های توسعه یافته‌ای ارائه می‌دهد که در پروفایل حفاظتی مشترک رمزگذاری کل درایو – اکتساب مجوز، استفاده شده است.

این مؤلفه‌ها در جدول زیر معرفی شده است:

نام مؤلفه	تعریف
FCS_AFA_EXT.1	اکتساب عامل مجوز
FCS_KYC_EXT.1	زنجیره کلید
FCS_PCC_EXT.1	ساخت و شرطی‌سازی کلمه‌عبور رمزنگاری
FCS_CKM_EXT.4	تخریب اجزای کلید و کلید رمزنگاری
FCS_SNI_EXT.1	عملیات رمزنگاری (salt، مقادیر مقطعی (nonce) و تولید بردار اولیه)
FPT_KYP_EXT.1	توسعه‌یافته: حفاظت از کلید و اجزای کلید
FPT_TUD_EXT.1	به‌روزرسانی امن
FCS_SMC_EXT.1	ترکیب submask

FCS_VAL_EXT.1	اعتبارسنجی
FPT_TST_EXT.1	توسعه یافته: آزمون توابع هدف امنیتی
FCS_KDF_EXT.1	استخراج کلید رمزنگاری
FCS_RBG_EXT.1	توسعه یافته: عملیات رمزنگاری (تولید بیت تصادفی)

۱. تعریف مؤلفه‌های توسعه یافته

❖ خانواده اکتساب عامل مجوز (FCS_AFA_EXT)

- **رفتار خانواده اکتساب عامل مجوز**

مؤلفه‌های این خانواده، توانایی محصول برای پذیرفتن عوامل مجوز متنوع را بررسی می‌کنند.

- **سطح‌بندی مؤلفه:**

اکتساب عامل مجوز نیاز دارد تا عوامل مجوز توسط محصول پذیرفته شود.

- **اقدامات مدیریتی اکتساب مجوز**

اقدامات زیر می‌تواند برای کارکردهای مدیریتی مدیریت امنیت در نظر گرفته شود:

- تغییر عوامل مجوزی که باید مورد استفاده قرار گیرد.
- تولید عوامل مجوز بیرونی با استفاده از تولیدکننده اعداد تصادفی توابع هدف امنیتی.

- **اقدامات ممیزی اکتساب مجوز**

هیچ رویداد ممیزی پیش‌بینی نشده‌است.

شماره الزام	نام الزام
۳۲	**اکتساب عامل مجوز ۱**

توابع هدف امنیتی باید عوامل مجوز زیر را بپذیرند:

[انتخاب:

- Submask به دست آمده از عامل مجوز کلمه‌عبور شرط‌گذاری‌شده طبق چیزی که در FCS_PCC_EXT.1 توصیف شده است،
- عامل کارت هوشمند بیرونی که طول بیت‌های آن حداقل به اندازه کلید رمزنگاری داده باشد و از submask ای حفاظت می‌کند که توسط محصول تولید شده است، (با استفاده از تولیدکننده بیت تصادفی توصیف شده در FCS_RBG_EXT.1)، نیز با استفاده از RSA (اندازه کلید ۲۰۴۸ یا بیشتر) محافظت می‌شود.
- عامل کارت هوشمند بیرونی که طول بیت‌های آن حداقل به اندازه کلید رمزنگاری داده باشد و از submask ای حفاظت می‌کند که توسط سکو میزبان تولید شده است، (با استفاده از تولیدکننده بیت تصادفی توصیف شده در FCS_RBG_EXT.1)، نیز با استفاده از RSA (اندازه کلید ۲۰۴۸ یا بیشتر) محافظت می‌شود.
- عامل نشانه USB بیرونی که حداقل استحکام امنیتی به اندازه مقدار رمزگذاری مرزی را داشته باشد و submask تولید شده توسط محصول را با استفاده از تولید کننده بیت تصادفی توصیف شده در FCS_RBG_EXT.1 ارائه دهد.
- عامل نشانه USB بیرونی که حداقل استحکام امنیتی مشابه با مقدار رمزگذاری مرزی را داشته باشد و submask تولید شده توسط سکو میزبان را ارائه می‌دهد.].

❖ زنجیره کلید (FCS_KYC_EXT)

- **رفتار خانواده زنجیره کلید**

این خانواده، مشخصات مورد نیاز برای استفاده از لایه‌های متعدد کلیدهای رمزگذاری به منظور امن ساختن نهایی داده‌های محافظت شده رمزگذاری شده روی درایو را ارائه می‌دهد.

- **سطح‌بندی مؤلفه:**

زنجیره‌ای کردن کلید به توابع هدف امنیتی جهت نگهداشت یک زنجیره کلید نیاز دارد و مشخصات آن زنجیره را مشخص می‌کند.

- **اقدامات مدیریتی زنجیره کلید**

هیچگونه فعالیت مدیریتی پیش‌بینی نشده‌است.

- **اقدامات ممیزی زنجیره کلید**

هیچ رویداد ممیزی پیش‌بینی نشده‌است.

شماره الزام	نام الزام
۳۳	**زنجیره کلید ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد توابع هدف امنیتی باید زنجیره‌ای از کلید را نگهداری کنند: [انتخاب: یک، استفاده از submask به عنوان مقدار رمزگذاری مرزی؛ کلیدهای میانی نشأت گرفته از یک یا چندین submask برای مقدار رمزگذاری مرزی با استفاده از روش‌های زیر: [انتخاب: استخراج کلید به نحوی که در الزام امنیتی استخراج کلید رمزنگاری (FCS_KDF_EXT.1) توصیف شده است؛ پوشاننده کلید به نحوی که در الزام امنیتی عملیات رمزنگاری -پوشاندن کلید ((FCS_COP.1(d)) توصیف شده است، ترکیب کننده کلید به نحوی که در الزام امنیتی ترکیب submask (FCS_SMC_EXT.1) توصیف شده است، انتقال کلید به نحوی که در الزام امنیتی عملیات رمزنگاری - انتقال کلید ((FCS_COP.1(e)) توصیف شده است، رمزنگاری کلید به نحوی که در الزام امنیتی عملیات رمزنگاری - رمزنگاری کلید ((FCS_COP.1(g)) توصیف شده است]] در حالیکه استحکام اثربخش [انتخاب: ۱۲۸ بیت، ۲۵۶ بیت] حفظ می‌شود.	
۳۴	**زنجیره کلید ۲**

توابع هدف امنیتی باید مقدار رمزگذاری مرزی [انتخاب:۱۲۸ بیت،۲۵۶ بیت] را به موتور رمزگذاری ارائه دهد [انتخاب: تنها بعد از آن که توابع هدف امنیتی فرایند اعتبارسنجی را به نحوی که در در FCS_VAL_EXT.1 توصیف شده است با موفقیت انجام دهند، بدون اینکه اعتبارسنجی اتفاق بیفتد]

نکته کاربردی ۲۴: زنجیره‌ای کردن کلید روش استفاده از لایه‌های متعدد کلیدهای رمزنگاری به منظور امن ساختن نهایی مقدار رمزگذاری مرزی می‌باشد. تعداد کلیدهای میانی ممکن است، متفاوت باشد- از یکی (مانند استفاده از عامل مجوز کلمه‌عبور شرطی شده و استفاده مستقیم از آن به عنوان مقدار رمزگذاری مرزی) تا بسیار. این روش برای تمام کلیدهایی که در پوشاندن نهایی یا استخراج مقدار رمزگذاری مرزی شرکت دارند، از جمله آن‌هایی که در نواحی انبارش حفاظت شده قرار دارند (مانند کلیدهای نگهداری شده در واحد سکوهای امن، مقادیر مقایسه‌ای) به کار برده می‌شود.

❖ **ساختن و شرطی‌سازی کلمه‌عبور** رمزنگاری (**FCS_PCC_EXT**)

- **رفتار خانواده ساختن و شرطی‌سازی کلمه عبور رمزنگاری**

این خانواده اطمینان حاصل می‌کند که کلمات‌عبور استفاده شده در تولید مقدار رمزگذاری مرزی قوی هستند (از دیدگاه ترکیب آن‌ها) و برای ارائه رشته بیتی با طول مناسب شرطی شده‌اند.

- **سطح‌بندی مؤلفه**

ساخت و شرط‌گذاری کلمه‌عبور رمزنگاری، مستلزم آن است که توابع هدف امنیتی کلمات‌عبور را از ترکیب معینی بپذیرد و آن‌ها را به طور مناسبی شرطی کند.

- **اقدامات مدیریتی ساختن و شرطی‌سازی کلمه‌عبور رمزنگاری**

هیچ گونه تابع مدیریتی خاصی تعریف نشده است.

- **اقدامات ممیزی ساختن و شرطی‌سازی کلمه عبور رمزنگاری**

هیچ گونه رویداد ممیزی پیش‌بینی نشده است.

شماره الزام	نام الزام
۳۵	**ساخت و شرطی‌سازی کلمه‌عبور رمزنگاری ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: عملیات رمزنگاری (FCS_COP.1(c (الگوریتم چکیده‌ساز کلیددار) کلمه عبوری که برای تولید عامل مجوز کلمه‌عبور استفاده می‌شود باید قادر به فعالسازی [اختصاص: عدد صحیح مثبت از ۶۴ یا بیشتر] نویسه‌هایی در مجموعه {نویسه‌های با حروف بزرگ، نویسه‌های با حروف کوچک، اعداد و [اختصاص: دیگر نویسه‌های خاص پشتیبانی شده]}و باید [توابع استخراج کلید مبتنی بر کلمه¬عبور] را مطابق با الگوریتم رمزنگاری مشخص شده [HMAC-[انتخاب:SHA-256،SHA-384، SHA-512]] با [اختصاص: عدد صحیح مثبت از ۱۰۰۰ یا بیشتر] تکرارها، اندازه کلید رمزنگاری خروجی [انتخاب:۱۲۸، ۲۵۶] که [توصیه‌ها یا مشخصات PBKDF] را برآورده می‌سازد، انجام دهد.	

❖ مدیریت کلید رمزنگاری (FCS_CKM)

- **رفتار خانواده مدیریت کلید رمزنگاری**

کلیدهای رمزنگاری باید در طول چرخه حیات خود مدیریت شوند. این خانواده در نظر دارد تا از این چرخه حیات پشتیبانی کند و در نتیجه الزامات مورد نیاز برای اقدامات زیر را تعریف می‌کند: تولید کلید رمزنگاری، توزیع کلید رمزنگاری، دسترسی کلید رمزنگاری، تخریب کلید رمزنگاری. این خانواده در هر زمان که الزامات کارکردی برای مدیریت کلیدهای رمزنگاری وجود دارد، باید گنجانده شوند.

- **سطح‌بندی مؤلفه:**

تخریب کلید و اجزای کلید رمزنگاری، مؤلفه‌ای توسعه‌یافته از FCS_CKM_EXT.4 می‌باشد و شامل الزامات زمان تخریب کلید می‌باشد.

- **اقدامات مدیریتی تخریب کلید و اجزای کلید رمزنگاری**

هیچ گونه تابع مدیریتی خاصی تعریف نشده است.

- **اقدامات ممیزی تخریب کلید و اجزای کلید رمزنگاری**

هیچ گونه رویداد ممیزی پیش‌بینی نشده است.

شماره الزام	نام الزام
۳۶	**تخریب کلید و اجزای کلید رمزنگاری ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد توابع هدف امنیتی باید تمام کلیدها و اجزای کلید را زمانیکه دیگر به آن‌ها نیازی نیست از بین ببرد.	

❖ عملیات رمزنگاری (تولید Salt، مقادیر مقطعی و بردار اولیه (FCS_SNI_EXT))

- **رفتار خانواده عملیات رمزنگاری (تولید Salt، مقادیر مقطعی و بردار اولیه)**

این خانواده این اطمینان را حاصل می‌کند که Salt ها، مقادیر مقطعی و بردارهای اولیه به درستی شکل گرفته باشند.

- **سطح‌بندی مؤلفه**

عملیات رمزنگاری (تولید Salt، مقادیر مقطعی و بردار اولیه) به تولید salt ها، مقادیر مقطعی و بردارهای اولیه نیاز دارد تا مورد استفاده مؤلفه‌های رمزگذاری محصول قرار گیرد و به شیوه‌ای خاص اعمال شود.

- **اقدامات مدیریتی عملیات رمزنگاری (تولید Salt، مقادیر مقطعی و بردار اولیه)**

هیچ گونه تابع مدیریتی خاصی تعریف نشده است.

- **اقدامات ممیزی عملیات رمزنگاری (تولید Salt، مقادیر مقطعی و بردار اولیه)**

هیچ گونه رویداد ممیزی پیش‌بینی نشده است.

شماره الزام	نام الزام
۳۷	**عملیات رمزنگاری (تولید Salt، مقادیر مقطعی و بردار اولیه) ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد. توابع هدف امنیتی باید تنها از Salt هایی استفاده کند که توسط [انتخاب: تولید اعداد تصادفی مطابق چیزی که در الزام امنیتی عملیات رمزنگاری- تولید بیت تصادفی (FCS_RBG_EXT.1) توصیف شده است، تولید اعداد تصادفی ارائه شده از طریق سکو میزبان] تولید شده‌اند.	
۳۸	**عملیات رمزنگاری (تولید Salt، مقادیر مقطعی و بردار اولیه) ۲**
توابع هدف امنیتی باید تنها از مقادیر مقطعی یکتایی با حداقل اندازه [۶۴] بیت استفاده کند.	
۳۹	**عملیات رمزنگاری (تولید Salt، مقادیر مقطعی و بردار اولیه) ۳**
توابع هدف امنیتی باید بردارهای اولیه را به شیوه زیر ایجاد نمایند: [– زنجیره قالب‌های رمز: بردارهای اولیه باید غیر تکراری باشند. – CCM: مقدار مقطعی باید غیر تکراری باشند.	

- XTS: بدون بردار اولیه. مقادیر تنظیم شده باید اعداد صحیح غیر منفی باشند که به طور متوالی اختصاص یافته و با عدد صحیح غیر منفی دلخواه شروع می‌شود.
- GCM: بردار اولیه باید غیر تکراری باشند. تعداد فراخوانی‌های GCM برای کلید راز داده شده نباید از 2^{32} تجاوز کند.].

❖ حفاظت از کلید و اجزای کلید (FPT_KYP_EXT)

- **رفتار خانواده حفاظت از کلید و اجزای کلید**

این خانواده مستلزم آن است که کلید و اجزای کلید، زمانیکه در حافظه غیر فرّار نوشته شده‌اند، محافظت شوند.

- **سطح‌بندی مؤلفه**

حفاظت از کلید و اجزای کلید مستلزم این است که توابع هدف امنیتی تضمین کند که هیچ گونه کلید یا اجزای کلید رمز نشده در حافظه غیر فرّار نوشته نشده است.

- **اقدامات مدیریتی حفاظت از کلید و اجزای کلید**

هیچگونه فعالیت مدیریتی پیش‌بینی نشده‌است.

- **اقدامات ممیزی حفاظت از کلید و اجزای کلید**

هیچ گونه رویداد ممیزی پیش‌بینی نشده است.

شماره الزام	نام الزام
۴۰	**حفاظت از کلید و اجزای کلید ۱**

وراثت: از هیچ مؤلفه دیگر ندارد

وابستگی: ندارد

توابع هدف امنیتی تنها باید زمانی کلیدها را در حافظه غیر فرّار ذخیره کنند که مطابق چیزی که در الزام امنیتی عملیات رمزنگاری-پوشاندن کلید ((FCS_COP.1(d) مشخص شده است پوشانده شده باشند، یا مطابق الزام امنیتی عملیات رمزنگاری-رمزگذاری کلید ((FCS_COP.1(g) یا الزام امنیتی عملیات رمزنگاری-انتقال کلید ((FCS_COP.1(e)، رمزگذاری شده باشند، مگر آنکه کلید هرکدام از معیارهای زیر را برآورده سازد[انتخاب:

- کلید متن خام بخشی از زنجیره کلید نیست، همانگونه که در الزام امنیتی زنجیره‌ای کردن کلید (FCS_KYC_EXT.1) مشخص شده است.
- کلید متن خام بعد از آماده‌سازی اولیه دیگر به داده‌های رمزگذاری شده دسترسی نداشته باشد.
- کلید متن خام طبق چیزی که در الزام امنیتی ترکیب Submask (FCS_SMC_EXT.1) مشخص شده است انشعاب از کلید است که ترکیب شده است و نیمه دیگر از انشعاب کلید یکی از این موارد است [انتخاب: پوشانده شده مطابق چیزی که در الزام امنیتی عملیات رمزنگاری-پوشاندن کلید ((FCS_COP.1(d) مشخص شده است، یا رمزگذاری شده است مطابق توضیحات (FCS_COP.1(g یا (FCS_COP.1(e، یا استخراج شده و در حافظه غیر فرّار ذخیره نشده است.]
- کلید متن خام در یک افزاره انبارش بیرونی ذخیره شده است تا به عنوان یک عامل مجوز استفاده شود.

کلید متن خام برای [انتخاب: پوشاندن یک کلید مطابق توضیحات مشخص در (FCS_COP.1(d، رمزگذاری شده است مطابق توضیحات الزام امنیتی عملیات رمزنگاری - رمزگذاری کلید ((FCS_COP.1(g یا الزام امنیتی عملیات رمزنگاری-انتقال کلید ((FCS_COP.1(e)] که هم اکنون [انتخاب: مطابق چیزی که در (FCS_COP.1(d مشخص شده است، پوشانده شده است، یا مطابق چیزی که در (FCS_COP.1(g یا (FCS_COP.1(e]] مشخص شده است رمزگذاری شده است] می‌باشد استفاده می‌شود.

❖ به‌روزرسانی امن (FPT_TUD_EXT)

- **رفتار خانواده به روزرسانی امن**

مؤلفه‌های این خانواده، الزامات مورد نیاز برای به‌روزرسانی میان‌افزار و یا نرم‌افزار محصول را مورد توجه قرار می‌دهد.

- **سطح‌بندی مؤلفه**

به‌روزرسانی امن، مستلزم توانایی‌هایی می باشد تا برای به‌روزرسانی میان‌افزار و نرم‌افزار محصول ازجمله توانایی اعتبارسنجی به‌روزرسانی‌ها قبل از نصب، ارائه شود.

- **اقدامات مدیریتی به‌روزرسانی امن**

اقدامات زیر می‌تواند برای کارکردهای مدیریتی توابع مدیریت امنیت در نظر گرفته شود:

- توانایی به‌روزرسانی محصول و بررسی به روزرسانی‌ها

- **اقدامات ممیزی به‌روزرسانی امن**

اگر تولید داده‌های ممیزی امنیتی FAU_GEN در هدف امنیتی یا پروفایل حفاظتی وجود داشته باشد اقدامات زیر باید قابل ممیزی باشند:

- شروع فرایند به‌روزرسانی
- هرگونه شکست در بررسی یکپارچگی به روزرسانی

شماره الزام	نام الزام
۴۱	**به‌روزرسانی امن ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: FCS_COP.1(a) عملیات رمزنگاری (درستی‌سنجی امضا)	

FCS_COP.1(b) عملیات رمزنگاری (الگوریتم چکیده‌ساز)	
توابع هدف امنیتی باید برای [کاربران مجاز] توانایی پرس‌وجوی نسخه فعلی نرم‌افزار یا میان‌افزار محصول را فراهم آورد.	
به‌روزرسانی امن ۲	**۴۲**
توابع هدف امنیتی باید برای [کاربران مجاز] توانایی آغاز به‌روزرسانی نرم‌افزار یا میان‌افزار محصول را فراهم آورد.	
به‌روزرسانی امن ۳	**۴۳**
توابع هدف امنیتی باید به‌روزرسانی‌های میان‌افزار محصول را با استفاده از [امضای دیجیتال] سازنده قبل از نصب آن به روزرسانی‌ها، بررسی کند.	

❖ **ترکیب Submask (FCS_SMC_EXT)**

- **رفتار خانواده ترکیب Submask**

اگر محصول از استفاده بیش از یک submask برای استخراج یا حفاظت مقدار رمزگذاری مرزی پشتیبانی کند، این خانواده روش‌های ترکیب submask را مشخص خواهد کرد.

- **سطح‌بندی مؤلفه**

ترکیب submask مستلزم آن است که توابع هدف امنیتی، submask ها را در الگویی قابل پیش‌بینی، با یکدیگر ترکیب کند.

- **اقدامات مدیریتی ترکیب submask**

هیچ گونه تابع مدیریتی خاصی تعریف نشده است.

- **اقدامات ممیزی ترکیب submask**

هیچ گونه رویداد ممیزی پیش‌بینی نشده است.

شماره الزام	نام الزام
۴۳	**ترکیب submask ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: FCS_COP.1(b) عملیات رمزنگاری (الگوریتم چکیده‌ساز) توابع هدف امنیتی باید submask ها را با استفاده از روش [انتخاب: تابع بولی XOR، SHA-256، SHA-512] جهت تولید کلید میانی یا مقدار رمزگذاری مرزی، ترکیب کند.	

❖ اعتبارسنجی عناصر رمزنگاری (FCS_VAL_EXT)

- **رفتار خانواده**

این خانواده ابزاری را مشخص می‌کند که به وسیله آن submask و یا مقادیر رمزگذاری مرزی، قبل از استفاده از آن‌ها اعتبارسنجی می‌شوند.

- **سطح‌بندی مؤلفه**

اعتبارسنجی مستلزم آن است که توابع هدف امنیتی، submask ها و مقادیر رمزگذاری مرزی را با یک یا چندین روش معرفی شده، اعتبارسنجی کند.

- **اقدامات مدیریتی اعتبارسنجی عناصر رمزنگاری**

هیچ گونه تابع مدیریتی خاصی تعریف نشده است.

- **اقدامات ممیزی اعتبارسنجی عناصر رمزنگاری**

هیچ گونه رویداد ممیزی پیش‌بینی نشده است.

شماره الزام	نام الزام
۴۴	**اعتبارسنجی ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: به FCS_COP.1(b) عملیات رمزنگاری (الگوریتم چکیده‌ساز) ، FCS_COP.1(d) عملیات رمزنگاری (پوشاندن کلید) توابع هدف امنیتی باید اعتبارسنجی را روی [انتخاب:submask، کلید میانی، مقدار رمزگذاری مرزی] با استفاده از این روش‌ها: [انتخاب: پوشاندن کلید به نحوی که در عملیات رمزنگاری (پوشاندن کلید) ((FCS_COP.1(d)) توصیف شده است، چکیده‌سازی [انتخاب:sub mask، کلید میانی، مقدار رمزگذاری مرزی] به نحوی که در [انتخاب: عملیات رمزنگاری (الگوریتم چکیده‌ساز) ((FCS_COP.1(b))، عملیات رمزنگاری (الگوریتم چکیده‌ساز کلیددار) ((FCS_COP.1(c))] مشخص شده انجام داده و آن را با مقدار چکیده‌ساز ذخیره شده [انتخاب: sub mask، کلید میانی، مقدار رمزگذاری مرزی] مقایسه کند، مقدار معلومی را با استفاده از [انتخاب:sub mask ، کلید میانی، مقدار رمزگذاری مرزی] به گونه مشخص شده در الزام امنیتی عملیات رمزنگاری (رمزگذاری/ رمزگشایی داده‌های استاندارد رمزگذاری پیشرفته) ((FCS_COP.1(f)) رمزگشایی کند و آن را با مقدار معلوم ذخیره شده مقایسه کند].	
۴۵	**اعتبارسنجی ۲**
توابع هدف امنیتی باید مقدار رمزگذاری مرزی را تنها بعد از اعتبارسنجی به موتور رمزگذاری ارسال نماید.	
۴۶	**اعتبارسنجی ۳**
توابع هدف امنیتی باید [انتخاب: صدور پاکسازی کلید مربوط به کلید رمزگذاری داده به موتور رمزگذاری تنظیم شده بر روی تعداد قابل پیکربندی از تلاش‌های اعتبارسنجی که به طور متوالی شکست خورده، ایجاد تأخیری که تنها [اختصاص: تعداد تلاش‌های مشخص شده توسط نویسنده هدف امنیتی]، که می‌تواند در یک دوره ۲۴ ساعته تعیین شود، بعد از [اختصاص: تعداد تلاش‌های مشخص شده توسط نویسنده هدف امنیتی] از تلاش‌های اعتبارسنجی که به طور متوالی شکست خورده اعتبارسنجی را مسدود کند.	

❖ خودآزمایی توابع هدف امنیتی (FPT_TST_EXT)

- **رفتارخانواده خودآزمایی توابع هدف امنیتی**

مؤلفه‌های این خانواده الزامات مورد نیاز برای خود آزمایی توابع هدف امنیتی جهت عملکرد صحیح انتخاب شده را مورد توجه قرار می‌دهد.

- **سطح‌بندی مؤلفه**

آزمون توابع هدف امنیتی مستلزم مجموعه‌ای از خودآزمایی‌هایی است تا در طول راه‌اندازی اولیه به منظور نشان دادن عملکرد صحیح توابع هدف امنیتی اجرا شوند.

- **اقدامات مدیریتی خودآزمایی توابع هدف امنیتی**

هیچ گونه تابع مدیریتی خاصی تعریف نشده است.

- **اقدامات ممیزی خودآزمایی توابع هدف امنیتی**

اگر تولید داده‌های ممیزی امنیتی FAU_GEN در هدف امنیتی یا پروفایل حفاظتی وجود داشته باشد اقدامات زیر باید قابل ممیزی باشند:

- نشانی که تکمیل شدن خود آزمایی توابع هدف امنیتی را نشان دهد.

شماره الزام	نام الزام
۴۷	**خودآزمایی توابع هدف امنیتی ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد	

توابع هدف امنیتی باید مجموعه‌ای از خود آزمایی‌های زیر را برای نشان دادن عملکرد صحیح توابع هدف امنیتی اجرا کند:[انتخاب: در *طول راه‌اندازی اولیه (روشن کردن)*، *قبل از اینکه تابع برای اولین بار فراخوانی شود*].

❖ استخراج کلید رمزنگاری (FCS_KDF_EXT.1)

- **رفتار خانواده استخراج کلید رمزنگاری**

این خانواده روشی را توصیف می‌کند که از طریق آن کلید میانی از مجموعه مشخصی از submask ها استخراج می‌شود.

- **سطح‌بندی مؤلفه**

استخراج کلید رمزنگاری مستلزم آن است که توابع هدف امنیتی کلیدهای میانی را از submask ها با استفاده از توابع چکیده‌ساز مشخص، استخراج کند.

- **اقدامات مدیریتی استخراج کلید رمزنگاری**

هیچ گونه تابع مدیریتی خاصی تعریف نشده است.

- **اقدامات ممیزی استخراج کلید رمزنگاری**

هیچ گونه رویداد ممیزی پیش‌بینی نشده است.

شماره الزام	نام الزام
۴۸	**استخراج کلید رمزنگاری ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: FCS_COP.1(c) عملیات رمزنگاری (الگوریتم چکیده‌ساز کلیددار)	

توابع هدف امنیتی باید [انتخاب: submask تولید شده توسط تولید کننده اعداد تصادفی مطابق چیزی که در FCS_RBG_EXT.1 تعیین شده است، submask کلمه‌عبور شرطی شده، submask وارد شده] را برای استخراج کلید واسطه طبق چیزی که در [انتخاب: NIST SP 800-108 [انتخاب: تابع استخراج کلید در مد شمارش، تابع استخراج کلید در مد بازخورد، تابع استخراج کلید در مد تکرار خطوط عبور دوتایی]، NIST SP 800-132] تعریف شده است، با استفاده از توابع چکیده‌ساز کلیددار مشخص شده در FCS_COP.1(c) بپذیرد، به طوریکه خروجی حداقل از نظر استحکام امنیتی (در تعداد بیت‌ها) با مقدار رمزگذاری مرزی برابری کند.

❖ تولید بیت تصادفی (FCS_RBG_EXT)

- **رفتار خانواده**

مؤلفه‌های این خانواده الزامات مورد نیاز برای تولید بیت/عدد تصادفی را مورد توجه قرار می‌دهند. این خانواده، خانواده جدیدی است که برای کلاس FCS تعریف شده است.

- **سطح‌بندی مؤلفه**

تولید بیت تصادفی مستلزم آن است که مطابق با استانداردهای انتخاب شده توسط یک منبع آنتروپی آغاز شود.

- **اقدامات مدیریتی تولید بیت تصادفی**

اقدامات زیر می‌تواند برای کارکردهای مدیریت در مدیریت امنیت در نظر گرفته شود:

- هیچ گونه فعالیت مدیریتی پیش‌بینی نشده است.

- **اقدامات ممیزی تولید بیت تصادفی**

- اگر تولید داده ممیزی امنیتی FAU_GEN در هدف امنیتی یا پروفایل حفاظتی وجود داشته باشد اقدامات زیر باید قابلیت ممیزی داشته باشند:

- حداقل: شکست فرایند تصادفی‌سازی.

شماره الزام	نام الزام
۴۹	**تولید بیت تصادفی ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: FCS_COP.1(b) عملیات رمزنگاری (الگوریتم چکیده‌ساز) یا FCS_COP.1(c) عملیات رمزنگاری (الگوریتم چکیده‌ساز کلیددار) توابع هدف امنیتی باید تمام خدمات مربوط به تولید بیت تصادفی قطعی را مطابق با ISO/IEC 18031:2011 با استفاده از [انتخاب: *Hash_DRBG (هرکدام)*، *HMAC_DRBG (هرکدام)*، *CTR_DRBG (AES) (هرکدام)*] انجام دهد.	
۵۰	**تولید بیت تصادفی ۲**
تولید بیت تصادفی قطعی باید حداقل توسط یک منبع آنتروپی آغاز شود که آنتروپی را از [انتخاب: *منابع پارازیت مبتنی بر نرم‌افزار*، *منابع پارازیت مبتنی بر سخت‌افزار*] با حداقل [انتخاب: *۱۲۸ بیت*، *۱۹۲ بیت*، *۲۵۶ بیت*] از آنتروپی که حداقل با بزرگ‌ترین استحکام امنیتی بر اساس جدول ISO/IEC 18031:2011 C.1 "جدول استحکام امنیتی برای توابع چکیده‌ساز" از کلیدها و چکیده‌سازهایی که تولید خواهد شد، برابری کند، تلفیق می‌کند. **نکته کاربردی ۲۵:** ISO/IEC 18031:2011 شامل سه روش مختلف برای تولید اعداد تصادفی می‌باشد. هرکدام از این‌ها به نوبه خود به اصول رمزنگاری زمینه‌ای (توابع چکیده‌ساز/ رمزها) وابسته هستند. نویسنده هدف امنیتی، تابع مورد استفاده را انتخاب خواهد کرد و اصول رمزنگاری زمینه‌ای استفاده شده در این الزام را خواهد گنجاند. درحالیکه هرکدام از توابع چکیده‌ساز معرفی شده (SHA-224، SHA-256، SHA-384، SHA-512) برای Hash_DRBG یا DRBG_HMAC مجازند، تنها برای پیاده‌سازی‌های مبتنی بر استاندارد رمزگذاری پیشرفته برای CTR_DRBG مجاز هستند.	

پیوست ۴ ارزیابی و مستندات آنتروپی

این بخش یک پیوست اختیاری در پروفایل حفاظتی مشترک می‌باشد و تنها زمانی به کار می‌رود که محصول، تولیدکننده بیت تصادفی را ارائه دهد.

این پیوست اطلاعات تکمیلی مورد نیاز برای منبع آنتروپی مورد استفاده توسط سیستم‌عامل را توصیف می‌کند.

مستندات منبع (منابع) آنتروپی بهتر است با جزئیات کافی ارائه شود تا ارزیاب بعد از خواندن، منبع آنتروپی و اینکه چرا برای فراهم کردن آنتروپی کافی قابل اتکا است را به طور کامل درک کند. این سند باید شامل چندین بخش تفصیلی باشد: توصیف طراحی، استدلال آنتروپی، شرایط عملیاتی و آزمون سلامت. نیازی نیست تا این سند بخشی از توصیف خلاصه محصول در مواجه عمومی هدف امنیتی باشد.

۱. توصیف طراحی

مستندات باید شامل طراحی منبع آنتروپی به عنوان یک کل، از جمله تعامل همه مؤلفه‌های منبع آنتروپی باشد. هر گونه اطلاعاتی که در خصوص طراحی قابل اشتراک‌گذاری باشد بهتر است برای هر منبع آنتروپی طرف سوم که در محصول موجود است نیز گنجانده شود.

مستندات، عملیات منبع آنتروپی را توضیح خواهد داد که نحوه تولید آنتروپی و نحوه کسب داده‌های (خام) پردازش نشده از درون منبع آنتروپی برای اهداف آزمایش را در بر می‌گیرد. مستندات باید سر تا سر طراحی منبع آنتروپی قدم بردارد تا نشان دهد آنتروپی از کجا می‌آید، بعد از آن خروجی آنتروپی کجا می‌رود، هر گونه خروجی خام بعد از پردازش (چکیده‌ساز، XOR و غیره) آیا/کجا ذخیره می‌شود، و در نهایت، چگونه خروجی‌ای از منبع آنتروپی است. همچنین هر شرطی که در فرایند وضع می‌شود (به طور مثال، مسدود کردن) بهتر است در طراحی منبع آنتروپی توضیح داده شود. نمودارها و مثال‌ها مورد تشویق قرار می‌گیرند.

طراحی همچنین باید شامل شرحی از محتوای مرزهای امنیتی منبع آنتروپی و توصیفی باشد از چگونگی حصول اطمینان توسط مرز امنیتی از اینکه که مهاجم خارج از مرز نمی‌تواند بر نرخ آنتروپی تأثیر بگذارد.

در صورت پیاده‌سازی، توصیف طراحی باید شامل توصیفی باشد از نحوه‌ای که برنامه‌های کاربردی طرف سوم می‌توانند آنتروپی را به تولید کننده بیت تصادفی بیفزایند. توصیفی از هر حالت تولید کننده بیت تصادفی ذخیره کننده بین خاموشی و روشنی نیز باید گنجانده شود.

۲. استدلال آنتروپی

باید استدلالی فنی در مورد اینکه غیر قابل پیش‌بینی بودن در منابع از کجا می‌آید و چرا به منبع آنتروپی برای تحویل آنتروپی کافی جهت استفاده از خروجی تولید کننده بیت تصادفی (RBG) (با این محصول خاص) اعتماد می‌شود، وجود داشته‌باشد. این استدلال شامل توصیفی از نرخ حداقل آنتروپی مورد انتظار (یعنی حداقل آنتروپی (به بیت) در هر بیت یا بایت از داده منبع) است و توضیح می‌دهد که آنتروپی کافی در حال رفتن به فرایند مقداردهی اولیه (مقداردهی اولیه (بذرپاشی)) تصادفی کننده محصول است. این مبحث قسمتی از استدلال برای این موضوع خواهد بود که چرا منبع آنتروپی برای تولید بیت‌ها با آنتروپی قابل اتکا است.

میزان اطلاعات ضروری برای منطق نرخ حداقل آنتروپی مورد انتظار به نوع منبع آنتروپی موجود در محصول بستگی دارد.

انتظار می‌رود برای توسعه دهنده‌ای که منابع آنتروپی را فراهم آورده است، به منظور منطق نرخ حداقل آنتروپی، تعداد زیادی از بیت‌های منبع خام جمع‌آوری شده، آزمون‌های آماری انجام شود، و نرخ حداقل آنتروپی از آزمون‌های آماری تعیین گردد. در حالی که هیچ آزمون آماری‌ای در حال حاضر مورد نیاز نیست، انتظار می‌رود که برخی از آزمون‌ها برای تعیین میزان آنتروپی حداقلی در هر خروجی ضروری باشد.

برای منابع آنتروپی ارائه شده توسط طرف سوم، که در آن فروشنده محصول دسترسی برای طراحی و منبع داده آنتروپی خام را محدود کرده است، مستندات برآوردی از میزان حداقل آنتروپی به دست آمده از این منبع طرف سوم را نشان می‌دهد. برای فروشنده قابل قبول است که یک مقداری از آنتروپی حداقلی را "فرض کند"، با این حال، این مفروضات باید به وضوح در مستندات ارائه شده بیان شود. به خصوص، برآورد آنتروپی حداقلی باید مشخص شود و مفروضات در هدف امنیتی گنجانده شود.

بدون در نظر گرفتن نوع منبع آنتروپی، استدلال همچنین شامل این موضوع خواهد بود که چگونه تولید کننده بیت تصادفی قطعی با آنتروپی بیان شده در هدف امنیتی مقدار دهی اولیه خواهد شد، برای مثال بررسی این موضوع که نرخ حداقل آنتروپی با مقداری از داده منبع مورد استفاده برای مقداردهی اولیه (بذرپاشی) تولید کننده بیت تصادفی قطعی ضرب شده یا اینکه نرخ آنتروپی مورد انتظار بر اساس مقدار داده منبع، به صورت صریح بیان شده و با نرخ آماری مقایسه گردیده است. چنانچه میزان داده منبع مورد استفاده برای مقداردهی اولیه (بذرپاشی) تولید کننده بیت تصادفی قطعی، مشخص نباشد یا نرخ محاسبه شده به صراحت به نقطه آغاز مرتبط نباشد، مستندات کامل در نظر گرفته نخواهند شد.

استدلال آنتروپی نباید شامل هیچ گونه داده اضافه شده از هر برنامه کاربردی طرف سوم یا از هر حالت ذخیره کننده بین راه‌اندازی‌های مجدد باشد.

۳. شرایط عملیات

نرخ آنتروپی ممکن است تحت تأثیر شرایط خارج از کنترل خود منبع آنتروپی باشد. برای مثال، ولتاژ، فرکانس، دما، و زمان سپری شده پس از روشنی تنها تعداد معدودی از عواملی هستند که ممکن است عملیات منبع آنتروپی را تحت تأثیر قرار دهند. به این ترتیب، مستندات شامل طیفی از شرایط عملیاتی است که تحت آن انتظار می‌رود منبع آنتروپی داده تصادفی تولید کند. این مستندات به صورت واضح اقدامات اتخاذ شده در طراحی سامانه را توضیح خواهد داد تا اطمینان حاصل شود که منبع آنتروپی به عملکرد خود تحت آن شرایط ادامه می‌دهد. به طور مشابه، این سند باید شرایطی را توصیف کند که منبع آنتروپی بیشتر دیگر ارائه آنتروپی کافی را تضمین نمی‌کند. روش‌های استفاده شده برای شناسایی شکست یا تخریب منبع باید گنجانده شود.

۴. آزمون سلامت

به طور خاص‌تر، همه آزمون‌های سلامت منبع آنتروپی و منطق آن‌ها باید مستند شود. این مستند شامل شرحی است از آزمون‌های سلامت، نرخ و شرایطی که تحت آن هر آزمون سلامت اجرا شده است (به طور مثال، در آغاز، به طور مداوم، یا بر اساس تقاضا)، نتایج مورد انتظار برای هر آزمون سلامت، و منطقی که نشان می‌دهد چرا هر آزمونی برای تشخیص یک یا چند شکست در منبع آنتروپی مناسب دانسته شده است.

پیوست ۵ توصیف مدیریت کلید

مستندات مدیریت کلید رمزگذاری محصول باید به اندازه کافی با جزئیات باشد به گونه‌ای که ارزیاب بعد از خواندن این مستندات، مدیریت کلید محصول و چگونگی رعایت الزامات توسط آن را برای حصول اطمینان از محافظت کافی کلید، به طور کامل درک کند. این سند باید شامل نوشتارها و نمودارها باشد. نیازی نیست این سند قسمتی از خلاصه مشخصات محصول باشد – می‌تواند به عنوان سند جداگانه‌ای ارائه شود و اختصاص توسعه‌دهنده مشخص شود.

۱. نوشتار:

نوشتار، اطلاعات زیر را برای تمام کلیدها در زنجیره کلید ارائه می‌دهد:

- هدف از کلید
- اگر کلید در حافظه غیر فرّار ذخیره شده باشد.
- چگونه و چه زمانی کلید محافظت شده است.
- چگونه و چه زمانی کلید استخراج شده است.
- استحکام کلید
- چه زمانی یا اگر کلید بیشتر از این مورد نیاز نمی‌باشد، به همراه استدلال کلید باید پاک شود.

این نوشتار همچنین موضوعات زیر را توضیح می‌دهد:

- توصیفی از تمام عوامل مجوز که توسط محصول پشتیبانی شده‌اند و توضیح اینکه هریک از عوامل چگونه به کار گرفته می‌شود از جمله هرگونه شرطی‌سازی و ترکیبی که اعمال می‌شود.

- اگر اعتبارسنجی پشتیبانی شده است، فرایند اعتبارسنجی باید توصیف شود و به مقادیر استفاده شده برای اعتبارسنجی و فرایند مورد استفاده برای انجام اعتبارسنجی نیز توجه شود. همچنین باید توضیح دهد که چگونه این فرایند تضمین می‌کند که هیچ یک از کلیدها در زنجیره کلید با این فرایند تضعیف نشده یا در معرض خطر قرار نمی‌گیرند.
- فرایند مجوز که منجر به انتشار نهایی مقدار رمزگذاری مرزی می‌شود. این بخش باید زنجیره کلید استفاده شده توسط محصول را با جزئیات بیان کند. همچنین این بخش باید توضیح دهد که کدامیک از کلیدها برای محافظت از مقدار رمزگذاری مرزی استفاه شده‌اند و چگونه فرایند استخراج، پوشاندن کلید، یا ترکیب ساختن دو الزام از جمله زنجیره مستقیم از مجوز اولیه تا مقدار رمزگذاری مرزی را برآورده می‌سازد. همچنین باید شامل هر مقداری باشد که به زنجیره کلید اضافه می‌شود یا با زنجیره کلید تعامل دارد و محافظت‌هایی جهت اطمینان از اینکه این مقادیر استحکام کلی زنجیره کلید را تضعیف نمی‌کنند و یا در معرض خطر قرار نمی‌دهد.
- نمودار و نوشتار باید به روشنی وراثت کلیدها را نشان دهند تا اطمینان حاصل کند که در هیچ نقطه‌ای، زنجیره بدون خروج از رمزنگاری شکسته نخواهد شد یا تمام مقادیر مجوز اولیه و استحکام اثربخش مقدار رمزگذاری مرزی در طول زنجیره کلید حفظ خواهد شد.
- توصیفی از موتور رمزگذاری داده، مؤلفه‌های آن، جزئیات پیاده‌سازی آن (از جمله برای سخت‌افزار: یکپارچه شدن با مرکز عملیات امنیت اصلی افزاره یا کمک پردازنده جداگانه، برای نرم‌افزار: مقداردهی اولیه محصول، درایورها، کتابخانه‌ها (در صورت وجود)، واسط‌های منطقی برای رمزگذاری/رمزگشایی و نواحی‌ای که رمزگذاری نشده‌اند (مانند بارگذارکننده راه‌انداز، بخش مرتبط با رکورد اصلی راه‌انداز (MBR)، جداول افرازی و ...)). این توضیحات باید شامل جریان داده از واسط میزبان افزاره به رسانه مانای دستگاه انبارش داده، اطلاعاتی راجع به شرایطی که داده، موتور رمزگذاری داده را دور می‌زند (مانند عملیات خواندن/ نوشتن بر روی ناحیه رکورد اصلی راه‌انداز رمزگذاری نشده) باشد. این توضیحات باید به اندازه کافی با جزئیات بیان شوند تا تمام سکوها را بررسی کنند و اطمینان حاصل کند که زمانی که کاربر رمزگذاری را فعال می‌کند، محصول، تمام

افزاره‌های انبارش سخت را رمزگذاری می‌کند. همچنین باید شروع راه‌اندازی سکو، فرایند آغاز رمزگذاری و اینکه در چه زمانی محصول رمزگذاری را فعال می‌کند، را نیز مشخص کند.

- فرایند تخریب کلید زمانی‌که دیگر به آن‌ها نیازی نیست از طریق توصیف محل انبارش تمام کلیدها و محافظت از تمام کلیدهای در حافظه غیرفرار ذخیره شده است.

۲. **نمودار**:

- نمودار شامل تمام کلیدها از عامل (عوامل) مجوز اولیه تا مقدار رمزگذاری مرزی و هرگونه کلید یا مقداری خواهد بود که در زنجیره مشارکت دارند. همچنین باید استحکام رمزنگاری هریک از کلیدها را فهرست کرده و نشان دهد که چگونه هر کلید در امتداد زنجیره با استخراج کلید یا پوشاندن کلید (از گزینه‌های مجاز) محافظت می‌شود. نمودار، ورودی استفاده شده برای استخراج یا عدم پوشاندن هریک از کلیدها در زنجیره را نیز نشان خواهد داد.
- یک نمودار عملیاتی(قالبی)، نشان دهنده مؤلفه‌های اصلی (مانند حافظه‌ها و پردازنده‌ها) و مسیر داده بین آن‌ها، برای سخت‌افزار، واسط میزبان دستگاه و رسانه پایای افزاره انبارش داده، یا برای نرم‌افزار، گام‌های اولیه مورد نیاز برای فعالیت‌هایی است که محصول انجام می‌دهد تا اطمینان حاصل کند زمانیکه مدیرسیستم یا کاربر برای اولین بار محصول را آماده می‌کنند، به طور کامل افزاره انبارش را رمز گذاری می‌کند، نمودار رمزگذاری سخت‌افزار باید مکان موتور رمزگذاری داده را درون مسیر داده نشان دهد.
- نمودار رمزگذاری سخت‌افزار باید مکان موتور رمزگذاری داده را درون مسیر داده نشان دهد. ارزیاب باید بررسی کند که نمودار رمزگذاری سخت‌افزار، شامل جزئیاتی باشد که مؤلفه‌های اصلی را درون مسیر داده نشان دهد و به وضوح موتور رمزگذاری داده را مشخص کند.

.

پیوست ۶ واژگان اختصاری

واژه اختصاری	معنای انگلیسی	ترجمه فارسی
AA	Authorization Acquisition	اکتساب مجوز
AES	Advanced Encryption Standard	استاندارد رمزگذاری پیشرفته
BEV	Border Encryption Value	مقدار رمزگذاری مرزی
BIOS	Basic Input Output System	سامانه ورودی خروجی اصلی
CBC	Cipher Block Chaining	زنجیره قالب‌های رمز
CC	Common Criteria	معیار مشترک
CCM	Counter with CBC-Message Authentication Code	کد احراز اصالت پیام زنجیره‌ای قالب‌های رمز شمارگر
CEM	Common Evaluation Methodology	روشگان ارزیابی مشترک
CPP	Collaborative Protection Profile	پروفایل حفاظتی مشترک
DEK	Data Encryption Key	کلید رمزگذاری داده
DRBG	Deterministic Random Bit Generator	تولید کننده بیت تصادفی قطعی
DSS	Digital Signature Standard	استاندارد امضای دیجیتال
ECC	Elliptic Curve Cryptography	رمزنگاری خم بیضی
ECDSA	Elliptic Curve Digital Signature Algorithm	الگوریتم امضای دیجیتال خم بیضوی
EE	Encryption Engine	موتور رمزگذاری
EEPROM	Electrically Erasable Programmable Read-Only Memory:	حافظه فقط خواندنی قابل برنامه‌ریزی و پاک شدن به صورت الکترونیکی
FIPS	Federal Information Processing Standards	استانداردهای پردازش اطلاعات فدرال
FDE	Full Drive Encryption	رمزگذاری کل درایو
FFC	Finite Field Cryptography	رمزنگاری رشته محدود
GCM	Galois Counter Mode	سبک شمارنده گالیوس

واژه اختصاری	معنای انگلیسی	ترجمه فارسی
KHMAC	Keyed-Hash Message Authentication Code	کد احراز هویت پیام چکیده‌ساز کلید دار
HW	Hardware	سخت‌افزار
IEEE	Institute of Electrical and Electronics Engineers	مؤسسه مهندسان برق و الکترونیک
IT	Information Technology	فناوری اطلاعات
ITSEF	Information Technology Security Evaluation Facility	افزارگان ارزیابی امنیت فناوری اطلاعات
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission	سازمان بین‌المللی استانداردسازی/کمیسیون الکترونیکی بین‌المللی
IV	Initialization Vector	بردار اولیه
KEK	key encryption key	کلید رمزگذاری کلید
KMD	Key Management Description	توصیف مدیریت کلید
KRK	Key Release Key	کلید انتشار کلید
KW	Key Wrap	پوشاندن کلید
KWP	Key Wrap with Padding	پوشاندن کلید با لایه‌گذاری
MBR	Master Boot Record	رکورد راه‌انداز اصلی
NIST	National Institute of Standards and Technology	مؤسسه ملی استاندارد و فناوری
OS	Operating System	سیستم‌عامل
PBKDF	Password-Based Key Derivation Function	تابع استخراج کلید مبتنی بر کلمه‌عبور
PRF	Pseudo Random Function	تابع شبه تصادفی
RBG	Random Bit Generator	تولید کننده بیت تصادفی
RNG	Random Number Generator	تولید کننده عدد تصادفی
RSA	Rivest Shamir Adleman Algorithm	الگوریتم آدلمن شامیر ریوست
SAR	Security Assurance Requirement	الزامات تضمین امنیت
SED	Self Encrypting Drive	درایو خودرمزنگار
SHA	Secure Hash Algorithm	الگوریتم چکیده‌ساز امن

واژه اختصاری	معنای انگلیسی	ترجمه فارسی
SFR	Security Functional Requirements	الزامات کارکرد امنیت
SPD	Security Problem Definition	تعریف مسئله امنیتی
SPI	Serial Peripheral Interface	واسط بیرونی سریال
ST	Security Target	هدف امنیتی
TOE	Target of Evaluation	محصول
TPM	Trusted Platform Module	واحد سکو امن
TSF	TOE Security Functionality	کارکرد امنیتی محصول
TSS	TOE Summary Specification	مشخصات خلاصه محصول
USB	Universal Serial Bus	گذرگاه جهانی سریال
XOR	Exclusive Or	اپراتور بولی (یای انحصاری)
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing	قالب رمز قابل پیچاندن بلوک XEX (XOR رمز گذاری XOR) با سرقت متن رمز

پیوست ۷ مراجع

National Institute of Standards and Technology (NIST) Special Publication 800-38F, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, National Institute of Standards and Technology, December 2012.

National Institute of Standards and Technology (NIST) Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, National Institute of Standards and Technology, August 2009.

National Institute of Standards and Technology (NIST) Special Publication 800-88 Revision 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, December 2014.

National Institute of Standards and Technology (NIST) Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, January 2012.

National Institute of Standards and Technology (NIST) Special Publication 800-132, Recommendation for Password-Based Key Derivation Part 1: Storage Applications, National Institute of Standards and Technology, December 2010.

Federal Information Processing Standard Publication (FIPS-PUB) 186-4, Digital Signature Standard (DSS), National Institute of Standards and Technology, July 2013.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 9796-2:2010 (3rd edition), Information technology — Security techniques — Digital signature schemes giving message recovery, International Organization for Standardization/International Electrotechnical Commission, 2010.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 9797-2:2011 (2nd edition), Information technology — Security techniques — Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function, International Organization for Standardization/International Electrotechnical Commission, 2011.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 10116:2006 (3rd edition), Information technology — Security techniques — Modes of operation for an n-bit block cipher, International Organization for Standardization/International Electrotechnical Commission, 2006.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 10118-3:2004 (3rd edition), Information technology — Security techniques — Hash-functions – Part 3: Dedicated hash-functions, International Organization for Standardization/International Electrotechnical Commission, 2004.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 14888-3:2006 (2nd edition), Information technology — Security techniques —Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, International Organization for Standardization/International Electrotechnical Commission, 2006.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18031:2011 (2nd edition), Information technology — Security techniques — Random bit generation, International Organization for Standardization/International Electrotechnical Commission, 2011.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18033-3:2011 (3rd edition), Information technology — Security techniques — Encryption algorithms – Part 3: Block ciphers, International Organization for Standardization/International Electrotechnical Commission, 2011.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19772:2009, Information technology — Security techniques Authenticated encryption, International Organization for Standardization/International Electrotechnical Commission, 2009.