به نام خدا

پروفایل حفاظتی مشترک رمزنگاری کل درایو – موتور رمزنگاری

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 ارائه‌شده‌اند، 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) رمزنگاری کل درایو به همراه نمایندگانی از صنعت، کارگزاری‌های دولتی، آزمایشگاه‌های آزمون معیار مشترک و اعضای دانشگاه‌ها توسعه‌یافته 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) رمزنگاری کل درایو - موتور رمزنگاری[۶] (FDE EE) را ارائه نماید. اقدامات ارزیابی که توصیف‌کننده اقداماتی است که توسط ارزیاب اجرا می‌شود، برای تعیین این موضوع است که آیا یک محصول الزامات کارکرد امنیتی اتخاذشده در این پروفایل حفاظتی مشترک را که در *سند پشتیبان (سند فنی الزامی) رمزنگاری کل درایو: موتور رمزنگاری ژانویه ۲۰۱۵* توصیف‌شده است برآورده می‌سازد یا خیر.

---

[۱] Common Criteria

[۲] collaborative Protection Profile

[۳] international Technical Community

[۴] security functional requirements

[۵] security assurance requirements

[۶] Full Drive Encryption - Encryption Engine

راه‌حل کامل رمزنگاری کل درایو (FDE)[۷] هم به مؤلفه‌های اکتساب مجوز[۸] و هم به مؤلفه‌های موتور رمزنگاری[۹] نیاز دارد. محصولی ممکن است تمام راه‌حل را ارائه دهد و ادعای انطباق با این پروفایل حفاظتی مشترک و پروفایل حفاظتی مشترک رمزنگاری کل درایو – اکتساب مجوز را داشته باشد.

بااین‌حال به دلیل اینکه پروفایل حفاظتی اکتساب مجوز یا موتور رمزنگاری در مراحل مقدماتی خود است، امکان صدور حکمی که تمام محصولات وابسته، منطبق بر یک پروفایل حفاظتی مشترک باشد وجود ندارد. محصولات وابسته اعتبارسنجی نشده (به‌عنوان‌مثال موتور رمزنگاری) ممکن است به‌عنوان قسمت قابل‌قبولی از محیط عملیاتی برای محصول یا محصول اکتساب مجوز در نظر گرفته شود که به‌صورت مورد به مورد توسط طرح ملی مربوطه تعیین‌شده است.

انجمن فنی بین‌المللی (iTC) رمزنگاری کل درایو در نظر دارد تا راهنمایی‌هایی را برای توسعه‌دهندگانی ارائه دهد که محصولات آن‌ها هر دو مؤلفه اکتساب مجوز و موتور رمزنگاری را فراهم می‌کند، در نتیجه به آن‌ها در توسعه هدف امنیتی[۱۰] (ST) کمک می‌کند تا بتوانند ادعای انطباق با هر دو پروفایل حفاظتی مشترک رمزنگاری 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. هر فردی به‌سادگی نمی‌تواند به الزامات تضمین امنیتی در این پروفایل حفاظتی مشترک ارجاع دهد.

۱-۲- دامنه کاربرد سند

دامنه کاربرد پروفایل حفاظتی مشترک در فرایندهای توسعه و ارزیابی در ارزیابی امنیت فناوری اطلاعات معیار مشترک توصیف‌شده 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.

---

[۷] Full Drive Encryption

[۸] Authorization Acquisition

[۹] Encryption Engine

[۱۰] Security Target

۱-۳- مخاطبان هدف

مخاطبان هدف این پروفایل حفاظتی مشترک، توسعه‌دهندگان، استفاده‌کنندگان از معیار مشترک، ایجادکنندگان سیستم، ارزیاب‌ها و طرح‌ها می‌باشند. بااین‌حال، ممکن است پروفایل‌های حفاظتی مشترک و اسناد پشتیبان خطاهای ویرایشی جزئی داشته باشند، پروفایل‌های حفاظتی مشترک به‌عنوان اسناد زنده بوده و انجمن‌های فنی بین‌المللی (iTC) برای انجام به‌روزرسانی‌ها و بازبینی‌های مداوم منصوب‌شده‌اند.

۱-۴- اسناد مرتبط

پروفایل‌های حفاظتی

[FDE-AA] پروفایل حفاظتی مشترک رمزنگاری درایو کامل - اکتساب مجوز، نسخه ۱، ۲۶ ژانویه، ۲۰۱۵

معیار مشترک[۱۱]

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

[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

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

[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)، رمزنگاری درایو کامل: موتور رمزنگاری ژانویه ۲۰۱۵

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

هدف از اولین مجموعه از پروفایل‌های حفاظتی مشترک (cPPها) برای رمزنگاری کل درایو (FDE): اکتساب مجوز (AA) و موتور رمزنگاری (EE)، ارائه الزاماتی برای محافظت از داده‌های غیرفعال[۱۲] برای افزاره مفقودی است که شامل انباره است. این پروفایل‌های حفاظتی مشترک به راه‌حل‌های رمزنگاری 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 مورداستفاده (USB، SATA و ...) برای اتصال افزاره انبارش به ماشین میزبان، خارج از دامنه کاربرد این پروفایل حفاظتی مشترک است.

رمزنگاری کل درایو، تمام داده‌ها (با استثنائات خاص) را در افزاره انبارش رمزنگاری می‌کند و تنها بعد از اعطای مجوز موفقیت‌آمیز اجازه دسترسی به داده‌ها را به راه‌حل رمزنگاری کل درایو می‌دهد. استثنائات شامل ضرورت عدم رمزنگاری بخشی از افزاره انبارش (اندازه ممکن است بر اساس پیاده‌سازی متفاوت باشد) برای مواردی مانند رکورد راه‌انداز اصلی[۱۳] (MBR) یا دیگر نرم‌افزارهای از پیش احراز هویت شده اکتساب مجوز یا موتور رمزنگاری است. این پروفایل‌های حفاظتی مشترک رمزنگاری کل درایو، اصطلاح " رمزنگاری کل درایو" را به نحوی تفسیر می‌کنند تا به راه‌حل‌های رمزنگاری کل درایو اجازه دهد تا بخشی از افزاره انبارش را تا زمانی که شامل داده کاربر یا داده مجوز باشند، به‌صورت رمزنگاری نشده باقی بگذارند.

---

[۱۲] Data-at-Rest

[۱۳] Master Boot Record

ازآنجایی‌که پروفایل حفاظتی مشترک رمزنگاری کل درایو، از راه‌حل‌های گوناگونی پشتیبانی می‌کند، دو پروفایل حفاظتی مشترک که الزامات مؤلفه‌های رمزنگاری کل درایو را توصیف می‌کنند در شکل ۱ نشان داده‌شده است.

شکل ۱: جزئیات مؤلفه‌های رمزنگاری کل درایو

پروفایل حفاظتی مشترک رمزنگاری کل درایو:-اکتساب مجوز، الزاماتی را برای بخش اکتساب مجوز توضیح داده و الزامات امنیتی و اقدامات تضمین لازم برای تعامل با کاربر را به‌طور مفصل توضیح داده و در نتیجه منجر به دسترس‌پذیری مقادیر رمزنگاری مرزی[۱۴] (BEV) می‌شود.

پروفایل حفاظتی مشترک رمزنگاری کل درایو: -موتور رمزنگاری، الزاماتی را برای بخش موتور رمزنگاری شرح داده و الزامات امنیتی و اقدامات تضمین لازم برای رمزنگاری یا رمزگشایی عملی داده را توسط کلید رمزنگاری داده[۱۵] (DEK) به‌طور مفصل توضیح می‌دهد. همچنین، هرکدام از پروفایل‌های حفاظتی مشترک شامل مجموعه‌ای از الزامات اصلی برای کارکردهای مدیریتی، ساماندهی مناسب کلیدهای رمزنگاری، به‌روزرسانی‌های صورت گرفته به شیوه‌ای امن، ممیزی و خودآزمایی‌ها می‌باشند.

توصیف محصول، دامنه کاربرد و کارکردهای موتور رمزنگاری را تعریف کرده و تعریف مسئله امنیتی به توصیف مفروضات در نظر گرفته‌شده درباره محیط عملیاتی و تهدیدات مربوط به موتور رمزنگاری که الزامات پروفایل حفاظتی مشترک را موردتوجه قرار می‌دهند، می‌پردازد.

---

[۱۴] Border Encryption Value

[۱۵] Data Encryption Key

۱-۶- پیاده‌سازی‌ها

راهکارهای رمزنگاری کل درایو با ترکیب‌های فروشندگان و روش‌های پیاده‌سازی، تنوع می‌یابند. بنابراین، فروشندگان، محصولاتی را ارزیابی خواهند کرد که هر دو مؤلفه راهکارهای رمزنگاری کل درایو (اکتساب مجوز و موتور رمزنگاری) 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 رمزنگاری کل درایو را ارائه می‌دهد تنها در برابر پروفایل حفاظتی مشترک کاربردپذیر ارزیابی می‌شود. پروفایل حفاظتی مشترک رمزنگاری کل درایو به دو سند تقسیم می‌شود تا به آزمایشگاه‌ها اجازه دهد راه‌حل‌های درخور هریک از پروفایل‌های حفاظتی مشترک را به‌طور مستقل ارزیابی کنند. زمانی که مشتری راهکار رمزنگاری کل درایو را کسب می‌کند، در واقع آن‌ها محصول منحصربه‌فرد فروشنده را به دست می‌آورند که پروفایل‌های حفاظتی مشترک اکتساب مجوز و یا موتور رمزنگاری را برآورده می‌سازد، یا دو محصولی که یکی از آن‌ها پروفایل حفاظتی مشترک اکتساب مجوز و دیگری پروفایل حفاظتی مشترک موتور رمزنگاری 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، رابطی برای درایو خود رمزگذار ارائه می دهد.
درایو خود رمزگذار[۱۶] (SED)	موتور رمزنگاری	درایو خود رمزگذار همراه با نرم‌افزار میزبان جداگانه‌ای استفاده می‌شود.
نرم‌افزار رمزنگاری کل درایو	اکتساب مجوز + موتور رمزنگاری	یک راهکار نرم‌افزاری رمزنگاری کل درایو

[۱۶] Self-Encrypting Drive

ترکیبی	اکتساب مجوز + موتور رمزنگاری	ترکیبی از سخت‌افزار (مثلاً سخت‌افزار موتور رمزنگاری، کمک پردازنده رمزنگاری) و نرم‌افزار منحصر به فروشنده

۲- فرهنگ اصطلاحات

- **عامل مجوز (Authorization Factor)**

مقداری که کاربر می‌داند یا آن را دارد یا (مانند کلمه عبور، نشانه و ...) به محصول ارسال‌شده است تا تعیین کند که کاربر جزء جامعه مجاز به استفاده از دیسک سخت است و از آن برای استخراج یا رمزگشایی مقدار رمزنگاری مرزی (BEV) و رمزگشایی احتمالی کلید رمزنگاری داده (DEK) استفاده می‌شود. قابل‌ذکر 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 رمزنگاری مرزی (Border Encryption Value)**

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

- **پاک‌سازی کلید (Key Sanitization)**

روشی برای پاک‌سازی داده رمزنگاری‌شده با استفاده از بازنویسی امن کلیدی که داده را رمزنگاری کرده است.

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

کلیدی که برای رمزنگاری داده در حال سکون استفاده می‌شود.

- **رمزنگاری 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. به خاطر تعریف برنامه امنیتی (SPD) و پروفایل حفاظتی مشترک، رمزنگاری کل درایو (FDE)، رمزنگاری و مجوز دهی را روی یک افزاره به‌گونه‌ای انجام می‌دهد که به‌طور مشترک توسط سیستم‌عامل و سامانه فایل پشتیبانی و تعریف‌شده است. محصولات رمزنگاری کل درایو، تمام داده‌ها (با استثنائات خاص) را روی افزاره انبارش رمزنگاری می‌کنند و اجازه دسترسی به داده به راه‌حل رمزنگاری کل درایو را تنها بعد از اعطای موفق مجوز می‌دهد. استثنائات شامل ضرورت رمزنگاری نشده رها کردن افزاره 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 رمزنگاری است. پروفایل حفاظتی مشترک رمزنگاری کل درایو اصطلاح "رمزنگاری کل درایو" را تفسیر می‌کند تا به راه‌حل‌های رمزنگاری کل درایو اجازه دهد، افزاره از افزاره انبارش را تا زمانی که شامل داده حفاظت نشده می‌باشند، رمزنگاری رها کند.

- **کلید میانی (Intermediate Key)**

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

- **سکوی میزبان (Host Platform)**

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

- **زنجیره کلید (Key Chaining)**

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

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

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

- **اجزای کلید (Key Material)**

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

- **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 به‌طور مستقیم منابع سخت‌افزاری را کنترل کند.

- **حافظه غیر فرّار (Non-Volatile Memory)**

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

- **حالت خاموش (Powered-Off State)**

حالتی که در آن دستگاه خاموش شده است.

- **داده حفاظت‌شده (Protected Data)**

به تمام داده‌های روی افزاره انبارش اشاره دارد به‌استثنای افزاره کوچکی که به‌منظور 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 است. داده حفاظت‌شده شامل رکورد اصلی راه‌اندازی یا نواحی از پیش احراز هویت شده درایو نیست – نواحی از درایو که ضرورتاً رمزنگاری نشده‌اند.

- **Submask**

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

- **محصول[۱۷] (TOE)**

محصول مورد ارزیابی که در این سند، سامانه رمزنگاری کل درایو- موتور رمزنگاری است و مجموعه‌ای است از سخت‌افزارها، میان‌افزارها و یا نرم‌افزارها که با دستورالعمل‌ها و راهنمایی‌هایی همراه هستند.

۳- شرح محصول

۳-۱- مرور کلی بر محصول

[۱۷] Target of Evaluation

محصول این پروفایل حفاظتی مشترک، موتور رمزنگاری و یا بخشی از ارزیابی ترکیبی این پروفایل‌های حفاظتی مشترک برای رمزنگاری کل درایو (اکتساب مجوز یا موتور رمزنگاری) است.

بخش زیر به‌مرور کلی قابلیت‌های کارکردی موتور رمزنگاری کل درایو پروفایل حفاظتی مشترک و همچنین قابلیت‌های امنیتی می‌پردازد.

۳-۱-۱- معرفی موتور رمزنگاری

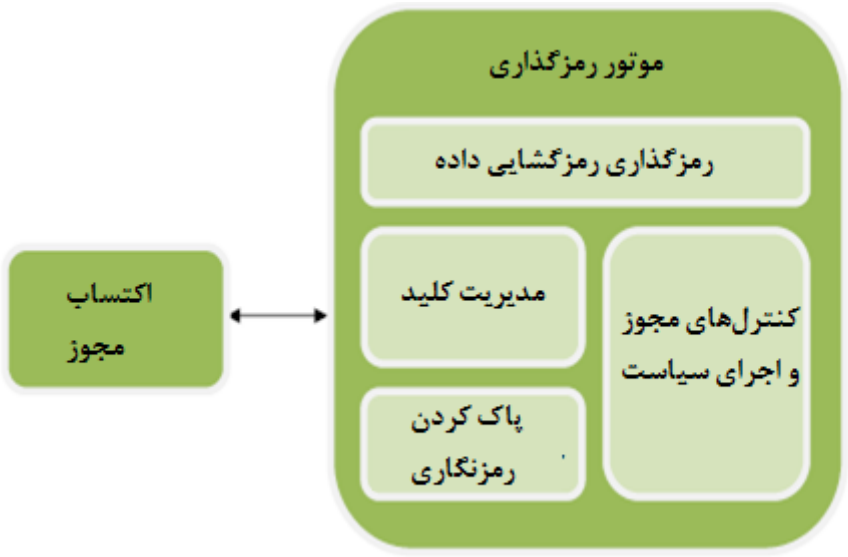
اهداف پروفایل حفاظتی مشترک موتور رمزنگاری بر روی رمزنگاری داده، اجرای خط‌مشی و مدیریت کلید تمرکز دارند. موتور رمزنگاری مسئول تولید، به‌روزرسانی، بایگانی، بازیابی، حفاظت و تخریب کلید رمزنگاری داده و دیگر کلیدهای میانی تحت کنترل خود است. موتور رمزنگاری، مقدار رمزنگاری مرزی را از اکتساب مجوز دریافت می‌کند و از آن برای رمزگشایی کلید رمزنگاری داده استفاده می‌کند، هر چند ممکن است کلیدهای میانی دیگری در بین این دو نقطه وجود داشته باشد. کلیدهای رمزنگاری کلید (KEK) سایر کلیدها به‌ویژه کلید رمزنگاری داده (DEK) و یا دیگر کلیدهای میانی که به کلید رمزنگاری داده متصل هستند را می‌پوشاند. کلیدهای انتشار کلید[۱۸] (KRK)، به موتور رمزنگاری مجوز می‌دهد که هرگونه کلید رمزنگاری داده یا دیگر کلیدهای میانی را انتشار دهد که به کلید رمزنگاری داده متصل هستند. این کلیدها تنها در استفاده کارکردی متفاوت می‌باشند.

موتور رمزنگاری تعیین می‌کند که آیا اکتساب مجوز پذیرش یا رد یک اقدام درخواست شده را بر اساس کلید رمزنگاری کلید یا کلید انتشار کلید ارائه می‌دهد یا خیر. اقدامات درخواست شده ممکن است، شامل تغییر کلیدهای رمزنگاری، رمزگشایی داده و پاک‌سازی کلید از کلیدهای رمزنگاری (از جمله کلید رمزنگاری داده) باشد ولی محدود به این موارد نیست. موتور رمزنگاری ممکن است خط‌مشی‌های بیشتری را برای جلوگیری از دسترسی به متن رمز یا بخش رمزنگاری نشده افزاره انبارش اعمال نماید. علاوه بر این، موتور رمزنگاری ممکن است برای کاربران مختلف، به‌صورت شخصی، پشتیبانی رمزنگاری ارائه دهد.

شکل۲، مؤلفه‌های موتور رمزنگاری و رابطه آن با اکتساب مجوز را نشان می‌دهد.

---

[۱۸] Key releasing keys



شکل ۲ جزئیات موتور رمزنگاری

۳-۱-۲-قابلیت‌های امنیتی موتور رمزنگاری

موتور رمزنگاری در نهایت مسئول حصول اطمینان از این موضوع است که داده‌ها با استفاده از مجموعه‌ای از الگوریتم‌های تعیین‌شده رمزنگاری‌شده‌اند. موتور رمزنگاری، رمزگشایی داده بر روی افزاره انبارش را از طریق رمزگشایی کلید رمزنگاری داده و بر اساس اعتبار مقدار رمزنگاری مرزی ارائه‌شده توسط اکتساب مجوز، مدیریت می‌کند. همچنین موتور رمزنگاری کارکردهای اجرایی را مدیریت می‌کند؛ از جمله زنجیره سازی کلید رمزنگاری داده، مدیریت مقدار رمزنگاری مرزی موردنیاز برای رمزگشایی یا انتشار کلید رمزگذاری داده، مدیریت کلیدهای پوشاننده میانی تحت کنترل موتور رمزنگاری و انجام پاک‌سازی کلید.

موتور رمزنگاری، ممکن است قابلیت کارکردی بازیابی و بایگانی کلیدها را ارائه دهد. موتور رمزنگاری ممکن است بازیابی و بایگانی کردن را خود ارائه داده، یا با اکتساب مجوز برای انجام این کار اتصال برقرار کند. موتور رمزنگاری همچنین ممکن است ویژگی‌های قابل پیکربندی‌ای ارائه دهد که حرکت اجزای کلید را محدود کرده و قابلیت بازیابی را غیرفعال کند.

در درجه نخست، هدف امنیتی رمزنگاری افزاره انبارش این است که مهاجم را مجبور کند تا به‌منظور بازیابی کلید رمزنگاری داده یا سایر کلیدهای میانی به جستجوی کامل فضای بسیار گسترده کلید بپردازد. موتور رمزنگاری از رمزنگاری مورد تأیید برای ایجاد، مدیریت و محافظت کلیدها استفاده می‌کند تا مهاجمی را که سکویِ مفقودی یا به سرقت رفته و روشن را بدون عوامل مجوز یا کلیدهای میانی به دست می‌آورد، مجبور کند تا فضای کلید رمزنگاری کلیدهای میانی یا کلید رمزنگاری داده را به‌دقت بررسی کند تا داده‌ای به دست آورد. موتور رمزنگاری، کلیدهای رمزنگاری داده - و در بعضی موارد- کلیدهای میانی را به‌صورت تصادفی تولید می‌کند. موتور رمزنگاری از کلیدهای رمزنگاری داده در الگوریتم رمزنگاری متقارن به‌صورت مناسب و با استفاده از بردارهای اولیه مناسب برای آن مد استفاده می‌کند تا واحدهای انبارش (به‌عنوان‌مثال بخش‌ها یا بلوک‌ها) را در افزاره انبارش رمزنگاری کند. همچنین، موتور رمزنگاری، کلید رمزنگاری داده را با استفاده از کلید رمزنگاری کلید یا یک کلید میانی رمزنگاری می‌کند.

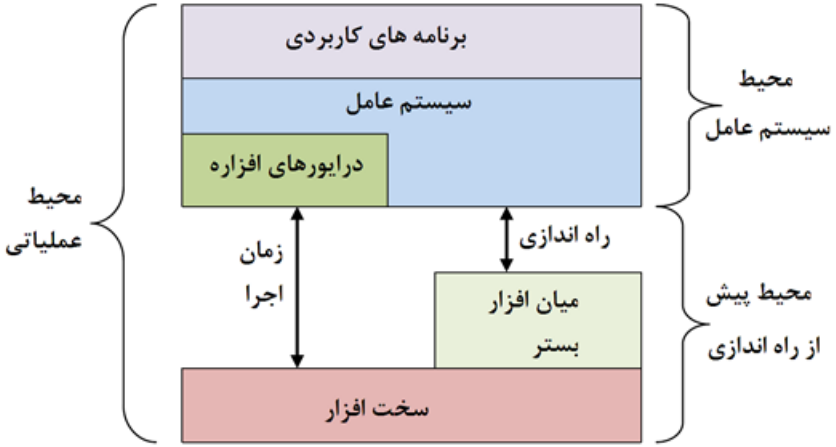
۳-۲- محصول و محیط‌های عملیاتی یا محیط‌های پیش از راه‌اندازی

محیطی که موتور رمزنگاری در آن عمل می‌کند ممکن است بسته به مرحله راه‌اندازی سکویی که در آن عمل می‌کند، متفاوت باشد، شکل ۳ را ببینید. جنبه‌های مقداردهی اولیه و شاید مجوز دهی ممکن است در محیط پیش از راه‌اندازی انجام شود، درحالی‌که به‌احتمال زیاد آماده‌سازی، رمزنگاری، رمزگشایی و کارکردهای مدیریتی در محیط سیستم‌عامل انجام می‌شود. بعضی از این جوانب ممکن است در هر دو محیط اتفاق بیافتد.

محیط سیستم‌عامل، ممکن است گستره کاملی از خدمات را برای موتور رمزنگاری در دسترس قرار دهد. این خدمات شامل درایورهای سخت‌افزاری، کتابخانه‌های رمزنگاری و شاید دیگر خدمات بیرونی محصول است.

محیط پیش از راه‌اندازی با قابلیت‌های محدودشده، بیشتر محدود می‌شود. این محیط حداقل تعداد دستگاه‌های جانبی را به کار می‌اندازد و تنها درایورهای ضروری را جهت آوردن سکو از یک شروع سرد[۱۹] تا اجرای سیستم‌عامل کارکردی کامل با اجرای برنامه‌های کاربردی بارگذاری می‌کند.

محصول موتور رمزنگاری، شامل یا تقویت‌کننده ویژگی‌ها و توابعی در محیط عملیاتی است.



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، بازیابی کلید و مدیریت روشن بودن (الزامات محافظت از حالت روشن بودن) است.

[۱۹] cold start

۳-۴- حالت استفاده محصول

حالت استفاده محصول منطبق با پروفایل‌های حفاظتی مشترک رمزنگاری کل درایو، برای محافظت از داده غیرفعالی است که روی افزاره گم‌شده یا به سرقت رفته‌ای قرار دارد که بدون هرگونه دسترسی قبلی توسط مهاجم، خاموش شده است. حالت استفاده‌ای که مهاجم به افزاره‌ای دسترسی دارد که در حالت روشن است و قادر به ایجاد تغییر محیط یا خود محصول را دارد (مانند حملات evil maid)، در این پروفایل (رمزنگاری کل درایو - اکتساب مجوز و رمزنگاری کل درایو - موتور رمزنگاری) موردتوجه نیست.

۴- مسائل امنیتی

۱-۴- تهدیدها

این بخش توضیح می‌دهد که 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 به شکل محدودی تضعیف کند.

تهدید شامل عامل تهدید، دارایی و اقدام مضر آن عامل تهدید روی آن دارایی است. عوامل تهدید، موجودیت‌هایی هستند که در صورتی دارایی‌ها را در معرض خطر قرار می‌دهند که مهاجم افزاره انبارش گم‌شده یا به سرقت رفته را به دست آورد. تهدیدات، الزامات کارکردی محصول را عقب می‌رانند. به‌عنوان‌مثال یکی از تهدیدات، دسترسی غیرمجاز به داده‌ها (T.UNAUTHORIZED_DATA_ACCESS) است. عامل تهدید، متصرف (کاربر غیرمجاز) افزاره انبارش گم‌شده یا به سرقت رفته است. دارایی، داده موجود بر روی افزاره انبارش است و اقدام مضر تلاش برای به دست آوردن این داده‌ها از افزاره انبارش است. این تهدید، باعث عقب راندن الزامات کارکردی افزاره انبارش رمزنگاری‌شده (محصول) می‌شود تا به فرد مجوز بدهد تا بتواند از محصول برای دسترسی به دیسک سخت و داده‌های رمزنگاری یا رمزگشایی استفاده کند. در اختیار داشتن کلید رمزنگاری کلید، کلید رمزنگاری 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 رمزنگاری را بشکند، این تعریف مسئله امنیتی، اجزای کلید را معادل داده با اهمیت در نظر 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 به سرقت رفته 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 به‌صورت 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 به‌روزرسانی برای محصول است، هر چند به‌جز 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 موردتوجه قرار نمی‌دهد، جایی که مهاجم ممکن است دیسک سخت را برداشته باشد، بخش رمزنگاری نشده 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 بتواند کد به خطر افتاده را اجرا کنند.

تهدیدات	توضیحات

تهدیدات دسترسی غیرمجاز به داده‌ها T.UNAUTHORIZED_DATA_ACCESS	تهدید اصلی، افشای غیرمجاز داده محافظت‌شده و ذخیره‌شده بر روی افزاره انبارش است که موردتوجه پروفایل حفاظتی مشترک است. اگر مهاجمی افزاره انبارش گم‌شده یا به سرقت رفته (به‌عنوان‌مثال افزاره انبارش موجود در یک لپ‌تاپ یا افزاره انبارش قابل‌حمل) را به دست 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 (به‌عنوان‌مثال بخش مشخصی از دیسک، قالب‌های مشخص) دارند. [FDP_DSK_EXT.1.1, FDP_DSK_EXT.1.2, FPT_KYP_EXT.1.1, FCS_CKM.1.1, FCS_KYC_EXT.2.1, FCS_SMV_EXT.1.1, FCS_SMV_EXT.1.2, FCS_SNI_EXT.1.1, FCS_SNI_EXT.1.2, FCS_SNI_EXT.1.3, FCS_CKM_EXT.4, FCS_CKM.4.1, FMT_SMF.1.1, FPT_TST_EXT.1.1] منطق: عناصر ۱ و ۲ الزام کارکرد امنیتی حفاظت از داده بر روی دیسک (FDP_DSK_EXT.1.1 و FDP_DSK_EXT.1.2) اطمینان حاصل می‌کند که محصول کل درایو را که دربرگیرنده تمام داده‌های محافظت شده است رمزنگاری می‌کند. "رمزنگاری کل درایو" در واژه‌نامه این پروفایل حفاظتی مشترک بدین صورت تعریف شده است: "به افزاره‌های بلوک‌های منطقی داده دسترس‌پذیر کاربر اشاره دارد که توسط سامانه فایل تعریف‌شده و شاخص گذاری و افزاره‌بندی شده است و سیستم‌عاملی که مجوز خواندن یا نوشتن داده در بلوک‌های این افزاره‌ها را طرح‌ریزی می‌کند". البته در مورد رکورد راه‌انداز اصلی و دیگر نرم‌افزارهای از پیش احراز هویت شده اکتساب مجوز یا موتور رمزنگاری استثنا وجود دارد. در نتیجه تضمین می‌شود که داده محافظت‌شده حتی اگر افزاره گم شود، قابل‌تصرف نیست. خطر کشف رمز کلیدها یا عوامل مجوز دهی، بازیابی آسان داده رمزنگاری‌شده بر روی درایو را ممکن می‌سازد. الزام کارکرد امنیتی حفاظت از کلید و اجزای کلید (FPT_KYP_EXT.1.1) این اطمینان را می‌دهد که اجزای کلید پوشانده نشده در حافظه غیر فرّار ذخیره نشوند. الزام کارکرد امنیتی تخریب اجزای کلید و کلید رمزنگاری (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، دسترس‌پذیری اجزای کلید را به حداقل رسانده و احتمال استفاده از این اجزا برای بازیابی کلید رمزنگاری داده یا عامل مجوز دهی را کاهش می‌دهد. الزامات کارکرد امنیتی تولید

	کلید رمزنگاری (FCS_CKM.1.1)، زنجیره‌ای کردن کلید (FCS_KYC_EXT.2.1)، اعتبارسنجی (FCS_SMV_EXT.1.1 و FCS_SMV_EXT.1.2)، عملیات رمزنگاری (Salt، مقدار مقطعی و بردار اولیه) (FCS_SNI_EXT.1.1، FCS_SNI_EXT.1.2 و FCS_SNI_EXT.1.3) تضمین می‌کنند که اجزای کلید با استحکام کافی و اثربخش تولیدشده و به‌روشی پوشانده می شود که استحکام آن حفظ گردد. این الزامات، هزینه به دست آوردن اجزای کلید یا عوامل مجوز را به‌اندازه حدس زدن کلید رمزنگاری داده، دشوار می‌کنند. الزام کارکرد امنیتی آزمون توابع هدف امنیتی (FPT_TST_EXT.1.1) عملکرد صحیح محصول را نشان می‌دهد و تضمین می‌کند که توابع رمزنگاری که از داده حفاظت‌شده، محافظت می‌کنند، مطابق با رفتار در نظر گرفته‌شده برایشان عمل کنند. الزام کارکرد امنیتی مشخصات توابع مدیریت (FMT_SMF.1.1) این اطمینان را می‌دهد که توابع هدف امنیتی، توابع ضروری برای مدیریت جوانب مهم محصول از جمله درخواست تغییر و پاک کردن کلید رمزنگاری داده را ارائه می‌دهند.

تهدید در معرض خطر قرار دادن اجزای کلید زنی T.KEYING_MATERIAL_COMPROMISE	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 رمزنگاری را بشکنند. پروفایل حفاظتی مشترک، تصاحب اجزای کلید زنی را با اهمیتی معادل خود داده‌ها در نظر می‌گیرد. عوامل تهدید ممکن است به دنبال اجزای کلید زنی در بخش‌های رمزنگاری نشده افزاره انبارش و دیگر دستگاه‌های جانبی در محیط عملیاتی (OE) مانند پیکربندی BIOS، فلش SPI یا TPMs باشند. [FCS_KYC _EXT.1.1, FCS_CKM_EXT.4, FCS_CKM.4.1, FCS_CKM.1.1, FCS_KYC_EXT.2, FCS_SMV_EXT.1.1, FMT_SMF.1.1] منطق: 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 غیر فرّار ذخیره نشوند و الزام کارکرد امنیتی تخریب اجزای کلید و کلید رمزنگاری توسعه‌یافته (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. الزامات کارکرد امنیتی تولید کلید رمزنگاری (FCS_CKM.1.1)، زنجیره‌ای کردن کلید (FCS_KYC_EXT.2) و اعتبارسنجی (FCS_SMV_EXT.1.1) این اطمینان را می‌دهند که اجزای کلید با استحکام اثربخش و کافی، تولید شده و به شیوه‌ای پوشانده شوند که استحکام آن حفظ شود. این الزامات، هزینه به دست آوردن اجزای کلید یا عوامل مجوز را به‌اندازه حدس کلید رمزنگاری داده، دشوار می‌کنند. الزام کارکرد امنیتی مشخصات توابع مدیریت (FMT_SMF.1.1) این اطمینان را می‌دهد که توابع هدف امنیتی، توابع ضروری برای مدیریت جوانب مهم محصول از جمله تولید و پیکربندی عوامل مجوز را ارائه می‌دهند.

تهدید حدس زدن مجوز T.AUTHORIZATION_GUESSING	این عامل تهدید ممکن ا ست به‌طور مکرر نرم‌افزار میزبان را برای حدس عوامل مجوز مانند کلمه‌های عبور و پین‌ها، به کار گیرد. حدس زدن موفق عوامل مجوز ممکن است باعث شود محصول کلیدهای رمزنگاری داده را منتشر کند یا آن را در حالتی قرار دهد که در آن داده محافظت‌شده را برای کاربران غیرمجاز افشا کند. [FCS_SMV_EXT.1.2] منطق: الزام کارکرد امنیتی اعتبار سنجی (FCS_SMV_EXT.1.2) به گزینه‌های مختلفی برای اجرای اعتبار سنجی نیاز دارد مانند پاک‌سازی کلید رمزنگاری داده، یا زمانی که تعداد قابل تنظیمی از تلاش‌های اعتبارسنجی شکست‌خورده در یک دوره ۲۴ ساعته به د ست می‌آید. این الزام از حملات جستجوی فراگیر در برابر عوامل مجوز مانند کلمه‌های عبور و پین‌ها جلوگیری می‌کند.
تهدید استفاده از تمام فضای کلید T.KEYSPACE_EXHAUST	عوامل تهدید ممکن است با رمزنگاری و یا به‌صورت مخفیانه از تمام فضای کلید استفاده کنند. انتخاب ضعیف الگوریتم‌های رمزنگاری و یا پارامترها به مهاجمان این اجازه را می‌دهد که با جستجوی فراگیر تمام فضای کلید را در دست بگیرند و به آن‌ها اجازه دسترسی غیرمجاز به داده را می‌دهد. [FCS_CKM.1, FCS_RBG_EXT.1.1] منطق: الزامات کارکرد امنیتی تولید کلید رمزنگاری (FCS_CKM.1) و عملیات رمزنگاری تولید بیت تصادفی (FCS_RBG_EXT.1.1) این اطمینان را می‌دهند که کلیدهای رمزنگاری تصادفی بوده و استحکام یا طول مناسب آن موانع هزینه‌ای و دشواری رمزنگاری را در برابر تلاش‌های استفاده از تمام فضا ایجاد می‌کند.

تهدید متن خام شناخته‌شده T.KNOWN_PLAINTEXT	عوامل تهدید، متن خام را در فضاهایی از افزاره انبارش به‌خصوص در فضاهای بدون مقدار اولیه (همگی صفر) و نیز فضاهایی که شامل نرم‌افزارهای به‌خوبی شناخته شده مانند سیستم‌عامل‌ها می‌باشند، می شناسند. انتخاب ضعیف الگوریتم‌های رمزنگاری، مدهای رمزنگاری و بردارهای اولیه ضعیف به همراه متن خام شناخته‌شده می‌تواند به مهاجم اجازه بازیابی کلید رمزنگاری داده اثربخش را بدهد، در نتیجه دسترسی غیرمجازی به متن‌های خام ناشناخته قبلی بر روی افزاره انبارش را فراهم آورد. [FCS_COP.1(f), FCS_SNI_EXT.1] منطق: الزام کارکرد امنیتی عملیات رمزنگاری (رمزنگاری یا رمزگشایی داده استاندارد رمزنگاری پیشرفته((FCS_COP.1(f)) انتخاب مناسب الگوریتم رمزنگاری و مد آن را تضمین می‌کند. الزام کارکرد امنیتی عملیات رمزنگاری (Salt، مقدار مقطعی و بردار اولیه) (FCS_SNI_EXT.1) از ساماندهی مناسب Saltها، مقادیر مقطعی و بردارهای اولیه اطمینان حاصل می‌کند.
تهدید متن خام منتخب T.CHOSEN_PLAINTEXT	عوامل تهدید ممکن است، کاربران مجاز را در ذخیره متن خام منتخب بر روی افزاره انبارش رمزنگاری‌شده در قالب یک تصویر، سند و یا فایل‌های دیگر فریب دهند. انتخاب ضعیف الگوریتم‌های رمزنگاری، مدهای رمزنگاری و بردارهای اولیه به همراه متن خام منتخب می‌تواند به مهاجم اجازه بازیابی کلید رمزنگاری داده اثربخش را بدهد، در نتیجه دسترسی غیرمجازی به متن‌های خام ناشناخته قبلی بر روی افزاره انبارش را فراهم آورد. [FCS_COP.1(f), FCS_SNI_EXT.1] منطق: الزام کارکرد امنیتی عملیات رمزنگاری (رمزنگاری یا رمزگشایی داده استاندارد رمزنگاری پیشرفته((FCS_COP.1(f)) انتخاب مناسب الگوریتم رمزنگاری و مد آن را تضمین می‌کند. الزام کارکرد امنیتی عملیات رمزنگاری (Salt، مقدار مقطعی و بردار اولیه) (FCS_SNI_EXT.1) از ساماندهی مناسب Saltها، مقادیر مقطعی و بردارهای اولیه اطمینان حاصل می‌کند.

تهدید به‌روزرسانی غیرمجاز T.UNAUTHORIZED_UPDATE	عوامل تهدید ممکن است اقدام به اجرای به‌روزرسانی محصولی کنند که ویژگی‌های امنیتی محصول را به خطر می‌اندازند. انتخاب ضعیف پروتکل‌های به‌روزرسانی، الگوریتم‌های تولید و درستی‌سنجی امضا و پارامترها ممکن است به مهاجمان این اجازه را بدهد که نرم‌افزار و یا سفت افزاری را نصب کنند که ویژگی‌های امنیتی در نظر گرفته‌شده 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 به‌روزرسانی امن (FPT_TUD_EXT.1.1، FPT_TUD_EXT.1.2 و FPT_TUD_EXT.1.3) برای کاربران مجاز قابلیت پرس‌وجوی نسخه فعلی سفت افزار یا نرم‌افزار محصول، به‌روزرسانی‌های نخستین و برر سی به‌روزر سانی‌ها را قبل از نصب با ا ستفاده از امضای دیجیتالی تولیدکننده ارائه می‌دهد. الزام کارکرد امنیتی مشخصات توابع مدیریت (FMT_SMF.1.1) این اطمینان را می‌دهد که توابع هدف امنیتی (TSF) توابع ضروری برای مدیریت جوانب مهم محصول از جمله آغاز به‌روزرسانی‌های نرم‌افزار یا سفت افزار سامانه را ارائه دهند.

۴-۲- مفروضات

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

مفروضات	توضیحات
فرض کانال مطمئن (A.TRUSTED_CHANNEL)	ارتباط میان و بین مؤلفه‌های محصول (اکتساب مجوز و موتور رمزنگاری) به‌اندازه کافی برای جلوگیری از افشای اطلاعات محافظت‌شده هستند. در مواردی که یک محصول منحصربه‌فرد هر دو پروفایل حفاظتی مشترک را برآورده می‌سازد، ارتباط بین مؤلفه‌ها فراتر از مرزهای محصول توسعه نمی‌یابد (به‌عبارت‌دیگر مسیر ارتباطی درون مرز محصول است). در مواردی که محصولات مستقل، الزامات اکتساب مجوز و موتور رمزنگاری را برآورده می‌سازند، نزدیکی فیزیکی دو محصول در طول عملیاتشان، بدین معنا است که عامل تهدید شانس بسیار کمی برای مداخله در کانال بین این دو بدون توجه کاربر و انجام اقدامات مناسب، دارد.[OE.TRUSTED_CHANNEL]
فرض حالت اولیه درایو (A.INITIAL_DRIVE_STATE)	کاربران، رمزنگاری کل درایو را روی افزاره انبارشی که جدیداً تهیه‌شده یا مقداردهی اولیه شده است و خالی از داده‌های محافظت‌شده در نواحی است که مورد هدف رمزنگاری نیستند، فعال می‌کنند. همچنین فرض می‌شود داده در نظر گرفته‌شده برای محافظت نباید تا بعد از آماده‌سازی در رسانه انبارش مورد هدف باشد. این پروفایل حفاظتی مشترک شامل الزاماتی نمی‌شود که تمام نواحی بر روی افزاره‌های انبارش را جستجو کند که به‌طور بالقوه حاوی داده‌های محافظت شده می‌باشند. در بعضی موارد ممکن است این کار غیرممکن باشد، برای مثال در حالتی که داده‌ها در بخش‌های "بد" گنجانده‌شده‌اند. درحالی‌که افشای ناخواسته داده‌های موجود در بخش‌های بد یا فضاهای افراز نشده، بعید است، بااین‌حال ممکن است کسی از ابزارهای قانونی برای بازیابی داده از چنین نواحی افزاره انبارش استفاده نماید. در نتیجه، پروفایل حفاظتی مشترک فرض می‌کند، بخش‌های بد، فضاهای افراز نشده و نواحی‌ای که ممکن است شامل کدهای رمز نشده باشند (مانند رکورد راه‌انداز اصلی و نرم‌افزار از قبل احراز هویت شده اکتساب مجوز یا موتور رمزنگاری) حاوی هیچ داده محافظت‌شده‌ای نمی‌باشند. [OE.INITIAL_DRIVE_STATE]

فرض کاربر آموزش‌دیده A.TRAINED_USER	کاربران از راهنمایی‌های ارائه‌شده برای امن ساختن محصول و عوامل مجوز پیروی می‌کنند. این راهنماها شامل انطباق با استحکام عامل مجوز، عدم استفاده از عوامل مجوز نشانه (توکن) خارجی برای اهداف دیگری و اطمینان از اینکه عوامل مجوز نشانه (توکن) خارجی مستقل از افزاره انبارش و یا سکو، به‌گونه‌ای امن ذخیره می شوند، است. همچنین کاربران باید در ارتباط با نحوه خاموش کردن سامانه خود نیز آموزش ببینند. [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 است (یا افزاره انبارش بیرونی به آن وصل شده است)، باید عاری از هرگونه نرم‌افزار مخربی باشد تا بتواند با عملکرد صحیح محصول ارتباط برقرار کند.[OE.PLATFORM_STATE]
فرض خاموش بودن A.POWER_DOWN	کاربر سکو و یا افزاره انبارش را تا زمانی که محصول خاموش شود، رها نمی‌کند، این کار حافظه‌ها را به‌درستی پاک‌کرده و افزاره را قفل می‌کند. کاربران مجاز، سکو و یا افزاره انبارش را در حالتی قرار نمی‌دهند که اطلاعات حساس در حافظه غیر فرّار باقی‌مانده باشند (مانند وضعیت خواب یا قفل صفحه‌نمایش). کاربر سکو و یا افزاره انبارش را خاموش می‌کند یا در حالت روشن ولی مدیریت‌شده مانند "مد هایبرنت" قرار می‌دهد.[OE.POWER_DOWN]
فرض رمزنگاری قوی A.STRONG_CRYPTO	تمام رمزنگاری‌های پیاده‌سازی شده در محیط عملیاتی و مورداستفاده 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 است 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 نواحی‌ای 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 رو شن مدیریت شده مانند حالت خواب زم ستانی قرار دهند. فرض خاموش بودن (A.POWER_DOWN) ت صریح 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 مح صول 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.

۶- الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول به‌صورت خلاصه در **Error! Reference source not found.** آورده شده است.

جدول ۲ الزامات کارکرد امنیتی

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**تولید کلید رمزنگاری ۱**	FCS_CKM.1.1
۲	**تخریب کلید رمزنگاری و اجزای کلید ۱**	FCS_CKM_EXT.4.1
۳	**تخریب کلید رمزنگاری ۱**	FCS_CKM.4.1
۴	**زنجیره‌ای کردن کلید ۱**	FCS_KYC_EXT.2.1
۵	**زنجیره‌ای کردن کلید ۲**	FCS_KYC_EXT.2.2
۶	**اعتبارسنجی ۱**	FCS_SMV_EXT.1.1
۷	**اعتبارسنجی ۲**	FCS_SMV_EXT.1.2
۸	**عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار) ۱**	FCS_SNI_EXT.1.1
۹	**عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار) ۲**	FCS_SNI_EXT.1.2
۱۰	**عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار) ۳**	FCS_SNI_EXT.1.3
۱۱	**حفاظت از داده بر روی دیسک ۱**	FDP_DSK_EXT.1.1
۱۲	**حفاظت از داده بر روی دیسک ۲**	FDP_DSK_EXT.1.2
۱۳	**مشخصات کارکردهای مدیریتی ۱**	FMT_SMF.1.1
۱۴	**حفاظت از کلید و اجزای کلید ۱**	FPT_KYP_EXT.1.1
۱۵	**به‌روزرسانی امن ۱**	FPT_TUD_EXT.1.1
۱۶	**به‌روزرسانی امن ۲**	FPT_TUD_EXT.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۷	**به‌روزرسانی امن ۱**	FPT_TUD_EXT.1.3
۱۸	**آزمون کارکرد هدف امنیتی**	FPT_TST_EXT.1

۶-۱- کلاس پشتیبانی رمزنگاری

شماره الزام	نام الزام
۱	**تولید کلید رمزنگاری داده ۱**

پالایش: توابع هدف امنیتی باید [انتخاب:

- تولید کلید رمزنگاری داده با استفاده از تولیدکننده بیت تصادفی همان‌طور که در الزام کارکردی تولید بیت تصادفی (FCS_RBG_EXT.1) (پیوست ۲) توصیف‌شده است.
- پذیرفتن کلید رمزنگاری داده که توسط تولیدکننده بیت تصادفی تولیدشده و توسط سکوی میزبان ایجادشده است.
- پذیرفتن کلید رمزنگاری داده که مطابق با شرح عملیات رمزنگاری (پوشاندن کلید) ((FCS_COP.1(d)) (پیوست ۲) مخفی‌شده است.]

که اندازه آن طول [انتخاب: ۱۲۸ بیت، ۲۵۶ بیت] است، را اجرا کند.

نکته کاربردی ۱: هدف این الزام توصیف تولید کلید رمزنگاری داده در طول آماده‌سازی است.

اگر محصول بتواند به‌گونه‌ای پیکربندی شود که با استفاده از چندین روش، کلید رمزنگاری داده را به دست آورد، نویسنده هدف امنیتی گزینه‌های کاربردی درخواستی را از انتخاب‌های بالا برمی‌گزینند. به‌عنوان‌مثال، محصول ممکن است اعداد تصادفی را با استفاده از تولیدکننده بیت تصادفی قابل‌قبول به‌منظور ایجاد کلید رمزنگاری داده تولید نماید و همچنین رابطی برای پذیرش کلید رمزنگاری داده از محیط فراهم آورد.

اگر نویسنده هدف امنیتی، اولین و یا سومین گزینه از انتخابات بالا را برگزیند، الزامات مربوطه را از پیوست ۱ بیرون آمده و در متن هدف امنیتی گنجانده خواهد شد.

۲	**تخریب کلید رمزنگاری و اجزای کلید ۱**

توابع هدف امنیتی باید تمام کلیدها یا اجزای کلید که دیگر موردنیاز نیستند را از بین ببرد.

نکته کاربردی ۲: 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.

۳	**تخریب کلید رمزنگاری ۱**

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 منحصربه‌فرد انجام شود [انتخاب: شامل الگوی شبه تصادفی با استفاده از تولیدکننده بیت تصادفی توابع هدف امنیتی، شامل الگوی شبه تصادفی با استفاده از تولیدکننده بیت تصادفی سکوی میزبان، شامل صفرها] که با خواندن-تأیید ادامه می‌یابد.
- برای انباره غیر فرّار پاک کردن توسط موارد زیر اجرا می‌شود:
  - یک [انتخاب: یک، سه یا دفعات بیشتری] بازنویسی مکان انبارش داده کلید شامل [انتخاب: الگوی شبه تصادفی با استفاده از تولیدکننده بیت تصادفی توابع هدف امنیتی همان‌گونه که در الزام کارکرد امنیتی تولید بیت تصادفی (FCS_RGB_EXT.1) توضیح داده‌شده است، الگوی شبه تصادفی با استفاده از تولیدکننده بیت تصادفی سکوی میزبان، الگوی ثابت]، که توسط [انتخاب: خواندن- تأیید، هیچ] ادامه می‌یابد. اگر خواندن-درستی‌سنجی داده‌های بازنویسی شده با شکست مواجه شود، فرایند دوباره باید تکرار شود؛] که از [انتخاب: NIST SP800-88، هیچ استانداردی] پیروی می‌کند.

نکته کاربردی ۳: کلیدها از جمله کلیدهای میانی یا اجزای کلید که دیگر موردنیاز نیستند با استفاده از یکی از این متدهای پذیرفته‌شده در حافظه فرار از بین می‌روند. در این موارد روش تخریب با یکی از روش‌های توضیح داده‌شده در این الزام مطابقت دارد. این الزام روشی را برای پاک کردن رمزنگاری فراخوانی می‌کند و شرایطی را برای

تخریب اطلاعات کلید در نظر می‌گیرد. بعضی از راه‌حل‌ها دسترسی نوشتن در مکان‌هایی از رسانه را که کلید ذخیره‌شده است 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 سامانه و یا سطح افزاره می‌تواند منجر به نسخه‌های متعدد از داده کلید و یا فناوری رسانه زیرین شود که از بازنویسی مستقیم مکان‌هایی که در آن داده کلید ذخیره‌شده‌اند پشتیبانی نکند. توجه داشته باشید حافظه‌هایی که یک‌بار قابل‌برنامه‌ریزی شدن هستند مستثنا هستند.	
زنجیره‌ای کردن کلید ۱	۴
توابع هدف امنیتی باید مقدار رمزنگاری مرزی [انتخاب: ۱۲۸ بیت، ۲۵۶ بیت] از اکتساب مجوز را بپذیرد.	
زنجیره‌ای کردن کلید ۲	۵
توابع هدف امنیتی باید حاوی زنجیره‌ای از کلیدهای میانی باشد که از مقدار رمزنگاری مرزی تا کلیدهای رمزنگاری داده نشأت می‌گیرد و از روش‌های زیر استفاده می‌کند: [انتخاب: استخراج کلید به‌نحوی‌که در الزام کارکرد امنیتی استخراج کلید رمزنگاری (FCS_KDF_EXT.1) توصیف‌شده است، پوشاندن کلید به‌نحوی‌که در الزام کارکرد امنیتی عملیات رمزنگاری پوشاندن کلید ((FCS_COP.1(d)) توصیف‌شده است]، انتقال کلید به‌نحوی‌که در الزام کارکرد امنیتی عملیات رمزنگاری انتقال کلید ((FCS_COP.1(e)) توصیف‌شده است، رمزنگاری کلید به‌نحوی‌که در الزام کارکرد امنیتی عملیات رمزنگاری - رمزنگاری کلید ((FCS_COP.1(g)) توصیف‌شده است]] درحالی‌که استحکام اثربخش [انتخاب: ۱۲۸ بیت،۲۵۶ بیت] را حفظ می‌کند.	

نکته کاربردی ۴: زنجیره‌ای کردن کلید، روشی است که از چندین لایه کلید رمزنگاری استفاده می‌کند تا در نهایت داده‌های حفاظت‌شده رمز شده روی درایو را امن سازد. تعداد کلیدهای میانی متفاوت خواهد بود - از دو تا بسیار (مانند استفاده از مقدار رمزنگاری مرزی به‌عنوان کلید میانی برای پوشاندن کلید رمزنگاری داده). این موضوع برای تمام کلیدهایی که در پوشاندن نهایی یا استخراج کلید رمزنگاری داده نقش دارند، اعمال می‌شود؛ از جمله آن‌هایی که در نواحی انبارش حفاظت‌شده، قرار دارند (مانند کلیدهای ذخیره‌شده واحد سکوی امن، مقادیر مقایسه‌ای).

زمانی که نویسنده هدف امنیتی روشی را برای ایجاد زنجیره انتخاب می‌کند (چه با استخراج کلید یا عدم پوشاندن آن‌ها) الزامات مناسب را از پیوست ۲ بیرون خواهند کشید. برای یک پیاده‌سازی استفاده از هر دو روش، مجاز است. روشی که محصول برای زنجیره کردن کلیدها و مدیریت یا حفاظت آن‌ها استفاده می‌کند در شرح مدیریت کلید، توضیح داده‌شده است. برای اطلاعات بیشتر شرح مدیریت کلید را ببینید.	
اعتبارسنجی ۱	۶
توابع هدف امنیتی باید با استفاده از این روش‌ها مقدار رمزنگاری مرزی را اعتبارسنجی کند: [انتخاب: مخفی سازی کلید همان‌طور که در الزام کارکرد امنیتی عملیات کلید پوشاندن کلید ((FCS_COP.1(d)) توصیف‌شده است، چکیده‌سازی مقدار رمزنگاری مرزی همان‌طور که در [انتخاب: عملیات رمزنگاری الگوریتم چکیده‌ساز ((FCS_COP.1(b))، عملیات رمزنگاری (الگوریتم چکیده‌ساز کلیددار) ((FCS_COP.1(c))] توصیف‌شده است و مقایسه آن با یک مقدار چکیده‌سازی شده ذخیره‌شده، رمزگشایی مقدار شناخته‌شده با استفاده از مقدار رمزنگاری مرزی یا یک کلید میانی همان‌گونه که در الزام کارکرد امنیتی عملیات رمزنگاری (رمزنگاری یا رمزگشایی داده استاندارد رمزنگاری پیشرفته) ((FCS_COP.1(f)) توصیف‌شده است و مقایسه در برابر یک مقدار شناخته‌شده ذخیره‌شده]	
اعتبارسنجی ۲	۷
توابع هدف امنیتی باید [انتخاب: انجام پاک‌سازی کلید رمزنگاری داده بعد از تعداد قابل تنظیمی از تلاش‌های اعتبارسنجی ناموفق متوالی، ایجاد تأخیر به‌نحوی‌که تنها [اختصاص: تعداد تلاش‌های تعیین‌شده توسط نویسنده هدف امنیتی] می‌تواند در طی ۲۴ ساعت اتفاق بیفتد، مسدود کردن اعتبارسنجی بعد از [اختصاص: تعداد تلاش‌های تعیین‌شده توسط نویسنده هدف امنیتی] تلاش‌های اعتبار سنجی ناموفق متوالی]. **نکته کاربردی ۵:** "اعتبارسنجی" مقدار رمزنگاری مرزی می‌تواند در هر نقطه‌ای از زنجیره کلید از جمله زمانی که کلید رمزنگاری داده، رمزگشایی می‌شود، اتفاق بیفتد. برای اهداف این الزام، اعتبارسنجی کلید به‌دست‌آمده از مقدار رمزنگاری مرزی معادل با "اعتبارسنجی" مقدار رمزنگاری مرزی است. هدف انجام اعتبارسنجی امن افشا نکردن هرگونه از اجزای کلیدی است که در معرض خطر submaskها است.	

محصول، مقدار رمزنگاری مرزی را قبل از اجازه دسترسی کاربر به داده ذخیره‌شده روی درایو اعتبارسنجی می‌کند. زمانی که کلید پوشانده شده در الزام کارکرد امنیتی عملیات رمزنگاری پوشاندن کلید ((FCS_COP.1(d)) مورداستفاده قرار می‌گیرد، اعتبارسنجی طبیعتاً انجام خواهد شد. تأخیر باید توسط محصول اجرا شود، اما این الزام برای رسیدگی به حملاتی که محصول را دور می‌زنند (مانند مهاجمی که مقدار چکیده یا مقدار رمزنگاری "معلوم" را به دست می‌آورد و نیز حملات شروع‌شده از بیرون از محصول مانند شکننده‌ی کننده کلمه عبور توسط طرف سوم در نظر گرفته نشده است. توابع رمزنگاری (مانند چکیده‌ساز، رمزگشایی) انجام‌شده، در الزام کارکرد امنیتی عملیات رمزنگاری (الگوریتم چکیده‌ساز) ((FCS_COP.1(b)) و عملیات رمزنگاری (رمزنگاری/رمزگشایی داده‌های استاندارد رمزنگاری پیشرفته) (FCS_COP.1(f)) تعیین‌شده‌اند.	
عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار) ۱	۸
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.	
عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار) ۲	۹
توابع هدف امنیتی تنها از مقدار مقطعی منحصربه‌فرد با حداقل اندازه [۶۴] بیت استفاده می‌کند.	
عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار) ۳	۱۰
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 به‌طور 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 ۲^۳۲ تجاوز کند.].

نکته کاربردی ۶: این الزام تعدادی از عوامل مهم را پوشش می‌دهد-salt باید تصادفی باشد اما مقادیر مقطعی (nonceها) تنها باید یکتا باشند. الزام کارکرد امنیتی عملیات رمزنگاری (salt، مقدار مقطعی و تولید بردار اولیه) (FCS_SNI_EXT.1.3) مشخص می‌کند که برای هر مد رمزنگاری چگونه باید با بردار اولیه رفتار شود. اختصاص متوالی می‌تواند به معنای استفاده از یک شمارنده رو به بالا باشد. به‌علاوه مقدار مقطعی در ISO/IEC 19772 متغیر شروع (SV) نام دارد.

مقادیر تنظیم‌شده باید اعداد صحیح غیر منفی باشند و با یک عدد صحیح غیر منفی دلخواه شروع می‌شوند و تمام مقادیر تنظیم‌شده بعدی باید از مقدار اولیه اضافه شوند.

۶-۲- کلاس حفاظت از داده کاربر

شماره الزام	نام الزام
۱۱	**حفاظت از داده بر روی دیسک ۱**
توابع هدف امنیتی باید رمزنگاری کل درایو را مطابق با الزام کارکرد امنیتی عملیات رمزنگاری (رمزنگاری یا رمزگشایی داده استاندارد رمزنگاری پیشرفته((FCS_COP.1(f)) انجام دهد به‌گونه‌ای که درایو شامل هیچ داده محافظت‌شده خامی نباشد.	
۱۲	**حفاظت از داده بر روی دیسک ۲**
توابع هدف امنیتی باید تمام داده محافظت‌شده را بدون دخالت کاربر، رمزنگاری کند. **نکته کاربردی ۷:** هدف این الزام این است که نشان دهد، رمزنگاری هر داده محافظت‌شده وابسته به کاربری که حفاظت از داده را انتخاب می‌کند نیست. رمزنگاری درایو به‌نحوی‌که در الزام کارکرد امنیتی حفاظت از داده بر روی دیسک توسعه‌یافته (FDP_DSK_EXT.1) توصیف‌شده است، به‌طور شفاف برای کاربر انجام می‌شود و تصمیم‌گیری برای محافظت از داده، خارج از اختیار کاربر است، که این ویژگی آن را از رمزنگاری فایل متمایز می‌کند. تعریف داده‌های محافظت‌شده در واژه‌نامه وجود دارد. توابع رمزنگاری که رمزنگاری یا رمزگشایی داده را انجام می‌دهند، ممکن است توسط محیط ارائه شوند. اگر محصول توابع رمزنگاری را برای رمزنگاری یا رمزگشایی داده ارائه دهد، نویسنده هدف امنیتی از الزام کارکرد امنیتی عملیات رمزنگاری (رمزنگاری یا رمزگشایی داده استاندارد رمزنگاری پیشرفته ((FCS_COP.1(f)) FCS_COP.1(f)) از پیوست ۱ استفاده می‌کند و آن را در متن اصلی هدف امنیتی می‌گنجاند.	

۶-۳- کلاس مدیریت امنیت

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

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

]

أ. تغییر کلید رمزنگاری داده همان‌طور که در الزام کارکرد امنیتی تولید کلید رمزنگاری (کلیدهای نامتقارن) (FCS_CKM.1) توصیف شده است به هنگام آماده سازی مجدد یا زمانی که دستور داده‌شده است.

ب. پاک کردن رمزنگاری کلید رمزنگاری داده

ت. آغاز به‌روزرسانی نرم‌افزار یا سفت افزار محصول

ث. [انتخاب: هیچ تابع دیگری، ورود کلید رمزنگاری داده پوشانده شده، تغییر عوامل مجوز پیش‌فرض، پیکربندی قابلیت رمزنگاری، غیرفعال کردن قابلیت بازیابی کلید، به‌روزرسانی امن کلید عمومی موردنیاز برای به‌روزرسانی امن، [اختصاص: دیگر توابع مدیریتی ارائه‌شده توسط توابع هدف امنیتی]].]

نکته کاربردی ۸: هدف 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 آخر برای تعیین قابلیت‌هایی استفاده می شود 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، به‌عنوان‌مثال مقدار رمزنگاری مرزی پوشانده یا رمزنگاری خواهد شد و موتور رمزنگاری نیاز دارد تا این مقدار را رمزگشایی کند یا از حالت پوشیده خارج نماید. در مورد آخر اگر هیچ تابع مدیریت دیگری ارائه نشود (یا ادعا نشود)، آنگاه "هیچ تابع دیگری" باید انتخاب شود. عوامل مجوز پیش‌فرض، مقادیر اولیه‌ای هستند که برای به کار انداختن درایو از آن‌ها استفاده می‌شود.

برای اهداف این سند، پاک‌سازی کلید به معنای از بین بردن کلید رمزنگاری داده با استفاده از یکی از روش‌های تخریب پذیرفته‌شده، است.

۶-۴- کلاس حفاظت از توابع هدف امنیتی

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

توابع هدف امنیتی باید تنها زمانی کلیدها را در حافظه غیر فرّار ذخیره سازند که مطابق موارد مشخص‌شده در الزام کارکرد امنیتی عملیات رمزنگاری پوشاندن کلید ((FCS_COP.1(d)) پوشیده شده باشد، یا مطابق با توضیحات الزام کارکرد امنیتی عملیات رمزنگاری کلید (FCS_COP.1(g)) رمزنگاری‌شده باشند، مگر آنکه کلید از هرکدام از معیارهای زیر تبعیت کند [انتخاب:

- همان‌گونه که در الزام کارکرد امنیتی عملیات رمزنگاری زنجیره‌ای کردن کلید (FCS_KYC_EXT.2) توضیح داده‌شده است، کلید متن خام قسمتی از زنجیره کلید نباشد.
- کلید متن خام دسترسی به داده‌های رمزنگاری‌شده را بعد از آماده‌سازی اولیه، امکان‌پذیر نخواهد ساخت.
- کلید متن خام یک انشعاب کلید است که مطابق شرح الزام کارکرد امنیتی عملیات رمزنگاری ترکیب (FCS_SMC_EXT.1) Sabmask ترکیب می‌شود و نیمی دیگر از انشعاب کلید [انتخاب: یا در حالت مخفی قرار دارند مطابق شرح الزام کارکرد امنیتی عملیات رمزنگاری پوشاندن کلید ((FCS_COP.1(d)) یا رمزنگاری‌شده‌اند مطابق شرح الزام کارکرد امنیتی عملیات رمزنگاری کلید (FCS_COP.1(g)) یا استخراج‌شده و در حافظه غیر فرار ذخیره نمی‌شوند]
- کلید متن خام در یک افزاره انبارش بیرونی برای استفاده به‌عنوان عامل مجاز ذخیره می‌شود.
- کلید متن خام برای [انتخاب: پوشاندن کلید مطابق توصیفات الزام کارکرد امنیتی عملیات رمزنگاری پوشاندن کلید ((FCS_COP.1(d)) یا رمزنگاری آن مطابق شرح الزام کارکرد امنیتی عملیات رمزنگاری کلید (FCS_COP.1(g)) که هم‌اکنون [انتخاب: مطابق شرح الزام کارکرد امنیتی عملیات رمزنگاری پوشاندن کلید ((FCS_COP.1(d)) مخفی‌شده است، مطابق شرح الزام کارکرد امنیتی عملیات رمزنگاری کلید (FCS_COP.1(g)) رمزنگاری‌شده است]]، استفاده می‌شود.

نکته کاربردی ۹: انبارش کلید متن خام در حافظه غیر فرّار به چند دلیل مجاز است. اگر کلیدهای موجود در حافظه حفاظت‌شده قابل‌دسترسی برای کاربر در محصول یا محیط عملیاتی نباشند، تنها روش‌هایی که اجازه می‌دهند، نقش امنیتی مربوطه را برای محافظت از مقدار رمزنگاری مرزی یا کلید رمزنگاری داده ایفا کنند، این است که یک انشعاب کلید یا لایه‌های افزوده‌های ارائه‌دهنده مخفی سازی یا رمزنگاری کلید که محافظت‌شده‌اند وجود داشته باشد.

کلید رمزنگاری داده زمانی که در حافظه غیر فرّار ذخیره می‌شود (حتی در حافظه محافظت‌شده) همیشه رمزنگاری می‌شود (مخفی می‌شود) و تنها زمانی که برای رمزنگاری یا رمزگشایی داده از آن استفاده می شود به صورت متن خام در حافظه فرّار وجود دارد. کلیدهای تهیه شده ممکن است قبل از ارائه به مالک درایو، به صورت متن خام در حافظه غیر فرّار وجود داشته باشد. اگر محصول کلیدها را در حافظه غیر فرّار ذخیره نکند، تنها چیزی که موردنیاز است بیانیه‌ای در خلاصه مشخصه محصول است که بیان کند کلیدها هرگز در حافظه غیر فرّار نگهداری نمی‌شوند و نیاز به انجام هیچ‌گونه اقدام ارزیابی نیست. این الزام کلیدهای مربوط به رمزنگاری داده کاربر، به‌ویژه کلیدهای در ارتباط با زنجیره کلید، را موردتوجه قرار می‌دهد.	
۱۵	**به‌روزرسانی امن ۱**
توابع هدف امنیتی باید برای کاربران مجاز توانایی پرس‌وجوی نسخه فعلی نرم‌افزار یا سفت افزار محصول را ارائه دهد.	
۱۶	**به‌روزرسانی امن ۲**
توابع هدف امنیتی باید برای کاربران مجاز توانایی آغاز به‌روزرسانی نرم‌افزار یا سفت افزار محصول را ارائه دهد.	
۱۷	**به‌روزرسانی امن ۳**
توابع هدف امنیتی باید به‌روزرسانی‌های سفت افزار یا نرم‌افزار محصول را با استفاده از امضای دیجیتال سازنده قبل از نصب آن به‌روزرسانی‌ها، بررسی کند. **نکته کاربردی ۱۰:** 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.	
۱۸	**توابع هدف امنیتی ۱**
توابع هدف امنیتی باید مجموعه‌ای از خودآزمایی‌های زیر را اجرا کند [انتخاب: در طول راه‌اندازی اولیه (روشن شدن)، قبل از اینکه تابع برای اولین بار فراخوانی شود] تا عملکرد صحیح توابع هدف امنیتی را نشان دهد.	

نکته کاربردی ۱۱: آزمون‌های مربوط به توابع رمزنگاری پیاده‌سازی شده در محصول می‌تواند آن‌قدر به تعویق بیفتد تا اینکه آزمون‌ها قبل از اینکه تابع فراخوانی شود، انجام شود.

اگر الزام کارکرد امنیتی 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 را شرح دهد.

اگر هرگونه توابع FCS_COP توسط محصول اجرا شود، خلاصه مشخصات محصول باید خودآزمایی‌های 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 به‌وسیله آن این توابع مورد آزمون قرار می‌گیرند را توضیح دهد. خلاصه مشخصات محصول، برای هرکدام از این توابع، روشی که توسط آن عملکرد صحیح تابع یا مؤلفه بررسی‌شده است را شرح خواهد داد. ارزیاب باید تعیین نماید که تمام توابع یا مؤلفه‌های شناسایی‌شده در ابتدای راه‌اندازی مورد آزمون قرارگرفته‌اند.

۷- الزامات تضمین امنیت

این پروفایل حفاظتی مشترک الزامات تضمین امنیتی[۲۰] (SAR) را شناسایی می‌کند تا میزانی که ارزیاب مستندات را برای ارزیابی کاربردپذیر تعیین می‌کند و آزمون‌های مستقل را انجام می‌دهد بیان کند.

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

[۲۰] Security Assurance Requirements

این بخش، مجموعه‌ای از الزامات تضمین امنیت از معیار مشترک قسمت ۴ را فهرست می‌کند که برای ارزیابی بر اساس این پروفایل حفاظتی مشترک موردنیاز است. اقدامات ارزیابی منحصربه‌فردی که باید انجام شود، در سند پشتیبانی‌کننده (سند فنی الزامی) رمزنگاری کل درایو: موتور رمزنگاری ژانویه ۲۰۱۵، توضیح داده‌شده است

مدل کلی ارزیابی اهداف ارزیابی بر اساس اهداف امنیتی نوشته‌شده‌اند 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[۲۱] (ITSEF)، محصول، فناوری اطلاعات محیطی پشتیبانی‌کننده (اگر نیاز باشد)، و راهنمایی کاربر یا مدیر سیستم برای محصول را به دست خواهد آورد. از افزارگان ارزیابی امنیت فناوری اطلاعات انتظار می‌رود تا اقدامات الزامی شده توسط متدولوژی ارزیابی مشترک[۲۲] (CEM) را برای الزامات تضمین امنیت پشتیبانی چرخه حیات[۲۳] (ALC) و ارزیابی هدف امنیتی[۲۴] (ASE) اعمال کند. همچنین افزارگان ارزیابی امنیت فناوری اطلاعات، اقدامات ارزیابی همراه با اسناد پشتیبانی که قبلاً به‌عنوان تفسیری از دیگر الزامات تضمین متدولوژی ارزیابی مشترک در نظر گرفته‌شده است، را انجام می‌دهد و برای فنّاوری خاص معرفی‌شده در محصول به‌کاربرده می‌شود. اقدامات ارزیابی که توسط اسناد پشتیبانی اتخاذشده است، به روشی مشخص مواردی که توسعه‌دهنده برای ارائه اثبات انطباق محصول با این پروفایل حفاظتی مشترک نیاز دارد را ارائه می‌دهد.

جدول ۲: 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

[۲۱] IT Security Evaluation Facility

[۲۲] Common Evaluation Methodology

[۲۳] Life cycle support

[۲۴] Security Target Evaluation

	ASE_OBJ.1	اهداف امنیتی برای محیط عملیاتی
	ASE_REQ.2	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) تعریف‌شده در متدولوژی ارزیابی مشترک، ارزیابی می‌شود. علاوه بر این، ممکن است اقدامات ارزیابی مشخص‌شده در اسناد پشتیبانی که توضیحات ضروری را برای گنجاندن در خلاصه مشخصه محصول (TSS) که خاص نوع فناوری محصول است فراخوانی کند.

الزامات کارکرد امنیتی در این پروفایل مشترک، به پیاده‌سازی‌های منطبق اجازه ادغام طیف گسترده‌ای از رویکردهای مدیریت کلید قابل‌قبول 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 توسعه‌دهنده شرح مفصلی از پیاده‌سازی

مدیریت کلید خود را ارائه دهد. این اطلاعات می‌تواند به‌عنوان پیوست هدف امنیتی ارسال شود و ازآنجاکه انتظار نمی‌رود چنین سطحی از جزئیات در دسترس عموم قرار بگیرد به‌صورت اختصاصی مشخص می‌شود. در پیوست ۵ جزئیات مورد انتظار از توصیف مدیریت کلید توسعه‌دهنده 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.

نام خانواده	عنصر امنیتی
خلاصه مشخصه هدف ارزیابی **(ASE_TSS)**	**نام عنصر: پالایش خلاصه مشخصه محصول ۱** **شماره مؤلفه: ASE_TSS.1.1C** **شرح مؤلفه:** 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[۲۵] آنتروپی، هیچ‌کدام از مستندات اختصاصی مشخص‌شده پروفایل حفاظتی مشترک].

۷-۲- توسعه (ADV)

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

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

[۲۵] Essay

مشخصات کارکردی، واسطهای توابع هدف امنیتی را توصیف می‌کند (TSFIها). توضیحات کامل و رسمی این واسطها موردنیاز نیست. به‌علاوه، به دلیل اینکه اهداف ارزیابی مطابق با این پروفایل حفاظتی مشترک با محیط عملیاتی واسطهایی دارند که به‌طور مستقیم توسط کاربران محصول درخواست نمی‌شود، توضیح کمی از این واسطها داده خواهد شد مگر زمانی که آزمون غیرمستقیم این واسطها ممکن باشد. برای این پروفایل حفاظتی مشترک، اقدامات ارزیابی برای این خانواده، بر روی فهم واسطهای ارائه‌شده در خلاصه مشخصه محصول در پاسخ به الزامات کارکردی و واسطهای ارائه‌شده در اسناد راهنما تمرکز دارد. هیچ سند اضافه‌ای از "مشخصات کارکردی" برای برآوردن اقدامات ارزیابی مشخص‌شده در اسناد پشتیبانی لازم نیست.

اقدامات ارزیابی در اسناد پشتیبانی با الزامات کارکرد امنیت کاربردپذیر مرتبط هستند؛ ازآنجایی‌که این اقدامات مستقیماً با الزامات کارکرد امنیتی در ارتباط هستند، ردگیری عنصر ADV_FSP.1.2D در حال حاضر به‌طور ضمنی انجام‌شده و هیچ سند اضافه‌ای لازم نیست.

۷-۳- مستندات راهنما (AGD)

مستندات راهنما که به همراه هدف امنیتی ارائه خواهد شد باید شامل شرحی از نحوه بررسی کارکنان IT در ارتباط با ایفای نقش محیط عملیاتی برای کارکردهای امنیتی باشد. مستندات باید در یک سبک غیررسمی و قابل‌خواندن توسط کارکنان IT ارائه شود.

همان‌گونه که در هدف امنیتی ادعاشده است این راهنمایی‌ها باید برای هر محیط عملیاتی که محصول از آن پشتیبانی می‌کند، ارائه شود. برای محصولات سخت‌افزاری، توسعه‌دهنده ممکن است از تمام سکوهایی که ادغام کننده[۲۶] برای تحویل محصول انتخاب می‌کند، آگاه نباشد. شرحی از دستوراتی که ادغام کننده نیاز دارد تا برای پیکربندی صحیح محصول آن‌ها را صادر کند (مانند برآورده ساختن الزامات کارکرد امنیتی در هدف امنیتی) هدف "هر محیط عملیاتی که محصول پشتیبانی می‌کند " را برآورده خواهد ساخت. این راهنمایی شامل:

- دستورالعمل‌هایی برای نصب موفقیت‌آمیز توابع هدف امنیتی (TSF) در آن محیط؛ و

[۲۶] integrator

- دستورالعمل‌هایی برای مدیریت امنیت توابع هدف امنیتی (TSF) به‌عنوان یک محصول و یک مؤلفه از محیط عملیاتی بزرگ‌تر؛ و
- دستورالعمل‌هایی برای فراهم کردن قابلیت‌های اجرایی محافظت‌شده.

همچنین باید راهنمایی‌های مربوط به کارکردهای امنیتی خاصی ارائه شود؛ الزامات چنین راهنمایی‌هایی در اقدامات ارزیابی مشخص‌شده 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، مدیران سیستم 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 راهنمایی بررسی‌شده توسط ارزیاب را معین کند. این کار اطلاعات ضروری برای آماده‌سازی راهنمای قابل‌قبول را ارائه می‌دهد.

۷-۳-۲- راهنمای آماده‌سازی (AGD_PRE.1)

با راهنمای عملیاتی، توسعه‌دهنده باید به دنبال اقدامات ارزیابی باشد تا محتوای موردنیاز را با توجه به روش‌های مقدماتی مشخص کند.

۷-۴- کلاس پشتیبانی چرخه حیات (ALC)

در سطح اطمینان فراهم‌شده برای اهداف ارزیابی منطبق بر این پروفایل حفاظتی مشترک، پشتیبانی چرخه حیات، به‌جای آزمایش توسعه مربوط به فروشنده محصول و فرایند مدیریت پیکربندی، به جوانب قابل‌مشاهده کاربر نهایی از چرخه حیات محدود می‌شود. این به معنای تضعیف نقش حیاتی که توسعه‌دهنده در کمک به امن بودن کلی محصول انجام می‌دهد، نیست؛ 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، استفاده می‌شود به‌طوری‌که بتوان آن را از دیگر محصولات یا نسخه‌های همان فروشنده متمایز کرد و زمانی که توسط کاربر نهایی تهیه می‌شود، بتواند به‌آسانی مشخص شود. برچسب می‌تواند شامل "برچسب سخت‌افزاری" باشد (به‌عنوان‌مثال مهر روی فلز، برچسب کاغذی) یا یک "برچسب نرم افزاری" باشد (مثلاً به‌صورت الکترونیکی زمانی که درخواست شود، ارائه می‌شود). ارزیاب، واحدهای کار متدولوژی ارزیابی مشترک مرتبط با برچسب‌گذاری محصول (ALC_CMC.1) را انجام می‌دهد.

۷-۴-۲- پوشش مدیریت 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 پوشش مدیریت پیکربندی محصول (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 مشخص‌شده است. اولی از طریق خانواده آزمون مستقل-انطباق (ATE_IND) و دومی از طریق خانواده ارزیابی آسیب‌پذیری (AVA_VAN) انجام‌شده است. برای این پروفایل حفاظتی مشترک، آزمودن بر اساس قابلیت‌های کارکردی اعلام‌شده و واسط‌هایی همراه با وابستگی به در دسترس بودن اطلاعات طراحی، است. یکی از خروجی‌های اصلی فرایند ارزیابی، همان‌گونه که در الزامات زیر مشخص‌شده است. گزارش آزمون است.

۷-۵-۱-آزمون مستقل- انطباق (ATE_IND.1)

آزمودن برای تأیید قابلیت کارکردی توصیف‌شده در خلاصه مشخصه محصول و نیز راهنمای عملیاتی (شامل دستورالعمل‌های "پیکربندی ارزیابی‌شده") انجام‌شده است. تمرکز این آزمون تأیید برآورده شدن الزاماتی است که در بخش ۵ مشخص‌شده‌اند. 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 سکوی محصول است که ادعای انطباق با این پروفایل حفاظتی مشترک را دارند.

۷-۶- کلاس ارزیابی آسیب‌پذیری (AVA)

برای گسترش مقدماتی این پروفایل حفاظتی مشترک، انتظار می‌رود که انجمن فنی بین‌المللی (iTC) به بررسی منابع باز بپردازد تا آسیب‌پذیری‌های کشف‌شده برای این نوع از محصولات را کشف کند و آن را برای محتوای مبحث ارزیابی آسیب‌پذیری (AVA_VAN) فراهم سازد. در اکثر موارد، این آسیب‌پذیری‌ها به مهارتی فراتر از مهاجم ابتدایی نیاز دارند. این اطلاعات در توسعه پروفایل‌های حفاظتی آینده، استفاده خواهند شد.

۷-۶-۱-بررسی آسیب‌پذیری (AVA_VAN.1)

پیوست ۱ به همراه سند پشتیبانی‌کننده، 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 مشخص‌شده‌اند.

اولین نوع (در این پیوست) الزاماتی است که می‌تواند در هدف امنیتی وجود داشته باشد اما به‌منظور 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 است: اگر انتخاب معینی انجام شود، آنگاه الزامات اضافه‌ای در آن پیوست نیاز است تا در بدنه هدف امنیتی قرار بگیرد (مانند پروتکل‌های رمزنگاری انتخاب‌شده در الزامات کانال امن).

بعضی از الزامات در این بخش تکرار شده‌اند، اما ازآنجاکه نویسنده هدف امنیتی در برابر ترکیب الزامات مناسب از ضمایم به بدنه هدف امنیتی آن‌ها، مسئول است، تعداد تکرار صحیح به نویسنده هدف امنیتی واگذار می‌شود.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۹	**استخراج کلید رمزنگاری ۱**	**FCS_KDF_EXT.1.1**
۲۰	**تولید کلید رمزنگاری (کلیدهای نامتقارن) ۱**	**FCS_CKM.1(b)**
۲۱	**تولید کلید رمزنگاری (کلیدهای متقارن) ۱**	**FCS_CKM.1(c)**
۲۲	**عملیات رمزنگاری (درستی‌سنجی امضا) ۱**	**FCS_COP.1(a)**
۲۳	**عملیات رمزنگاری (الگوریتم چکیده‌ساز) ۱**	**FCS_COP.1(b)**
۲۴	**عملیات رمزنگاری (الگوریتم چکیده‌ساز کلیددار) ۱**	**FCS_COP.1(c)**
۲۵	**عملیات رمزنگاری (انتقال کلید) ۱**	**FCS_COP.1(e)**
۲۶	**عملیات رمزنگاری (رمزنگاری یا رمزگشایی داده استاندارد رمزنگاری پیشرفته) ۱**	**FCS_COP.1(f)**
۲۷	**عملیات رمزنگاری (رمزنگاری کلیددار) ۱**	**FCS_COP.1(g)**

۲۸	ترکیب submask ۱	FCS_SMC_EXT.1.1

۱. کلاس: پشتیبانی رمزنگاری

همان‌طور که در بدنه این پروفایل حفاظتی مشترک مشخص شد، برای محصول قابل‌قبول است که یا به‌طور مستقیم کارکردهای رمزنگاری پیاده‌سازی نماید که از فرایند رمزنگاری یا رمزگشایی درایو پشتیبانی می‌کند و یا از این کارکردها در محیط عملیاتی استفاده کند (به‌عنوان‌مثال فراخوانی واسط ارائه‌دهنده رمزنگاری سیستم‌عامل؛ کتابخانه رمزنگاری طرف سوم؛ یا یک شتاب‌دهنده 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 مورداستفاده محصول باشد و توسط محیط عملیاتی فراهم‌شده باشد، آنگاه توسعه‌دهنده توابعی را در هر محیط عملیاتی شناسایی خواهد کرد که در هدف امنیتی، فهرست شده است. این شناسایی باید به‌گونه‌ای 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 اعتبار دهی هریک از محیط‌های عملیاتی فهرست شده برای محصول انجام دهد و 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
۱۹	**استخراج کلید رمزنگاری ۱**
توابع هدف امنیتی باید [انتخاب: submask تولیدشده توسط تولیدکننده اعداد تصادفی مطابق چیزی که در الزام کارکرد امنیتی عملیات رمزنگاری تولید بیت تصادفی (FCS_RBG_EXT.1) مشخص‌شده است، submask واردشده] 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 خطی دوتایی]، NIST SP 800-132] تعریف‌شده است، با استفاده از توابع چکیده‌ساز		

کلیددار توصیف‌شده در الزام کارکرد امنیتی عملیات رمزنگاری - الگوریتم چکیده‌ساز ((FCS_COP.1(c)) استخراج کند به‌نحوی‌که خروجی حداقل از نظر استحکام امنیتی (در تعداد بیت‌ها) با کلید رمزنگاری داده برابری کند. **نکته کاربردی ۱۲:** درصورتی‌که نویسنده هدف امنیتی استفاده از استخراج کلید را در روش زنجیره کلید توصیف‌شده در الزام کارکرد امنیتی عملیات رمزنگاری - استخراج کلید رمزنگاری (FCS_KYC_EXT.2) انتخاب کند، این الزام در بدنه هدف امنیتی استفاده می‌شود.	
تولید کلید رمزنگاری (کلیدهای نامتقارن) ۱	۲۰
توابع هدف امنیتی باید کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم تولید کلید رمزنگاری مشخص‌شده، 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 رمزنگاری خم بیضوی که 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 FFC (رمزنگاری رشته محدود) که از اندازه کلید رمزنگاری ۲۰۴۸ بیت یا بیشتر استفاده می‌کند و FIPS PUB 186-4، "استاندارد امضای دیجیتال (DSS)"، پیوست B.1 را برآورده می‌سازد. **نکته کاربردی ۱۳:** کلیدهای نامتقارن ممکن است برای "پوشاندن" کلید یا submask استفاده شود. این الزام کارکرد امنیتی باید توسط نویسنده هدف امنیتی هنگامی‌که انتخاب درستی در خانواده عملیات رمزنگاری (FCS_COP) صورت می‌گیرد، به‌کاربرده شود. نویسنده هدف امنیتی باید تمام طرح‌های تولید کلید را برای برقراری کلید انتخاب نماید. زمانی که تولید کلید برای برقراری کلید استفاده می‌شود، طرح‌های موجود در الزام کارکرد امنیتی برقراری کلید (FCS_CKM.2.1) و پروتکل‌های رمزنگاری انتخاب‌شده باید با انتخاب مطابقت داشته باشد. اگر محصول به‌عنوان دریافت‌کننده در طرح برقراری امضای RSA ایفای نقش نماید، نیاز نیست محصول تولید کلید RSA را پیاده‌سازی نماید.	

تولید بیت تصادفی (RBG) برای تمامی طرح‌ها (طرح‌های RSA، طرح‌های ECC و طرح‌های (FFC) نیاز دارد تا الف) مقادیر اولیه‌ای برای RSA تولید نماید ب) کلیدهای خصوصی را به‌طور مستقیم برای ECC و FFC تولید نماید. بنابراین الزام کارکرد امنیتی تولید بیت تصادفی FCS_RBG_EXT.1 به همراه الزامات کارکرد امنیتی به کار می‌روند. الگوریتم چکیده‌ساز نیز زمانی موردنیاز است که الگوریتم تولید زوج کلید بر اساس پیوست B.3.2 یا B.3.5 از FIPS 186-4 انتخاب‌شده است. در این موارد، FCS_COP.1(d) به همراه این الزام کارکرد امنیتی استفاده می‌شود.	
تولید کلید رمزنگاری (کلیدهای متقارن) ۱	۲۱
توابع هدف امنیتی باید کلیدهای رمزنگاری متقارن را با استفاده از تولیدکننده بیت به‌صورت تصادفی مطابق با توضیحات الزام کارکرد امنیتی تولید بیت تصادفی (FCS_RBG_EXT.1) و اندازه‌های کلید رمزنگاری مشخص‌شده [انتخاب:۱۲۸ بیت، ۲۵۶ بیت] تولید نماید که از [هیچ استانداردی] پیروی نمی‌کند. **نکته کاربردی ۱۴:** کلیدهای متقارن ممکن است برای تولید کلید در طول زنجیره کلید استفاده شود.	
عملیات رمزنگاری (درستی سنجی امضا) ۱	۲۲
توابع هدف امنیتی باید خدمات امضای رمزنگاری (درستی سنجی) را انجام دهند مطابق با [انتخاب: • الگوریتم امضای الکترونیکی RSA با اندازه کلید ۲۰۴۸ بیت یا بیشتر • الگوریتم امضای الکترونیکی خم بیضوی با اندازه کلید ۲۵۶ بیت یا بیشتر]. که موارد زیر را برآورده می‌سازد: [انتخاب: • FIPS PUB 186-4 "استاندارد امضای دیجیتال (DSS)". بخش ۵،۵. با استفاده از PKCS#1 v2.1 طرح‌های امضا 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 D. 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 ۱۵: نویسنده هدف امنیتی باید الگوریتم پیاده‌سازی امضای دیجیتال را انتخاب نماید. برای الگوریتم‌های انتخاب‌شده، نویسنده هدف امنیتی باید اختصاص‌ها یا انتخاب‌های مناسبی برای تعیین پارامترهایی داشته باشد که برای آن الگوریتم پیاده‌سازی می‌شوند.	
عملیات رمزنگاری (الگوریتم چکیده‌ساز) ۱	۲۳
توابع هدف امنیتی باید خدمات چکیده‌ساز رمزنگاری را مطابق با [انتخاب: SHA-256،SHA-512] که [ISO/IEC 10118-3:2004] را برآورده می‌سازد، انجام دهد. **نکته کاربردی ۱۶:** انتخاب چکیده‌ساز باید مطابق با استحکام کلی الگوریتم استفاده‌شده برای الزام کارکرد امنیتی عملیات رمزنگاری – درستی‌سنجی امضا ((FCS_COP.1(a)) 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 انتخاب‌شده، صورت می‌گیرد.	
عملیات رمزنگاری (الگوریتم چکیده‌ساز کلیددار) ۱	۲۴
توابع هدف امنیتی باید احراز هویت پیغام‌های چکیده‌ساز کلیددار را مطابق با [انتخاب: HMAC-SHA-256،HMAC-SHA-512] و اندازه‌های کلید رمزنگاری [اختصاص: اندازه کلید (برحسب بیت) استفاده‌شده در HMAC] که [ISO/IEC 9797-2:2011، بخش ۷ "الگوریتم MAC 2 "] را برآورده می‌سازد، انجام دهد. **نکته کاربردی ۱۷:** اندازه کلید [k] در اختصاص محدوده بین L1 و L2 درجایی که L2≤k≤L1 است، قرار می‌گیرد (که در ISO/IEC 10118 برای تابع چکیده‌ساز مناسب به‌عنوان‌مثال برای SHA-256، L1=512 و L2=256 تعریف‌شده است).	
پالایش عملیات رمزنگاری (انتقال کلید) ۱	۲۵
توابع هدف امنیتی باید [انتقال کلید] را مطابق با الگوریتم رمزنگاری مشخص [RSA] در مدهای [انتخاب:KTS-OAEP،KTS-KEM-KWS] و با اندازه کلید رمزنگاری [انتخاب:۲۰۴۸ بیت، ۳۰۷۲ بیت] انجام دهد که [NIST 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 الزام کارکرد امنیتی زنجیره‌ای کردن کلید (FCS_KYC_EXT.2) مشخص‌شده است، این الزام در بدنه هدف امنیتی استفاده می‌شود.	

۲۶	**عملیات رمزنگاری (رمزنگاری یا رمزگشایی داده استاندارد رمزنگاری پیشرفته) ۱**
توابع هدف امنیتی باید [رمزنگاری یا رمزگشایی داده] را مطابق با الگوریتم رمزنگاری مشخص استاندارد رمزنگاری پیشرفته استفاده‌شده در مدهای [انتخاب: زنجیره قالب‌های رمز، سبک شمارنده گالیوس، قالب رمز قابل پیچاندن بلوک XEX (XOR رمزنگاری XOR) با سرقت متن رمز (XTS)]] و با اندازه کلید رمزنگاری [انتخاب:۱۲۸ بیت، ۲۵۶ بیت] انجام دهد که [استاندارد رمزنگاری پیشرفته توصیف‌شده در ISO/IES 18033-3، [انتخاب: زنجیره قالب‌های رمز توصیف‌شده در ISO/IEC 10116، سبک شمارنده گالیوس توصیف‌شده در ISO/IEC 19772 و قالب رمز قابل پیچاندن بلوک XEX (XOR رمزنگاری XOR) با سرقت متن رمز (XTS) توصیف‌شده در IEEE 1619] را برآورده می‌سازد. **نکته کاربردی ۱۹:** این پروفایل حفاظتی مشترک اجازه رمزنگاری سخت‌افزار یا نرم‌افزار را می‌دهد. برای رمزنگاری نرم‌افزار، محصول یا سکوی میزبان، رمزنگاری یا رمزگشایی داده را فراهم می‌آورد. در رمزنگاری سخت‌افزار، رمزنگاری یا رمزگشایی با سازوکارهای مختلف می‌تواند انجام شود – سخت‌افزار اختصاصی درون یک کنترل‌کننده با هدف عمومی، دستگاه انبارش SOC یا یک پردازنده اختصاصی. اگر مد XTS انتخاب می‌شود، همان‌گونه که در IEEE 1619 توضیح داده‌شده است، استفاده از کلید رمزنگاری ۲۵۶ بیتی یا ۵۱۲ بیتی مجاز است. کلید XTS-AES به دو کلید AES با اندازه مساوی تقسیم می‌شود - به‌عنوان‌مثال، زمانی که کلید ۲۵۶ بیتی و مد XTS انتخاب‌شده باشد AES-128 برای الگوریتم زیرین استفاده می‌شود. یا زمانی که کلید ۵۱۲ بیتی و مد XTS انتخاب‌شده است، از AES-256 استفاده می‌شود. هدف این الزام توصیف حالات قابل‌قبول استاندارد رمزنگاری پیشرفته است که نویسنده هدف امنیتی ممکن است برای رمزنگاری استاندارد رمزنگاری پیشرفته مناسب روی اطلاعات درایو سخت انتخاب کند. برای انتخاب اول نویسنده هدف امنیتی باید مد یا مدهایی را مشخص نماید که با پیاده‌سازی محصول پشتیبانی می‌شود. انتخاب دوم اندازه کلیدی که باید استفاده شود را تعیین می‌کند، که با آنچه در FCS_CKM.1(۱) توصیف‌شده است، یکسان است. انتخاب سوم باید با مد یا مدهای انتخاب‌شده در انتخاب اول موافقت کند. اگر مدهای مختلف پشتیبانی می‌شود، تکرار این مؤلفه ممکن است در هدف امنیتی مشخص‌تر باشد.	
۲۷	**عملیات رمزنگاری (رمزنگاری کلید) ۱**

توابع هدف امنیتی باید رمزنگاری و رمزگشایی کلید را مطابق با الگوریتم رمزنگاری استاندارد رمزنگاری پیشرفته استفاده‌شده در حالت [انتخاب:GCM،CBC] و اندازه کلید رمزنگاری [انتخاب:۱۲۸ بیت، ۲۵۶ بیت] انجام دهد که استاندارد رمزنگاری پیشرفته توصیف‌شده در ISO/IES 18033-3، [انتخاب: CBC توصیف‌شده در ISO/IEC 10116، GCM توصیف‌شده در ISO/IEC 19772]] را رعایت می‌کند. **نکته کاربردی ۲۰:** در صورتی‌که نویسنده هدف امنیتی انتخاب کند از رمزنگاری یا رمزگشایی استاندارد رمزنگاری پیشرفته برای حفاظت از کلیدها به‌عنوان بخشی از رویکرد زنجیره‌ای کردن کلید که در FCS_KYC_EXT.1 مشخص‌شده است استفاده نماید، این الزام در بدنه هدف امنیتی استفاده می‌شود.	
ترکیب submask ۱	۲۸
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 رمزنگاری مرزی، ترکیب کند. **نکته کاربردی ۲۱:** این الزام روشی را معرفی می‌کند که یک محصول ممکن است با استفاده از XOR یا SHA-hash، submask های مختلف را با هم ترکیب کند. توابع چکیده‌ساز قابل‌قبول در FCS_COP.1(b) و FCS_COP.1(c) اتخاذشده‌اند.	

پیوست ۲ الزامات مبتنی بر انتخاب

همان‌طور که در مقدمه این پروفایل حفاظتی مشترک بیان شد، الزامات پایه (آن‌هایی که باید توسط محصول یا سکوی 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
۲۹	عملیات رمزنگاری (تولید بیت تصادفی) توسعه‌یافته ۱	FCS_RBG_EXT.1.1
۳۰	عملیات رمزنگاری (تولید بیت تصادفی) توسعه‌یافته ۲	FCS_RBG_EXT.1.2
۳۱	عملیات رمزنگاری (پوشاندن کلید) ۱	FCS_COP.1(d)

۱. کلاس: پشتیبانی رمزنگاری

شماره الزام	نام الزام
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 بر اساس ISO/IEC 18031:2011 جدول C.1 " جدول استحکام امنیتی برای توابع چکیده‌ساز" از کلیدها و مقادیر چکیده‌ساز که تولید خواهد کرد، مطابقت می‌کند، به دست می‌آورد. **نکته کاربردی ۲۲:** ISO/IEC 18031:2011 شامل روش‌های مختلفی برای تولید اعداد تصادفی است. هرکدام از این‌ها به‌نوبه خود به اصول رمزنگاری زمینه‌ای (توابع چکیده سازی، رمزها) وابسته هستند. نویسنده هدف امنیتی، تابع موردا ستفاده را انتخاب خواهد کرد و نیز ا صول رمزنگاری زمینه‌ای ا ستفاده شده در این الزام را خواهد گنجاند. درحالی‌که هرکدام از توابع چکیده ساز معرفی شده (SHA-224،SHA-256، SHA-384،SHA-524) برای Hash-DRBG یا HMAC-DRBG مجاز هستند، تنها پیاده سازی مبتنی بر ا ستاندارد رمزنگاری پیشرفته برای CTR_DRBG مجاز ا ست. جدول C.2 در ISO/IEC 18031:2011 شنا سایی‌ای از ا ستحکام 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، درحالی‌که NIST SP 800-90A الزامی نکرده است. هردو مدل قابل‌قبول هستند. در اولین انتخاب FCS_RBG_EXT.1.1، نویسنده هدف امنیتی استانداردی را انتخاب می‌کند که با آن‌ها سازگار است. اولین انتخاب در 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 به‌عنوان بخشی از تولید بیت تصادفی در نظر گرفته می‌شود و اگر تولید بیت تصادفی در محصول وجود داشته باشد، توسعه‌دهنده ملزم به ارائه توصیف آنتروپی مشخص‌شده در پیوست ۴ است. اسناد *و آزمون‌های* موردنیاز برای اقدام ارزیابی این عنصر ضرورتاً هرکدام از منابع نشان داده‌شده در FCS_RBG_EXT.1.2 را پوشش می‌دهد.	
عملیات رمزنگاری (پوشاندن کلید) ۱	۳۱

توابع هدف امنیتی باید [کلید مخفی] را مطابق با الگوریتم رمزنگاری م شخص [ا ستاندارد رمزنگاری پی شرفته] در مدهای [انتخاب: پو شاندن کلید، پو شاندن کلید با لایه گذاری، ســـبک شـــمارنده گالیوس، کد احراز اصـــالت پیام زنجیره‌ای قالب‌های رمز شـــمارگر] 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 سازد.

نکته کاربردی ۲۳: اگر نویسنده هدف امنیتی، کلید مخفی را در روش زنجیره کلید انتخاب نماید، این الزام همان‌گونه که در FCS_KYC_EXT.2 توصیف شده است در بدنه هدف امنیتی استفاده می‌شود یا به‌عنوان روشی برای پذیرفتن کلید رمزنگاری داده مخفی‌شده که در FCS_CKM.1 توصیف شده است، استفاده می‌شود. هدف این الزام، مخفی سازی کلید شامل رمزنگاری یا رمزگشایی احراز هویت شده است.

پیوست ۳ تعریف مؤلفه‌های توسعه‌یافته

این پیوست، شامل تعریف الزامات توسعه‌یافته‌ای است که در این پروفایل حفاظتی مشترک از جمله موارد موجود در پیوست‌های ۱و ۲ استفاده‌شده است.

۱. پیش‌زمینه و دامنه

این سند تعریفی برای تمام مؤلفه‌های توسعه‌یافته که در پروفایل حفاظتی مشترک رمزنگاری کل درایو – موتور رمزنگاری، استفاده‌شده است، ارائه می‌دهد. این مؤلفه‌ها در جدول زیر معرفی‌شده است:

جدول ۳ مؤلفه‌های توسعه‌یافته

نام مؤلفه	تعریف
FCS_CKM_EXT.4	تخریب اجزای کلید و کلید رمزنگاری
FCS_KYC_EXT.2	زنجیره کلید
FCS_SMV_EXT.1	اعتبارسنجی
FDP_DSK_EXT.1	توسعه‌یافته: حفاظت از داده بر روی دیسک
FPT_KYP_EXT.1	توسعه‌یافته: حفاظت از کلید و اجزای کلید
FPT_TUD_EXT.1	به‌روزرسانی امن
FCS_SMC_EXT.1	ترکیب submask
FPT_TST_EXT.1	توسعه‌یافته: آزمون توابع هدف امنیتی
FCS_SNI_EXT.1	عملیات رمزنگاری (salt، مقادیر مقطعی (nonce) و تولید بردار)
FCS_RBG_EXT.1	توسعه‌یافته: عملیات رمزنگاری (تولید بیت تصادفی)

۲. تعریف مؤلفه‌های توسعه‌یافته

۲-۱ کلاس: پشتیبانی رمزنگاری (FCS)

۲-۱-۱ مدیریت کلید رمزنگاری (FCS_CKM)

رفتار خانواده

کلیدهای رمزنگاری باید در طول چرخه حیات خود مدیریت شوند. این خانواده در نظر دارد تا از این چرخه حیات پشتیبانی کند و درنتیجه الزامات موردنیاز برای فعالیت‌های 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 شود.

مدیریت: FCS_CKM_EXT.4

هیچ‌گونه تابع مدیریتی خاصی تعریف‌نشده است.

ممیزی: FCS_CKM_EXT.4

هیچ‌گونه رویداد ممیزی پیش‌بینی‌نشده است.

شماره الزام	نام الزام
۳۲	**تخریب کلید و اجزای کلید رمزنگاری توسعه‌یافته ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد	

تخریب کلید و اجزای کلید رمزنگاری، مؤلفه‌ای توسعه‌یافته از FCS_CKM_EXT.4 است و شامل الزامات زمان تخریب کلید است. توابع هدف امنیتی باید تمام کلیدها (کلیدهای میانی، submaskها و مقدار رمزنگاری مرزی) و اجزای کلید را زمانی که دیگر به آن‌ها نیازی نیست از بین ببرد.

۲-۲-۲- استخراج کلید رمزنگاری (FCS_KDF_EXT.1)

رفتار خانواده

این خانواده مشخصاتی را فراهم می‌آورد که برای نحوه استخراج کلیدها مورداستفاده است.

استخراج کلید (FCS_KDF_EXT.1) به توابع هدف امنیتی نیاز دارد تا یک یا چندین کلید میانی را از submaskها، استخراج کند.

مدیریت: FCS_KDF_EXT.1

هیچ‌گونه تابع مدیریتی خاصی تعریف‌نشده است.

ممیزی: FCS_KDF_EXT.1

هیچ‌گونه رویداد ممیزی پیش‌بینی‌نشده است.

شماره الزام	نام الزام
۳۳	**استخراج کلید ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد	

توابع هدف امنیتی باید [انتخاب: submask تولید شده توسط تولیدکننده اعداد تصادفی را همان‌گونه که در [اختصاص: مشخصات تأیید شده تولیدکننده بیت تصادفی] توضیح داده‌شده است، submask واردشده] را برای استخراج کلیدهای میانی 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 خطی دوتایی]، NIST SP 800-132] تعریف‌شده است، با استفاده از توابع چکیده‌ساز کلیددار مشخص شده در [انتخاب: [اختصاص: توابع چکیده سازی قابل‌قبول]] بپذیرد، به‌نحوی‌که خروجی حداقل از نظر استحکام امنیتی (در تعداد بیت‌ها) با کلید رمزنگاری داده برابری کند.

۲-۱-۲ زنجیره کلید (FCS_KYC_EXT)

رفتار خانواده

این خانواده، مشخصات موردنیاز برای استفاده از لایه‌های متعدد کلیدهای رمزنگاری به‌منظور امن ساختن نهایی داده‌های محافظت‌شده رمزنگاری‌شده روی درایو، را ارائه می‌دهد.

زنجیره‌ای کردن کلید (FCS_KYC_EXT.2) به توابع هدف امنیتی جهت نگهداشت یک زنجیره کلید نیاز دارد و مشخصات آن زنجیره را مشخص می‌کند.

مدیریت: FCS_KYC_EXT.2

توابع مدیریتی خاصی شناسایی نشده است.

ممیزی: FCS_KYC_EXT.2

هیچ رویداد ممیزی پیش‌بینی‌نشده است.

شماره الزام	نام الزام
۳۴	**زنجیره کلید ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد توابع هدف امنیتی باید مقدار رمزنگاری مرزی [انتخاب: ۱۲۸ بیت، ۲۵۶ بیت] از اکتساب مجوز را بپذیرد.	
۳۵	**زنجیره کلید ۲**
توابع هدف امنیتی باید زنجیره‌ای از یک یا چند کلیدهای میانی از مقدار رمزنگاری مرزی گرفته تا کلید رمزنگاری داده را با اســـتفاده از روش‌های زیر نگهداری کند: [اختصاص: روش‌های مورداستفاده برای ایجاد کلیدهای میانی در زنجیره کلید]. **نکته کاربردی ۲۴:** زنجیره کلید روش استفاده از لایه‌های متعدد کلیدهای رمزنگاری به‌منظور امن ساختن نهایی داده محافظت شده رمز شده بر روی درایو است. تعداد کلیدهای میانی ممکن است، متفاوت باشد- از یکی (مانند استفاده از مقدار رمزنگاری مرزی به‌عنوان کلید رمزنگاری کلید (KEK)) تا بسیار. این روش به تمام کلیدهایی که در پوشاندن نهایی یا استخراج کلید رمزنگاری داده شرکت دارند، از جمله آن‌هایی که در نواحی ذخیره‌سازی حفاظت‌شده قرار دارند (مانند کلیدهای نگهداری شده در واحد سکوهای امن، مقادیر مقایسه‌ای) به‌کاربرده می‌شود.	

۳-۲-۲ اعتبارسنجی کلید (FCS_SMV_EXT)

رفتار خانواده

این خانواده روش‌هایی را معرفی می‌کند که به‌وسیله آن مقادیر رمزنگاری مرزی، قبل از استفاده از آن‌ها اعتبارسنجی می‌شوند.

اعتبارسنجی (FCS_SMV_EXT.1) به توابع هدف امنیتی نیاز دارد تا مقادیر رمزنگاری مرزی را از طریق یک یا چندین روش معرفی‌شده، اعتبارسنجی کند.

مدیریت: FCS_SMV_EXT.1

توابع مدیریتی خاصی شناسایی نشده است.

ممیزی: FCS_SMV_EXT.1

هیچ رویداد ممیزی پیش‌بینی‌نشده است.

شماره الزام	نام الزام
۳۶	**اعتبارسنجی ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ممکن است وابستگی‌هایی وجود داشته باشد که به‌عنوان روش‌های اعتبارسنجی ممکن استفاده می‌شود. توابع هدف امنیتی باید اعتبار سنجی مقدار رمزنگاری مرزی را با استفاده از روش‌های پیش رو انجام دهند: [انتخاب: مخفی سازی کلید توصیف شده در FCS_COP.1(d)، چکیده‌سازی مقدار رمزنگاری مرزی توصیف‌شده در [انتخاب: FCS_COP.1(b)، FCS_COP.1(c)] و مقایسه آن با مقدار چکیده شده ذخیره‌شده، رمزگشایی مقدار شناخته‌شده با استفاده از مقدار رمزنگاری مرزی یا کلید میانی همان‌طور که در FCS_COP.1(f) توصیف‌شده است و مقایسه آن با مقدار شناخته‌شده ذخیره‌شده].	
۳۷	**اعتبارسنجی ۲**
توابع هدف امنیتی باید [انتخاب: انجام پاک سازی کلید مربوط به کلید رمزنگاری داده بر روی تعداد قابل تنظیمی از تلاش‌های اعتبار سنجی که به‌طور متوالی با شکست مواجه شده‌اند، ایجاد تأخیری که تنها [اختصاص: تعداد تلاش‌های مشخص‌شده توسط نویسنده هدف امنیتی] می‌تواند در یک دوره ۲۴ ساعته ایجاد شود، اعتبارسنجی را بعد از [اختصاص: تعداد تلاش‌های مشخص‌شده توسط نویسنده هدف امنیتی] از تلاش‌های اعتبارسنجی که به‌طور متوالی با شکست مواجه شده‌اند] مسدود کند.	

۲-۲-۴ ترکیب Submask (FCS_SMC_EXT)

رفتار خانواده

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

ترکیب submask (FCS_SMC_EXT.1) مستلزم آن است که توابع هدف امنیتی، submask ها را در الگویی قابل پیش‌بینی، با یکدیگر ترکیب کند.

مدیریت: FCS_SMC_EXT.1

هیچ‌گونه تابع مدیریتی خاصی تعریف‌نشده است.

ممیزی: FCS_SMC_EXT.1

هیچ‌گونه رویداد ممیزی پیش‌بینی‌نشده است.

شماره الزام	نام الزام
۳۸	**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 اســـتفاده از روش [انتخاب: تابع بولی XOR، SHA-256، SHA-512] جهت تولید کلید میانی یا مقدار رمزنگاری مرزی، ترکیب کنند	

۲-۲-۵ عملیات رمزنگاری (تولید Salt، مقادیر مقطعی و بردار اولیه (FCS_SNI_EXT))

رفتار خانواده

این خانواده این اطمینان را می‌دهد که Salt ها، مقادیر مقطعی و بردارهای اولیه به‌درستی شکل گرفته‌اند.

عملیات رمزنگاری (تولید Salt، مقادیر مقطعی و بردار) (FCS_SNI_EXT.1) به تولید salt ها، مقادیر مقطعی و بردارهای اولیه نیاز دارد تا مورداستفاده مؤلفه‌های رمزنگاری محصول قرار گیرد و به شیوه‌ای خاص اعمال شود.

مدیریت: FCS_SNI_EXT.1

هیچ‌گونه تابع مدیریتی خاصی تعریف‌نشده است.

ممیزی: FCS_SNI_EXT.1

هیچ‌گونه رویداد ممیزی پیش‌بینی‌نشده است.

شماره الزام	نام الزام
۳۹	**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 FCS_RBG_EXT.1 توصیف شده است، تولید اعداد تصادفی ارائه‌شده از طریق سکوی میزبان] تولیدشده‌اند.	
۴۰	**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.	

۴۱	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 (CBC): بردارهای اولیه باید غیرتکراری باشند.

کد احراز اصالت پیام زنجیره‌ای قالب‌های رمز شمارگر (CCM): مقدار مقطعی باید غیرتکراری باشد.

XTS: بدون بردار اولیه. مقادیر تنظیم‌شده باید اعداد صحیح غیر منفی باشند که به‌طور متوالی اختصاص‌یافته و با عدد صحیح غیر منفی دلخواه شروع می‌شود.

GCM: بردار اولیه باید غیرتکراری باشند. تعداد فراخوانی‌های GCM برای کلید راز داده‌شده نباید از ۳۲^۲ تجاوز کند.].

۲-۲-۶ تولید بیت تصادفی (FCS_RBG_EXT)

رفتار خانواده

مؤلفه‌های این خانواده الزامات موردنیاز برای تولید بیت یا عدد تصادفی را موردتوجه قرار می‌دهند. این خانواده، خانواده جدیدی است که برای کلاس پشتیبانی رمزنگاری (FCS) تعریف‌شده است.

تولید بیت تصادفی توسعه‌یافته (FCS_RBG_EXT.1) مستلزم آن است که تولید بیت تصادفی مطابق با استانداردهای انتخاب‌شده توسط یک منبع آنتروپی آغاز شود.

مدیریت: FCS_RBG_EXT.1

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

هیچ‌گونه فعالیت مدیریتی پیش‌بینی‌نشده است.

ممیزی: FCS_RBG_EXT.1

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 تصادفی سازی.

شماره الزام	نام الزام
۴۲	**عملیات رمزنگاری (تولید بیت تصادفی) توسعه‌یافته 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.	
۴۳	**عملیات رمزنگاری (تولید بیت تصادفی) توسعه‌یافته 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 C.1 از ISO/IEC 18031:2011 «جدول استحکام امنیتی برای توابع چکیده‌ساز» از کلیدها و چکیده‌سازهایی که تولید خواهد شد، برابری کند، تلفیق می‌کند..	

۲-۲ کلاس حفاظت از داده کاربر (FDP)

۲-۲-۱ حفاظت از داده بر روی دیسک (FDP_DSK_EXT)

رفتار خانواده

این خانواده جهت اجباری نمودن رمزنگاری تمام داده‌های محافظت‌شده نوشته‌شده روی دیسک استفاده می‌شود.

الزام کارکرد امنیتی محافظت از داده‌های روی دیسک (FDP_DSK_EXT.1) نیاز دارد تا توابع هدف امنیتی، ترکیب و شرایط خاص عوامل مجوز را به‌گونه‌ای مناسب بپذیرد.

مدیریت: FCS_DSK_EXT.1

توابع مدیریتی خاصی شناسایی نشده است.

ممیزی: FCS_DSK_EXT.1

هیچ رویداد ممیزی پیش‌بینی‌نشده است.

شماره الزام	نام الزام
۴۴	**حفاظت از داده روی دیسک توسعه‌یافته ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد توابع هدف امنیتی باید رمزنگاری کل درایو را مطابق با FCS_COP.1(f) انجام دهد، به‌گونه‌ای که حاوی هیچ‌گونه داده محافظت‌شده متن خامی نباشد	
۴۵	**حفاظت از داده روی دیسک توسعه‌یافته ۲**
توابع هدف امنیتی باید تمام داده‌ها را بدون دخالت کاربر رمزنگاری کند.	

۲-۳ کلاس حفاظت از توابع هدف امنیتی (FPT)

۲-۳-۱ حفاظت از کلید و اجزای کلید (FPT_KYP_EXT)

رفتار خانواده

این خانواده نیاز دارد زمانی که کلید و اجزای کلید در حافظه غیر فرار نوشته‌شده‌اند از آن‌ها محافظت شود.

حفاظت از کلید و اجزای کلید (FPT_KYP_EXT.1) توسعه‌یافته مستلزم این است که توابع هدف امنیتی تضمین کند که هیچ‌گونه کلید یا اجزای کلید رمز نشده در حافظه غیر فرّار نوشته‌نشده است.

مدیریت: FPT_KYP_EXT.1

هیچ‌گونه تابع مدیریتی خاصی تعریف‌نشده است.

ممیزی: FPT_KYP_EXT.1

هیچ‌گونه رویداد ممیزی پیش‌بینی‌نشده است.

شماره الزام	نام الزام
۴۶	**حفاظت از کلید و اجزای کلید توسعه‌یافته 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 کارکرد امنیتی عملیات رمزنگاری (پوشاندن کلید) ((FCS_COP.1(d) مشخص‌شده است پوشانده شده باشند، یا مطابق الزام کارکرد امنیتی عملیات رمزنگاری – رمزنگاری کلید FCS_COP.1(g) یا الزام کارکرد امنیتی عملیات رمزنگاری – انتقال کلید ((FCS_COP.1(e) رمزنگاری‌شده باشند، مگر آنکه کلید هرکدام از معیارهای زیر را برآورده سازد [انتخاب:

- همان‌گونه که در الزام کارکرد امنیتی حفاظت از کلید و اجزای کلید (FCS_KYC_EXT.1) مشخص‌شده است، کلید متن خام بخشی از زنجیره کلید نباشد.
- کلید متن خام بعد از آماده‌سازی اولیه دیگر به داده‌های رمزنگاری‌شده دسترسی نداشته باشد.
- کلید متن خام طبق چیزی که در FCS_SMC_EXT.1 مشخص‌شده است انشعابی از کلید است که ترکیب‌شده است و نیمه دیگر از انشعاب کلید یکی از این موارد است [انتخاب: پوشانده شده مطابق چیزی که در FCS_COP.1(d) مشخص‌شده است، یا رمزنگاری‌شده است مطابق توضیحات FCS_COP.1(g) یا FCS_COP.1(e)، یا استخراج‌شده و در حافظه غیر فرّار ذخیره نشده است.]
- کلید متن خام در یک افزاره انبارش بیرونی ذخیره‌شده است تا به‌عنوان یک عامل مجوز استفاده شود.

کلید متن خام برای [انتخاب: پوشاندن یک کلید مطابق توضیحات مشخص در FCS_COP.1(d)، رمزنگاری‌شده است مطابق توضیحات FCS_COP.1(g) یا FCS_COP.1(e)] که هم‌اکنون [انتخاب: مطابق چیزی که در FCS_COP.1(d) مشخص‌شده است، پوشانده شده است، یا مطابق چیزی که در FCS_COP.1(g) یا FCS_COP.1(e)]] مشخص‌شده است رمزنگاری‌شده است] است استفاده می‌شود.

۲-۳-۲ به‌روزرسانی امن (FPT_TUD_EXT)

رفتار خانواده

مؤلفه‌های این خانواده، الزامات موردنیاز برای به‌روزرسانی میان‌افزار و یا نرم‌افزار محصول را مشخص می‌کند.

به‌روزرسانی امن (FPT_TUD_EXT.1)، به قابلیت‌هایی نیاز دارد که برای به‌روزرسانی میان‌افزار و نرم‌افزار محصول ازجمله توانایی اعتبارسنجی به‌روزرسانی‌ها قبل از نصب، ارائه شود.

مدیریت: FPT_TUD_EXT.1

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

توانایی به‌روزرسانی محصول و بررسی به‌روزرسانی‌ها

ممیزی: FPT_TUD_EXT.1

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 به‌روزرسانی

شماره الزام	نام الزام
۴۷	**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.	
۴۸	**به‌روزرسانی امن ۲**

توابع هدف امنیتی باید برای کاربران مجاز توانایی آغاز به‌روزرسانی نرم‌افزار یا میان‌افزار محصول را فراهم آورد.	
۴۹	**به‌روزرسانی امن ۳**
توابع هدف امنیتی باید به‌روزرسانی‌های میان‌افزار یا نرم‌افزار محصول را با استفاده از امضای دیجیتال سازنده قبل از نصب آن به‌روزرسانی‌ها، بررسی کند.	

۲-۳-۳ خودآزمایی توابع هدف امنیتی (FPT_TST_EXT)

رفتار خانواده

مؤلفه‌های این خانواده الزامات موردنیاز برای خود آزمایی توابع هدف امنیتی جهت عملکرد صحیح انتخاب‌شده را موردتوجه قرار می‌دهد.

آزمون توابع هدف امنیتی (FPT_TST_EXT.1) توسعه‌یافته مستلزم مجموعه‌ای از خودآزمایی‌هایی است تا در طول راه‌اندازی اولیه به‌منظور نشان دادن عملکرد صحیح توابع هدف امنیتی اجرا شوند.

مدیریت: FPT_TST_EXT.1

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

هیچ‌گونه تابع مدیریتی.

ممیزی: FPT_TST_EXT.1

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
۵۰	**آزمون توابع هدف امنیتی توسعه‌یافته ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد توابع هدف امنیتی باید مجموعه‌ای از خودآزمایی‌های 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*].	

پیوست ۴ ارزیابی و مستندات آنتروپی

این بخش یک پیوست اختیاری در پروفایل حفاظتی مشترک است و تنها زمانی اعمال می‌شود که محصول، تولیدکننده بیت تصادفی را ارائه می‌دهد.

این پیوست اطلاعات تکمیلی موردنیاز برای هر منبع آنتروپی استفاده‌شده توسط محصول را توصیف می‌کند.

مستندات منابع آنتروپی، بهتر است با جزئیات کافی ارائه شود به‌گونه‌ای که ارزیاب بعد از خواندن، منبع آنتروپی را به‌طور کامل درک کند و بفهمد که چرا می‌توان به آن جهت ارائه آنتروپی مناسب اتکا کرد. چنین مستندی باید شامل چندین بخش با جزئیات باشد: توصیف طراحی، منطق آنتروپی، شرایط عملیاتی و آزمون سلامت. نیازی نیست این سند بخشی از خلاصه مشخصات محصول در مواجهه عمومی هدف امنیتی باشد.

۱. توصیف طراحی

مستندات باید شامل طراحی هر منبع آنتروپی به‌عنوان یک کل از جمله تعامل تمام مؤلفه‌های منبع آنتروپی باشد هرگونه اطلاعاتی که در خصوص طراحی قابل اشتراک‌گذاری باشد بهتر است برای هر منبع آنتروپی طرف سوم که در محصول موجود است نیز گنجانده شود.

این سند عملیات منبع آنتروپی را شرح خواهد داد از جمله اینکه چگونه آنتروپی تولیدشده است و چگونه داده‌های فرآوری نشده (خام) برای اهداف آزمون می‌تواند از منبع آنتروپی به دست آیند. این اسناد باید در طول طراحی منبع آنتروپی حضورداشته باشند تا نشان دهد آنتروپی از کجا می‌آید، خروجی آنتروپی بعداً به کجا فرستاده خواهد شد، پردازش‌های بعدی روی خروجی‌های خام کدام است (چکیده‌ساز،XOR و ...)، آیا/کجا ذخیره می‌شود و در نهایت چگونه از منبع آنتروپی خارج می‌شود. هرگونه شرایطی که روی فرایند گذاشته‌شده است (مانند مسدود کردن) نیز در طراحی منبع آنتروپی باید توصیف شود. وجود مثال‌ها و دیاگرام‌ها نیز خوب است.

همچنین این طراحی باید شامل محتوایی در ارتباط با مرز امنیتی منبع آنتروپی و توصیفی از چگونگی تضمین مرز امنیتی از اینکه مهاجمی در خارج از مرز نمی‌تواند بر روی نرخ آنتروپی تأثیر بگذارد، باشد.

در صورت پیاده‌سازی، توصیف طراحی همچنین باید چگونگی اضافه نمودن آنتروپی به تولیدکننده بیت تصادفی توسط برنامه کاربردی طرف سوم را شرح دهد. توصیفی از هر حالت تولیدکننده بیت تصادفی ذخیره کننده بین خاموشی و روشنی نیز باید گنجانده شود.

۲. استدلال آنتروپی

باید استدلالی فنی در مورد اینکه غیرقابل پیش‌بینی بودن در منابع از کجا می‌آید و چرا به منبع آنتروپی برای تحویل آنتروپی کافی جهت استفاده از خروجی تولیدکننده بیت تصادفی (RBG) (با این محصول خاص) اعتماد می‌شود، وجود داشته باشد. این استدلال شامل توصیفی از حداقل نرخ آنتروپی مورد انتظار (به عبارت دیگر، حداقل آنتروپی (برحسب بیت) به ازای هر بیت یا بایت از داده منبع) است و توضیح می‌دهد که آنتروپی مناسب به فرایند مقداردهی اولیه (بذرپاشی) تصادفی محصول اعمال می‌شود. این بحث بخشی از استدلال برای این موضوع خواهد بود که چرا منبع آنتروپی برای تولید بیت‌ها با آنتروپی قابل‌اتکا است.

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

برای توسعه‌دهندگان ارائه‌دهنده منابع آنتروپی، به‌منظور منطق نرخ حداقل آنتروپی، انتظار می‌رود که تعداد زیادی از بیت‌های منبع خام، جمع‌آوری شود، آزمون‌های آماری انجام شود و حداقل نرخ آنتروپی از این آزمون‌های آماری تعیین شود. درحالی‌که هیچ آزمون آماری خاصی در حال حاضر موردنیاز نیست، اما انتظار می‌رود بعضی از آزمون‌ها برای تعیین مقدار حداقل آنتروپی در هریک از خروجی‌ها، انجام شود.

برای منابع آنتروپی ارائه‌شده 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 به‌دست‌آمده از این منبع طرف سوم را نشان می‌دهد. برای فروشنده قابل‌قبول است که یک مقداری از آنتروپی حداقلی را "فرض کند"، بااین‌حال، این مفروضات باید به‌وضوح در مستندات ارائه‌شده بیان شود. به‌خصوص، 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 تولیدکننده بیت تصادفی قطعی با آنتروپی بیان‌شده در هدف امنیتی مقداردهی اولیه خواهد شد، برای مثال با بررسی این موضوع که نرخ حداقل آنتروپی با مقداری از داده منبع مورداستفاده برای مقداردهی اولیه (بذرپاشی) تولیدکننده بیت تصادفی قطعی ضرب شده یا اینکه نرخ آنتروپی مورد انتظار بر اساس مقدار داده منبع به‌صورت صریح بیان‌شده و با نرخ آماری مقایسه گردیده است.

چنانچه میزان داده منبع مورداستفاده برای مقداردهی اولیه (بذرپاشی) تولیدکننده بیت تصادفی قطعی مشخص نباشد یا نرخ محاسبه‌شده به‌صراحت به نقطه آغاز مرتبط نباشد، مستندات کامل در نظر گرفته نخواهند شد.

استدلال آنتروپی نباید شامل هیچ‌گونه داده اضافه‌شده 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 سپری‌شده بعد از روشن شدن تنها تعداد محدودی از عواملی هستند که ممکن است عملیات منبع آنتروپی را تحت تأثیر قرار دهند. به‌این‌ترتیب، این سند شامل طیفی از شرایط عملیاتی است که منبع آنتروپی با توجه به این شرایط به تولید داده‌های تصادفی می‌پردازد. مشابه همین، این سند باید شرایطی را توصیف کند که مطابق با آن منبع آنتروپی بیشتر از این ارائه آنتروپی کافی را تضمین نمی‌کند. روش‌های مورداستفاده برای تشخیص شکست یا تخریب منبع نیز باید گنجانده شود.

۴. آزمون سلامت

به‌طور خاص، تمام آزمون‌های سلامت منبع آنتروپی و منطق آن‌ها باید مستند شود که شامل توصیفی از آزمون‌های سلامت، نرخ و شرایطی که با توجه به آن آزمون سلامت صورت می‌گیرد (از جمله به هنگام راه‌اندازی، برحسب تقاضا یا به‌طور مداوم) است و نتایج مورد انتظار برای هر آزمون سلامت، رفتار محصول بر اساس شکست منبع آنتروپی و منطق 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 رمزنگاری محصول باید به‌اندازه کافی با جزئیات باشد به‌گونه‌ای که ارزیاب بعد از خواندن این مستندات، مدیریت کلید محصول و چگونگی رعایت الزامات توسط آن برای اطمینان از محافظت کلید، را درک کند. این سند باید شامل نوشتارها و نمودارها باشد. نیازی نیست این سند قسمتی از خلاصه مشخصات محصول باشد - می‌تواند به‌عنوان سند جداگانه‌ای ارائه شود و مخصوص توسعه‌دهنده مشخص شود.

۱. نوشتار

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

- هدف کلید
- آیا کلید در حافظه غیر فرار ذخیره‌شده است.
- چگونه و چه زمانی کلید محافظت‌شده است.
- چگونه و چه زمانی کلید استخراج‌شده است.
- قدرت و استحکام کلید
- چه زمانی یا اگر کلید بیشتر از این موردنیاز نیست، به همراه منطق لازم

این نوشتار همچنین موضوعات زیر را توضیح می‌دهد:

- فرایند اعتبارسنجی باید توصیف شود و به مقادیر استفاده‌شده برای اعتبارسنجی و فرایند استفاده‌شده برای انجام اعتبارسنجی نیز اشاره شود. همچنین باید توضیح دهد که چگونه این فرایند تضمین می‌کند که هیچ‌کدام از کلیدها در زنجیره کلید، از طریق این فرایند تضعیف نشده یا در معرض خطر قرار نمی‌گیرند. همچنین روشی را توضیح دهد که از طریق آن، تعداد شکست‌های متوالی تلاش‌های مجوز دهی را محدود می‌کند.

- فرایند مجوز که نهایتاً کلید رمزنگاری داده را منتشر می‌کند. این بخش باید زنجیره کلید استفاده‌شده توسط محصول را با جزئیات بیان کند. همچنین این بخش باید مشخص کند کدام‌یک از کلیدها برای محافظت از کلید رمزنگاری داده استفاده‌شده و چگونه فرایند استخراج یا مخفی ساختن کلید را انجام می‌دهند. 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 به‌روشنی سلسله‌مراتب کلیدها را نشان دهند تا تضمین کند که در هیچ نقطه‌ای، زنجیره بدون استفاده از رمزنگاری شکسته نخواهد شد یا دانش مقدار رمزنگاری مرزی و استحکام اثربخش کلید رمزنگاری داده در طول زنجیره کلید حفظ خواهد شد.
- توصیفی از موتور رمزنگاری 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 رمزنگاری یا رمزگشایی و نواحی‌ای که رمزنگاری نشده‌اند (مانند بارگذارکننده راه‌انداز، بخش مرتبط با رکورد اصلی راه‌انداز (MBR)، جداول افراز شده و ...)). این توضیحات باید شامل جریان داده از رابط میزبان افزاره به رسانه ماندگار افزاره انبارش داده، اطلاعاتی راجع به شرایطی که داده، موتور رمزگذاری داده را دور می‌زند (مانند عملیات خواندن یا نوشتن بر روی ناحیه رکورد اصلی راه‌انداز رمزنگاری نشده) باشد. این توضیحات باید به‌اندازه کافی با جزئیات بیان شوند تا تمام سکوها را بررسی کنند و مطمئن شوند که زمانی که کاربر رمزنگاری را فعال می‌کند، محصول، تمام افزاره‌های انبارش سخت را رمز می‌کند. همچنین باید شروع راه‌اندازی سکوی، فرایند آغاز رمزنگاری و اینکه در چه زمانی محصول رمزنگاری را فعال می‌کند، را نیز توضیح دهد.
- فرایند تخریب کلید زمانی که دیگر به آن‌ها نیازی نیست از طریق مشخص کردن محل انبارش تمام کلیدها و روش تخریب برای آن انباره، باید مشخص شود.

۲. نمودار

- نمودار شامل تمام کلیدها از مقدار رمزنگاری مرزی تا کلید رمزنگاری داده و هرگونه کلید یا مقداری که در زنجیره مشارکت دارند، خواهد بود. همچنین باید استحکام رمزنگاری هریک از کلیدها را فهرست کند و نشان دهد که چگونه هر کلید در طول زنجیره با استخراج کلید یا مخفی سازی کلید (از گزینه‌های مجاز) محافظت می‌شود. نمودار، ورودی استفاده‌شده برای استخراج یا عدم مخفی سازی هریک از کلیدها در زنجیره را نیز نشان خواهد داد.
- یک نمودار (بلوک) عملیاتی، نشان‌دهنده مؤلفه‌های اصلی (مانند حافظه‌ها و پردازنده‌ها) و مسیر داده میان آن‌ها، برای سخت‌افزار، رابط میزبان دستگاه و رسانه پایای افزاره انبارش داده، یا برای نرم‌افزار، گام‌های اولیه موردنیاز برای فعالیت‌هایی است که محصول انجام می‌دهد تا اطمینان حاصل کند زمانی که مدیر سیستم یا کاربر برای اولین بار محصول را آماده می‌کند، به‌طور کامل افزاره انبارش را رمز می‌کند. نمودار رمزنگاری سخت‌افزار باید مکان موتور رمزنگاری داده به همراه مسیر داده را نشان دهد.
- نمودار رمزنگاری سخت‌افزار باید مکان موتور رمزنگاری داده به همراه مسیر داده را نشان دهد.

ارزیاب باید بررسی کند که نمودار رمزنگاری سخت‌افزار، شامل جزئیاتی باشد که مؤلفه‌های اصلی به همراه مسیر داده را نشان دهد و به‌وضوح موتور رمزنگاری داده را تعیین می‌کند.

پیوست ۶ واژگان اختصاری

واژه اختصاری	معنای انگلیسی	ترجمه فارسی
AA	Authorization Acquisition	اکتساب مجوز
AES	Advanced Encryption Standard	استاندارد رمزنگاری پیشرفته
BEV	Border Encryption Value	مقدار رمزنگاری 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	متدولوژی ارزیابی مشترک
CPP	Collaborative Protection Profile	پروفایل حفاظتی مشترک
DEK	Data Encryption Key	کلید رمزنگاری داده
DRBG	Deterministic Random Bit Generator	تولیدکننده بیت تصادفی قطعی
DSS	Digital Signature Standard	استاندارد امضای دیجیتال
ECC	Elliptic Curve Cryptography	رمزنگاری منحنی بیضی
ECDSA	Elliptic Curve Digital Signature Algorithm	الگوریتم امضای دیجیتال منحنی بیضوی
EE	Encryption Engine	موتور رمزنگاری
EEPROM	Electrically Erasable Programmable Read-Only Memory:	حافظه فقط خواندنی قابل‌برنامه‌ریزی و پاک شدن به‌صورت الکترونیکی
FIPS	Federal Information Processing Standards	استانداردهای پردازش اطلاعات فدرال

واژه اختصاری	معنای انگلیسی	ترجمه فارسی
FDE	Full Drive Encryption	رمزنگاری کل درایو
FFC	Finite Field Cryptography	رمزنگاری رشته محدود
GCM	Galois Counter Mode	سبک شمارنده گالیوس
KHMAC	Keyed-Hash Message Authentication Code	کد احراز هویت پیام چکیده‌ساز کلیددار
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
iTC	International Technical Community	انجمن فنی بین‌المللی
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 رمزنگاری 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 لایه گذاری
MBR	Master Boot Record	رکورد راه‌انداز اصلی
NIST	National Institute of Standards and Technology	مؤسسه ملی استاندارد و فناوری

واژه اختصاری	معنای انگلیسی	ترجمه فارسی
OS	Operating System	سیستم‌عامل
PBKDF	Password-Based Key Derivation Function	تابع استخراج کلید مبتنی بر کلمه عبور
PRF	Pseudo Random Function	تابع شبه تصادفی
RBG	Random Bit Generator	تولیدکننده بیت تصادفی
RNG	Random Number Generator	تولیدکننده عدد تصادفی
RSA	Rivest Shamir Adleman Algorithm	الگوریتم آدلمن شامیر ریوست
SAR	Security Assurance Requirement	الزامات تضمین امنیت
SED	Self Encrypting Drive	درایو خود رمزنگار
SHA	Secure Hash Algorithm	الگوریتم چکیده‌ساز امن
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 سکوی امن
TSF	TOE Security Functionality	تابع هدف امنیتی
TSS	TOE Summary Specification	خلاصه مشخصه محصول
USB	Universal Serial Bus	گذرگاه جهانی سریال

واژه اختصاری	معنای انگلیسی	ترجمه فارسی
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 رمزنگاری 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