به نام خدا

پروفایل حفاظتی
برنامه کاربردی

مهرماه ۹۵

نسخه ۱/۰

فهرست

۱ مقدمه ۵

۲ اصطلاحات ۵

۳ شرح محصول ۱۰

۴ مسائل امنیتی ۱۴

۴,۱ تهدیدات ۱۴

۴,۲ فرضیات ۱۵

۴,۳ خطمش‌های امنیتی سازمانی ۱۵

۵ اهداف امنیتی ۱۶

۵,۱ اهداف امنیتی برای محصول ۱۶

۵,۲ اهداف امنیتی برای محیط عملیاتی ۱۸

۶ الزامات کارکرد امنیتی ۱۸

۶,۱ کلاس پشتیبانی از رمزنگاری ۲۲

۶,۲ کلاس حفاظت از داده‌ها ۲۳

۶,۳ کلاس محرمانگی ۲۷

۶,۴ کلاس مدیریت امنیت ۲۷

۶,۵ کلاس حفاظت از محصول ۲۹

۶,۶ کلاس کانال‌ها و مسیرهای مورد اعتماد ۳۴

۷ الزامات تضمین امنیت ۳۵
۷,۱ کلاس توسعه ۳۸
۷,۲ کلاس راهنمای کاربر ۴۰
۷,۲,۱ راهنمای کاربردی ۴۰
۷,۲,۲ راهنمای آمادهسازی ۴۲
۷,۳ کلاس آزمون ۴۲
۷,۳,۱ آزمون مستقل ۴۳
۷,۴ کلاس آسیب‌پذیری ۴۴
۷,۴,۱ تحلیل آسیب‌پذیری ۴۴
۷,۵ کلاس پشتیبانی از چرخه حیات ۴۴
۷,۵,۱ قابلیتهای پیکربندی ۴۵
۷,۵,۲ حوزه پیکربندی ۴۵
۸ پیوست یک: الزامات اختیاری ۴۶
۹ پیوست دوم: الزامات بر اساس انتخاب ۴۷
۱۰ پیوست سوم: الزامات اضافی ۶۱

۱ مقدمه

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی که در این سند برای برآورده نمودن الزامات ارائه‌شده‌اند را در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد نمود. مرکز افتا با مشارکت سازمان فناوری اطلاعات این سند را در راستای این هدف تهیه نموده است. این پروفایل حفاظتی، به بیان الزامات برنامه کاربردی می‌پردازد. این سند بر اساس سند نظام[۱] ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 تهیه گردیده است.

۲ اصطلاحات

استاندارد ارزیابی معیار مشترک (CC): استاندارد ارزیابی معیار مشترک برای ارزیابی امنیت فناوری‌های اطلاعات.

متدلوژی ارزیابی معیار مشترک[۲] (CEM): متدلوژی ارزیابی معیار مشترک برای ارزیابی امنیت فناوری‌های اطلاعات.

محیط عملیاتی (Operational Environment): محیطی که محصول در آن عمل می‌کند.

پروفایل حفاظتی (PP[۳]): مجموعه‌ای از الزامات امنیتی برای دسته‌ای از محصولات؛ مجموعه‌ای که مستقل از پیاده‌سازی است.

هدف امنیتی (ST[۴]): مجموعه‌ای از الزامات امنیتی برای یک محصول خاص؛ مجموعه‌ای که وابسته به پیاده‌سازی است.

بسته (Package): نام مجموعه‌ای از الزامات کارکرد امنیتی یا تضمین امنیتی است. به‌عنوان مثال EAL3.

سطح تضمین ارزیابی (EAL[۵]): مجموعه‌ای از الزامات تضمین که از قسمت سوم از سندهای سه‌گانه «استاندارد ارزیابی معیار مشترک» برگرفته‌شده است و نشان‌دهنده سطح امنیتی محصول است. سطوح تضمین از سطح ۱ تا سطح ۷ می‌باشند، لازم به ذکر است که «سطح تضمین امنیتی» یک نوع «بسته» است.

---

[۲] Common Evaluation Methodology(CEM)

[۳] Protection Profile

[۴] Security Target

[۵] Evaluation Assurance Level

خلاصه مشخصه محصول[۱] **(TSS)**: شرحی از این‌که یک محصول چگونه الزامات کارکرد امنیتی را در یک هدف امنیتی برآورده می‌سازد.

داده کاربری (User data): داده‌های کاربری هستند که کارکرد امنیتی محصول را تحت تأثیر قرار نمی‌دهند. این داده‌ها اطلاعاتی ذخیره‌شده در منابع محصول هستند که توسط کاربران مطابق با الزامات کارکرد امنیتی به‌کاربرده می‌شود. محتویات یک پیام الکترونیک نوعی داده کاربری است.

سرپرست (Administrator): موجودیتی که مسئولیت مدیریت و اعمال خط‌مشی‌ها را بر روی محصول بر عهده دارد و معمولاً دارای بالاترین سطح مجوز است.

موجودیت فعال (Subject): موجودیت فعال، موجودیتی در محصول است که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون سرپرست، کاربر نهایی و غیره؛ به عبارت دیگر موجودیت فعال عامل انجام عملی بر روی محصول است.

موجودیت غیرفعال (Object): موجودیت غیرفعال، موجودیتی در سیستم مورد ارزیابی (محصول) است که شامل اطلاعات است و یا اطلاعات را دریافت می‌نماید و روی آن توسط موجودیت‌های فعال، عملیاتی انجام می‌گیرد. همانند داده‌ها و اطلاعاتی همچون متن‌های رمز شده و کلیدها و غیره؛ به عبارت دیگر موجودیتی است که توسط موجودیت فعال بر روی آن رخدادی اتفاق می‌افتد، مانند لیست کردن رکوردها توسط سرپرست، حذف فایل‌ها توسط حمله‌کننده که در این دو مثال رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.

راز (Secret): اطلاعاتی که باید تنها به کاربران مجاز و/یا محصول شناسانده شود تا یک «خط‌مشی کارکرد امنیتی» اجرا گردد.

مشخصه امنیتی (Security attribute): کاربران، موجودیت‌های فعال، اطلاعات، موجودیت‌های غیرفعال، نشست‌ها و منابع تحت کنترل قوانین «الزامات کارکرد امنیتی» ممکن است دارای اطلاعات خاصی باشند که جهت کارکرد صحیح محصول، مورداستفاده قرار گیرند. دسته‌ای از این اطلاعات حالت آگاهی‌دهنده دارند همچون نام فایل که ممکن است برای معرفی منابع منحصربه‌فرد استفاده شود، اما دسته‌ی دیگر از این اطلاعات ممکن است به‌طور خاص برای اجراشدن الزامات کارکرد امنیتی وجود داشته باشند، همانند اطلاعات کنترل دسترسی، این دسته از اطلاعات به‌طورکلی «مشخصه امنیتی» نامیده می‌شود.

خط‌مشی کارکرد امنیتی (SFP[۲]): رفتار امنیتی که توسط «کارکرد امنیتی محصول» اجرا می‌گردد تحت مجموعه قوانینی در «الزامات کارکرد امنیتی» بیان می‌شوند، این مجموعه قوانین «خط‌مشی کارکرد امنیتی» نامیده می‌شوند. «الزامات کارکرد امنیتی» ممکن است چندین خط‌مشی جهت معرفی قوانینی

---

۱ TOE Summary Specification (TSS)

۲ Security Functionality Policy

که محصول باید اجرا نماید، تعریف کند. هرکدام از خط‌مشی‌ها باید حوزه کنترلی‌اش را توسط موجودیت‌های فعال، موجودیت‌های غیرفعال، منابع یا اطلاعات و عملکردهایی که بکار برده است، مشخص نماید. تمام این خط‌مشی‌ها توسط «محصول» پیاده‌سازی می‌شوند.

خط‌مشی کارکرد امنیتی کنترل دسترسی (Access control SFP): چندین خط‌مشی کارکرد امنیتی وجود دارد که برای حفاظت از داده‌ها بکار برده می‌شوند، همچون «خط‌مشی کنترل دسترسی» و «خط‌مشی کنترل جریان اطلاعات». «خط‌مشی کنترل دسترسی» سازوکارهایی هستند که بر اساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی کاربران، منابع، موجودیت‌های فعال، موجودیت‌های غیرفعال، نشست‌ها، وضعیت داده‌های محصول و کارکردها در حوزه کنترلی‌شان پیاده‌سازی می‌شوند.

این مشخصه‌های امنیتی در مجموعه قوانینی استفاده می‌شوند که حاکم بر عملیاتی است که موجودیت‌های فعال ممکن است بر روی موجودیت‌های غیرفعال اجرا نمایند.

خط‌مشی کنترل جریان اطلاعات (Information Flow Control SFP): «خط‌مشی جریان اطلاعات» سازوکارهایی هستند که بر اساس احکام خط-مشی‌هایشان، بر روی مشخصه‌های امنیتی موجودیت‌های فعال و اطلاعات در حوزه کنترلی‌شان و مجموعه قوانین حاکم بر عملیات که توسط موجودیت فعال بر روی اطلاعات صورت می‌گیرد، پیاده‌سازی می‌شوند.

تصادفی‌سازی نمایه فضای آدرس[۱] (ASLR): یک قابلیت ضد اکسپلویت که نگاشت حافظه را در مکان‌های غیرقابل پیش‌بینی انجام می‌دهد. ASLR، کار مهاجمان را برای به دست گرفتن کنترل دستگاه از طریق کدی که وارد فضای آدرس برنامه کاربردی کرده‌اند، دشوارتر می‌نماید.

برنامه کاربردی[۲] (App): نرم‌افزاری که به همراه واسط برنامه‌نویسی برنامه کاربردی (API)، روی یک پلتفرم اجرا می‌شود و از جانب کاربر یا مالک پلتفرم وظایفی را انجام می‌دهد. در این سند می‌توان دو اصطلاح محصول و برنامه کاربردی را به‌جای یکدیگر به کار برد.

واسط برنامه‌نویسی برنامه کاربردی[۳] (API): مجموعه‌ی معینی از روش‌ها، ساختارهای داده، رده‌بندی اشیا و متغیرهایی که به یک برنامه کاربردی اجازه می‌دهند تا از سرویس‌هایی که توسط مؤلفه نرم‌افزاری دیگری فراهم‌شده است، مانند یک کتابخانه، استفاده کند. APIها اغلب برای مجموعه‌ای از کتابخانه‌هایی که در یک پلتفرم وجود دارد، ایجاد می‌شوند.

---

[۱] Address Space Layout Randomization

[۲] Application

[۳] Application Programming Interface

اعتبارنامه[۱]: داده‌های حساب کاربری که هویت کاربر را شکل می‌دهند، مانند گذرواژه‌ها و کلیدهای رمزنگاری.

جلوگیری از اجرای داده‌ها[۲] **(DEP)**: یک قابلیت ضد اکسپلویت در سیستم‌عامل‌های مدرن که روی سخت‌افزارهای کامپیوتری مدرن اجرا می‌شود و اجرای دستورات را در برخی از صفحات حافظه غیرممکن می‌سازد. قابلیت جلوگیری از داده‌ها به صفحات حافظه اجازه نمی‌دهد که حاوی داده‌ها و هم دستورالعمل‌ها باشند. در این صورت، کار مهاجمان برای تزریق و اجرای کد، سخت‌تر می‌شود.

تولیدکننده [۳]: نهادی که نرم‌افزار برنامه‌های کاربردی را می‌نویسد. در این سند، فروشنده و تولیدکننده در یک معنا به‌کار می‌روند.

کد موبایل: نرم‌افزاری که از یک سیستم راه دور برای اجرا درون یک محیط اجرایی محدود روی سیستم‌های محلی، ارسال می‌شود. عموماً این کدها به‌صورت دائمی نصب نمی‌شوند و اجرای آن‌ها بدون اطلاع کاربر یا حتی هشدار آغاز می‌شود. مثال‌هایی از فناوری‌های کد موبایل عبارت‌اند از: جاوا اسکریپت، جاوا اپلت‌ها، Adobe Flash و Microsoft Silverlight.

سیستم‌عامل (OS): نرم‌افزاری که منابع سخت‌افزاری را مدیریت می‌کنند و برای برنامه‌های کاربردی، خدمات فراهم می‌کند.

اطلاعات شناسایی شخصی[۴] **(PII):** هرگونه اطلاعات در مورد یک فرد که توسط یک سازمان نگهداری می‌شود؛ اطلاعاتی مانند سوابق تحصیلی، تراکنش‌های مالی، سابقه پزشکی، سابقه کیفری یا سابقه استخدامی و هرگونه اطلاعاتی که بتوان از آن‌ها هویت یک فرد را تشخیص داد یا ره‌گیری کرد؛ مانند نام، شماره تأمین اجتماعی، تاریخ و محل تولد، نام خانوادگی مادر قبل از ازدواج، اطلاعات جسمی و هرگونه اطلاعات شخصی دیگری که مرتبط با فرد باشد یا بتوان از طریق آن به فرد ارتباطی پیدا کرد.

پلتفرم: محیطی که نرم‌افزار برنامه کاربردی در آن اجرا می‌شود. پلتفرم می‌تواند یک سیستم‌عامل باشد، یک محیط اجرایی باشد که روی سیستم‌عامل کار می‌کند، یا ترکیبی از این حالت‌ها باشد.

داده‌های حساس: داده‌های حساس ممکن است شامل تمامی داده‌های شخصی یا سازمانی شود و یا بخش خاصی از داده‌های برنامه‌های کاربردی مثل ایمیل، پیام‌ها، سندها، اطلاعات تقویم و تماس‌ها را در برگیرد. برای این‌که داده‌ای، حساس محسوب شود باید حداقل حاوی اطلاعات شناسایی شخصی، اطلاعات

---

۱ Credential

۲ Data Execution Prevention

۳ Developer

۴ Personally Identifiable Information

حساب کاربری یا کلیدها باشد. داده‌های حساس در خلاصه مشخصه محصول برنامه کاربردی و توسط فردی که هدف امنیتی را تعیین می‌کند، شناسایی می‌شوند.

کوکی پشته[۱]: یک قابلیت ضد اکسپلویت که ابتدای فراخوانی تابع، یک مقدارِ عددی را به آن نسبت می‌دهد و در پایان فراخوانی تابع بررسی می‌کند که آیا این مقدار عددی تغییر کرده است یا خیر. به این کار محافظ پشته[۲] یا قناری‌های پشته[۳] نیز می‌گویند.

فروشنده: نهادی که نرم‌افزار برنامه کاربردی را می‌فروشد. در این سند، دو اصطلاح تولیدکننده و فروشنده، معادل با یکدیگرند. فروشندگان مسئول نگهداری و به‌روزرسانی نرم‌افزار برنامه کاربردی خود هستند.

انتخاب: «انتخاب» یکی از عملیاتی است که در الزامات پروفایل جهت منعطف شدن پروفایل به‌منظور تدوین سند هدف امنیتی توسط تولیدکننده آمده است. در الزاماتی با این عملیات نویسنده با توجه به کارکرد امنیتی محصول یک یا چند مورد از موارد ذکرشده در الزام را انتخاب می‌نماید و به‌عنوان ادعا در بخش الزامات کارکردی سند هدف امنیتی ذکر می‌نماید.

اختصاص: «اختصاص» یکی از عملیاتی است که در الزامات پروفایل جهت منعطف شدن پروفایل به‌منظور تدوین سند هدف امنیتی توسط تولیدکننده آمده است. در الزاماتی با این عملیات نویسنده با توجه به کارکرد امنیتی محصول، مقدار یا پارامتر مشخصی را اختصاص می‌دهد.

۳ شرح محصول

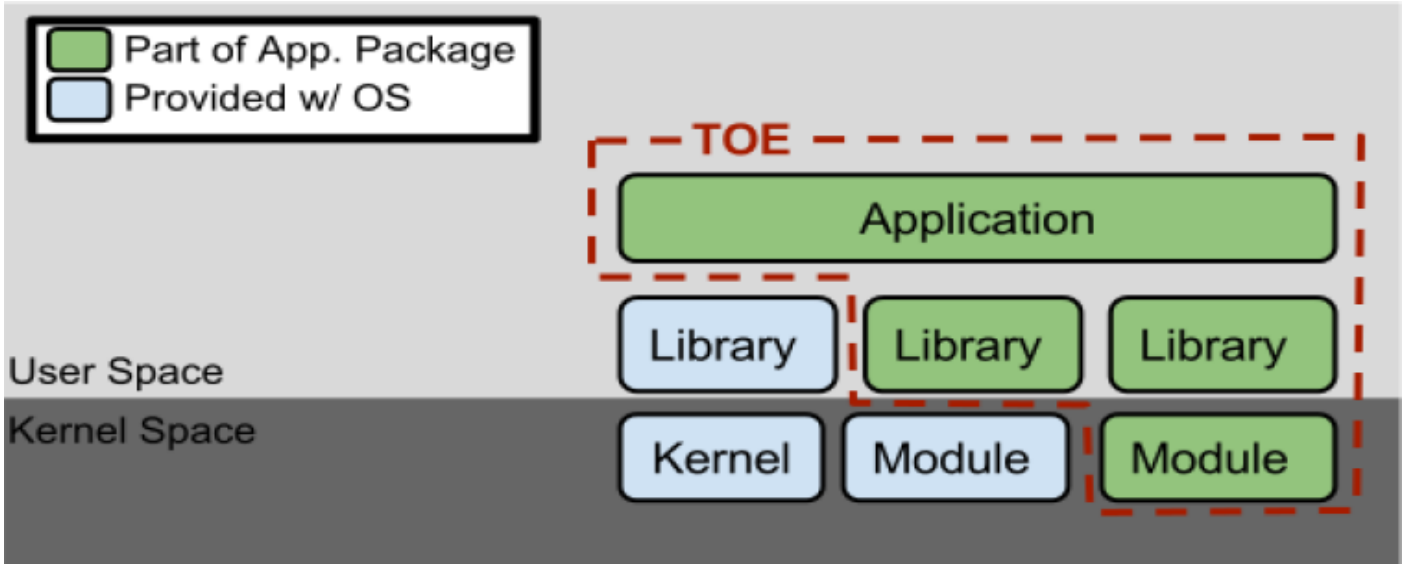
یک برنامه کاربردی، نرم‌افزاری است که روی یک پلتفرم اجرا می‌شود و وظایفی را از جانب کاربر یا مالک سیستم انجام می‌دهد. برنامه کاربردی متشکل از نرم‌افزاری است که توسط تولیدکننده ارائه شده و درون فایل سیستمی فراهم‌شده توسط سیستم‌عامل نصب می‌گردد. برنامه کاربردی، روی پلت‌فرمی اجرا می‌شود که ممکن است یک سیستم‌عامل (شکل ۱) یا یک محیط اجرایی و یا ترکیبی از این دو (شکل ۲) باشد. چند اقدام اعتبارسنجی برای هر پلتفرم خاص وجود دارد تا دقت و تکرارپذیری برنامه کاربردی را ضمانت کند. آزمون و اقدامات آزمایشی نیز به‌طور فعال توسط فروشندگان پلتفرم انجام می‌شود تا پوشش

---

۱ Stack Cookie
۲ Stack Guard
۳ Stack Canaries

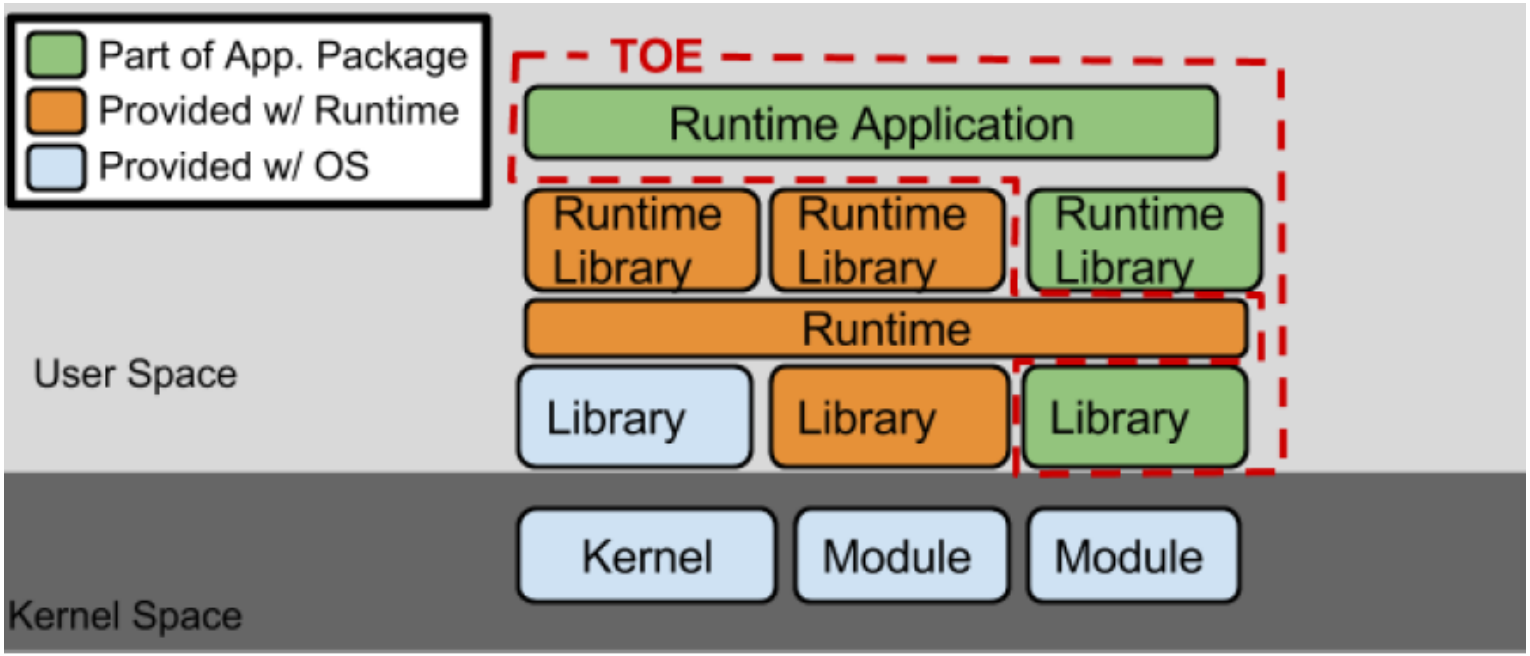
در تمام قسمت‌های پلتفرم، در کامل‌ترین و دقیق‌ترین میزان ممکن، فراهم شود. این کار، امکان تضمین کیفیت و کارکرد برنامه کاربردی روی این پلتفرم‌ها را نیز فراهم می‌کند.

برنامه‌های کاربردی شامل گستره‌ی وسیعی از نرم‌افزارها مانند مجموعه‌های آفیس، تین کلاینت، پی‌دی‌اف ریدر و برنامه‌های کاربردی قابل دانلود در گوشی‌های هوشمند است. محصول هرگونه نرم‌افزار در بسته‌ی نصب برنامه‌ی کاربردی را شامل می‌شود؛ حتی نرم‌افزارهایی که عملکرد پلتفرم زیرین را توسعه می‌دهند، مثل درایورهای کرنل. بسیاری از پلتفرم‌ها به همراه چند برنامه کاربردی پیش‌فرض همانند مرورگر وب، کلاینت ایمیل و مدیا پلیر عرضه می‌شوند. این دسته از برنامه‌ها نیز باید تحت پوشش الزاماتی قرار گیرند که در این سند تعریف‌شده است؛ BIOS و دیگر ثابت‌افزارها[۱]، سیستم‌عامل کرنل و دیگر نرم‌افزارهای سیستمی و درایورهایی که به‌عنوان بخشی از پلتفرم ارائه‌شده‌اند، خارج از حوزه‌ی این سند هستند.



شکل ۱: محصول به‌عنوان یک برنامه کاربردی و ماژول کرنل که روی یک سیستم‌عامل اجرا می‌شود.

[۱] Firmware



شکل ۲: محصول به‌عنوان یک برنامه کاربردی که روی یک محیط اجرایی به همراه یک کد مختص دستگاه اجرا می‌شود.

الزامات مطرح‌شده در این پروفایل حفاظتی برای رفع مشکلات امنیتی در موارد استفاده‌ی زیر می‌باشند. این موارد استفاده، عمداً بسیار گسترده در نظر گرفته‌شده‌اند، زیرا موارد استفاده‌ی خاص از نرم‌افزارهای برنامه‌های کاربردی، بسیار فراوان است. خیلی از برنامه‌های کاربردی ممکن است در ترکیب با این موارد استفاده‌ی گسترده به کار گرفته شوند. ارزیابی این برنامه‌های کاربردی با استفاده از بسته‌های تکمیلی این پروفایل حفاظتی (اگر بسته‌ی تکمیلی موجود بود) می‌تواند برای برخی از انواع برنامه‌های کاربردی، بسیار مناسب باشد.

مورداستفاده ۱: ایجاد محتوا

برنامه کاربردی به کاربر اجازه می‌دهد تا تولید محتوا کند و آن را در فضای حافظه محلی یا از راه دور، ذخیره نماید. برخی از نمونه‌های این محتوا عبارت‌اند از: سند متنی، اسلاید و تصویر.

مورداستفاده ۲: مصرف محتوا

برنامه کاربردی به کاربر اجازه می‌دهد تا محتوا را از فضای حافظه‌ی محلی یا از راه دور به دست آورده و بکار برد. برخی از نمونه‌های این محتوا عبارت‌اند از: ویدئو و صفحات وب.

مورداستفاده ۳: ارتباطات

برنامه کاربردی به کاربر اجازه می‌دهد تا از طریق یک کانال ارتباطی، به‌صورت تعاملی یا غیرتعاملی با دیگر کاربران یا برنامه‌های کاربردی ارتباط برقرار کند. نمونه‌هایی از ارتباطات عبارت‌اند از: پیام فوری، ایمیل و ارتباط صوتی.

۴ مسائل امنیتی

مسائل امنیتی یعنی تهدیداتی که از محصول انتظار می‌رود آنان را رفع کند، فرضیاتی که در مورد محیط عملیاتی وجود دارد و هرگونه سیاست امنیتی سازمانی که از محصول برای اجرای آن استفاده می‌شود.

۴,۱ تهدیدات

تهدیدات	توضیحات
T.NETWORK_ATTACK	فرد مهاجم روی یک کانال ارتباطی یا هر جای دیگری از زیرساخت شبکه قرار می‌گیرد. مهاجمان ممکن است سعی در برقراری ارتباط با برنامه کاربردی نمایند یا در ارتباطات میان نرم‌افزار برنامه کاربردی و دیگر نقاط پایانی دست ببرند تا بتوانند به آن نفوذ کنند.
T.NETWORK_EAVESDROP	فرد مهاجم روی یک کانال ارتباطی یا هر جای دیگری از زیرساخت شبکه قرار می‌گیرد. مهاجمان ممکن است داده‌های انتقالی بین برنامه کاربردی و دیگر نقاط پایانی را مشاهده کنند یا به آن‌ها دسترسی یابند.
T.LOCAL_ATTACK	فرد مهاجم ممکن است از طریق نرم‌افزارهای عادی (نرم‌افزارهایی که امتیاز دسترسی ویژه ندارند) موجود روی پلت‌فرمی که برنامه کاربردی روی آن اجرا می‌شود، وارد عمل شود. مهاجمان ممکن است ورودی‌های آلوده را در قالب فایل یا ارتباطات محلی، وارد برنامه کاربردی کنند.
T.PHYSICAL_ACCESS	مهاجم ممکن است به اطلاعات حساس بایگانی‌شده، دسترسی پیدا کند.

۴,۲ فرضیات

A.TYPES	توضیحات
A.PLATFORM	اجرای محصول منوط به یک پلتفرم رایانشی قابل‌اعتماد است و شامل پلتفرم زیرین و هرگونه محیط زمان اجرا که پلت فرم برای محصول فراهم کرده است، است.
A.PROPER_USER	کاربر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، به کار می‌گیرد.
A.PROPER_ADMIN	راهبر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند، بی‌دقت نیست و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، راهبری می‌نماید.

۴,۳ خط‌مشی‌های امنیتی سازمانی

هیچ‌گونه خط‌مشی امنیتی سازمانی[۱] برای برنامه کاربردی وجود ندارد.

۵ اهداف امنیتی

۵,۱ اهداف امنیتی برای محصول

هدف امنیتی	توضیحات
O.INTEGIRITY	محصولات انطباق‌پذیر، صحت نصب خود و بسته‌های به‌روزرسانی را تضمین می‌کنند و همچنین اقدامات اجرایی محیط محور را در جهت کاهش تهدیدات، تسهیل می‌نمایند. نرم‌افزارهای خیلی کمی، اگر نگوییم

[۱] OSP

هدف امنیتی	توضیحات
	هیچ، عاری از خطا ه ستند؛ بنابراین، توانایی ن صب ب سته‌های تعمیر و عیب‌یابی و به‌روز سانی نرم‌افزارهای نصب‌شده به‌صورت منسجم، اقدامی ضروری برای امنیت شبکه‌های سازمانی است. سازندگان پردازشگرها، برنامه‌نویسان کامپایلر، فروشندگان محیط‌های اجرا و فروشندگان سیستم‌عامل‌ها، اقدامات اجرایی محیط‌محوری را در جهت کاهش تهدیدات ایجاد کرده‌اند که با پیچیده‌تر کردن وظایف سیستم‌ها، کار نفوذ به آن‌ها را برای مهاجمان، دشوارتر و پرهزینه‌تر می‌کند. نرم‌افزارهای برنامه کاربردی اغلب می‌توانند از این سازوکارها بهره ببرند. این کار با ا ستفاده از APIهایی انجام می شود که در زمان اجرا فراهم شده ا ست؛ یا توسط فعال‌سازی این سازوکارها از طریق کامپایلر یا لینکر.
O.QUALITY	برای تضمین کیفیت پیاده‌سازی، محصولات انطباق‌پذیر به‌جای پیاده‌سازی سرویس‌ها و APIهای خود، سرویس‌ها و APIهایی را به کار می‌گیرند که توسط محیط زمان اجرا تأمین‌شده است. اهمیت این کار به‌طور خاص برای سرویس‌های رمزنگاری و دیگر عملیات پیچیده‌ای مثل تجزیه فایل و رسانه، بیشتر است. بهره‌گیری از این قابلیت پلتفرم، فقط منوط به استفاده از APIهای مستند و پشتیبانی شده است.
O.MANAGEMENT	برای تسهیل روند مدیریت توسط کاربران و سازمان، محصولات انطباق‌پذیر، واسط‌های منسجم و پشتیبانی شده‌ای را برای نگهداری و پیکربندی امنیتی خود فراهم می‌کنند. این کار شامل پیاده‌سازی و به‌روزرسانی برنامه کاربردی با استفاده از قالب‌ها و سازوکار پیاده‌سازی پشتیبانی شده توسط پلتفرم و همچنین فراهم کردن سازوکاری برای پیکربندی است.
O.PROTECTED_STORAGE	برای جلوگیری از افشای اطلاعات محرمانه‌ی کاربر در نتیجه‌ی حوادثی که منجر به از دست رفتن کنترل فیزیکی ابزارهای ذخیره‌سازی می‌شوند، محصولات انطباق‌پذیر از شیوه‌های حفاظت داده‌های بایگانی‌شده

هدف امنیتی	توضیحات
	استفاده می‌کنند. این کار شامل رمزگذاری داده‌ها و ذخیره کلیدها توسط محصول است تا از دسترسی غیرمجاز به این داده‌ها جلوگیری شود.
O.PROTECTED_COMMS	برای جلوگیری از حملات تهدیدآمیز فعال (دست‌کاری بسته‌های داده) و غیرفعال (استراق سمع)، محصولات انطباق‌پذیر از یک کانال مورد اعتماد برای انتقال داده‌های حساس استفاده می‌کنند. داده‌های حساس شامل کلیدهای رمزنگاری، گذرواژه‌ها و هرگونه داده‌های دیگری است که مربوط به برنامه کاربردی بوده و نباید خارج از برنامه کاربردی، در معرض دید باشند.

۵,۲ اهداف امنیتی برای محیط عملیاتی

OE.TYPES	توضیحات
OE.PLATFORM	اجرای محصول متکی به یک پلتفرم رایانشی مورد اعتماد است. این شامل سیستم‌عامل زیرین و هرگونه محیط اجرایی دیگری نیز می‌شود که در اختیار محصول قرارگرفته است.
OE.PROPER_USER	کاربر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، به کار می‌گیرد.
OE.PROPER_ADMIN	راهبر برنامه کاربردی بی‌دقت نیست و از روی عمد دست به اشتباه یا خرابکاری نمی‌زند و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، راهبری می‌نماید.

۶ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند. در ادامه هر یک از الزامات شرح و بسط داده شده‌اند.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۲	ذخیره‌سازی اسرار ۱	FCS_STO_EXT.1.1
۳	دسترسی به منابع پلتفرم ۱	FDP_DEC_EXT.1.1
۴	دسترسی به منابع پلتفرم ۲	FDP_DEC_EXT.1.2
۵	ارتباطات شبکه‌ای۱	FDP_NET_EXT.1.1
۶	رمزگذاری داده‌های حساس برنامه کاربردی ۱	FDP_DAR_EXT.1.1
۷	استفاده کاربر از یک سرویس بدون افشاء هویت ۴	FPR_ANO_EXT.1.1
۸	سازوکار پیکربندی پشتیبان‌شده ۱	FMT_MEC_EXT.1.1
۹	تأمین امنیت با پیکربندی پیش‌فرض۱	FMT_CFG_EXT.1.1
۱۰	تأمین امنیت با پیکربندی پیش‌فرض ۲	FMT_CFG_EXT.1.2
۱۱	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۱۲	استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱	FPT_API_EXT.1.1
۱۳	قابلیت‌های ضد اکسپلویت ۱	FPT_AEX_EXT.1.1
۱۴	قابلیت‌های ضد اکسپلویت ۲	FPT_AEX_EXT.1.2
۱۵	قابلیت‌های ضد اکسپلویت ۳	FPT_AEX_EXT.1.3
۱۶	قابلیت‌های ضد اکسپلویت ۴	FPT_AEX_EXT.1.4

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۷	قابلیت‌های ضد اکسپلویت ۵	FPT_AEX_EXT.1.5
۱۸	به‌روزرسانی امن۱	FPT_TUD_EXT.1.1
۱۹	به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۲۰	به‌روزرسانی امن ۳	FPT_TUD_EXT.1.3
۲۱	به‌روزرسانی امن ۴	FPT_TUD_EXT.1.4
۲۲	به‌روزرسانی امن ۵	FPT_TUD_EXT.1.5
۲۳	به‌روزرسانی امن ۶	FPT_TUD_EXT.1.6
۲۴	استفاده از کتابخانه‌های شخص ثالث ۱	FPT_LIB_EXT.1.1
۲۵	حفاظت از تبادل داده‌ها ۱	FTP_DIT_EXT.1.1
الزامات پیوست یک		
۲۶	مدیریت کلید رمزنگاری ۳	FCS_CKM.1.1(2)
۲۷	الزامات پروتکلTLS Client/ احراز هویت دستی ۵	FCS_TLSC_EXT.2.1
الزامات پیوست دو		
۲۸	تولید بیت تصادفی ۳	FCS_RBG_EXT.2.1
۲۹	تولید بیت تصادفی ۴	FCS_RBG_EXT.2.2
۳۰	مدیریت کلید رمزنگاری ۵	FCS_CKM_EXT.1.1
۳۱	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1(1)
۳۲	مدیریت کلید رمزنگاری ۲	FCS_CKM.2.1
۳۳	عملیات رمزنگاری – رمزنگاری/رمزگشایی ۱ (۱)	FCS_COP.1.1(1)

شماره الزام	نام الزام	تطابق الزام با استاندارد
۳۴	عملیات رمزنگاری – درهم‌سازی ۱ (۲)	FCS_COP.1.1(2)
۳۵	عملیات رمزنگاری – امضاء ۱ (۳)	FCS_COP.1.1(3)
۳۶	عملیات رمزنگاری – امضاء ۲ (۴)	FCS_COP.1.1(4)
۳۷	پروتکل TLSC(۱)	FCS_TLSC_EXT.1.1
۳۸	پروتکل TLSC (۲)	FCS_TLSC_EXT.1.2
۳۹	پروتکل TLSC(۳)	FCS_TLSC_EXT.1.3
۴۰	پروتکل TLSC (۷)	FCS_TLSC_EXT.4.1
۴۱	الزامات پروتکلTLS Server/ احراز هویت ۱	FCS_TLSS_EXT.1.1
۴۲	الزامات پروتکلTLS Server/ احراز هویت ۲	FCS_TLSS_EXT.1.2
۴۳	الزامات پروتکلTLS Server/ احراز هویت ۳	FCS_TLSS_EXT.1.3
۴۴	الزامات پروتکلTLS Server/ احراز هویت ۴	FCS_TLSS_EXT.1.4
۴۵	الزامات پروتکلTLS Server/ احراز هویت ۵	FCS_TLSS_EXT.1.5
۴۶	الزامات پروتکلTLS Server/ احراز هویت ۶	FCS_TLSS_EXT.1.6
۴۷	پروتکل DTLS(۱)	FCS_DTLS_EXT.1.1
۴۸	پروتکل DTLS(۲)	FCS_DTLS_EXT.1.2
۴۹	پروتکل DTLS(۳)	FCS_DTLS_EXT.1.3
۵۰	پروتکل HTTPS(۱)	FCS_HTTPS_EXT.1.1
۵۱	پروتکل HTTPS(۲)	FCS_HTTPS_EXT.1.2
۵۲	پروتکل HTTPS(۳)	FCS_HTTPS_EXT.1.3

شماره الزام	نام الزام	تطابق الزام با استاندارد
۵۳	الزامات پروتکل X509 (۱)	FIA_X509_EXT.1.1
۵۴	الزامات پروتکل X509 (۲)	FIA_X509_EXT.1.2
۵۵	الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1
۵۶	الزامات پروتکل X509 (۴)	FIA_X509_EXT.2.2
الزامات پیوست سه		
۵۷	پروتکل TLSS(۶)	FCS_TLSC_EXT.3.1
۵۸	استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۲	FPT_API_EXT.2.1
۵۹	شناسایی نرم‌افزار و نسخه‌ها ۱	FPT_IDV_EXT.1.1

۶,۱ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱	**تولید بیت تصادفی ۱**
برنامه‌ی کاربردی برای عملیات رمزنگاری باید [انتخاب: از هیچ‌گونه عملکرد تولید بیت تصادفی قطعی[۱] استفاده نکند، از عملکرد تولید بیت تصادفی قطعی که توسط پلتفرم ارائه‌شده است کمک بگیرد،	

[۱] Deterministic Random Bit Generation (DRBG)

عملکرد تولید بیت تصادفی قطعی را پیاده‌سازی نماید] **نکته کاربردی ۱:** اگر گزینه‌ی «عملکرد تولید بیت تصادفی قطعی را پیاده‌سازی کند» انتخاب شود، آنگاه عناصر تکمیلی الزامات شماره ۲۸و ۲۹ «بیت تصادفی ۴و ۳» نیز در سند هدف امنیتی لحاظ خواهند شد. در این الزام، عملیات رمزنگاری شامل تمامی توافقات/ مشتقات/ روش‌های تولید کلید رمزنگاری، بردار شروع[۱] (برای حالت‌های معین) و همچنین مقادیر عددی تصادفی خاص پروتکل نیز هستند.	
۲	**ذخیره‌سازی اسرار ۱**
برنامه‌ی کاربردی در فضای حافظه‌ی غیر فرّار باید [انتخاب: هیچ‌گونه اطلاعات کاربری را ذخیره نکند، از عملکردهای ارائه‌شده در پلتفرم برای ذخیره‌ی امن[اختصاص: لیست اعتبارنامه‌ها] استفاده کند، عملکردی را برای ذخیره‌ی امن [اختصاص: لیست اعتبارنامه‌ها]، پیاده‌سازی کند.] **نکته کاربردی ۲:** این الزام، تضمین می‌کند که امنیت مشخصات دائمی حساب کاربری (کلیدهای مخفی، کلیدهای خصوصی PKI، گذرواژه‌ها) در هنگام استفاده نشدن نیز حفظ می‌گردد.	

[۱] Initial Vectors (IVs)

۶,۲ کلاس حفاظت از داده‌ها

شماره الزام	نام الزام
۳	**دسترسی به منابع پلتفرم ۱**

برنامه کاربردی باید کاربر را از قصد خود برای دسترسی به این منابع، آگاه کند:

[انتخاب:

- هیچ‌گونه منبع سخت‌افزاری،
- اتصال شبکه،
- دوربین،
- میکروفون،
- سرویس‌های موقعیت‌یاب،
- NFC،
- USB،
- بلوتوث،
- [اختصاص: لیست تکمیلی منابع سخت‌افزاری]

].

نکته کاربردی ۳:

ارزیاب باید تضمین کند که این گزینه‌ها تمامی منابع سخت‌افزاری پلتفرم را که برنامه کاربردی قصد دسترسی به آنان را دارد، پوشش می‌دهند. این الزام به دلیل تنوع روش‌های آگاه‌سازی کاربر روی هر پلتفرم، از این عبارات استفاده کرده است. گزینه‌ها باید طوری بیان شوند که هماهنگ با نحوه بیان برنامه کاربردی از نیاز خود به دسترسی به پلتفرم زیرین باشد. برای مثال، پلتفرم ممکن است خدمات موقعیت‌یابی ارائه کند که مستلزم استفاده از منابع متنوع سخت‌افزاری است (گیرنده‌های ماهواره‌ای، WiFi، سیم‌کارت رادیویی). در این صورت، «سرویس‌های موقعیت‌یاب» گزینه‌ی مناسب

شماره الزام	نام الزام
است؛ زیرا استفاده از این منابع را می‌توان به‌صورت ضمنی مشخص کرد. همچنین کاربرد آن‌ها ممکن است بنا بر هر پلتفرم، تغییر کند. منابعی که نیازی به تأیید مستقیم ندارند، آن‌هایی هستند که معمولاً توسط هر برنامه کاربردی مورداستفاده قرار می‌گیرند؛ مثل واحدهای پردازش مرکزی، حافظه اصلی، نمایشگر، ابزارهای ورودی (کیبورد، ماوس) و ابزارهای ذخیره‌سازی دائمی که توسط پلتفرم ارائه‌شده‌اند	
۴	**دسترسی به منابع پلتفرم ۲**
برنامه کاربردی باید کاربر را از قصد خود برای دسترسی به این منابع، آگاه کند: [انتخاب: • هیچ نوع از منابع اطلاعات حساس، • دفترچه نشانی‌ها، • تقویم، • لیست تماس‌ها، • اطلاعات ورود و خروج به سیستم، • [اختصاص: لیست تکمیلی منابع اطلاعات حساس]]. **نکته کاربردی ۴:** «منابع اطلاعات حساس» به مجموعه‌هایی از اطلاعات حساس گفته می‌شود که می‌توان انتظار داشت که میان چند برنامه کاربردی، کاربر یا نقش کاربری خاص به اشتراک گذاشته شوند، اما به‌طور معمول همه برنامه‌های کاربردی و کاربران و نقش‌های کاربری نیازی به دسترسی به منابع ندارند. هدف این است که ارزیاب تضمین کند تمامی منابع اطلاعات حساسی که برنامه کاربردی قصد دسترسی به آن‌ها را دارد، در لیست گزینه‌ها گنجانده‌شده است. این الزام به دلیل تنوع روش‌های آگاه‌سازی کاربر روی هر پلتفرم، از این عبارات استفاده کرده است.	
۵	**ارتباطات شبکه‌ای۱**

شماره الزام	نام الزام
برنامه کاربردی باید ارتباطات شبکه‌ای خود را محدود کند به [انتخاب: • هیچ ارتباطی با شبکه وجود نداشته باشد، • ارتباطاتی که کاربر برای [اختصاص: لیست عملکردهایی که کاربر می‌تواند برای آن‌ها ارتباط با شبکه را فراهم کند] ایجاد کرده است، • پاسخ به [اختصاص: لیست ارتباطاتی که از دور ایجادشده‌اند]، • [اختصاص: لیست ارتباطات شبکه که برنامه کاربردی ایجاد کرده است]]. **نکته کاربردی ۵:** این الزام بدین علت است که ارتباطات شبکه‌ای به/از سیستم، تنها محدود به ارتباطات ضروری یا ارتباطات شبکه‌ای شود که توسط کاربر ایجادشده است. این در مورد ارتباطات شبکه‌ای که برنامه کاربردی در آن‌ها عموماً به فایل سیستم دسترسی دارد، صدق نمی‌کند. در مورد اخیر، ممکن است پلتفرم به درایوها یا اطلاعات از راه دور دسترسی داشته باشد.	
۶	**رمزگذاری داده‌های حساس برنامه کاربردی ۱**
برنامه کاربردی باید [انتخاب: • *از عملکرد ارائه‌شده توسط پلتفرم برای رمزگذاری داده‌های حساس استفاده کند،* • *عملکردی برای رمزگذاری داده‌های حساس پیاده‌سازی کند،* • *هیچ‌گونه داده‌های حساسی را در حافظه غیر فرار ذخیره نکند.*] **نکته کاربردی ۶:**	

شماره الزام	نام الزام
در صورت انتخاب رمزگذاری داده‌های حساس، نیاز به ارزیابی بر اساس بسته‌ی تکمیلی پروفایل حفاظتی برنامه کاربردی است: بسته‌ی رمزگذاری فایل. هر فایلی که ممکن است حاوی داده‌های حساس باشد (یا به‌طور موقت شامل آن‌ها باشد) باید مورد حفاظت قرار گیرد. مگر آنکه کاربر از روی عمد داده‌های حساس را به یک فایل حفاظت‌نشده منتقل نماید.	

۶,۳ کلاس محرمانگی

شماره الزام	نام الزام
۷	**استفاده کاربر از یک سرویس بدون افشاء هویت4**
برنامه کاربردی باید [انتخاب: اطلاعات شناسایی شخصی (PII) را در شبکه انتقال ندهد، قبل از اجرای [اختصاص: لیست عملکردهایی که اطلاعات شناسایی شخصی را در شبکه انتقال می‌دهند] تأیید کاربر را کسب کند.] **نکته کاربردی ۷:** این الزام تنها در مورد اطلاعات شناسایی شخصی صدق می‌کند که اختصاصاً توسط برنامه کاربردی درخواست شده است؛ و شامل مواقعی نمی‌شود که کاربر به‌صورت داوطلبانه و بدون درخواست برنامه کاربردی اطلاعات شناسایی شخصی خود را در یک صفحه عمومی (یا نامناسب) وارد می‌کند. باز شدن	

شماره الزام	نام الزام
یک جعبه گفتگو[1] حین آغاز برنامه کاربردی که قصد برنامه کاربردی را از ارسال اطلاعات شناسایی شخصی به کاربر اطلاع می‌دهد، اقدامی کافی برای تبعیت از این الزام است.	

۶,۴ کلاس مدیریت امنیت

شماره الزام	نام الزام
۸	**سازوکار پیکربندی پشتیبان‌شده ۱**
برنامه کاربردی باید سازوکار توصیه‌شده توسط تولیدکننده‌ی پلتفرم را برای ذخیره‌سازی و تنظیم گزینه‌های پیکربندی، استفاده نماید. **نکته کاربردی ۸:** گزینه‌های پیکربندی که از راه دور ذخیره می‌شوند، شامل این الزام نمی‌شوند.	
۹	**تأمین امنیت با پیکربندی پیش‌فرض ۱**
هنگامی که برنامه کاربردی بدون اعتبارنامه یا با اعتبارنامه پیش‌فرض پیکربندی‌شده است، برنامه کاربردی باید اقدامات لازم برای ایجاد اعتبارنامه جدید را فراهم آورد. **نکته کاربردی ۹:** اعتبارنامه‌ها پیش‌فرض (مثل گذرواژه‌ها و کلیدها)، مشخصاتی است که به‌طور خودکار (بدون تعامل کاربر) حین نصب برنامه کاربردی روی پلتفرم بارگذاری می شوند. اعتبارنامه‌های که حین نصب برنامه کاربردی با استفاده از الزامات ارائه شده در الزام شماره ۱ «تولید بیت تصادفی ۱» ایجاد شده‌اند، طبق تعریف، اعتبارنامه‌ها پیش‌فرض محسوب نمی‌شوند.	
۱۰	**تأمین امنیت با پیکربندی پیش‌فرض ۲**

[1] Dialog Box

شماره الزام	نام الزام
برنامه کاربردی باید به‌طور پیش‌فرض طوری پیکربندی شود که با قرار دادن مجوزهای دسترسی به فایل مناسب، خود برنامه کاربردی و داده‌های آن را از دسترسی‌های غیرمجاز محافظت کند. **نکته کاربردی ۱۰:** محدوده دقیق مجوز دسترسی به فایل‌ها برای هر نوع از پلتفرم‌ها متفاوت است؛ اما هدف کلی این است که با ایجاد محدوده‌ای امن و مورد اعتماد، برنامه کاربردی و داده‌هایش را مورد حفاظت قرار دهد.	
۱۱	**کارکرد مدیریتی محصول ۱**
محصول باید قابلیت اجرای کارکردهای امنیتی زیر را داشته باشد: [انتخاب: • بدون کارکرد مدیریتی، • فعال‌سازی/ غیر فعال‌سازی تبادل هرگونه اطلاعاتی که سخت‌افزار، نرم‌افزار یا پیکربندی سیستم را توصیف می‌کند، • • فعال‌سازی/ غیر فعال‌سازی تبادل هرگونه اطلاعات شناسایی شخصی، • فعال‌سازی/ غیر فعال‌سازی تبادل هرگونه اطلاعات در مورد وضعیت برنامه کاربردی (مثل ازکارافتادن)، • فعال‌سازی/ غیر فعال‌سازی کارکرد پشتیبان‌گیری تحت شبکه در [اختصاص: لیست سیستم‌های پشتیبان‌گیری رایانش ابری تجاری یا سازمانی[۱]]، • [اختصاص: لیست دیگر عملکردهای مدیریتی که توسط محصول ارائه می‌شوند]]. **نکته کاربردی ۱۱:**	

[۱] Enterprise or commercial cloud backup system

شماره الزام	نام الزام
این الزام تصریح می‌کند که یک برنامه کاربردی باید قابلیت فعال‌سازی/ غیر فعال‌سازی تنها آن دسته از کارکردها را داشته باشد که خود پیاده‌سازی کرده است. برنامه کاربردی مسئول کنترل رفتار پلتفرم یا برنامه‌های کاربردی دیگر نیست.	

۶,۵ کلاس حفاظت از محصول

شماره الزام	نام الزام
۱۲	**استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱**
برنامه کاربردی باید تنها از واسط برنامه‌نویسی کاربردی‌های (API) پلتفرم پشتیبانی شده استفاده کند. **نکته کاربردی ۱۲:** اصطلاح «پشتیبانی شده» ممکن است تعاریف متفاوتی داشته باشد. این تفاوت‌ها می‌تواند به این دلیل باشد که برنامه کاربردی توسط شخص ثالث ارائه‌شده است (شخص ثالثی که تنها از APIهای مستندشده پلتفرم استفاده می‌کند) یا اینکه توسط تولیدکننده پلتفرم تهیه‌شده باشد که در این حالت ممکن است بتواند از واسط برنامه‌نویسی کاربردی‌های پلتفرم که برای استفاده خارجی مستند نشده‌اند نیز استفاده نماید.	
۱۳	**قابلیت‌های ضد اکسپلویت ۱**
برنامه کاربردی جز برای [اختصاص: لیست استثنائات صریح و واضح]، نباید درخواست نگاشت حافظه به آدرس مشخصی نماید. **نکته کاربردی ۱۳:** درخواست نگاشت حافظه برای یک آدرس مشخص، تصادفی‌سازی نمایه فضای آدرس (ASLR) را از کار می‌اندازد.	
۱۴	**قابلیت‌های ضد اکسپلویت ۲**

برنامه کاربردی باید

[انتخاب:

- هیچ بخشی از حافظه را هم‌زمان هم به نوشتن اطلاعات و هم اجرای مجوزها اختصاص ندهد،
- بخش‌هایی از حافظه را تنها برای [اختصاص: فهرستی از کارکردهایی که تنها در زمان کامپایل اجرا می‌شوند] به نوشتن اطلاعات و اجرای مجوزها اختصاص دهد.

]

نکته کاربردی ۱۴:

درخواست نگاشت حافظه برای ثبت اطلاعات و مجوزهای اجرا به‌صورت هم‌زمان، مغایر با الزامات حفاظت پلتفرم است که توسط DEP ارائه‌شده است. اگر برنامه کاربردی به‌صورت کامپایل درجا کار نمی‌کند، آنگاه باید گزینه اول را انتخاب نمود.

۱۵	**قابلیت‌های ضد اکسپلویت ۳**

برنامه کاربردی باید با امکانات امنیتی که توسط تولیدکننده‌ی پلتفرم ارائه‌شده است، سازگار باشد.

نکته کاربردی:

این الزام برای آن طراحی شده است تا تضمین کند که برای اجرای برنامه کاربردی، نیازی به غیرفعال کردن امکانات امنیتی پلتفرم نیست.

۱۶	**قابلیت‌های ضد اکسپلویت ۴**

برنامه کاربردی نباید فایل‌هایی را که توسط کاربر قابل‌تغییر هستند در دایرکتوری‌هایی بنویسد که حاوی فایل‌های اجرایی‌اند، مگر این‌که کاربر به‌طور مستقیم چنین دایرکتوری‌ها را انتخاب نماید.

نکته کاربردی ۱۵:

فایل‌های اجرایی و فایل‌هایی که توسط کاربر قابل‌تغییر هستند، نباید از دایرکتوری والد[۱] مشابهی استفاده نمایند، اما ممکن است از دایرکتوری‌هایی بالاتر از دایرکتوری والد استفاده کنند.	
۱۷	**قابلیت‌های ضد اکسپلویت ۵**
برنامه کاربردی باید با قابلیت محافظت از سرریز بافر مبتنی بر پشته کامپایل شود.	
۱۸	**به‌روزرسانی امن ۱**
برنامه کاربردی باید [انتخاب: این قابلیت را ارائه کند، این قابلیت را برای پلتفرم فراهم نماید] که به‌روزرسانی‌ها و وصله‌های برنامه‌های کاربردی را بررسی نماید. **نکته کاربردی ۱۶:** این الزام، در مورد قابلیت «چک کردن» برای نسخه‌های به‌روزرسانی است. نصب هرگونه نسخه به‌روزرسانی باید توسط پلتفرم انجام شود. هدف این الزام تضمین آن است که برنامه کاربردی نسخه‌های به‌روزرسانی ارائه‌شده توسط تولیدکننده را چک می‌نماید؛ زیرا نسخه‌های به‌روزرسانی ارائه‌شده توسط منابع دیگر ممکن است دارای کدهای آلوده باشند.	
۱۹	**به‌روزرسانی امن ۲**
برنامه کاربردی باید با استفاده از قالب مدیریت بسته که توسط آن پلتفرم پشتیبانی می‌شود، توزیع و منتشر شود. **نکته کاربردی ۱۷:** برای سیستم‌عامل ویندوز دارای فرمت فایل‌های " msi" و یا " appx" باشد.	
۲۰	**به‌روزرسانی امن ۳**
برنامه کاربردی باید طوری بسته‌بندی[۲] شود که حذف آن، منجر به پاک شدن تمامی آثار برنامه کاربردی شود؛ به‌استثناء تنظیمات پیکربندی، فایل‌های خروجی و ثبت وقایع/ ممیزی.	

[۱] Parent Directory

[۲] Packaged

نکته کاربردی ۱۸:

در مورد برنامه‌های کاربردی که به همراه سیستم/ ثابت‌افزار عرضه می‌شوند، اگر کاربر نتواند برنامه کاربردی را از طریق ابزارهای ارائه‌شده توسط سیستم‌عامل حذف نماید، این برنامه‌های کاربردی لازم نیست این الزام را رعایت کنند.

۲۱	**به‌روزرسانی امن ۴**

برنامه کاربردی نباید کد باینری خود را دانلود، اصلاح، جایگزین یا به‌روزرسانی کند.

نکته کاربردی ۱۹:

این الزام در مورد کد برنامه کاربردی است و شامل کد فناوری‌های موبایل که برای دانلود و اجرا توسط برنامه کاربردی طراحی شده‌اند، نمی‌شود.

۲۲	**به‌روزرسانی امن ۵**

برنامه کاربردی باید [انتخاب: حداقل یا این قابلیت را ارائه کند، یا این قابلیت را برای پلتفرم فراهم نماید] تا نسخه فعلی برنامه کاربردی را بازیابی کند.

۲۳	**به‌روزرسانی امن ۶**

بسته‌ی نصب برنامه کاربردی و نسخه‌های به‌روزرسانی آن باید به‌طور دیجیتالی امضا شوند به‌طوری‌که پلتفرم بتواند رمزنگاری آنان را قبل از نصب برنامه کاربردی، چک کند.

نکته کاربردی ۲۰:

جزئیات بررسی نصب بسته‌ی برنامه کاربردی و نسخه‌های به‌روزرسانی آن شامل الزاماتی در مورد پلتفرم (و نه برنامه کاربردی) است؛ بنابراین این جزئیات به‌طور کامل در این سند شرح داده نشده‌اند.

۲۴	**استفاده از کتابخانه‌های شخص ثالث ۱**

هدف از این الزام آن است که ارزیاب کتابخانه‌های شخص ثالث غیرضروری یا پیش‌بینی‌نشده در برنامه کاربردی را تشخیص و ثبت نماید. این شامل کتابخانه‌هایی که جهت امور تبلیغاتی ایجادشده‌اند نیز می‌شود که می‌تواند تهدیدی برای حریم خصوصی به شمار رود. همچنین شامل تضمین مستندسازی این کتابخانه‌ها برای مواقعی که آسیب‌پذیری‌هایی در آینده کشف شوند نیز است.

۶,۶ کلاس کانال‌ها و مسیرهای مورد اعتماد

شماره الزام	نام الزام
۲۵	**حفاظت از تبادل داده‌ها ۱**
برنامه کاربردی باید بین خود و دیگر محصولات مورد اعتماد IT **[انتخاب:** هیچ داده‌ای را تبادل نکند، هیچ داده‌ی حساسی را تبادل نکند تمامی داده‌های حساس مورد تبادل را با استفاده از حداقل یکی از این [انتخاب: HTTPS، TLS، DTLS،] رمزگذاری کند: تمامی داده‌های مورد تبادل را با استفاده از[انتخاب: HTTPS، TLS، DTLS،SSH] رمزگذاری کند]. **نکته کاربردی ۲۱:**	

شماره الزام	نام الزام
بسته‌های تکمیلی ممکن است این الزام را به نفع پروتکل‌های دیگر، لغو نمایند. رمزگذاری برای برنامه‌های کاربردی که داده‌های غیر حساس را تبادل می‌کنند الزامی نیست. اگر HTTPS انتخاب شود، آنگاه ارزیابی عناصر از الزام شماره ۳۷ «پروتکل TLSC(۱)» ضروری است. اگر TLS انتخاب شود، آنگاه ارزیابی عناصر از الزام شماره ۴۷ «پروتکل HTTPS(۱)» ضروری است. اگر DTLS انتخاب شود، آنگاه ارزیابی عناصر از الزام شماره ۵۰ «پروتکل DTLS(۱)» ضروری است. اگر SSH انتخاب شود، آنگاه TSF باید بر اساس بسته‌های تکمیلی Secure Shell ارزیابی شود.	

۷ الزامات تضمین امنیت

اهداف امنیتی تعریف‌شده در بخش ۵ جهت مقابله نمودن با تهدیدات معرفی‌شده در بخش ۳ در نظر گرفته‌شده‌اند. الزامات کارکردی در بخش ۶ بیان رسمی و استانداردی از «اهداف امنیتی» است. الزامات تضمین امنیتی که برگرفته از استاندارد ارزیابی امنیتی معیار مشترک می‌باشند تا بر اساس این الزامات ارزیابی، مستندات را ارزیابی و آزمون مستقل بر روی محصول انجام دهد.

مدل کلی ارزیابی محصول در برابر سند هدف امنیتی که مطابق این پروفایل حفاظتی است، به‌صورت زیر است:

پس از تائید سند هدف امنیتی برای ارزیابی، تولیدکننده محصول را در اختیار آزمایشگاه قرار می‌دهد و محیط آزمون آن را فراهم می‌نماید؛ و سپس فعالیت‌های تضمین که در سند هدف امنیتی مطرح‌شده، توسط آزمایشگاه انجام می‌شود. نتایج این فعالیت‌ها مستند و برای اعتباربخشی به مرکز گواهی ارائه می‌شود.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests	ATE_IND.1	آزمون مستقل-منطبق

Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب‌گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	مشخصات کارکرد ابتدایی۱	ADV_FSP.1.1D
۲	مشخصات کارکرد ابتدایی۲	ADV_FSP.1.2D
۳	مشخصات کارکرد ابتدایی۳	ADV_FSP.1.1C
۴	مشخصات کارکرد ابتدایی۴	ADV_FSP.1.2C
۵	مشخصات کارکرد ابتدایی۵	ADV_FSP.1.3C
۶	مشخصات کارکرد ابتدایی۶	ADV_FSP.1.4C
۷	مشخصات کارکرد ابتدایی۷	ADV_FSP.1.1E
۸	مشخصات کارکرد ابتدایی۸	ADV_FSP.1.2E
۹	راهنمای کاربردی ۱	AGD_OPE.1.1D
۱۰	راهنمای کاربردی ۲	AGD_OPE.1.1C
۱۱	راهنمای کاربردی ۳	AGD_OPE.1.2C
۱۲	راهنمای کاربردی ۴	AGD_OPE.1.3C
۱۳	راهنمای کاربردی ۵	AGD_OPE.1.4C
۱۴	راهنمای کاربردی ۶	AGD_OPE.1.5C
۱۵	راهنمای کاربردی ۷	AGD_OPE.1.6C

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۶	راهنمای کاربردی ۸	AGD_OPE.1.7C
۱۷	راهنمای کاربردی ۹	AGD_OPE.1.1E
۱۸	راهنمای آماده‌سازی ۱	AGD_PRE.1.1D
۱۹	راهنمای آماده‌سازی ۲	AGD_PRE.1.1C
۲۰	راهنمای آماده‌سازی ۳	AGD_PRE.1.2C
۲۱	راهنمای آماده‌سازی ۴	AGD_PRE.1.1E
۲۲	راهنمای آماده‌سازی ۵	AGD_PRE.1.2E
۲۳	آزمون مستقل ۱	ATE_IND.1.1D
۲۴	آزمون مستقل ۲	ATE_IND.1.1C
۲۵	آزمون مستقل ۳	ATE_IND.1.1E
۲۶	آزمون مستقل ۱	ATE_IND.1.2E
۲۷	آسیب‌پذیری ۱	AVA_VAN.1.1D
۲۸	آسیب‌پذیری ۲	AVA_VAN.1.1C
۲۹	آسیب‌پذیری ۳	AVA_VAN.1.1E
۳۰	آسیب‌پذیری ۴	AVA_VAN.1.2E
۳۱	آسیب‌پذیری ۵	AVA_VAN.1.3E
۳۲	برچسب‌گذاری محصول ۱	ALC_CMC.1.1D
۳۳	برچسب‌گذاری محصول ۲	ALC_CMC.1.1C
۳۴	برچسب‌گذاری محصول ۳	ALC_CMC.1.1E

شماره الزام	نام الزام	تطابق الزام با استاندارد
۳۵	پوشش پیکربندی محصول ۱	ALC_CMS.1.1D
۳۶	پوشش پیکربندی محصول ۲	ALC_CMS.1.1C
۳۷	پوشش پیکربندی محصول ۳	ALC_CMS.1.1C
۳۸	پوشش پیکربندی محصول ۴	ALC_CMS.1.1E

۷,۱ کلاس توسعه

اطلاعات محصول، از طریق «مستندات راهنمای کاربر» و بخش «مشخصات امنیتی محصول» از سند هدف امنیتی در اختیار کاربر نهایی قرار می‌گیرد. الزامی بر وجود بخش «مشخصات امنیتی محصول» در سند هدف امنیتی نیست، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه‌دهندگان محصول باشد.

مشخصات کارکردی:

مشخصات کارکردی، واسطهای کارکرد امنیتی محصول را توصیف می‌نماید اما نیازی به شرح مفصل و کاملی از این واسطها نیست. فعالیت‌های این خانواده باید بر روی شناخت واسطهای معرفی‌شده در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و «مستندات راهنما» متمرکز گردد.

شماره الزام	نام الزام
۱	**مشخصات کارکرد ابتدایی۱**
توسعه‌دهنده باید مشخصات کارکردی را ارائه نماید.	
۲	**مشخصات کارکرد ابتدایی۲**

شماره الزام	نام الزام
توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده‌سازی (AGD_PRE) و اطلاعاتی که در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی ارائه‌شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح‌شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نیست.	
۳	**مشخصات کارکرد ابتدایی۳**
مشخصات کارکردی باید اهداف و متدهای مورداستفاده برای هر واسط اجراکننده کارکرد امنیتی [۱]و پشتیبان کننده‌ی الزام کارکرد امنیتی[۲]توصیف نماید.	
۴	**مشخصات کارکرد ابتدایی۴**
مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجراکننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.	
۵	**مشخصات کارکرد ابتدایی۵**
مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.	
۶	**مشخصات کارکرد ابتدایی۶**
ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌های کارکرد امنیتی در سند مشخصات کارکردی باشد.	
۷	**مشخصات کارکرد ابتدایی۷**
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.	

[۱]-SFR-enforcing TSFI

[۲]-SFR-supporting TSFI

شماره الزام	نام الزام
۸	**مشخصات کارکرد ابتدایی۸**
ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.	

مستندات «مشخصات کارکردی» جهت پشتیبانی از ارزیابی الزامات کارکردی و اقدامات لازم در کلاس‌های «راهنما»، «آزمون» و «آسیب‌پذیری» ارائه‌شده است.

۷,۲ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل سرپرستی و نحوه بررسی محیط عملیاتی توسط سرپرست (تا مشخص گردد که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می‌شود.
برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد. این راهنما شامل:

- دستورالعمل نصب موفقیت‌آمیز محصول در محیط
- دستورالعمل مدیریت امنیت محصول به‌عنوان یک محصول و به‌عنوان بخشی از یک محیط عملیاتی بزرگ‌تر
- دستورالعمل‌هایی که ارائه‌دهنده قابلیت سرپرستی محافظت‌شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو است.

۷,۲,۱ راهنمای کاربردی

شماره الزام	نام الزام
۹	**راهنمای کاربردی ۱**

شماره الزام	نام الزام
توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.	
۱۰	**راهنمای کاربردی ۲**
سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.	
۱۱	**راهنمای کاربردی ۳**
سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه‌شده توسط محصول به‌صورت امن استفاده می‌گردد.	
۱۲	**راهنمای کاربردی ۴**
سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های در دسترس، به‌خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به‌صورت مناسبی تعیین نماید.	
۱۳	**راهنمای کاربردی ۵**
سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل محصول.	
۱۴	**راهنمای کاربردی ۶**
سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آن‌ها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.	
۱۵	**راهنمای کاربردی ۷**
سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا گردند.	

شماره الزام	نام الزام
۱۶	**راهنمای کاربردی ۸**
سند راهنمای کاربردی باید واضح و قابل‌فهم باشد	
۱۷	**راهنمای کاربردی ۹**
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌نماید.	

۷,۲,۲ راهنمای آماده‌سازی

شماره الزام	نام الزام
۱۸	**راهنمای آماده‌سازی ۱**
توسعه‌دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.	
۱۹	**راهنمای آماده‌سازی ۲**
مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه‌دهنده شرح دهند.	
۲۰	**راهنمای آماده‌سازی ۳**
مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکرشده در سند هدف امنیتی، شرح دهند.	
۲۱	**راهنمای آماده‌سازی ۴**
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.	

شماره الزام	نام الزام
۲۲	**راهنمای آماده‌سازی ۵**
ارزیاب باید رویه‌های آماده‌سازی شرح داده‌شده در سند را بکار ببرد تا تائید نماید، محصول می‌تواند به‌صورت امن برای عمل نمودن آماده شود.	

۷,۳ کلاس آزمون

آزمون محصول برای بررسی بخش‌های کارکردی سیستم و همچنین بخش‌هایی که طراحی و پیاده‌سازی آن‌ها برای سیستم دارای آسیب‌های امنیتی است، در نظر گرفته می‌شود. آزمون بخش‌های کارکردی سیستم از طریق خانواده ATE_IND؛ و آزمون بخش‌هایی که طراحی و پیاده‌سازی آسیب‌زایی دارند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) آزمون بر اساس کارکردی که برای محصول در نظر گرفته‌شده و واسط‌هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌گردد. نتایج آزمون و تحلیل آسیب‌پذیری باید در گزارش آزمون لحاظ شوند این مسئله در الزامات زیر در نظر گرفته‌شده است.

۷,۳,۱ آزمون مستقل

«آزمون مستقل» برای تائید عملکرد محصول که در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و مستندات «راهنمای سرپرست» ارائه‌شده، صورت می‌گیرند. هدف اصلی آزمون اطمینان از برآورده شدن الزامات کارکردی مشخص‌شده در سند هدف امنیتی است. ارزیاب باید در سند «گزارش آزمون»، طرح آزمون و نتایج آن را مستند نماید.

شماره الزام	نام الزام
۲۳	**آزمون مستقل ۱**
توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.	

شماره الزام	نام الزام
۲۴	**آزمون مستقل ۲**
محصول باید مناسب آزمودن باشد.	
۲۵	**آزمون مستقل ۳**
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، مؤلفه‌های محتوایی را برآورده می‌نماید.	
۲۶	**آزمون مستقل ۱**
ارزیاب باید زیرمجموعه‌ای از کارکرد امنیتی محصول را آزمون نماید تا تائید نماید که کارکرد امنیتی محصول به‌صورت مشخص‌شده عمل می‌نمایند.	

۷,۴ کلاس آسیب‌پذیری

۷,۴,۱ تحلیل آسیب‌پذیری

شماره الزام	نام الزام
۲۷	**آسیب‌پذیری ۱**
توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.	
۲۸	**آسیب‌پذیری ۲**
محصول باید مناسب آزمودن باشد.	
۲۹	**آسیب‌پذیری ۳**
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، تمام مؤلفه‌های محتوایی را برآورده می‌نماید.	

شماره الزام	نام الزام
۳۰	**آسیب‌پذیری ۴**
ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.	
۳۱	**آسیب‌پذیری ۵**
ارزیاب باید بر اساس آسیب‌پذیری‌های بالقوه شناسایی‌شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.	

۷,۵ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه‌شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی‌هایی از چرخه حیات محدود می‌گردد که توسط کاربر نهایی قابل‌مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه‌دهنده نقش کمرنگی در قابل‌اعتماد بودن محصول دارد، بلکه در این سطح اطمینان (EAL1) تنها به این اطلاعات نیاز است.

۷,۵,۱ قابلیت‌های پیکربندی

این مؤلفه جهت معرفی محصول به‌صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه‌شده، است (بدین معنی که جدا از برچسب‌گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به‌تنهایی، برچسب‌گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصول که توسط مرکز گواهی تائید شده است را به‌آسانی تشخیص دهد.

شماره الزام	نام الزام
۳۲	**برچسب‌گذاری محصول ۱**
توسعه‌دهنده باید محصول و مرجع محصول را ارائه نماید.	
۳۳	**برچسب‌گذاری محصول ۲**

شماره الزام	نام الزام
محصول باید با یک مرجع یکتا برچسب زده شود.	
۳۴	**برچسب‌گذاری محصول ۳**
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.	

۷,۵,۲ حوزه پیکربندی

شماره الزام	نام الزام
۳۵	**پوشش پیکربندی محصول ۱**
ارزیاب باید لیست پیکربندی محصول را ارائه نماید.	
۳۶	**پوشش پیکربندی محصول ۲**
لیست پیکربندی باید شامل خود محصول و مدارک موردنیاز توسط الزامات تضمین امنیتی باشد.	
۳۷	**پوشش پیکربندی محصول ۳**
لیست پیکربندی باید موارد پیکربندی را به‌صورت یکتا معرفی نماید.	
۳۸	**پوشش پیکربندی محصول ۴**
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.	

۸ پیوست یک: الزامات اختیاری

شماره الزام	نام الزام
۲۶	**مدیریت کلید رمزنگاری 3**
برنامه کاربردی باید قادر به تولید کلیدهای رمزنگاری متقارن با استفاده از تولیدکننده بیت تصادفی که در الزام شماره ۱ «تولید بیت تصادفی ۱» تعریف‌شده است باشد و اندازه کلید رمزنگاری مشخص‌شده [انتخاب: ۱۲۸ بیت، ۲۵۶ بیت] است. نکته کاربردی: کلیدهای متقارن برای تولید کلیدها در راستای کلید زنجیره مورداستفاده قرار می‌گیرند.	
۲۷	**الزامات پروتکلTLS Client/ احراز هویت دستی ۵**
برنامه کاربردی باید با استفاده از گواهی X.509v3 از احراز هویت متقابل (دوسویه) پشتیبانی نماید. **نکته کاربردی ۲۲:** در الزامات «پروتکل X509 (3)» استفاده از گواهی x.509v3 مطرح‌شده است. این الزام اشاره به این موضوع دارد که یک کلاینت باید قادر به ارائه یک گواهی به سرور TLS برای احراز هویت متقابل TLS باشد.	

۹ پیوست دوم: الزامات بر اساس انتخاب

شماره الزام	نام الزام
۲۸	**تولید بیت تصادفی ۳**
برنامه کاربردی باید تمام خدمات تولید بیت تصادفی قطعی را مطابق با استانداردهای زیر انجام دهد: [انتخاب:	

NIST Special Publication 800-90A با استفاده از [انتخاب: Hash_DRBG(any)، HMAC_DRBG(any)، CTR_DRBG(AES)]، FIPS Pub 140-2 پیوست C:X9.31 بخش ۲,۴ با استفاده از الگوریتم AES]
نکته کاربردی ۲۳:
این الزام بستگی به انتخاب‌هایی دارد که در الزام شماره ۱ «تولید بیت تصادفی ۱» صورت می‌گیرد.
۲۹ **تولید بیت تصادفی ۴**
تولید بیت تصادفی قطعی باید توسط یک منبع آنتروپی که آنتروپی‌های یک مولد بیت تصادفی قطعی وابسته به پلتفرم را تجمیع می‌کند و [انتخاب: یک منبع نرم‌افزاری نویز هیچ منبع نویز دیگری با [انتخاب: ۱۲۸ بیت، ۲۵۶ بیت] از آنتروپی، حداقل برابر با بالاترین قدرت امنیت (بر اساس NIST SP 800-57) از کلیدها و هش‌هایی که تولید می‌کند، پر شود.
۳۰ **مدیریت کلید رمزنگاری ۵**
برنامه کاربردی باید برای تولید کلید رمزنگاری یکی از اقدامات زیر را انجام دهد: [انتخاب: • هیچ کلید رمزنگاری نامتقارن تولید نشود، • فراخوانی کارکردهای ارائه‌شده توسط پلتفرم برای تولید کلید نامتقارن، • پیاده‌سازی نمودن تولید کلید نامتقارن]
نکته کاربردی ۲۴:
این الزام بستگی به انتخابی دارد که در الزام شماره‌های ۳۷ تا ۴۰ «پروتکل «TLSC صورت می‌گیرد. در صورت انتخاب دو گزینه «پیاده‌سازی تولید کلید نامتقارن» و «فراخوانی کارکردهای ارائه‌شده توسط پلتفرم برای تولید کلید نامتقارن»، لازم است الزام شماره ۳۱ «مدیریت کلید رمزنگاری» در سند «هدف امنیتی» در نظر گرفته شود.

۳۱	مدیریت کلید رمزنگاری ۱

برنامه کاربردی باید کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم زیر تولید نماید:

[انتخاب:

طرح RSA با استفاده از اندازه کلید رمزنگاری [۲۰۴۸ بیت یا بیشتر] که استانداردهای زیر را برآورده می‌نماید:

[انتخاب:

استاندارد FIPS PUB 186-4، «استاندارد امضای دیجیتال»، پیوست B.3

استاندارد ANSI X9.31-1998، بخش ۴,۱

]،

طرح ECC با استفاده از [منحنی‌های P-256، P-384 و [انتخاب: P-521، هیچ منحنی دیگر]] که استانداردهای زیر را برآورده می‌نماید:

[استاندارد FIPS PUB 186-4، «استاندارد امضای دیجیتال»، پیوست B.4]

طرح FFC با استفاده از اندازه کلیدهای [۲۰۴۸ بیت یا بیشتر] که استانداردهای زیر را برآورده می‌کند:

[استاندارد FIPS PUB 186-4، «استاندارد امضای دیجیتال»، پیوست B.1]

نکته کاربردی ۲۵:

این الزام بستگی به انتخاب در الزام شماره ۳۰ «مدیریت کلید رمزنگاری ۵» دارد. نویسنده سند هدف امنیتی باید طرح‌های تولید کلید مورداستفاده استقرار کلید و احراز هویت را انتخاب نماید. زمانی که کلید تولیدشده برای استقرار کلید استفاده می‌شود، طرح‌های مطرح‌شده در الزام شماره ۳۲ « مدیریت کلید رمزنگاری ۲» و پروتکل‌های رمزنگاری انتخاب‌شده باید با انتخاب‌ها در این الزام منطبق باشند. زمانی که کلید تولیدشده برای احراز هویت استفاده می‌شود، کلید عمومی با گواهی X.509v3 همراه می‌گردد.

درصورتی‌که محصول به‌عنوان گیرنده در طرح برقراری کلید RSA عمل نماید، لزومی به پیاده‌سازی تولید کلید RSA در محصول نیست.

۳۲	مدیریت کلید رمزنگاری ۲

برنامه کاربردی باید [انتخاب: درخواست نمودن کارکردی که پلتفرم ارائه می‌دهد، پیاده‌سازی کارکرد] برای استقرار کلید رمزنگاری مطابق با طرح‌های استقرار کلید مبتنی بر RSA که استانداردهای زیر را برآورده می‌نماید:

NIST SP 800-56B و [انتخاب:

طرح برقراری کلید مبتنی بر منحنی بیضوی که برآورده کننده استاندارد NIST SP 800-56A،
طرح برقراری کلید مبتنی بر میدان متناهی که برآورده کننده استاندارد NIST SP 800-56A،
هیچ طرح دیگر]

نکته کاربردی ۲۶:

این الزام به انتخاب صورت گرفته در الزام شماره ۳۷ «پروتکل TLSC(۱)» بستگی دارد.

نویسنده سند هدف امنیتی باید با توجه به پروتکل رمزنگاری مورداستفاده، طرح‌های برقراری کلید را انتخاب نماید. الزام شماره ۳۷ «پروتکل TLSC» مجموعه رمزنگاری‌ها را ملزم می‌نماید که از طرح‌های برقراری کلید مبتنی بر RSA استفاده نمایند.

طرح‌های برقراری کلید مبتنی بر RSA در فصل نهم استاندارد NIST SP 800-56B شرح داده شده‌اند. هرچند این فصل مبتنی بر پیاده‌سازی دیگر فصول این استاندارد است. درصورتی‌که محصول به‌عنوان یک گیرنده در طرح برقراری کلید عمل نماید، لزومی به پیاده‌سازی تولید کلید RSA در محصول نیست.

منحنی‌های بیضوی مورداستفاده برای طرح برقراری کلید باید با منحنی‌های مشخص‌شده در الزام شماره ۳۱ «مدیریت کلید رمزنگاری ۱» همبسته شوند.

دامنه پارامترهای مورداستفاده برای طرح برقراری کلید مبتنی بر میدان متناهی توسط تولید کلید در الزام شماره ۳۱«مدیریت کلید رمزنگاری ۱» مشخص می‌گردد.

۳۳	**عملیات رمزنگاری – رمزنگاری/رمزگشایی ۱ (۱)**

برنامه کاربردی باید رمزنگاری/رمزگشایی را مطابق با الگوریتم‌های رمزنگاری زیر انجام دهد:

AES-CBC mode(به صورتی که در NIST SP 800-38A تعریف‌شده)،

و [انتخاب:

AES-GCM(به صورتی که در NIST SP 800-38D تعریف‌شده)،

هیچ مد دیگر]

و اندازه کلید رمزنگاری 128 بیت و [انتخاب: ۲۵۶ بیت، هیچ اندازه دیگر]

نکته کاربردی ۲۷:

این الزام بستگی به انتخاب در الزام شماره ۳۷ « پروتکل TLSC(۱)» دارد. در اولین «انتخاب» نویسنده سند هدف امنیتی باید مد یا مدهایی را انتخاب نماید که AES در آن مد عمل می‌نماید. برای «انتخاب» دوم، نویسنده سند هدف امنیتی باید اندازه کلیدی را انتخاب نماید که توسط این کارکرد پشتیبانی می‌شود.	
۳۴	**عملیات رمزنگاری – درهم‌سازی ۱ (۲)**
برنامه کاربردی باید خدمات درهم‌سازی رمزنگاری را مطابق با الگوریتم درهم‌سازی SHA-1 و [انتخاب: SHA-256، SHA-384، SHA-512، هیچ الگوریتم دیگر] و اندازه چکیده پیام ۱۶۰ و [انتخاب: ۲۵۶، ۳۸۴، ۵۱۲، هیچ اندازه چکیده پیام دیگر] بیت انجام دهد که استاندارد FIPS Pub 180-4 را برآورده می‌نماید. **نکته کاربردی ۲۸:** این الزام بستگی به انتخاب در الزام شماره ۳۷ « پروتکل TLSC(۱)» دارد. NIST SP 800-131A، SHA-1 برای تولید امضای دیجیتال مجاز نیست و SHA-1 برای تائید امضای دیجیتال پیشنهاد نمی‌شود چراکه ممکن است در قبول این امضاها ریسک وجود داشته باشد.	
۳۵	**عملیات رمزنگاری – امضاء ۱ (۳)**
برنامه کاربردی باید خدمات امضاء رمزنگاری (تولید و وارسی) را مطابق با الگوریتم رمزنگاری زیر انجام دهد: [انتخاب: طرح RSA با استفاده از اندازه کلید رمزنگاری ۲۰۴۸ بیت یا بزرگ‌تر که برآورده‌کننده‌ی استاندارد FIPS PUB 186-4 «استاندارد امضای دیجیتال DSS»، بخش چهارم است، طرح ECDSA با استفاده از «منحنی NIST»P-256، P-384 و [انتخاب: P-521، هیچ منحنی دیگر] که برآورده‌کننده‌ی استاندارد FIPS PUB 186-4 «استاندارد امضای دیجیتال DSS»، بخش پنجم است] **نکته کاربردی ۲۹:**	

این الزام بستگی به انتخاب در الزام شماره ۳۴ « عملیات رمزنگاری – درهم‌سازی ۱ (۲)» دارد. نویسنده سند هدف امنیتی باید برای انجام امضای دیجیتال، الگوریتم پیاده‌سازی شده‌ای را انتخاب نماید. در صورت وجود یک الگوریتم در دسترس، این الزام باید «تکرار» شود تا کارکرد مشخص گردد. برای الگوریتم انتخاب‌شده، نویسنده سند هدف امنیتی باید در قسمت «انتخاب» و «اختصاص» پارامترهای مناسبی را برای پیاده‌سازی آن الگوریتم انتخاب نماید.

۳۶	**عملیات رمزنگاری – امضاء ۱ (۴)**

برنامه کاربردی باید کد اصالت‌سنجی پیام بر پایه درهم‌سازی (HMAC) مطابق با الگوریتم رمزنگاری HMAC-SHA-256 و [انتخاب:SHA-1، SHA-384، SHA-512، هیچ الگوریتم دیگر] با اندازه کلید [اختصاص: اندازه کلید استفاده شده در HMAC] و اندازه خلاصه پیام ۲۵۶ بیت و [انتخاب: ۱۶۰، ۳۸۴، ۵۱۲، هیچ اندازه دیگر] انجام دهد که استاندارد FIPS Pub 198-1 «کد اصالت‌سنجی پیام بر پایه درهم‌سازی» و استاندارد FIPS Pub 180-4 «استاندارد درهم‌سازی امن» را برآورده می‌نماید.

نکته کاربردی ۳۰:

این الزام بستگی به انتخاب در الزام شماره ۳۷ «پروتکل TLSC(۱)» دارد. منظور این الزام مشخص نمودن کارکرد اصالت‌سنجی پیام بر پایه درهم‌سازی است که به‌منظور برقراری کلید برای پروتکل‌های رمزنگاری مختلف به‌کاررفته در برنامه کاربردی استفاده می‌شود (به‌طور مثال، کانال امن). انتخاب درهم‌سازی باید از انتخاب اندازه خلاصه پیام پشتیبانی نماید.

۳۷	**پروتکل TLSC(۱)**

برنامه کاربردی باید با پشتیبانی از مجموعه رمز[۱] لیست شده در زیر، [انتخاب: TLS 1.2 ارائه‌شده توسط پلتفرم را درخواست نماید، TLS 1.2(RFC 5246) پیاده‌سازی نماید]

مجموعه رمز الزامی:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA به‌صورت تعریف‌شده در RFC 5246

مجموعه رمز اختیاری:

[۱] CipherSuite

TLS_DHE_RSA_WITH_AES_128_CBC_SHA به‌صورت تعریف‌شده در RFC 5246،
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246،
TLS_DHE_RSA_WITH_AES_256_CBC_SHA به‌صورت تعریف‌شده در RFC 5246،
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246،
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA به‌صورت تعریف‌شده در RFC 4492،
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5289،
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 به‌صورت تعریف‌شده در RFC 5289،
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA به‌صورت تعریف‌شده در RFC 4492،
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 به‌صورت تعریف‌شده در RFC 5289،
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 به‌صورت تعریف‌شده در RFC 5289،
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA به‌صورت تعریف‌شده در RFC 4492،
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 به‌صورت تعریف‌شده در RFC 5289،
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA به‌صورت تعریف‌شده در RFC 4492،
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 به‌صورت تعریف‌شده در RFC 5289،
TLS_RSA_WITH_AES_128_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246،
TLS_RSA_WITH_AES_256_CBC_SHA به‌صورت تعریف‌شده در RFC 5246،
TLS_RSA_WITH_AES_256_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246،
هیچ مجموعه رمز دیگر]

نکته کاربردی ۳۱:

این الزام بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها» دارد.

این الزام محدود به منحنی‌های بیضوی مجاز برای احراز هویت و توافق کلید بر اساس منحنی‌های بیضوی از الزام شماره ۳۵ «عملیات رمزنگاری – امضاء ۱ (۳)» و الزام شماره۳۱ و۳۲ « مدیریت کلید رمزنگاری ۱» و « مدیریت کلید رمزنگاری ۲» است.	
پروتکل TLSC(۲)	**۳۸**
برنامه کاربردی باید منطبق بودن شناسه ارائه‌شده با شناسه مرجع را بر طبق RFC 6125 وارسی نماید. **برنامه کاربردی ۳۲:** این الزام بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها ۱» دارد. در بخش ۶ از RFC 6125 قوانینی برای وارسی هویت شرح داده‌شده است. شناسه مرجع با توجه به سرویس برنامه کاربردی توسط کاربر (به‌طور مثال، وارد نمودن یک URL در مرورگر وب یا کلیک نمودن یک لینک)، توسط پیکربندی (به‌طور مثال، پیکربندی نمودن نام یک سرور پست الکترونیک یا سرور احراز هویت) یا توسط برنامه کاربردی (به‌طور مثال، یک پارامتر از یک API) استقرار می‌یابد. بر اساس دامنه منبع شناسه مرجع منحصربه‌فرد و نوع سرویس برنامه کاربردی (به‌طور مثال، HTTP، SIP، LDAP)، کلاینت تمام شناسه‌های مرجع قابل‌پذیرش را برقرار می‌نماید، همچون نام رایجی برای فیلد Subject Name گواهی، نام DNS، نام URI و نام سرویس برای فیلد Alternative Name. کلاینت سپس این لیست از تمام شناسه‌های مرجع را با شناسه‌های ارائه‌شده در گواهی سرور TLS مقایسه می‌نماید. روش ارجح برای وارسی Subject Alternative Name با استفاده از نام‌های DNS، نام‌های URI یا نام‌های سرویس است. وارسی با استفاده از نام رایج به جهت مقایسه، لازم و ضروری است. علاوه بر این، پشتیبانی از استفاده از آدرس IP در Subject Name یا Subject Alternative Name به‌عنوان بهترین تجربه شناخته‌نشده است اما ممکن است پیاده‌سازی شود.	
پروتکل TLSC(۳)	**۳۹**
برنامه کاربردی باید در صورت معتبر بودن گواهی همتا، تنها یک کانال امن برقرار نماید. **نکته کاربردی ۳۳:** این الزام بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها ۱» دارد. اعتبار تعیین‌شده توسط وارسی شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت لغو مطابق با RFC 5280 تعیین می‌شود. اعتبار گواهی باید مطابق با آزمون انجام‌شده برای الزامات پروتکل X509 (۱) بررسی گردد.	

برای اتصالات TLS در صورت نامعتبر بودن گواهی همتا، این کانال نباید برقرار شود. لازم به ذکر است این الزام برای اتصالات TLS بدون پروتکل HTTPS است.	
پروتکل TLSC(۷)	**۴۰**
برنامه کاربردی باید بسط‌های منحنی بیضوی پشتیبانی شده در مرحله Hello کلاینت را بر اساس منحنی‌های NIST [انتخاب: secp256r1 ، secp521r1، secp384r1] ارائه دهد. **نکته کاربردی ۳۴:** این الزام بستگی به انتخاب در الزام شماره ۳۷ «پروتکل TLSC(۱)» دارد. این الزام منحنی بیضوی‌های مجاز برای احراز هویت و توافق کلید را به منحنی‌های NISTشامل الزامات شماره ۳۱و ۳۲و ۳۵ (عملیات رمزنگاری – امضاء ۱ (۳)، مدیریت کلید رمزنگاری ۱ و مدیریت کلید رمزنگاری۲) محدود می‌کند. این بسط برای کلاینتی که مجموعه رمز منحنی بیضوی را پشتیبانی می‌کند لازم است.	
الزامات پروتکلTLS Server/ احراز هویت ۱	**۴۱**
برنامه کاربردی باید [انتخاب: TLS1.2 وابسته به پلتفرم را فراخوانی کند TLS1.2 را پیاده‌سازی کند که از مجموعه رمزهای زیر پشتیبانی می‌کند: مجموعه رمزهای اجباری: TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246 مجموعه رمزهای اختیاری:[انتخاب: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,	

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246]
۴۲ **الزامات پروتکلTLS Server/ احراز هویت ۲**
برنامه کاربردی باید اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و [انتخاب: TLS1.1، TLS1.2، هیچ‌کدام] دارند، رد نماید. **نکته کاربردی ۳۵:** تمام نسخه‌های SSL و نسخه TLS 1.0 رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در الزام شماره ۴۱ «پروتکلTLS Server/ احراز هویت ۱» انتخاب‌نشده است، در اینجا انتخاب شود.
۴۳ **الزامات پروتکلTLS Server/ احراز هویت ۳**
برنامه کاربردی باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت و [انتخاب: ۳۰۷۲ بیت، ۴۰۹۶ بیت، یا هیچ اندازه دیگری] و [انتخاب: منحنی‌های NIST [انتخاب: secp256r1, secp384r1] و هیچ منحنی دیگری، اندازه‌های پارامتر Diffie-Hellman و [انتخاب: ۳۰۷۲بیت، هیچ اندازه دیگری]] ایجاد نماید. **نکته کاربردی ۳۶:** اگر در الزام شماره ۴۱ « الزامات پروتکلTLS Server/ احراز هویت ۱» سند هدف امنیتی مجموعه رمزهای DHE یا ECDHE لیست شده باشند، سند هدف امنیتی باید شامل Diffie-Hellman یا منحنی‌هایNIST لیست شده در این الزام باشد. کارکرد مدیریتی محصول برای ایجاد امنیت در اتصال TLS، به پارامترهای توافقی کلید نیاز دارد.
۴۴ **الزامات پروتکلTLS Server/ احراز هویت ۴**
محصول باید با استفاده از گواهی‌های نسخه سوم X.۵۰۹ احراز هویت دوسویه کاربران TLS را پشتیبانی نماید.

۴۵	الزامات پروتکلTLS Server/ احراز هویت ۵
درصورتی‌که گواهی همتا معتبر نباشد، برنامه کاربردی نباید کانال امن را برقرار سازد. **نکته کاربردی ۳۷:** استفاده از گواهی‌های نسخه سوم X.509 برای محصول در الزام شماره ۵۳ «الزامات پروتکلX.509» توضیح داده‌شده است. در کنار این الزام، باید در این استفاده گواهی‌های کلاینت نیز برای احراز هویت دوسویه پشتیبانی شوند.	
۴۶	الزامات پروتکلTLS Server/ احراز هویت ۶
درصورتی‌که نام مشخص‌شده[۱] (DN) یا نام مستعار موجودیت فعال[۲] (SAN) در یک گواهی با شناسه مورد انتظار برای همتا مطابقت نداشته باشد، برنامه کاربردی نباید کانال امن را برقرار سازد. **نکته کاربردی ۳۸:** ممکن است شناسه همتا در قسمت موجودیت فعال یا افزونه نام مستعار موجودیت فعال از گواهی ذکرشده باشد. شناسه مورد انتظار ممکن است پیکربندی شود، با نام دامنه، آدرس IP، نام کاربری یا آدرس ایمیل استفاده‌شده توسط همتا مقایسه شود یا به‌منظور مقایسه به یک سرور دایرکتوری ارسال شود. برای این منظور مقایسه بیتی انجام می‌شود.	
۴۷	پروتکل DTLS(۱)
برنامه کاربردی باید پروتکل DTLS را مطابق با DTLS 1.2(RFC 6347) پیاده‌سازی نماید. **نکته کاربردی ۳۹:** این الزام بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها ۱» دارد.	

[۱] Distinguished name

[۲] Subject Alternative Name

۴۸	**پروتکل DTLS(۲)**
برنامه کاربردی باید جهت پیاده‌سازی پروتکل DTLS، الزام شماره ۳۷ (الزام پروتکل TLSC(۱)) را پیاده‌سازی نماید، مگر آنکه تغییرات مطابق با DTLS 1.2 (RFC 6347) مجاز باشد. **نکته کاربردی ۴۰:** الزامات بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها ۱» دارد. تفاوت بین دو پروتکل DTLS1.2 و TLS 1.2 در RFC 6347 فهرست شده است؛ هرچند این دو پروتکل مشابه هستند. بالاخص در زمینه امنیت تعریف‌شده برای محصول، دو پروتکل تفاوتی با هم ندارند؛ بنابراین، تمام نکات کاربردی که برای TLS مطرح‌شده برای پیاده‌سازی DTLS نیز کاربرد دارد.	
۴۹	**پروتکل DTLS(۳)**
برنامه کاربردی درصورتی‌که به نظر آید گواهی همتا نامعتبر است، نباید کانال ارتباطی امنی را برقرار نماید. **نکته کاربردی ۴۱:** این الزام بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها ۱» دارد. اعتبار گواهی توسط مسیر گواهی، تاریخ انقضاء، وضعیت لغو مطابق با RFC 5280 تعیین می‌گردد.	
۵۰	**پروتکل HTTPS(۱)**
برنامه کاربردی باید پروتکل HTTPS را مطابق با RFC 2818 پیاده‌سازی نماید. **نکته کاربردی ۴۲:** این الزام بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها ۱» دارد.	
۵۱	**پروتکل HTTPS(۲)**
برنامه کاربردی باید پروتکل HTTPS را با استفاده از TLS، الزام شماره ۳۷ «پروتکل TLSC(۱)» پیاده‌سازی نماید.	

۵۲	پروتکل HTTPS(۳)
برنامه کاربردی باید درصورتی‌که گواهی همتا به نظر نامعتبر آید به کاربر اطلاع دهد و [انتخاب: اتصال را برقرار ننماید، جهت برقراری اتصال مجوز برنامه کاربردی درخواست گردد، هیچ اقدام دیگر]. **نکته کاربردی ۴۳:** این الزام بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها ۱» دارد. اعتبار گواهی توسط مسیر گواهی، تاریخ انقضاء، وضعیت لغو مطابق با RFC 5280 تعیین می‌گردد.	
۵۳	**الزامات پروتکل X509 (۱)**
برنامه کاربردی باید [انتخاب: کارکرد ارائه‌شده توسط پلتفرم را درخواست نماید، کارکردی را پیاده‌سازی نماید] تا مطابق با قوانین زیر، گواهی‌ها را معتبر نماید: • اعتبارسنجی گواهی و مسیر گواهی RFC 5280 • مسیر گواهی باید با یک گواهی CA امن خاتمه یابد. • برنامه کاربردی باید مسیر گواهی را اعتبارسنجی نماید با تضمین نمودن وجود آیتم basicConstraints و اینکه پرچم CA برای تمامی گواهینامه‌ها وضعیت TRUE داشته باشد. • برنامه کاربردی باید وضعیت لغو گواهی را با استفاده از [انتخاب: پروتکل وضعیت گواهی آنلاین (OCSP[۱]) به‌صورت مشخص‌شده در RFC 2560، لیست لغو گواهی (CRL[۲]) به‌صورت مشخص‌شده در RFC 5759] • برنامه کاربردی باید فیلد extendedKeyUsage را مطابق با قوانین زیر اعتبارسنجی نماید: ○ گواهی استفاده شده برای به‌روزرسانی امن و بررسی صحت کد اجرایی باید در فیلد extendedKeyUsage دارای هدف Code Signing باشد (id-kp 3 با OID 1.3.6.1.5.5.7.3.3) ○ گواهی‌های سرور ارائه‌شده برای TLS باید در فیلد extendedKeyUsage دارای هدف احراز هویت سرور باشد (id-kp 1 با OID 1.3.6.1.5.5.7.3.1)	

[۱] Online Certificate Status Protocol

[۲] Certificate Revocation List

- گواهی‌های کلاینت ارائه‌شده برای TLS باید در فیلد extendedKeyUsage دارای هدف احراز هویت کلاینت باشد (id-kp 2 با OID 1.3.6.1.5.5.7.3.2)
- گواهی‌های S/MIME ارائه‌شده برای امضاء و رمزنگاری ایمیل باید در فیلد extendedKeyUsage دارای هدف حفاظت از ایمیل باشد (id-kp 4 با OID 1.3.6.1.5.5.7.3.4)
- گواهی‌های OCSP ارائه شده برای پاسخ‌های OCSP باید در فیلد extendedKeyUsage دارای هدف امضای OCSP باشد (id-kp 9 با OID 1.3.6.1.5.5.7.3.9)
- گواهی‌های سرور ارائه شده برای EST باید در فیلد extendedKeyUsage دارای هدف مرکز ثبت گواهی CMC باشد (id-kp-cmcRA با OID 1.3.6.1.5.5.7.3.28)

نکته کاربردی ۴۴:

این الزام بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها ۱» دارد. این الزام قوانینی برای معتبر نمودن گواهی لیست نموده است. نویسنده سند هدف امنیتی باید انتخاب نماید که وضعیت ابطال گواهی با استفاده از OCSP یا CRL بررسی می‌گردد. الزام شماره ۵۵ « پروتکل X509 (۳)» ملزم می‌نماید که گواهی‌ها برای پروتکل‌های HTTPS، TLS و DTLS استفاده گردد و بدین ترتیب بررسی قوانین ExtendedKeyUsage ملزم می‌گردد.

۵۴	**الزامات پروتکل X509 (۲)**

برنامه کاربردی باید در صورت وجود basicConstraints extension و true بودن CA Flag، گواهی را به‌عنوان گواهی CA تلقی نماید.

نکته کاربردی ۴۵:

این الزام بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها ۱» دارد. این الزام به گواهی‌های که توسط محصول استفاده و پردازش می‌شود، اعمال می‌گردد و گواهی‌هایی که ممکن است به‌عنوان گواهی CA مورد اعتماد اضافه شوند را محدود می‌نماید.

۵۵	**الزامات پروتکل X509 (۳)**

برنامه کاربردی باید از گواهی X.509v3 به‌صورت تعریف‌شده توسط RFC 5280 استفاده نماید تا از احراز هویت برای [انتخاب: HTTPS، TLS، DTLS] پشتیبانی نماید.

نکته کاربردی ۴۶:

این الزام بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها ۱» دارد. انتخاب نویسنده سند هدف امنیتی باید با انتخاب در الزام شماره ۲۵ منطبق باشد.

۵۶	**الزامات پروتکل X509 (۴)**

زمانی که برنامه کاربردی نمی‌تواند جهت تعیین اعتبار گواهی، اتصالی را برقرار نماید؛ برنامه کاربردی باید [انتخاب: پذیرش گواهی در این مورد به سرپرست داده می‌شود، گواهی پذیرفته می‌شود، گواهی پذیرفته نمی‌شود].

نکته کاربردی ۴۷:

این الزام بستگی به انتخاب در الزام شماره ۲۵ «حفاظت از تبادل داده‌ها ۱» دارد. غالباً یک اتصال باید برقرار شود تا وضعیت لغو گواهی بررسی شود (یا با دانلود CRL یا با OCSP). انتخابات صورت گرفته در این الزام بیانگر رفتار در زمانی است که یک اتصال نمی‌تواند برقرار شود. درصورتی‌که محصول مشخص نماید که گواهی مطابق با تمام قوانین در الزام شماره ۵۳ «الزامات پروتکل X509 (۱)» معتبر است، رفتار مشخص‌شده در انتخاب باید تعیین‌کننده اعتبار باشد. محصول تنها در شرایطی نباید گواهی را بپذیرد که هریک از قوانین اعتبارسنجی در الزام شماره ۵۳ «الزامات پروتکل X509 (۱)» رد گردد.

۱۰ پیوست سوم: الزامات اضافی

این پیوست شامل الزامات کارکرد امنیتی است که باعث کاهش تهدیدات محصول می‌گردد. در حال حاضر استفاده از این الزامات در پروفایل حفاظتی به اجباری نیست. با این حال این الزامات می‌تواند در سند هدف امنیتی آورده شود که با الزامات پروفایل حفاظتی سازگار است.

شماره الزام	نام الزام
۵۷	**پروتکل TLSS(۶)**

برنامه کاربردی باید افزونه الگوریتم‌های امضای دیجیتال را به همراه مقادیر الگوریتم‌های امضای دیجیتال مورد پشتیبانی شامل الگوریتم‌های درهم‌سازی [انتخاب: SHA256, SHA384, SHA512] و هیچ الگوریتم‌های درهم‌ساز دیگری] در پیام ClientHello ارائه دهد.

نکته کاربردی ۴۸:

این الزامات الگوریتم‌های درهم‌ساز مورد پشتیبان را برای اهداف وارسی امضای دیجیتال از طریق کلاینت‌ها محدود می‌کند و همچنین درهم‌سازهای پشتیبانی شده توسط سرور برای اهداف تولید امضای دیجیتال محدود می‌نماید. افزونه الگوریتم دیجیتال تنها برای TLS1.2 پشتیبانی می‌شود.

۵۸	**استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۲**

برنامه کاربردی برای تجزیه[۱][انتخاب: باید از کتابخانه‌های فراهم‌شده توسط پلتفرم استفاده کند، هیچ کارکردی را پیاده‌سازی نکند] و [اختصاص: شامل فهرستی از قالب‌های تجزیه که در انواع داده رسانه‌ای IANA MIME است باشند.]

نکته کاربردی ۴۹:

انواع داده IANA MIME در ht tp:// /www.iana.org/assignments/media-types لیست شده‌اند و شامل قالب‌های عکس، صوت، ویدئو و محتوای فایل هستند.

۵۹	**شناسایی نرم‌افزار و نسخه‌ها ۱**

برنامه کاربردی باید شامل تگ‌های SWID باشد و با حداقل‌ترین الزامات تگ‌هایSWID و استاندارد ISO/ IEC 19770-2:2009سازگار باشد.

نکته کاربردی ۵۰:

تگ‌های معتبر SWID باید شامل یک عنصر Sof twareIdentit y و یک عنصر Entity همان‌گونه که در استاندارد ISO/ IEC 19770-2:2009تعریف‌شده است باشد. تگ‌های SWID باید در فایل با پسوند swidtag که در استاندارد ISO/ IEC 19770-2:2009 است ذخیره گردد.

[۱] Parsing