به نام خدا

پروفایل حفاظتی تجهیزات شبکه

مهرماه ۹۵

نسخه ۲,۰

پیشگفتار

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 مدیریت راهبردی افتا با مشارکت سازمان فناوری اطلاعات ایران این سند را در راستای این اهداف تهیه نموده است. این سند معرفی کننده‌ی الزامات کارکرد امنیتی برای تجهیزات شبکه می‌باشد تا تولیدکنندگان محصولات تجهیزات شبکه بتوانند بر مبنای این سند، کارکردهای امنیتی را در محصول خود لحاظ نموده و همچنین سند هدف امنیتی آن را ارائه نمایند.

در بخش اول به معرفی تجهیزات شبکه پرداخته‌شده است. سپس در بخش «اهداف امنیتی» مواردی جهت مقابله با تهدیدات، اجرای خط‌مشی‌ها و بکار بردن فرضیات مطرح می‌گردد. در بخش بعدی «الزامات کارکرد امنیتی» آورده شده؛ بر اساس استاندارد ارزیابی معیار مشترک این قسمت از چندین کلاس تشکیل‌شده است که هریک از این کلاس‌ها حوزه‌ی خاصی از امنیت را پوشش می‌دهد. کلاس‌هایی که برای تجهیزات شبکه در این سند مطرح‌شده است، عبارت‌اند از:

- کلاس ممیزی امنیت
- کلاس پشتیبانی از رمزنگاری
- کلاس حفاظت از داده‌های کاربری
- کلاس شناسایی و احراز هویت
- کلاس مدیریت امنیت
- کلاس حفاظت از توابع امنیتی هدف ارزیابی
- کلاس دسترسی به هدف ارزیابی
- کلاس کانال‌ها / مسیرهای مورد اعتماد

هریک از این کلاس‌ها، از مجموعه‌ای از خانواده‌ها تشکیل یافته و هر خانواده از مجموعه‌ای عنصر و هر عنصر از مجموعه‌ای مؤلفه تشکیل یافته است. با استفاده از «الزامات کارکرد امنیتی» درواقع «اهداف امنیتی» بر مبنای استاندارد معیار مشترک بیان می‌گردد.

در بخش پایانی «الزامات تضمین امنیتی» که از ساختاری مشابه بخش قبلی برخوردار است مطرح گردیده است، این بخش الزامات لازم جهت ارزیابی محصول را عنوان می‌نماید.

فهرست

۱ شرح محصول تجهیزات شبکه

سند حاضر، پروفایل حفاظتی برای ارزیابی محصولی است که به‌عنوان یک دستگاه شبکه شناخته می‌شود. منظور از یک دستگاه شبکه در این پروفایل حفاظتی، دستگاهی متشکل از سخت‌افزار و نرم‌افزار می‌باشد که به شبکه متصل است و یک نقش زیرساخت را در شبکه فراهم می‌آورد.

این پروفایل حفاظتی، مجموعه‌ای از حداقل الزامات امنیتی را ارائه می‌کند که دستگاه‌های شبکه باید به‌منظور کاهش تهدیدات، آن‌ها را رعایت نمایند. این الزامات اولیه برای هر نوع از تجهیزات شبکه است و سایر الزامات آن از اسناد پروفایل حفاظتی اختصاصی آن محصول تکمیل خواهد شد تا مجموعه‌ای از روش‌های امنیتی را برای شبکه‌های سازمانی فراهم آورند. هدف سند حاضر این است که مجموعه‌ای از کارکردهای امنیتی معمول را ارائه کند که تمام شبکه‌ها، صرف‌نظر از کارکرد خاص هر تجهیزات شبکه‌ای یا هرگونه ابزار امنیتی اضافه، باید آن‌ها را بکار گیرند. این مجموعه اولیه کارکردهای امنیتی، شامل مواردی ازجمله حفاظت از تمام مسیرهای مدیریتی راه دور، ارائه خدمات شناسایی و احراز هویت برای ورودهای محلی و راه دور، ممیزی رویدادهای امنیتی، تأیید رمزنگاری امن تمام به‌روزرسانی‌ها و حفاظت در برابر حملات مرسوم به شبکه است. هدف این است که تمام دستگاه‌های شبکه که در حیطه شمول این پروفایل حفاظتی قرار می‌گیرند، به گونه مناسبی در شبکه «رفتار» کنند و آسیبی را به شبکه وارد ننمایند. بدین منظور، انتظار می‌رود که دستگاه شبکه از پروتکل‌های استانداردی مانند IPsec یا TLS یا SSH استفاده کند و بدین ترتیب از مسیرهای ارتباطی برقرارشده با موجودیت‌های خارجی محافظت نماید. همچنین لازم است که گواهی‌نامه‌های X.509 به‌منظور احراز هویت مورداستفاده قرار گیرند. استفاده از این گواهی‌نامه‌ها گزینه‌ای برای امضای دیجیتال و امضای کد است.

محصولات توزیع‌شده در دامنه شمول این پروفایل حفاظتی قرار نمی‌گیرند، اما انتظار می‌رود که در پروفایل حفاظتی آینده به آن‌ها پرداخته شود. کارکردهای امنیتی اضافه‌ای که ممکن است نوع خاصی از دستگاه‌های شبکه بکار گیرند، نیز در دامنه شمول این پروفایل حفاظتی قرار نمی‌گیرد، بلکه در سایر پروفایل‌های حفاظتی مربوط به انواع مختلف دستگاه‌ها پوشش داده خواهند شد. علاوه بر این، اسکن ویروس‌ها و ایمیل‌ها، قابلیت‌های تشخیص و جلوگیری از نفوذ[۱]، ترجمه آدرس شبکه[۲] (NAT) به‌عنوان یک کارکرد امنیتی و کارکردهای شبکه مجازی نیز در دامنه شمول این پروفایل حفاظتی قرار نمی‌گیرند. انتظار می‌رود که این پروفایل حفاظتی توسعه یابد و مواردی ازجمله افزایش قابلیت انعطاف، کاربردهای مختلف و انطباق با فناوری‌های جدید را پوشش دهد. در حال حاضر تجهیزات شبکه باید به‌طور کامل از این پروفایل حفاظتی تبعیت نمایند.

---

۱ [ntrusion detection/prevention

۲ Network Address Translation

۱,۱ موارد کاربرد محصول

نکته اصلی در الزامات اهداف ارزیابی دستگاه‌های شبکه این است که این دستگاه‌ها را می‌توان از راه دور به‌طور امن مدیریت کرد و تمامی به‌روزرسانی‌های مورداستفاده از منابع امن تأمین می‌شوند. به‌عنوان مثالی از دستگاه‌های شبکه که الزامات این پروفایل حفاظتی در مورد آن‌ها صدق می‌کند، می‌توان به مسیریاب‌ها، فایروال‌ها، دروازه‌های VPN، IDS ها و سوئیچ‌ها اشاره کرد. درصورتی‌که این دستگاه‌ها دارای کارکردهای مهم دیگری باشند که الزامات امنیتی خاص خود را داشته باشند، پروفایل حفاظتی دیگری تهیه می‌شود که به آن موارد پرداخته باشد. پروفایل حفاظتی مذکور، مجموعه گسترده‌تری از الزامات را برای دستگاه‌های شبکه شامل خواهد شد. به‌عنوان‌مثال، یک پروفایل حفاظتی جداگانه برای فایروال‌های فیلتر ترافیک حالت‌مند[۱] تهیه‌شده است. برخی دستگاه‌ها نیز به شبکه متصل می‌شوند، اما بر اساس این پروفایل حفاظتی ارزیابی نمی‌گردند. به‌عنوان‌مثال، می‌توان به دستگاه‌های همراه، ایستگاه‌های کاری کاربر نهایی و کارکرد دستگاه شبکه مجازی اشاره کرد.

۲ تعریف مسائل امنیتی

هر دستگاه شبکه باید نقش خود را به عنوان یک زیرساخت شبکه ایفا نماید. ب منظور ایفای این نقش، دستگاه مذکور ارتباطاتی را از طریق شبکه با دیگر دستگاه‌های شبکه و سایر موجودیت‌های شبکه (موجودیتی که به عنوان یک دستگاه شبکه تعریف نشده است) برقرار می‌نماید. در عین حال، دستگاه شبکه باید مجموعه‌ای از حداقل کارکردهای امنیتی معمول که از همه دستگاه‌های شبکه انتظار می‌رود را ارائه نماید. مسئله امنیتی که یک دستگاه شبکه مطابق با پروفایل حاضر باید به آن بپردازد، حداقل کارکردهای امنیتی معمول برای مقابله با تهدیدات معمول پیش روی دستگاه‌های شبکه است. این تهدیدات در مقابل تهدیداتی قرار می‌گیرند که یک کارکرد خاص از یک نوع خاص از دستگاه شبکه را هدف قرار می‌دهند. مجموعه حداقل کارکردهای امنیتی معمول باید قابلیت‌های زیر را داشته باشند:

- برقراری ارتباط با دستگاه‌های مجاز و غیر مجاز شبکه
- توانایی انجام به‌روزرسانی‌های معتبر و امن
- توانایی ممیزی فعالیت‌های دستگاه‌ها
- توانایی ذخیره‌سازی و استفاده امن از داده‌ها و اطلاعات محرمانه راهبر و دستگاه
- توانایی انجام خودآزمایی در صورت از کار افتادن مؤلفه‌های کلیدی.

---

[۱] Stateful Traffic Filter Firewall

۱,۲ تهدیدات

در ادامه، تهدیدات پیش روی دستگاه‌های شبکه بر اساس عملکرد این دستگاه‌ها دسته‌بندی شده‌اند.

۱,۱,۲ ارتباط با دستگاههای شبکه

یک دستگاه شبکه با سایر دستگاه‌های شبکه و موجودیت‌های شبکه ارتباط برقرار می‌کند. مقصد این ارتباط ممکن است از لحاظ منطقی یا جغرافیایی یک دستگاه راه دور به شمار آید و مسیر ارتباط ممکن است از سیستم‌های متعدد دیگری بگذرد. این احتمال وجود دارد که سیستم‌های میانی مورد اعتماد نباشند و ارتباط غیر مجازی را با دستگاه شبکه برقرار کنند یا ارتباطات مجاز را در معرض خطر قرار دهند. کارکرد امنیتی دستگاه شبکه باید این قابلیت را داشته باشد که از ترافیک حساس شبکه (مانند ترافیک راهبری، ترافیک احراز هویت، ترافیک ممیزی و موارد دیگری از این دست) محافظت نماید. ارتباطات برقرارشده با دستگاه شبکه را می‌توان به دو دسته تقسیم‌بندی کرد: ارتباطات مجاز و ارتباطات غیر مجاز. ارتباطات مجاز شامل ترافیکی است که بر اساس خط‌مشی دستگاه شبکه، اجازه جریان یافتن دارد. ارتباطات مجاز ترافیک حساس شبکه را شامل می‌شود که از آن جمله می‌توان به ترافیک راهبری دستگاه شبکه و ارتباطات آن با یک سرور ممیزی یا احراز هویت اشاره کرد. حفاظت از این ارتباطات نیازمند استفاده از یک کانال امن است. کارکرد امنیتی دستگاه شبکه باید به گونه‌ای باشد که اطمینان حاصل نماید تنها ارتباطات مجاز می‌توانند برقرار شوند. این کارکرد امنیتی باید کانال امنی را برای جریان یافتن ترافیک حساس شبکه فراهم آورد. تمامی ارتباطات دیگر، ارتباطات غیر مجاز به شمار می‌آیند. تهدید اصلی علیه ارتباطات دستگاه شبکه که در این پروفایل حفاظتی به آن پرداخته می‌شود، یک موجودیت غیر مجاز خارجی است که تلاش می‌کند به ترافیک حساس شبکه دسترسی پیدا کند، آن را تغییر دهد یا به هر طریقی آن را افشا نماید. در صورتی که از الگوریتم‌های رمزنگاری نامناسبی استفاده شده باشد یا پروتکل‌های تونل‌زنی غیر استاندارد و اطلاعات محرمانه راهبری ضعیفی به کار گرفته شده باشند، یک عامل تهدید می‌تواند به صورت غیر مجاز به دستگاه دسترسی پیدا کند. استفاده از رمزنگاری ضعیف یا عدم استفاده از چنین الگوریتمی به طور کل، باعث می‌شود که عامل تهدید بتواند با کمترین تلاش، ترافیک را بخواند، دستکاری کند یا کنترل نماید. استفاده از پروتکل‌های تونل‌زنی غیر استاندارد نه تنها قابلیت هم‌کنش‌پذیری دستگاه را محدود می‌کند، بلکه ضمانت و اعتماد حاصل از استانداردسازی را نیز از دستگاه می‌گیرد.

دسترسی راهبری غیر مجاز

ممکن است عامل تهدید تلاش کند تا با استفاده از ابزارهای بدخواهانه، به دستگاه شبکه دسترسی راهبری پیدا کند. به عنوان مثال، عامل تهدید خود را به عنوان راهبر به دستگاه معرفی می‌کند، به عنوان دستگاه به راهبر

معرفی می‌نماید، نشست راهبری را بازپخش می‌کند (به طور کامل یا بخش‌هایی خاص از آن)، یا حملات کسی در میانه را ترتیب می‌دهد تا به نشست‌های راهبری یا نشست‌های بین دستگاه‌های شبکه دسترسی پیدا کند. بدین ترتیب، عامل تهدید قادر خواهد بود تا اقدامات بدخواهانه‌ای را انجام دهد و کارکرد امنیتی دستگاه و شبکه را به خطر اندازد.

رمزنگاری ضعیف

ممکن است عامل تهدید از ضعیف بودن الگوریتم رمزنگاری بهره‌برداری کند یا حملات رمزنگاری گسترده را علیه حافظه اصلی ترتیب دهد. انتخاب نادرست الگوریتم رمزنگاری، مُدها یا اندازه کلیدها به مهاجمان اجازه می‌دهد تا به الگوریتم رمزنگاری حمله کنند یا با ترتیب دادن حملات جستجوی فراگیر علیه حافظ اصلی، با کمترین تلاش موفق به خواندن، دستکاری یا کنترل ترافیک شوند.

کانال‌های ارتباطی غیر قابل اعتماد

ممکن است عامل تهدید آن دسته از دستگاه‌های شبکه را هدف قرار دهد که از پروتکل‌های تونل‌زنی استاندارد برای حفاظت از ترافیک حساس شبکه خود استفاده نمی‌کنند. مهاجمان می‌توانند با بهره‌گیری از پروتکل‌های با طراحی نامناسب یا فرایندهای ضعیف مدیریت کلید، حملات مردی در میانس، حملات بازپخش یا حملات دیگری از این دست را ترتیب دهند. حملات موفق باعث از دست رفتن محرمانگی و یکپارچگی ترافیک حساس شبکه می‌شوند و حتی می‌توانند دستگاه شبکه را به خطر اندازند.

نقاط پایانی با احراز هویت ضعیف

ممکن است عامل تهدید به پروتکل‌های امنی حمله کند که برای احراز هویت در دستگاه‌های انتهایی از روش‌های ضعیفی استفاده می‌کنند (مثلاً گذرواژه‌های اشتراکی که قابل حدس هستند یا به صورت متن ساده ارسال شده‌اند). عواقب این فرایند، مشابه وقتی است که از پروتکل‌های با طراحی ضعیف استفاده شده باشد. مهاجم می‌تواند خود را به جای راهبر به دستگاه دیگری معرفی کند یا خود را در جریان شبکه قرار دهد و حملات مردی در میان را طراحی نماید. در نتیجه، ممکن است مهاجم به ترافیک حساس شبکه دسترسی پیدا کند، محرمانگی و یکپارچگی آن را به خطر اندازد و حتی دستگاه شبکه را در معرض خطر قرار دهد.

۲,۱,۲ به‌روزرسانی‌های معتبر

برای حصول اطمینان از صحت کارکرد امنیتی دستگاه شبکه، لازم است که نرم‌افزار و ثابت‌افزار آن به‌روزرسانی شوند. منبع و محتوای به‌روزرسانی‌ها را باید با استفاده از روش‌های رمزنگاری تأیید کرد؛ در غیر این صورت، یک منبع غیر معتبر می‌تواند به‌روزرسانی خود را به کار گیرد و کارکرد امنیتی دستگاه شبکه را دور بزند. نسخه‌های به‌روزنشده نرم‌افزارها و ثابت‌افزارها می‌توانند دستگاه شبکه را در معرض خطر عوامل تهدیدی قرار دهند که در پی سوءاستفاده از آسیب‌پذیری‌های شناخته‌شده آن‌ها هستند. به‌روزرسانی‌های تأییدنشده یا به‌روزرسانی‌هایی که با استفاده از ابزارهای رمزنگاری ضعیف یا غیر امن تأیید شده‌اند، نرم‌افزار یا ثابت‌افزار به‌روزشده را در معرض خطر عوامل تهدیدی قرار می‌دهند که به دنبال بهره‌گیری از نرم‌افزار یا ثابت‌افزار برای رسیدن به مقاصد خویش هستند.

به‌روزرسانی‌های مخرب

ممکن است عامل تهدید یک به‌روزرسانی معیوب و دستکاری‌شده را برای نرم‌افزار یا ثابت‌افزار دستگاه شبکه ارائه کند و کارکرد امنیتی دستگاه را در معرض خطر قرار دهد. . به‌روزرسانی‌های تأییدنشده یا به‌روزرسانی‌هایی که با استفاده از ابزارهای رمزنگاری ضعیف یا غیر امن تأیید شده‌اند، نرم‌افزار یا ثابت‌افزار به‌روزشده را در معرض خطر دستکاری غیر مجاز قرار می‌دهد.

۳,۱,۲ فعالیت‌های ممیزی‌شده

راهبران می‌توانند با ممیزی فعالیت‌های دستگاه شبکه، وضعیت دستگاه را به خوبی پایش نمایند. این فرایند امکان بررسی، گزارش‌دهی در خصوص کارکردهای امنیتی، بازسازی رویدادها و تحلیل مشکل امنیتی را برای راهبر فراهم می‌آورد. پردازش‌هایی که در پاسخ به فعالیت‌های دستگاه انجام می‌شوند، نشانه‌هایی از به خطر افتادن یا از کار افتادن کارکردهای امنیتی را ارائه می‌کنند. در صورتی که فعالیت‌هایی انجام شده و بر کارکرد امنیتی تأثیر گذاشته باشند اما نشانه‌ای دال بر انجام شدن آن‌ها تولید و پایش نشده باشد، ممکن است که این فعالیت‌ها بدون آگاهی راهبر صورت گرفته باشند. علاوه بر این، در صورتی که سوابق تولید و نگهداری نشده باشند، امکان بازسازی شبکه و درک شدت و میزان آسیب‌های وارده تحت تأثیر قرار خواهد گرفت. داده‌های ممیزی ثبت‌شده در خصوص تغییر و حذف غیر مجاز، باید به دقت محافظت شوند. داده‌های مذکور ممکن است در درون محصول یا در هنگام انتقال به حافظه‌های خارجی مورد حمله قرار گیرند. توجه داشته باشید که بر اساس این پروفایل حفاظتی مشارکتی، دستگاه شبکه باید داده‌های ممیزی را تولید کند و قابلیت ارسال آن‌ها به یک موجودیت شبکه مورد اعتماد را داشته باشد.

فعالیت ردیابی‌نشده

ممکن است عامل تهدید تلاش کند تا بدون اطلاع راهبر، به کارکرد امنیتی دستگاه شبکه دسترسی پیدا کند، آن را تغییر دهد و/یا دستکاری نماید. بدین ترتیب، ممکن است مهاجم راهی برای حمله دستگاه شبکه پیدا کند و راهبر نیز آگاه نشود که دستگاه در معرض خطر قرار گرفته است.

۴,۱,۲ داده‌ها و اطلاعات محرمانه دستگاه و راهبر

دستگاه شبکه در بر دارنده داده‌ها و اطلاعات محرمانه‌ای است که باید به طور امن ذخیره‌سازی شوند و امکان دسترسی به آن‌ها تنها برای موجودیت‌های مجاز وجود داشته باشد. به عنوان مثال، می‌توان به اطلاعات محرمانه احراز هویت و پیکربندی نرم‌افزار و ثابت‌افزار و اطلاعات محرمانه راهبری اشاره کرد. کلیدهای راهبر و دستگاه، اطلاعات کلید و اطلاعات محرمانه احراز هویت را باید در برابر دستکاری و افشای غیر مجاز محافظت نمود. علاوه بر این، کارکرد امنیتی دستگاه باید کاربران را ملزم کند تا اطلاعات محرمانه احراز هویت پیش‌فرض را تغییر دهند (مثلاً راهبران ملزم باشند که اطلاعات محرمانه ورود پیش‌فرض را عوض کنند). عدم ذخیره‌سازی امن و مدیریت نامناسب داده‌ها و اطلاعات محرمانه (مانند رمزگذاری نکردن اطلاعات محرمانه درون فایل‌های پیکربندی یا دسترسی به کلیدهای نشست کانال امن) به مهاجم امکان می‌دهد تا به دستگاه شبکه دسترسی پیدا کند و حتی امنیت شبکه را از طریق دستکاری ظاهراً مجاز پیکربندی یا ترتیب دادن حملات کسی در میانه در معرض خطر قرار دهد. این حملات به موجودیت غیر مجاز امکان می‌دهند تا با استفاده از اطلاعات محرمانه راهبر امنیتی، به کارکردهای راهبری دست پیدا کند و آن‌ها را اجرا نماید و همچنین به عنوان یک دستگاه پایانی مجاز، تمامی ترافیک را دریافت نماید. بدین ترتیب، شناسایی حملات امنیتی و بازسازی شبکه دشوار خواهد شد و حتی دسترسی غیر مجاز مهاجم به داده‌های دستگاه و راهبر ادامه خواهد یافت.

به خطر افتادن کارکرد امنیتی

ممکن است عامل تهدید داده‌های دستگاه و اطلاعات محرمانه را به خطر اندازد و بدین ترتیب، دسترسی غیر مجاز و مستمری به دستگاه شبکه و داده‌های آن پیدا کند. منظور از به خطر انداختن اطلاعات محرمانه، مواردی از این قبیل است: جایگرین کردن اطلاعات محرمانه فعلی حساب‌های کاربری با اطلاعات محرمانه مهاجم، دستکاری اطلاعات محرمانه حساب‌های کاربری یا دست یافتن به اطلاعات محرمانه دستگاه و راهبر و استفاده از آن‌ها توسط مهاجم.

هک شدن گذرواژه

ممکن است عامل تهدید از ضعیف بودن گذرواژه‌های راهبری بهره‌گیری کند و از سطح دسترسی ویژه‌ای به دستگاه برخوردار گردد. دسترسی ویژه به دستگاه، مهاجم را قادر می‌سازد تا به ترافیک شبکه نیز دسترسی پیدا کند و حتی از روابط مبتنی بر اعتماد دستگاه با سایر دستگاه‌های شبکه سوءاستفاده نماید.

۵,۱,۲ از کار افتادن کارکردهای امنیتی دستگاه

سازوکارهای دستگاه شبکه معمولاً از مراجع اعتماد[۱] آغاز می‌شوند و تا سازوکارهای بسیار پیچیده‌تر ادامه می‌یابند. از کار افتادن این سازوکارها باعث به خطر افتادن کارکرد امنیتی دستگاه می‌شود. دستگاه شبکه برای حصول اطمینان از صحت کارکرد امنیتی خود می‌تواند خودآزمایی‌هایی را در هنگام راه‌اندازی اولیه و همچنین در حین عملیات انجام دهد.

از کار افتادن کارکرد امنیتی

ممکن است یکی از مؤلفه‌های دستگاه شبکه در هنگام راه‌اندازی اولیه یا در حین عملیات از کار بیفتد و این امر سبب از کار افتادن کارکرد امنیتی دستگاه شود. بدین ترتیب، دستگاه در معرض حملات مختلف قرار خواهد گرفت.

۲,۲ فرضیات

در این بخش به فروض مربوط به شناسایی تهدیدات و الزامات امنیتی دستگاه‌های شبکه می‌پردازیم. انتظار نمی‌رود که دستگاه شبکه در هیچ یک از این موارد ضمانتی ارائه کند و در نتیجه، الزاماتی برای کاهش خسارات ناشی از مخاطرات نیز در نظر گرفته نشده‌اند.

۱,۲,۲ حفاظت فیزیکی

چنین فرض می‌شود که دستگاه شبکه در محیط عملیاتی خود به صورت فیزیکی محافظت شده و در معرض حملات فیزیکی و خسارت‌های ناشی از آن‌ها قرار ندارد. چنین فرض می‌شود که این محافظت برای تأمین امنیت دستگاه و داده‌های آن کافی است. در نتیجه، این پروفایل حفاظتی مشارکتی شامل هیچ الزامی در زمینه حفاظت فیزیکی و ابزارهای لازم برای کاستن از خسارات ناشی از حملات فیزیکی نیست. این پروفایل از محصولات انتظار

[۱] Roots of trust

ندارد که از دسترسی فیزیکی به دستگاه (که به موجودیت‌های غیر مجاز امکان می‌دهد تا داده‌ها را استخراج کنند، سایر کنترل‌ها را دور بزنند یا به هر طریق دیگری دستگاه را دستکاری کنند) جلوگیری به عمل آورند.

۲,۲,۲ کارکرد محدود

چنین فرض می‌شود که دستگاه کارکردهای شبکه را به عنوان کارکرد اصلی خود ارائه می‌کند و خدمات و کارکردهایی که در دسته رایانش همه‌منظوره قرار می‌گیرند را ارائه نمی‌نماید. به عنوان مثال، دستگاه نباید پلت‌فرم رایانشی را برای کاربردهای همه‌منظوره (کاربردهای غیر مرتبط با کارکرد شبکه) ارائه کند.

۳,۲,۲ عدم محافظت از ترافیک

یک دستگاه شبکه عمومی یا استاندارد، هیچ ضمانتی در خصوص حفاظت از داده‌هایی که از آن می‌گذرند ارائه نمی‌کند. دستگاه شبکه باید از داده‌هایی حفاظت کند که از آن نشأت گرفته یا به آن ارسال شده‌اند. این داده‌ها، داده‌های ممیزی و راهبری را در بر می‌گیرند. ترافیکی که صرفاً از دستگاه شبکه می‌گذرد و مقصد آن دستگاه شبکه دیگری است، در این پروفایل حفاظتی پوشش داده نشده است. چنین فرض می‌شود که این حفاظت برای انواع خاصی از دستگاه‌های شبکه (مانند فایروال)، در پروفایل‌های حفاظتی مشارکتی پوشش داده شود.

۴,۲,۲ راهبر مورد اعتماد

چنین فرض می‌شود که راهبران امنیتی دستگاه شبکه مورد اعتماد هستند و در راستای منافع امنیتی سازمان فعالیت می‌کنند. آن‌ها آموزش مناسب دیده‌اند، از خط‌مشی‌ها پیروی می‌کنند و اسناد راهنما را رعایت می‌نمایند. چنین فرض می‌شود که راهبران امنیتی از اطلاعات محرمانه حساب کاربری و گذرواژه‌هایی با قدرت امنیتی و انتروپی مناسب استفاده می‌کنند و در هنگام راهبری دستگاه، اهداف بدخواهانه‌ای در سر ندارند. از دستگاه شبکه انتظار نمی‌رود که در صورت انجام اقدامات بدخواهاه توسط راهبر امنیتی، در مقابل اقدامات وی از خود محافظتی به عمل آورد.

۵,۲,۲ به‌روزرسانی منظم

چنین فرض می‌شود که در صورت منتشر شدن به‌روزرسانی‌های جدید در پاسخ به آسیب‌پذیری‌های شناخته‌شده، راهبر نرم‌افزار و ثابت‌افزار دستگاه شبکه را به صورت منظم به‌روزرسانی می‌کند.

۶,۲,۲ امنیت اطلاعات محرمانه راهبر

اطلاعات محرمانه راهبر (کلید خصوصی) که برای دسترسی به دستگاه شبکه استفاده می‌شوند، توسط پلت‌فرمی که روی آن قرار دارند محافظت می‌گردند.

۳,۲ خط‌مشی امنیتی سازمان

خط‌مشی امنیتی سازمان مجموعه‌ای است از قوانین، اقدامات و رویه‌های سازمان برای برآورده ساختن نیازهای امنیتی آن. یک خط‌مشی امنیتی در بخش زیر ارائه شده است.

۱,۳,۲ بنر دسترسی

محصول باید یک بنر اولیه را نمایش دهد که محدودیت‌های کاربرد، موافقت‌نامه‌های قانونی و هرگونه اطلاعات مقتضی دیگر (که کاربران با دسترسی به محصول با آن‌ها موافقت کرده‌اند) را به نمایش می‌گذارد.

۳ اهداف امنیتی

۱,۳ اهداف امنیتی مربوط به محیط عملیاتی

بخش‌های زیر، اهداف امنیتی مربوط به محیط عملیاتی را تشریح می‌کنند.

۱,۱,۳ امنیت فیزیکی

امنیت فیزیکی، متناسب باارزش محصول مورد ارزیابی و داده‌هایی که در آن قرار دارند، توسط محیط ارائه می‌شود.

۲,۱,۳ عدم کارکرد عمومی

در محصول مورد ارزیابی، هیچ قابلیت محاسباتی عمومی (مانند کامپایلرها یا برنامه‌های کاربردی کاربری) به‌جز خدمات لازم برای کارکرد، مدیریت سیستم و پشتیبانی از محصول مورد ارزیابی وجود ندارد.

۳,۱,۳ محافظت از ترافیک

محصول مورد ارزیابی از ترافیکی که از آن عبور می‌کند، محافظت نمی‌نماید. فرض بر این است که حفاظت از این ترافیک توسط سایر ابزارهای امنیتی و تضمینی موجود در محیط عملیاتی صورت می‌گیرد.

۴,۱,۳ راهبر مورد اعتماد

راهبران محصول مورد ارزیابی امن هستند و فرض بر این است که تمام موارد ذکرشده در اسناد راهنما را به‌طور صحیح انجام می‌دهند.

۵,۱,۳ به‌روزرسانی

نرم‌افزارها و میان‌افزارهای محصول مورد ارزیابی به‌طور منظم توسط سرپرست محصول به‌روز می‌شوند تا بتوانند خود را با به‌روزرسانی‌های محصولات همگام سازند و آسیب‌پذیری‌های شناخته‌شده را برطرف نمایند.

۶,۱,۳ امنیت حساب کاربری راهبر

اطلاعات حساب کاربری سرپرست محصول (کلید خصوصی) مورداستفاده برای دسترسی به محصول، باید در هر پلتفرمی که قرار دارند حفاظت‌شده باشند.

۴ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول ۴-۱ هستند و در ادامه هریک از الزامات شرح و بسط داده‌شده‌اند. همچنین الزامات مربوط به پیوست این سند نیز در ادامه جدول ۴-۱ آمده‌اند. الزامات تشریح شده در این بخش الزامی هستند و تمامی محصولات باید آن‌ها را رعایت نمایند. بر اساس انتخاب‌هایی که در این الزامات صورت می‌گیرند، لازم خواهد بود که برخی الزامات مورداشاره در پیوست دو نیز رعایت شوند. برخی الزامات اختیاری نیز ممکن است از پیوست یک برگزیده شوند. موارد ذکرشده در قالب فعالیت‌های ارزیابی، بیان می‌کنند که توسعه‌دهندگان محصول مورد ارزیابی باید چه مواردی را رعایت کنند.

به‌طورکلی، الزامات کارکرد امنیتی مورداشاره در پیوست دو که در هدف امنیتی به‌عنوان موارد ضروری به آن‌ها اشاره‌شده است، در اثر انتخاب‌های صورت گرفته در سایر الزامات کارکرد امنیتی تعیین و تکمیل می‌شوند. به‌عنوان‌مثال، در هر یک از الزامات «کانال امن» و «مسیر امن» باید پروتکل‌هایی را برای انواع کانال‌های امن تشریح شده در الزامات کارکرد امنیتی انتخاب کرد. انتخاب این پروتکل‌ها تعیین می‌کند که کدام‌یک از الزامات کارکرد امنیتی مورداشاره، در هدف امنیتی نیز لازم هستند. درصورتی‌که الزامات کارکرد امنیتی تشریح شده در

پیوست یک توسط محصول مورد ارزیابی فراهم‌شده باشند، می‌توان آن‌ها را در هدف امنیتی گنجاند، اما این الزامات برای این‌که محصول مورد ارزیابی مطابق با این پروفایل حفاظتی باشد ضروری نیستند.

جدول ۴-۱ الزامات کارکرد امنیتی

شماره الزام	نام الزام	عنصر متناظر با الزام
۱	تولید داده ممیزی ۱	FAU_GEN.1.1
۲	تولید داده ممیزی ۲	FAU_GEN.1.2
۳	تولید داده ممیزی ۳	FAU_GEN.2.1
۴	محل ذخیره‌سازی داده‌های ممیزی ۱	FAU_STG_EXT.1.1
۵	محل ذخیره‌سازی داده‌های ممیزی ۲	FAU_STG_EXT.1.2
۶	محل ذخیره‌سازی داده‌های ممیزی ۳	FAU_STG_EXT.1.3
۷	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1
۸	مدیریت کلید رمزنگاری ۲	FCS_CKM.2.1
۹	مدیریت کلید رمزنگاری ۴	FCS_CKM.4.1
۱۰	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1(1)
۱۱	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1(2)
۱۲	عملیات رمزنگاری ۱ (۳)	FCS_COP.1.1(3)
۱۳	عملیات رمزنگاری ۱ (۴)	FCS_COP.1.1(4)
۱۴	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۱۵	تولید بیت تصادفی ۲	FCS_RBG_EXT.1.2
۱۶	مدیریت رمز عبور ۱	FIA_PMG_EXT.1.1
۱۷	شناسایی و احراز هویت کاربر ۱	FIA_UIA_EXT.1.1
۱۸	شناسایی و احراز هویت کاربر ۲	FIA_UIA_EXT.1.2
۱۹	سازوکار احراز هویت بر اساس رمز عبور ۲	FIA_UAU_EXT.2.1
۲۰	احراز هویت کاربر ۱۰	FIA_UAU.7.1
۲۱	الزامات پروتکل X509 (۱)	FIA_X509_EXT.1.1
۲۲	الزامات پروتکل X509 (۲)	FIA_X509_EXT.1.2

شماره الزام	نام الزام	عنصر متناظر با الزام
۲۳	الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1
۲۴	الزامات پروتکل X509 (۴)	FIA_X509_EXT.2.2
۲۵	الزامات پروتکل X509 (۵)	FIA_X509_EXT.3.1
۲۶	الزامات پروتکل X509 (۶)	FIA_X509_EXT.3.2
۲۷	مدیریت احراز هویت ناموفق ۱	FIA_AFL.1.1
۲۸	مدیریت احراز هویت ناموفق ۲	FIA_AFL.1.2
۲۹	مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن	FMT_MOF.1.1(1)/TrustedUpdate
۳۰	مدیریت داده‌های محصول ۱	FMT_MTD.1.1
۳۱	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۳۲	نقش‌های امنیتی ۳	FMT_SMR.2.1
۳۳	نقش‌های امنیتی ۴	FMT_SMR.2.2
۳۴	نقش‌های امنیتی ۵	FMT_SMR.2.3
۳۵	محافظت از داده‌های محصول (کلیدهای متقارن) ۱	FPT_SKP_EXT.1.1
۳۶	حفاظت از کلمه عبور سرپرست محصول ۱	FPT_APW_EXT.1.1
۳۷	حفاظت از کلمه عبور سرپرست محصول ۲	FPT_APW_EXT.1.2
۳۸	خودآزمایی محصول ۱	FPT_TST_EXT.1.1
۳۹	به‌روزرسانی امن ۱	FPT_TUD_EXT.1.1
۴۰	به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۴۱	به‌روزرسانی امن ۳	FPT_TUD_EXT.1.3
۴۲	مهرهای زمانی ۱	FPT_STM.1.1
۴۳	قفل‌کردن و خاتمه دادن به نشست‌ها ۷	FTA_SSL_EXT.1.1
۴۴	قفل‌کردن و خاتمه دادن به نشست‌ها ۵	FTA_SSL.3.1
۴۵	قفل‌کردن و خاتمه دادن به نشست‌ها ۶	FTA_SSL.4.1
۴۶	پیغام‌های هشدار در رابطه با استفاده محصول ۱	FTA_TAB.1.1
۴۷	کانال امن ۱	FTP_ITC.1.1

شماره الزام	نام الزام	عنصر متناظر با الزام
۴۸	کانال امن ۲	FTP_ITC.1.2
۴۹	کانال امن ۳	FTP_ITC.1.3
۵۰	مسیر امن ۱	FTP_TRP.1.1
۵۱	مسیر امن ۲	FTP_TRP.1.2
۵۲	مسیر امن ۳	FTP_TRP.1.3
الزامات مربوط به پیوست یک		
۵۳	ذخیره‌سازی رویدادهای ممیزی ۱	FAU_STG.1.1
۵۴	ذخیره‌سازی رویدادهای ممیزی ۲	FAU_STG.1.2
۵۵	محل ذخیره‌سازی داده‌های ممیزی ۳	FAU_STG_EXT.2.1
۵۶	محل ذخیره‌سازی داده‌های ممیزی ۴	FAU_STG_EXT.3.1
۵۷	مدیریت کارکرد در محصول ۱ (۱)/ ممیزی	FMT_MOF.1.1(1)/Audit
۵۸	مدیریت کارکرد در محصول ۱ (۲)/ ممیزی	FMT_MOF.1.1(2)/Audit
۵۹	مدیریت کارکرد در محصول ۱ (۱)/ اقدامات مدیریتی	FMT_MOF.1.1(1)/AdminAct
۶۰	مدیریت کارکرد در محصول ۱ (۲)/ اقدامات مدیریتی	FMT_MOF.1.1(2)/AdminAct
۶۱	مدیریت کارکرد در محصول ۱ (۱)/ فضای ذخیره‌سازی ممیزی محلی	FMT_MOF.1.1/LocSpace
۶۲	مدیریت داده‌های محصول ۱/ اقدامات مدیریتی	FMT_MTD.1.1/AdminAct
۶۳	حفظ وضعیت امن در زمان شکست ۱/ فضای ذخیره‌سازی ممیزی محلی	FPT_FLS.1.1/LocSpace
الزامات مربوط به پیوست دو		
۶۴	الزامات پروتکل HTTPS (۱)	FCS HTTPS_EXT.1.1
۶۵	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2
۶۶	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۶۷	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1

شماره الزام	نام الزام	عنصر متناظر با الزام
۶۸	الزامات پروتکل IPSEC (۲)	FCS_IPSEC_EXT.1.2
۶۹	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
۷۰	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
۷۱	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.1.5
۷۲	الزامات پروتکل IPSEC (۶)	FCS_IPSEC_EXT.1.6
۷۳	الزامات پروتکل IPSEC (۷)	FCS_IPSEC_EXT.1.7
۷۴	الزامات پروتکل IPSEC (۸)	FCS_IPSEC_EXT.1.8
۷۵	الزامات پروتکل IPSEC (۹)	FCS_IPSEC_EXT.1.9
۷۶	الزامات پروتکل IPSEC (۱۰)	FCS_IPSEC_EXT.1.10
۷۷	الزامات پروتکل IPSEC (۱۱)	FCS_IPSEC_EXT.1.11
۷۸	الزامات پروتکل IPSEC (۱۲)	FCS_IPSEC_EXT.1.12
۷۹	الزامات پروتکل IPSEC (۱۳)	FCS_IPSEC_EXT.1.13
۸۰	الزامات پروتکل IPSEC (۱۴)	FCS_IPSEC_EXT.1.14
۸۱	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.1.1
۸۲	الزامات پروتکل SSH Client (۲)	FCS_SSHC_EXT.1.2
۸۳	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.1.3
۸۴	الزامات پروتکل SSH Client (۴)	FCS_SSHC_EXT.1.4
۸۵	الزامات پروتکل SSH Client (۵)	FCS_SSHC_EXT.1.5
۸۶	الزامات پروتکل SSH Client (۶)	FCS_SSHC_EXT.1.6
۸۷	الزامات پروتکل SSH Client (۷)	FCS_SSHC_EXT.1.7
۸۸	الزامات پروتکل SSH Client (۸)	FCS_SSHC_EXT.1.8
۸۹	الزامات پروتکل SSH Client (۹)	FCS_SSHC_EXT.1.9
۹۰	الزامات پروتکل SSH Server (۱)	FCS_SSHS_EXT.1.1
۹۱	الزامات پروتکل SSH Server (۲)	FCS_SSHS_EXT.1.2
۹۲	الزامات پروتکل SSH Server (۳)	FCS_SSHS_EXT.1.3

شماره الزام	نام الزام	عنصر متناظر با الزام
۹۳	الزامات پروتکل SSH Server (۴)	FCS_SSHS_EXT.1.4
۹۴	الزامات پروتکل SSH Server (۵)	FCS_SSHS_EXT.1.5
۹۵	الزامات پروتکل SSH Server (۶)	FCS_SSHS_EXT.1.6
۹۶	الزامات پروتکل SSH Server (۷)	FCS_SSHS_EXT.1.7
۹۷	الزامات پروتکل SSH Server (۸)	FCS_SSHS_EXT.1.8
۹۸	الزامات پروتکل TLS Client/ احراز هویت ۱	FCS_TLSC_EXT.1.1
۹۹	الزامات پروتکل TLS Client/ احراز هویت ۲	FCS_TLSC_EXT.1.2
۱۰۰	الزامات پروتکل TLS Client/ احراز هویت ۳	FCS_TLSC_EXT.1.3
۱۰۱	الزامات پروتکل TLS Client/ احراز هویت ۴	FCS_TLSC_EXT.1.4
۱۰۲	الزامات پروتکل TLS Client/ احراز هویت دوطرفه ۱	FCS_TLSC_EXT.2.1
۱۰۳	الزامات پروتکل TLS Client/ احراز هویت دو طرفه ۲	FCS_TLSC_EXT.2.2
۱۰۴	الزامات پروتکل TLS Client/ احراز هویت دو طرفه ۳	FCS_TLSC_EXT.2.3
۱۰۵	الزامات پروتکل TLS Client/ احراز هویت دو طرفه ۴	FCS_TLSC_EXT.2.4
۱۰۶	الزامات پروتکل TLS Client/ احراز هویت دو طرفه ۵	FCS_TLSC_EXT.2.5
۱۰۷	الزامات پروتکل TLS Server/ احراز هویت ۱	FCS_TLSS_EXT.1.1
۱۰۸	الزامات پروتکل TLS Server/ احراز هویت ۲	FCS_TLSS_EXT.1.2
۱۰۹	الزامات پروتکل TLS Server/ احراز هویت ۳	FCS_TLSS_EXT.1.3
۱۱۰	الزامات پروتکل TLS Server/ احرازهویت دوطرفه ۱	FCS_TLSS_EXT.2.1
۱۱۱	الزامات پروتکل TLS Server/ احرازهویت دو طرفه ۲	FCS_TLSS_EXT.2.2
۱۱۲	الزامات پروتکل TLS Server/ احرازهویت دو طرفه ۳	FCS_TLSS_EXT.2.3
۱۱۳	الزامات پروتکل TLS Server/ احرازهویت دو طرفه ۴	FCS_TLSS_EXT.2.4
۱۱۴	الزامات پروتکل TLS Server/ احرازهویت دو طرفه ۵	FCS_TLSS_EXT.2.5
۱۱۵	الزامات پروتکل TLS Server/ احرازهویت دو طرفه ۶	FCS_TLSS_EXT.2.6
۱۱۶	خودآزمایی محصول مورد ارزیابی۲	FPT_TST_EXT.2.1
۱۱۷	الزامات به‌روزرسانی امن ۴	FPT_TUD_EXT.2.1

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۱۸	الزامات به‌روزرسانی امن ۵	FPT_TUD_EXT.2.2
۱۱۹	مدیریت کارکرد در محصول مورد ارزیابی ۱ (۲)/ به‌روزرسانی امن	FMT_MOF.1.1(2)/TrustedUpdate

۱,۴ کلاس ممیزی امنیت

برای حصول اطمینان از این‌که سرپرست محصول، اطلاعات لازم برای شناسایی مشکلات عمدی و غیرعمدی موجود درزمینه پیکربندی و/یا کارکرد سیستم را در اختیاردارند، محصول باید این قابلیت را داشته باشد که داده‌های ممیزی موردنیاز برای تشخیص چنین فعالیت‌هایی را تولید نماید. ممیزی فعالیت‌های مدیریت سیستم سبب تولید اطلاعاتی می‌شود که در صورت نیاز به تغییر پیکربندی سیستم، می‌توان برای طراحی اقدامات اصلاحی از آن‌ها استفاده کرد. ممیزی رویدادهای گزینش‌شده نشان می‌دهد که آیا بخش‌هایی مهم محصول مورد ارزیابی در معرض شکست قرار دارند یا خیر (مثلاً این‌که فرایند رمزنگاری اجرا نشود) و همچنین به شناسایی فعالیت‌های غیرمعمول (مانند ایجاد یک نشست کاربری در زمان مشکوک، شکست مکرر نشست‌ها یا احراز هویت ناموفق به سیستم) یک مورد مشکوک، کمک می‌کند. در برخی موارد، ممکن است حجم اطلاعات ممیزی تولیدشده به‌اندازه‌ای زیاد شود که محصول مورد ارزیابی یا راهبران مسئول بازبینی این اطلاعات را دچار سردرگمی کند. محصول مورد ارزیابی باید بتواند اطلاعات ممیزی را به یک موجودیت مورداعتماد خارجی ارسال کند. این اطلاعات باید دارای مهرهای زمانی قابل‌اعتماد باشند، این امر سبب می‌شود که بتوان اطلاعات را پس از ارسال به دستگاه‌های خارجی مرتب کرد. از دست رفتن ارتباط با سرور ممیزی می‌تواند مشکل‌ساز شود. هرچند که راه‌های مختلفی برای کاهش این تهدید وجود دارد، اما این پروفایل حفاظتی هیچ اقدام خاصی را الزام نمی‌کند. مناسب بودن محصول مورد ارزیابی در یک محیط خاص، متأثر از میزان حفاظت از اطلاعات ممیزی با این اقدامات و توانایی محصول مورد ارزیابی برای انجام کارکردهای خود در اثر انجام اقدامات مذکور است.

از محصول مورد ارزیابی دستگاه‌های شبکه انتظار نمی‌رود که تمام داده‌های ممیزی را ذخیره کند. هرچند که لازم است داده‌ها به‌صورت محلی در زمان تولید ذخیره شوند و در صورت تجاوز از ظرفیت ذخیره‌سازی، اقدامات مقتضی صورت گیرند، محصول مورد ارزیابی همچنین باید بتواند یک لینک امن را با یک سرور ممیزی خارجی ایجاد کند تا بتوان داده‌های ممیزی خارجی را ذخیره کرد.

شماره الزام	نام الزام
۱	**تولید داده ممیزی ۱**

محصول مورد ارزیابی باید بتواند سوابق ممیزی را برای رویدادهای قابل ممیزی زیر تهیه کند:

الف) آغاز و اتمام توابع ممیزی؛

ب) تمام اقدامات مدیریتی شامل موارد زیر:

- ورود و خروج مدیریتی به سیستم (درصورتی‌که مدیران سیستم نیاز به حساب کاربری شخصی داشته باشند، نام حساب کاربری آن‌ها نیز باید ثبت شود)
- تغییرات امنیتی در پیکربندی (علاوه بر اطلاعات حاکی از ایجاد تغییرات، باید تعیین شود که چه مواردی تغییر کرده‌اند)
- تولید، واردکردن، تغییر یا پاک کردن کلیدهای رمزنگاری (علاوه بر این کار، نام کلید اختصاصی یا یک مرجع کلید نیز باید ثبت شود)
- تغییر کلمه عبور (نام حساب کاربری مربوطه نیز باید ثبت شود)
- آغاز و توقف سرویس‌ها
- [انتخاب: هیچ اقدام دیگر، اختصاص: [لیست سایر کاربردهای ویژه]]؛

ت) [انتخاب: دیگر رویدادهای ممیزی لیست در نکته کاربردی ۳].

نکته کاربردی ۱:

در صورتیکه لیست «اقدامات مدیریتی» ارائه شده در این الزام کارکردهای امنیتی محصول را به طور کامل پوشش ندهد، نویسنده سند هدف امنیتی باید با استفاده از قسمت «اختصاص» که در «انتخاب» قرارگرفته است اقدامات مدیریتی دیگری را به لیست اضافه نماید.

نکته کاربردی ۲:

در این الزام «سرویس» اشاره دارد به ارتباطات صورت‌گرفته از طریق کانال امن و مسیر امن، خودآزمایی‌های درخواست شده، به‌روزرسانی امن و نشست‌های مدیریتی سیستم.

۲	**تولید داده ممیزی ۲**

محصول مورد ارزیابی باید در هر یک از سوابق ممیزی، دست‌کم اطلاعات زیر را ثبت نماید:

الف) تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت[۱] فعال و نتیجه رویداد (موفقیت یا شکست)؛ و
ب) در مورد هر یک از انواع رویدادهای ممیزی و بر اساس تعریف رویدادهای قابل ممیزی ارائه‌شده در پروفایل حفاظتی یا هدف امنیتی، اطلاعات در نکته کاربردی ۳ مشخص‌شده است.

نکته کاربردی ۳:

نویسنده هدف امنیتی با توجه به رویدادهای ممیزی ثبت‌شده برای هر یک از الزامات زیر باید اطلاعات مناسب دیگر علاوه بربند الف این الزام فراهم نماید. برای نمونه توسعه‌دهنده با توجه به الزام شماره ۱۸ «شناسایی و احراز هویت کاربر ۲» برای ثبت رکورد ممیزی علاوه بر اطلاعات بند الف این الزام باید آدرس IP منشأ احراز هویت را در رکورد ممیزی (به‌عنوان نمونه در قسمت توضیحات رکورد) ثبت نماید؛ بنابراین این اطلاعات توسط نویسنده سند هدف امنیتی در این قسمت قرار داده می‌شود.

- برای الزام شماره ۱۹ «سازوکار احراز هویت بر اساس رمز عبور» اطلاعات ممیزی تمام کاربردهای مکانیسم تعیین هویت و احراز هویت ثبت می‌شود. این اطلاعات باید شامل منشأ تلاش صورت گرفته (مانند آدرس IP) باشد.
- برای الزامات ۲۱ الی ۲۶ «الزامات پروتکل X509» اطلاعات ممیزی مربوط به تلاش‌های ناموفق صورت گرفته شده جهت تأیید یک گواهی‌نامه ثبت می‌شود. این اطلاعات ثبت شده باید شامل دلیل شکست (عدم موفقیت در تایید گواهینامه) باشد.
- برای الزام شماره ۲۹ «مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن» اطلاعات ممیزی مربوط به هرگونه تلاش برای آغاز یک به‌روزرسانی، دستی ثبت می‌شود.
- برای الزام شماره ۳۰ «مدیریت داده‌های محصول» اطلاعات ممیزی تمام فعالیت‌های مدیریتی داده‌های محصول ثبت می‌شود.
- برای الزامات شماره ۳۹ الی ۴۱ «به‌روزرسانی امن» اطلاعات ممیزی مربوط به آغاز به‌روزرسانی، نتیجه تلاش‌های به‌روزرسانی (موفقیت یا شکست) ثبت می‌شود.
- برای الزام شماره ۴۲ «مهرهای زمانی[۲]» اطلاعات ممیزی مربوط به تغییرات صورت گرفته در زمان ثبت می‌شود. این اطلاعات باید شامل زمان‌های جدید و قدیم، منشأ تلاش (مانند آدرس IP) برای تغییر زمان موفق یا ناموفق باشد.
- برای الزام ۴۳«قفل‌کردن و خاتمه دادن به نشست‌ها ۷» اطلاعات ممیزی تمام تلاش‌های صورت گرفته برای باز کردن قفل یک نشست تعاملی ثبت می‌شود.
- برای الزام ۴۴«قفل‌کردن و خاتمه دادن به نشست‌ها ۵» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست راه دور از طریق یک مکانیسم قفل‌کردن نشست ثبت می‌شود.

[۱] Subject
[۲] Time stamps

- برای الزام ۴۵« قفل‌کردن و خاتمه دادن به نشست‌ها ۶» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست تعاملی ثبت می‌شود.
- برای الزامات ۴۷ الی ۴۹ «کانال امن» اطلاعات ممیزی مربوط به آغاز کردن کانال امن / خاتمه دادن کانال امن / شکست توابع کانال امن ثبت می‌شود. این اطلاعات باید شامل شناسایی دلیل و هدف تلاش ناموفق برای ایجاد کانال امن باشد.
- برای الزامات ۵۰ الی ۵۲ «مسیر امن» اطلاعات ممیزی مربوط به آغاز کردن مسیر امن / خاتمه دادن مسیر امن / شکست توابع مسیر امن ثبت می‌شود. این اطلاعات باید شامل شناسایی هویت ادعاشده توسط کاربر باشد.

نکته کاربردی ۴:

رویدادهای ممیزی دیگر بر اساس الزامات اختیاری و انتخابی برگرفته‌شده از پیوست‌های یک و دو به محصول مورد ارزیابی اضافه می‌شوند؛ بنابراین، نویسنده هدف امنیتی باید رویدادهای اضافی را اضافه نماید.

رویداد ممیزی «الزامات پروتکل X509» در صورتی رخ می‌دهد که محصول مورد ارزیابی نتواند از موارد زیر اطمینان حاصل نماید و گواهی‌نامه‌ها را تأیید کند:

- وجود افزونه basicConstraints و تأیید اینکه پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم‌شده است
- تأیید امضای دیجیتال CA سلسله مراتبی مورد اعتماد
- خواندن و دسترسی به CRL یا دسترسی به سرور OCSP

اگر هر یک از این موارد وجود نداشته باشند، باید یک رویداد ممیزی با نتیجه شکست را در سوابق ممیزی ثبت نمود.

۳	**تولید داده ممیزی ۳**

در مورد آن دسته از رویدادهای ممیزی که حاصل اقدامات کاربران احرازهویت‌شده هستند، محصول مورد ارزیابی باید بتواند هر رویداد قابل ممیزی را با هویت کاربری که مسبب آن رویداد شده است، مرتبط سازد.

۴	**محل ذخیره‌سازی داده‌های ممیزی ۱**

محصول باید قادر به ارسال داده ممیزی تولید شده به یک موجودیت IT خارجی با استفاده از کانال مورد اعتماد پیاده‌سازی شده با پروتکل:[انتخاب: IPsec، SSH، TLS، TLS/HTTPS] باشد.

تذکر: در صورتی که هر یک از پروتکل‌های IPsec،SSH،TLS،HTTPS به عنوان پروتکل‌های ارتباطی امن استفاده شود نیاز است از پیوست دو تمامی الزامات مربوط به آن پروتکل تکمیل و به سند هدف امنیتی اضافه گردد.

نکته کاربردی ۵:

محصول مورد ارزیابی برای انتقال داده‌های ممیزی تولیدشده به یک موجودیت IT خارجی، ذخیره‌سازی و بازبینی سوابق ممیزی از یک سرور ممیزی به‌جز سرور محصول مورد ارزیابی استفاده می‌کند. ذخیره‌سازی این سوابق ممیزی و اجازه دادن به سرپرست محصول جهت بازبینی این سوابق، توسط محیط عملیاتی صورت می‌گیرد.

۵	**محل ذخیره‌سازی داده‌های ممیزی ۲**
محصول مورد ارزیابی باید بتواند داده‌های ممیزی تولیدشده را در خود ذخیره کند.	
۶	**محل ذخیره‌سازی داده‌های ممیزی ۳**
درصورتی‌که حافظه محلی محصول پرشده باشد و ظرفیتی برای ذخیره‌سازی داده‌های ممیزی نداشته باشد، محصول مورد ارزیابی باید [انتخاب: داده‌های ممیزی جدید را کنار بگذارد، سوابق ممیزی گذشته را بر اساس این قوانین بازنویسی[۱] کند: [اختصاص: قوانین بازنویسی سوابق ممیزی گذشته]، [اختصاص: اقدامات دیگر]].	

نکته کاربردی ۶:

درصورتی‌که حافظه محلی پرشده باشد، سرور خارجی ثبت رویدادها[۲] می‌تواند به‌عنوان فضای ذخیره‌سازی جایگزین مورداستفاده قرار گیرد. «اقدامات دیگر» که در بخش «اختصاص» ذکرشده است، می‌تواند مواردی ازجمله «ارسال داده‌های ممیزی جدید به یک موجودیت IT خارجی» را شامل شود.

۲,۴ پشتیبانی رمزنگاری (FCS)

در این بخش، الزامات رمزنگاری مربوط به سایر ویژگی‌های امنیتی محصول مورد ارزیابی تعریف می‌شوند. این الزامات شامل تولید کلید و تولید بیت تصادفی، روش‌های استقرار کلید[۳]، نابودی کلید و انواع مختلف عملیات رمزنگاری برای رمزگذاری و رمزگشایی AES، تأیید امضا، تولید درهم‌ساز و تولید درهم‌ساز کلید گذاری شده[۴] هستند. این الزامات کارکرد امنیتی، از پیاده‌سازی الزامات مبتنی بر انتخاب و پروتکل لیست شده در پیوست دو پشتیبانی می‌کنند.

[۱] Overwrite
[۲] External log server
[۳] Key establishment
[۴] Keyed hash generation

شماره الزام	نام الزام
۷	**مدیریت کلید رمزنگاری ۱**

محصول مورد ارزیابی باید بر اساس الگوریتم‌های تولید کلید رمزنگاری، کلیدهای رمزنگاری نامتقارن را تولید کند: [انتخاب:

- الگوهای RSA با استفاده از کلیدهای رمزنگاری با اندازه‌های ۲۰۴۸ بیت یا بزرگ‌تر که این الزامات را رعایت کنند: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.3؛
- الگوهای ECC با استفاده از «منحنی‌های NIST» [انتخاب: P-256, P-384, P-521] بر اساس این الزامات: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.4.
- الگوهای FFC با استفاده از کلیدهای رمزنگاری با اندازه‌های ۲۰۴۸ بیت یا بزرگ‌تر که این الزامات را رعایت کنند: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.1.

نکته کاربردی ۷:

نویسنده هدف امنیتی، تمام الگوهای تولید کلید مورداستفاده برای استقرار کلید و احراز هویت دستگاه‌ها را انتخاب می‌کند. درصورتی‌که برای استقرار کلید از الگوهای تولید کلید استفاده شود، الگوهای لیست‌شده در «مدیریت کلید رمزنگاری ۲» و پروتکل‌های رمزنگاری انتخاب‌شده باید مطابق با انتخاب باشند. درصورتی‌که برای احراز هویت دستگاه‌ها از الگوهای تولید کلید استفاده شود، انتظار می‌رود که کلید عمومی مرتبط با یک گواهی‌نامه X.509v3 باشد.

اگر محصول مورد ارزیابی به‌عنوان یک دریافت‌کننده در الگوی استقرار کلید RSA عمل کند، نیازی نیست که محصول، الگوی تولید کلید RSA را پیاده‌سازی نماید.

شماره الزام	نام الزام
۸	**مدیریت کلید رمزنگاری ۲**

محصول مورد ارزیابی باید استقرار کلید[۱] رمزنگاری را بر اساس یک روش خاص استقرار کلید رمزنگاری انجام دهد: [انتخاب:

- الگوهای استقرار کلید RSA که این الزامات را رعایت کنند: شماره ویژه NIST 800-56B، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری فاکتورگیری عدد صحیح»[۲]؛
- الگوهای استقرار کلید منحنی بیضوی [۳]که این الزامات را رعایت کنند: شماره ویژه NIST 800-56A، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته»[۴]؛

[۱] Key establishment
[۲] Integer factorization cryptography
[۳] Elliptic curve-based
[۴] Discrete logarithm cryptography

شماره الزام	نام الزام
• الگوهای استقرار کلید میدانی[۱] که این الزامات را رعایت کنند: شماره ویژه NIST 800-56A، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته». **نکته کاربردی ۸:** این عنصر درواقع نسخه اصلاح‌شده الزام«مدیریت کلید رمزنگاری ۲[۲]» در استاندارد ISO 15408 می‌باشد که به‌جای توزیع کلید، به استقرار کلید می‌پردازد. نویسنده هدف امنیتی، تمام الگوهای استقرار کلید مورداستفاده برای پروتکل‌های رمزنگاری منتخب را انتخاب می‌کند. الگوهای استقرار کلید مبتنی بر RSA در بخش ۹ از NIST SP 800-56B تشریح شده‌اند؛ اما این بخش وابسته به پیاده‌سازی موارد مذکور در سایر بخش‌های SP 800-56B است. اگر محصول مورد ارزیابی در الگوی استقرار کلید به‌عنوان گیرنده عمل کند، نیازی نخواهد بود که محصول، الگوی تولید کلید RSA را اجرا نماید. منحنی‌های بیضوی مورداستفاده در الگوهای استقرار کلید، با منحنی‌های مشخص‌شده در الزام شماره‌ی ۷ «مدیریت کلید رمزنگاری ۱» ارتباط دارند. پارامترهای دامنه مورداستفاده در الگوهای استقرار کلید میدانی، به الگوهای تولید کلید مورداشاره در «مدیریت کلید رمزنگاری ۱» وابسته هستند.	
۹	**مدیریت کلید رمزنگاری ۴**
محصول مورد ارزیابی باید کلیدهای رمزنگاری را بر اساس یک روش خاص برای نابودی کلیدهای رمزنگاری، از بین ببرد: [انتخاب: • در مورد حافظه فرار[۳]، نابودی باید از طریق یک بازنویسی ساده و مستقیم [انتخاب: شامل الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی، شامل صفرها] انجام شود و سپس از طریق خواندن تائید شود. o درصورتی‌که داده‌های بازنویسی شده پس از خواندن تائید نشود، فرایند باید مجدداً تکرار شود. • در مورد EEPROM غیر فرار، نابودی باید از طریق یک بازنویسی ساده و مستقیم شامل الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی انجام شود (طبق آنچه در «تولید بیت تصادفی» تشریح شده است) و سپس تأیید از طریق خواندن صورت گیرد. o درصورتی‌که داده‌های بازنویسی شده پس از خواندن تائید نشود، فرایند باید مجدداً تکرار شود.	

[۱] Finite filed-based

[۲] FCS_CKM.2

[۳] Volatile memory

شماره الزام	نام الزام
• در مورد حافظه فلش غیر فرار، نابودی باید از طریق [انتخاب: یک بازنویسی ساده و مستقیم شامل صفرها، پاک کردن بلوک] انجام شود و پس از خواندن تائید شود. o درصورتی‌که داده‌های بازنویسی شده پس از خواندن تائید نشود، فرایند باید مجدداً تکرار شود. • در مورد حافظه‌های غیر فرار به‌جز فلش و EEPROM، نابودی باید از طریق سه بار بازنویسی با الگوی تصادفی انجام شود، به‌گونه‌ای که این الگو پیش از هر بار بازنویسی عوض شود.]	
۱۰	**عملیات رمزنگاری ۱ (۱)**
محصول مورد ارزیابی باید رمزگذاری و رمزگشایی را بر اساس الگوریتم‌های رمزنگاری خاص که در حالت [انتخاب: CBC، GCM] استفاده می‌شوند و در اندازه‌های کلید [انتخاب: ۱۲۸ بیتی، ۱۹۲ بیتی، ۲۵۶ بیتی] و با توجه به استاندارد AES که در ISO 18033-3 تعریف‌شده است، [انتخاب: CBC که در ISO 10116 تعریف‌شده است، GCM که در ISO 19772 تعریف‌شده است]. انجام دهد. **نکته کاربردی ۹:** در مورد نخستین انتخاب عملیات رمزنگاری ۱(۱)، نویسنده هدف امنیتی باید حالت یا حالت‌های کارکردی AES را تعیین کند. در مورد دومین انتخاب، نویسنده هدف امنیتی باید اندازه کلیدهای پشتیبانی شده توسط این کارکرد را انتخاب کند. حالت‌ها و اندازه کلیدهای انتخاب‌شده در این مرحله، متناظر با انتخاب مجموعه رمز[۱] در الزامات کانال امن هستند.	
۱۱	**عملیات رمزنگاری ۱ (۲)**
محصول مورد ارزیابی باید خدمات امضای رمزنگاری (تولید و تأیید) را بر اساس الگوریتم‌های رمزنگاری زیر ارائه کند: [انتخاب: • الگوریتم امضای دیجیتال RSA و اندازه کلیدهای [اختصاص: ۲۰۴۸ بیتی یا بزرگ‌تر] • الگوریتم امضای دیجیتال بیضوی و اندازه کلیدهای [اختصاص: ۲۵۶ بیتی یا بزرگ‌تر]] با رعایت موارد زیر: [انتخاب: • در مورد الگوهای RSA: FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۵,۵، با استفاده از الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSAPKCS2v1_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال ۲ یا الگوی امضای دیجیتال ۳،	

[۱] Cipher suite

شماره الزام	نام الزام
• در مورد الگوهای ECDSA: FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۶ و پیوست D، با اجرای منحنی‌های NISTP-256 و P-384 و [انتخاب: P-521، هیچ منحنی دیگر]؛ ISO/IEC 14888-3، بخش ۶,۴] **نکته کاربردی ۱۰:** نویسنده هدف امنیتی باید الگوریتم مورداستفاده برای اجرای امضای دیجیتال را تعیین کند. برای الگوریتم‌های انتخاب‌شده، نویسنده هدف امنیتی باید انتخاب‌ها و اختصاص‌های مناسب را انجام دهد و پارامترهای الگوریتم‌ها را به شکل مناسب تعیین نماید.	
۱۲	**عملیات رمزنگاری ۱ (۳)**
محصول مورد ارزیابی باید خدمات درهم‌سازی رمزنگاری را بر اساس یک الگوریتم رمزنگاری مشخص [انتخاب: SHA-1, SHA-256, SHA-384, SHA-512] با رعایت استاندارد ISO/IEC 10118-3:2004. ارائه نماید. نکته کاربردی ۱۱: به تولیدکنندگان اکیداً توصیه می‌شود که از پروتکل‌های به‌روزرسانی شده‌ای که از خانواده SHA-2 پشتیبانی می‌نمایند، استفاده کنند. تا زمانی که پروتکل‌های به‌روز شده پشتیبانی شوند، این پروفایل حفاظتی اجازه پشتیبانی از SHA-1 را بر اساس SP 800-131A فراهم می‌کند. طبق SP 800-131 A الگوریتم SHA-1 فقط می‌تواند برای عملیات‌های غیر از امضای دیجیتال همچون درهم سازی پسورد و ... استفاده شود. انتخاب درهم‌ساز باید بر اساس قدرت کلی الگوریتم مورداستفاده برای الزام شماره ۱۰ «عملیات رمزنگاری ۱(۱)» و الزام شماره ۱۱ «عملیات رمزنگاری ۱(۲)» انجام شود (مثلاً SHA 256 برای کلیدهای ۱۲۸ بیتی).	
۱۳	**عملیات رمزنگاری ۱ (۴)**
محصول مورد ارزیابی باید احراز هویت پیام مبتنی بر کلید درهم‌سازی شده[۱] را بر اساس الگوریتم رمزنگاری خاص [انتخاب:HMAC-SHA-1, HMAC-SHA-256,HMAC-SHA-384, HMAC-SHA-512] و با استفاده از اندازه کلید	

[۱] Keyed-hash message authentication

شماره الزام	نام الزام
[اختصاص: اندازه کلید مورداستفاده در HMAC (بر حسب بیت)] و اندازه خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیت و با توجه به موارد مطرح‌شده در بخش هفتم ISO/IEC 9797-2:2011 با نام «الگوریتم ۲ MAC» انجام دهد. **نکته کاربردی ۱۲:** اندازه کلید k در عبارت «اختصاص» بین L1 و L2 خواهد بود (که در ISO/IEC 10118 مربوط به توابع درهم‌ساز تعریف شده است). به عنوان مثال، در مورد SHA-256 داریم: L1=512, L2=256 که L2<=k<=L1.	
۱۴	**تولید بیت تصادفی ۱**
محصول مورد ارزیابی باید خدمات تولید بیت تصادفی را بر اساس ISO/IEC 18031:2011 و با استفاده از [انتخاب: Hash_DRBG، HMAC_DRBG، CTR_DRBG (AES)] ارائه دهد.	
۱۵	**تولید بیت تصادفی ۲**
RBG قطعی باید دست کم توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی را از [انتخاب: [اختصاص: تعداد منابع مبتنی بر نرم افزار] منبع نویز مبتنی بر نرم‌افزار، [اختصاص: تعداد منابع مبتنی بر سخت افزار] منبع نویز مبتنی بر سخت‌افزار] گردآوری کند. این آنتروپی باید دست کم [انتخاب: ۱۲۸ بیت، ۱۹۲ بیت، ۲۵۶ بیت] و حداقل معادل بالاترین قدرت امنیتی کلیدها و درهم‌سازهای تولیدشده مورداشاره در بخش جدول C.1 «Security Strength Table for Hash Functions» ISO/IEC 18031:2011 باشد. **نکته کاربردی ۱۳:** در مورد نخستین عبارت این الزام، هدف امنیتی باید حداقل به یکی از انواع منابع نویز اشاره کند. اگر محصول مورد ارزیابی شامل چند منبع نویز از یک نوع باشد، نویسنده هدف امنیتی عبارت اختصاص را با تعداد مناسبی از هر یک از انواع منابع پر می‌کند (مثلاً دو منبع نویز مبتنی بر نرم‌افزار و یک منبع نویز مبتنی بر سخت‌افزار). مستندات و آزمون‌های مورداشاره در فعالیت‌های ارزیابی، تمام منابع مورداشاره در هدف امنیتی را پوشش می‌دهند. سند ISO/IEC 18031:2011 شامل سه روش مختلف تولید اعداد تصادفی است که هر یک از آن‌ها به عناصر اولیه فرایند رمزنگاری (توابع درهم‌ساز و مجموعه‌های رمز) بستگی دارد. نویسنده هدف امنیتی، تابع مورداستفاده را انتخاب خواهد کرد و عناصر اولیه فرایند رمزنگاری را تعیین خواهد نمود. با اینکه تمام توابع درهم‌ساز تعیین‌شده (SHA-1,SHA-224, SHA-256, SHA-384, SHA-512) را می‌توان در Hash_DRBG یا HMAC_DRBG مورداستفاده قرار داد، تنها اجازه استفاده از موارد مبتنی بر AES در CTR_DRBG وجود دارد.	

شماره الزام	نام الزام
اگر اندازه کلید برای پیاده‌سازی AES متفاوت از اندازه کلید مورداستفاده برای رمزگذاری داده‌های کاربری باشد، ممکن است نیاز به تغییر یا تکرار «عملیات رمزنگاری» باشد تا تفاوت اندازه کلید در آن لحاظ گردد. در مورد عبارت انتخاب «تولید بیت تصادفی ۲»، نویسنده هدف امنیتی حداقل تعداد بیت‌های انتروپی تزریق‌شده به RBG را تعیین می‌کند.	

۳,۴ کلاس شناسایی و احراز هویت

محصول، یک مکانیسم ورود مبتنی بر کلمه عبور را به عنوان ابزاری امن در اختیار راهبران قرار می‌دهد تا بتوانند با استفاده از آن با محصول مورد ارزیابی ارتباط برقرار کنند. سرپرست محصول باید یک کلمه عبورقدرتمند را تهیه کند و مکانیسمی را برای تغییر منظم آن در نظر گیرد. برای جلوگیری از حملاتی که در آن‌ها فرد مهاجم تایپ شدن کلمه عبور را می‌بیند، کلمه عبور را باید در هنگام ورود به حالت محو و ناخوانا درآورد. قفل‌کردن و خاتمه دادن نشست را نیز می‌توان برای جلوگیری از ورود غیر مجاز به حساب کاربری مورداستفاده قرار داد. کلمه‌های عبور باید به شکل محو و ناخوانا ذخیره شوند، به گونه‌ای که هیچ واسطی برای خواندن آن به شکل متن ساده وجود نداشته باشد.

شماره الزام	نام الزام
۱۶	**مدیریت رمز عبور ۱**
محصول مورد ارزیابی باید قابلیت‌های مدیریت کلمه عبور زیر را برای کلمه عبور سرپرست محصول فراهم آورد: الف) کلمه عبور را باید بتوان با هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای ویژه مطرح شده در این بخش ساخت: [انتخاب: "(", ")", "*", "&", "^", "%", "$", "#", "@", "!"، [اختصاص: سایر کاراکترها]]؛ ب) حداقل طول کلمه عبور باید توسط سرپرست محصول قابل تعیین باشد، کلمه‌های عبور باید بتوانند ۱۵ کاراکتر یا بزرگ‌تر باشند. **نکته کاربردی ۱۴:** نویسنده هدف امنیتی کاراکترهای ویژه قابل استفاده در کلمه عبور را تعیین می‌کند. وی می‌تواند با استفاده از عبارت اختصاص، کاراکترهای دیگری را به لیست بیفزاید. منظور از «کلمه‌های عبور جایگزین»، کلمه‌های عبوری هستند که توسط مدیران سیستم در کنسول محلی مورداستفاده قرار می‌گیرند. این کلمه‌های عبور روی پروتکل‌هایی استفاده می‌شوند که از آن‌ها پشتیبانی کنند. به عنوان مثال، می‌توان از SSH و HTTPS نام برد. این کلمه‌های عبور گاهی نیز برای ارائه آن دسته از داده‌های پیکربندی مورداستفاده قرار می‌گیرند که از دیگر الزامات کارکرد امنیتی در محصول پشتیبانی می‌کنند.	
۱۷	**شناسایی و احراز هویت کاربر ۱**

محصول مورد ارزیابی پیش از آن که از دیگر موجودیت‌های خارج از محصول بخواهد که فرایند تعیین و احراز هویت را انجام دهد، باید اجازه انجام فعالیت‌های زیر را بدهد: [انتخاب: هیچ اقدامی، [اختصاص: لیست خدمات، اقدامات انجام‌شده توسط محصول مورد ارزیابی در پاسخ به درخواست‌های خارجی]]

۱۸	**شناسایی و احراز هویت کاربر ۲**

پیش از آن که محصول مورد ارزیابی امکان انجام اقدامات مدیریتی سیستم را فراهم آورد، باید مدیرسیستم را احراز هویت نماید.

نکته کاربردی ۱۵:

این الزام برای کاربران خدماتی که به طور مستقیم توسط محصول مورد ارزیابی در دسترس قرار می‌گیرند (چه مدیران سیستم و چه کارشناسان IT خارجی) اعمال می‌شود و در مورد خدماتی که از طریق ارتباطات محصول مورد ارزیابی فراهم می‌گردند، اعمال نمی‌شود. از آنجا که موجودیت‌های خارجی پیش از تعیین و احراز هویت تنها باید به چند خدمت محدود (و یا هیچ خدمتی) دسترسی داشته باشند، این خدمات باید در عبارت اختصاص ذکر شوند. در غیر این صورت، باید «هیچ اقدام دیگر» را انتخاب کرد.

احراز هویت ممکن است مبتنی بر کلمه عبور باشد و از طریق کنسول محلی و یا از طریق پروتکلی صورت گیرد که از کلمه‌های عبور پشتیبانی می‌کند (مانند SSH)، یا اینکه بر اساس گواهی‌نامه انجام شود (مانند SSH و TLS). در مورد ارتباط با موجودیت‌های IT خارجی (مانند یک سرور ممیزی یا سرور NTP) این ارتباطات باید بر اساس الزام‌های شماره ۴۷ تا ۴۹ «کانال امن» انجام شوند که پروتکل آن از تعیین و احراز هویت پشتیبانی می‌کند. این امر بدین معنی است که نیازی نیست ارتباطاتی از قبیل ایجاد ارتباط IPsec با سرور احراز هویت، در عبارت اختصاص ذکر شوند، زیرا ایجاد ارتباط به معنی آغاز فرایند تعیین و احراز هویت است.

۱۹	**سازوکار احراز هویت بر اساس رمزعبور ۲**

محصول مورد ارزیابی باید یک مکانیسم احراز هویت مبتنی بر کلمه عبور، [انتخاب: [اختصاص: سایر مکانیسم‌های احراز هویت]، هیچ مکانیسمی] را برای احراز هویت مدیران سیستم فراهم آورد.

نکته کاربردی ۱۶:

عبارت اختصاص باید تمام مکانیسم‌های احراز هویت پشتیبانی‌شده را نشان دهد. مکانیسم‌های احراز هویت محلی از طریق کنسول محلی انجام می‌شوند. نشست‌های مدیریتی از راه دور (و مکانیسم‌های احراز هویت مربوط به آن‌ها) در «مسیر امن» مشخص شده‌اند.

۲۰	**احراز هویت کاربر ۱۰**

هنگامی که فرایند احراز هویت در در حال جریان است، محصول مورد ارزیابی تنها باید بازخورد مبهم[۱] را در اختیار سرپرست محصول قرار دهد.

نکته کاربردی ۱۷:

«بازخورد مبهم» به معنی بازخوردی است که در آن محصول مورد ارزیابی داده‌های احراز هویت وارد شده توسط کاربر را به صورت واضح و قابل خواندن نشان نمی‌دهد؛ البته ممکن است روند پیشرفت به شکل مبهم نشان داده شود (مانند یک ستاره برای هر کاراکتر). بازخورد مبهم همچنین نشان می‌دهد که محصول مورد ارزیابی در جریان احراز هویت هیچ اطلاعاتی را که ممکن است نشان‌دهنده داده‌های احراز هویت باشد، نمایش نمی‌دهد.

۲۱	**الزامات پروتکل X509 (۱)**

محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند:

- تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه
- مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد
- محصول مورد ارزیابی باید برای تأیید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است
- محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) چنان که در RFC 2560 تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در RFC 5759 تعریف شده است] تأیید کند
- محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید کند:

o گواهی‌نامه‌های مورداستفاده برای تأیید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی، باید هدف «Code Signing» (id-kp 3 با OID 1.3.6.1.5.5.7.3.3) را در فیلد extendedKeyUsage خود داشته باشند

o گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف "Server Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.

o گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف "Client Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.

o گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های OCSP باید هدف «OCSP Signing» (id-kp9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.

[۱] Obscured feedback

نکته کاربردی ۱۸:

این الزام قوانین مورداستفاده برای تأیید گواهی‌نامه‌ها را لیست کرده است. نویسنده هدف امنیتی تعیین می‌کند که وضعیت فسخ گواهی‌نامه توسط OCSP تأیید می‌شود یا CRL. پروتکل‌های مسیر و کانال‌های امن لازم است که از گواهی‌نامه استفاده شود؛ بنابراین لازم است که قوانین extendedKeyUsage تأیید شوند. انتظار می‌رود که این تأیید در یک گواهی‌نامه اصلی CA مورد اعتمادی که توسط پلت‌فرم مدیریت می‌شود، خاتمه یابد.

۲۲	**الزامات پروتکل X509 (۲)**

محصول مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد.

نکته کاربردی ۱۹:

این الزام در مورد گواهی‌نامه‌هایی اعمال می‌شود که توسط محصول مورد ارزیابی بکار رفته و پردازش شده باشند. این الزام همچنین اضافه شدن گواهی‌نامه‌ها به لیست گواهی‌نامه‌های معتبر CA را محدود می‌کند.

۲۳	**الزامات پروتکل X509 (۳)**

محصول مورد ارزیابی باید برای پشتیبانی از احراز هویت در [انتخاب: IPsec, TLS, HTTPS, SSH] و همچنین برای [انتخاب: امضای کد برای به‌روزرسانی نرم‌افزار سیستم، امضای کد برای تأیید صحت و یکپارچگی، [اختصاص: سایر کاربردها]، هیچ کاربرد دیگر] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.

نکته کاربردی ۲۰:

پروتکل انتخاب شده در این الزام توسط نویسنده هدف امنیتی معادل با انتخابی است که در الزام «کانال امن ۱» صورت می‌گیرد. لازم به ذکر است می‌توان از گواهی‌نامه‌ها به صورت اختیاری برای به‌روزرسانی‌های امن نرم‌افزار سیستم (به روز رسانی امن) و برای تأیید صحت و یکپارچگی (خودآزمایی محصول مورد ارزیابی۲) استفاده نمود.

۲۴	**الزامات پروتکل X509 (۴)**

اگر محصول مورد ارزیابی نتواند اتصال مورد نیاز برای تأیید اعتبار یک گواهی‌نامه را برقرار کند، باید [انتخاب: به سرپرست محصول اجازه دهد که در این مورد تصمیم‌گیری کند، گواهی‌نامه را بپذیرد، گواهی‌نامه را نپذیرد].

نکته کاربردی ۲۱:

معمولاً برای بررسی وضعیت فسخ یک گواهی‌نامه باید اتصالی را برقرار نمود. این اتصال هم برای دانلود کردن یک CRL و هم برای جستجو با استفاده از OCSP لازم است. با استفاده از انتخاب فوق، می‌توان تعیین نمود که اگر برقراری این اتصال ممکن نباشد، باید چه اقدامی را انجام داد. اگر محصول مورد ارزیابی بر اساس تمام قوانین مورداشاره در الزام شماره ۲۱ و الزام شماره ۲۲ به این نتیجه برسد که گواهی‌نامه معتبر است، می‌تواند آن را بپذیرد. اگر هر یک از این قوانین نشان‌دهنده عدم تأیید گواهی‌نامه باشند، محصول مورد ارزیابی نباید آن را بپذیرد. اگر نویسنده هدف امنیتی انتخاب اول را انجام دهد و به سرپرست محصول قدرت تصمیم‌گیری بدهد، باید تابع مربوطه از «کارکرد مدیریتی محصول» را نیز انتخاب نماید.

۲۵	**الزامات پروتکل X509 (۵)**

محصول مورد ارزیابی باید مطابق با آنچه که در RFC 2986 تشریح شده است، یک Certificate Request Message تولید کند و بتواند این اطلاعات را در درخواست فراهم کند: کلید عمومی[۱] و [انتخاب: اطلاعات مخصوص به دستگاه[۲]، Common Name، Orgsnization، Organization Unit،Country].

نکته کاربردی ۲۲:

کلید عمومی در واقع بخش عمومی از جفت کلیدهای عمومی-خصوصی است که بر اساس آن چه در «مدیریت کلید رمزنگاری» شرح داده‌شده است، توسط محصول مورد ارزیابی تولید می‌شود.

۲۶	**الزامات پروتکل X509 (۶)**

محصول مورد ارزیابی باید زنجیره گواهی‌نامه‌ها از Root CA را بر اساس پاسخ گواهینامه‌های CA دریافت شده اعتبارسنجی کند.

۲۷	**مدیریت احراز هویت ناموفق ۱**

محصول، باید [انتخاب: [اختصاص: یک عدد صحیح مثبت]،یک عدد مثبت قابل تنظیم توسط سرپرست [اختصاص: از یک بازه عددی قابل‌قبول]] از تلاش‌های ناموفق احراز هویت را نسبت به آخرین احراز هویت موفق مشخص نمایند

۲۸	**مدیریت احراز هویت ناموفق ۲**

[۱] Public Key

[۲] Device-specific information

زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت [انتخاب: به حد تعیین‌شده رسید، از آن بیشتر شد]، توابع امنیتی هدف ارزیابی باید [اختصاص: اقداماتی را که بدین منظور در نظر گرفته شده است] انجام دهند.

۴,۴ کلاس مدیریت امنیت

توابع مدیریتی مورد نیاز در این بخش، شامل قابلیت‌های مورد نیاز برای پشتیبانی از نقش سرپرست محصول و همچنین مجموعه‌ای از توابع مدیریتی امنیت مورد نیاز برای مدیریت بخش‌های قابل پیکربندی الزامات کارکرد امنیتی (کارکرد مدیریتی محصول)، مدیریت داده‌های محصول مورد ارزیابی (مدیریت داده‌های محصول) و فعال کردن به‌روزرسانی‌های محصول مورد ارزیابی (مدیریت کارکرد در محصول ۱ (۱)/به‌روزرسانی‌های امن) هستند. در کنار این الزامات مدیریتی اصلی، برخی الزامات اختیاری نیز در پیوست اول و تعدادی الزامات انتخابی نیز در پیوست دوم ذکر شده‌اند.

شماره الزام	نام الزام
۲۹	**مدیریت کارکرد در محصول ۱ (۱)/ به روزرسانی امن**
محصول مورد ارزیابی باید توانایی فعال کردن توابع به‌منظور به‌روزرسانی دستی را به سرپرست امنیتی محصول محدود نماید. **نکته کاربردی ۲۳:** این الزام امکان آغاز به‌روزرسانی دستی را به سرپرست محصول امنیتی محدود می‌کند.	
۳۰	**مدیریت داده‌های محصول ۱**
محصول مورد ارزیابی باید امکان «مدیریت» داده‌های محصول را به سرپرست محصول محدود کند. **نکته کاربردی ۲۴:** منظور از «مدیریت» می‌تواند هر یک از این اقدامات و موارد دیگری از این دست باشد: تولید، آغاز، بازدید، تغییر پیش فرض، تغییر، پاک کردن و اضافه نمودن. الزام حاضر همچنین شامل بازگرداندن کلمه عبورکاربری به حالت پیش‌فرض توسط سرپرست محصول امنیتی است.	
۳۱	**کارکرد مدیریتی محصول ۱**

شماره الزام	نام الزام

محصول مورد ارزیابی باید قابلیت انجام کارکردهای مدیریتی زیر را داشته باشد:

- مدیریت محصول به‌صورت محلی و از راه دور
- پیکربندی بنر دسترسی
- پیکربندی زمان غیرفعال بودن نشست پیش از قفل‌کردن یا خاتمه دادن آن
- به‌روزرسانی محصول مورد ارزیابی و تأیید به‌روزرسانی‌ها با استفاده از امضای دیجیتال پیش از نصب شدن این به‌روزرسانی‌ها
- [انتخاب:
  - پیکربندی رفتار ممیزی
  - پیکربندی لیست خدمات ارائه‌شده توسط محصول مورد ارزیابی پیش از شناسایی یا احراز هویت یک موجودیت، چنان که در «شناسایی و احراز هویت کاربر» تشریح شده است
  - پیکربندی کارکرد رمزنگاری
  - هیچ قابلیت دیگری]

نکته کاربردی ۲۵:

محصول مورد ارزیابی باید کارکردهای لازم برای مدیریت سیستم به‌صورت محلی و مدیریت از راه دور را فراهم آورد این کارکردها شامل پیکربندی بنر دسترسی برای الزام « پیغام‌های هشدار در رابطه با استفاده محصول ۱» و زمان غیر فعال بودن نشست برای الزام « قفل‌کردن و خاتمه دادن به نشست‌ها ۵» و « قفل‌کردن و خاتمه دادن به نشست‌ها ۶» هستند. آیتم به‌روزرسانی محصول مورد ارزیابی و تأیید به‌روزرسانی‌ها با استفاده از امضای دیجیتال پیش از نصب شدن این به‌روزرسانی‌ها، شامل توابع مدیریتی مربوطه در الزام شماره ۲۹ « مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن» و الزام شماره ۱۱۹ « مدیریت کارکرد در محصول مورد ارزیابی ۱ (۲)/ به‌روزرسانی امن» و الزام شماره ۲۴ « الزامات پروتکل X509 (۴)» و الزام شماره ۱۱۸ «الزامات به روز رسانی امن۵» است. اگر محصول مورد ارزیابی پیش از شناسایی و احراز هویت، امکان پیکربندی رفتار ممیزی و خدمات موجود را برای سرپرست محصول فراهم کند، یا امکان پیکربندی هر یک از کارکردهای رمزنگاری محصول مورد ارزیابی وجود داشته باشد، نویسنده هدف امنیتی باید گزینه یا گزینه‌های مناسب را در دومین عبارت «انتخاب» برگزیند و در غیر این صورت گزینه «هیچ قابلیت دیگری» را انتخاب کند.

۳۲	نقش‌های امنیتی ۳

شماره الزام	نام الزام
محصول باید نقش‌های زیر را نگهداری کند. • سرپرست محصول	
۳۳	**نقش‌های امنیتی ۴**
محصول مورد ارزیابی باید بتواند بین کاربران و نقش‌ها ارتباط برقرار نماید.	
۳۴	**نقش‌های امنیتی ۵**
محصول مورد ارزیابی باید از برقرار بودن شرایط زیر اطمینان حاصل کند: • سرپرست محصول باید بتواند محصول مورد ارزیابی را به صورت دستی مدیریت کند. • سرپرست محصول باید بتواند محصول مورد ارزیابی را از راه دور مدیریت کند. **نکته کاربردی ۲۶:** بر اساس این الزام سرپرست محصول باید بتواند محصول مورد ارزیابی را از طریق یک کنسول محلی و یک مکانیسم راه دور مدیریت کند (IPsec, SSH, TLS, HTTPS).	

۵,۴ کلاس حفاظت از محصول مورد ارزیابی

در این بخش، الزامات مربوط به محصول مورد ارزیابی برای حفاظت از داده‌های امنیتی حساس مانند کلیدها و کلمه‌های عبور، انجام خودآزمایی‌ها برای پایش کارکرد صحیح محصول مورد ارزیابی (شامل از بین بردن نقایص کارکرد میان‌افزار یا ضعف در یکپارچگی نرم‌افزار) و ارائه روش‌های امن برای به‌روزرسانی نرم‌افزار و میان‌افزار محصول مورد ارزیابی را مرور می‌کنیم. علاوه بر این، محصول مورد ارزیابی باید مهرهای زمانی قابل اعتمادی را برای پشتیبانی از ممیزی صحیح خانواده «تولید داده ممیزی» فراهم آورد.

شماره الزام	نام الزام
۳۵	**محافظت از داده‌های محصول (کلیدهای متقارن) ۱**
محصول مورد ارزیابی باید از خواندن تمام کلیدهایی که از پیش به اشتراک گذاشته شده‌اند، کلیدهای متقارن و کلیدهای خصوصی جلوگیری به عمل آورد.	

نکته کاربردی ۲۷:

هدف از الزام حاضر این است که دستگاه بتواند مانع از دسترسی غیر مجاز به کلیدها، اطلاعات کلیدها و اطلاعات احراز هویت شود. این داده‌ها باید تنها برای کارکردهای امنیتی مربوطه، قابل دسترسی باشند و نیازی به دسترسی و نمایش آن‌ها در هر زمان دیگر نخواهد بود. این الزام مانع ازمشخص شدن وجود این اطلاعات، در حال استفاده بودن آن‌ها، یا معتبر بودن آن‌ها نیست. با این حال، الزام حاضر امکان خواندن این اطلاعات را محدود می‌کند.

۳۶	**حفاظت از کلمه عبور سرپرست محصول ۱**
محصول مورد ارزیابی نباید کلمه‌های عبور را به شکل متن ساده ذخیره کند.	
۳۷	**حفاظت از کلمه عبور سرپرست محصول ۲**
محصول مورد ارزیابی باید از خوانده شدن کلمه‌های عبوری که به‌صورت متن ساده[۱] هستند، جلوگیری کند.	

نکته کاربردی ۲۸:

هدف از الزام حاضر این است که داده‌های خام مربوط به احراز هویت از طریق گذرواژه، به شکل واضح ذخیره نشوند و هیچ کاربر و سرپرست محصول نتواند کلمه عبورمتن ساده را از طریق واسط «عادی» بخواند. البته سرپرست محصولی که تمام دسترسی‌ها را داشته باشد می‌تواند کلمه عبوررا بخواند؛ اما به وی اعتماد می‌شود و فرض می‌گردد که وی این کار را نخواهد کرد.

۱,۵,۴ آزمون محصول مورد ارزیابی

محصول مورد ارزیابی، برای اینکه برخی شکست‌های مکانیسم‌های امنیتی خود را شناسایی کند، خودآزمایی‌هایی را انجام می‌دهد. میزان و حجم این خودآزمایی‌ها به تصمیم تولیدکننده محصول بستگی دارد؛ اما هر چه خودآزمایی‌های جامع‌تری انجام شوند، پلت‌فرم قابل‌اعتمادتری برای استقرار معماری سازمان پدید خواهد آمد. (تعدادی الزام مبتنی بر انتخاب برای این بخش در پیوست دو ارائه شده‌اند.)

شماره الزام	نام الزام
۳۸	**خودآزمایی محصول۱**

[۱] Plaintext

شماره الزام	نام الزام
محصول مورد ارزیابی باید مجموعه‌ای از این خودآزمایی‌ها را [انتخاب: در مرحله راه‌اندازی اولیه (روشن شدن دستگاه)، به طور دوره‌ای در حین کارکرد دستگاه، در صورت درخواست کاربر مجاز، در شرایط [اختصاص: شرایطی که باید در آن‌ها خودآزمایی‌ها را انجام داد]] برای نشان دادن کارکرد صحیح محصول مورد ارزیابی انجام دهد: [اختصاص: لیست خودآزمایی‌هایی که باید توسط محصول مورد ارزیابی انجام شوند]. **تذکر: در صورتی که برای خودآزمایی‌ها از مکانیسم امضای دیجیتال استفاده شود نیاز است الزام «خودآزمایی محصول ۲» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه گردد.** **نکته کاربردی ۲۹:** انتظار می‌رود که خودآزمایی‌ها در مرحله راه‌اندازی اولیه (روشن شدن دستگاه) انجام شوند. سایر گزینه‌ها در صورتی در نظر گرفته می‌شوند که تولیدکننده دستگاه توجیه کند که چرا خودآزمایی در مرحله راه‌اندازی اولیه (روشن شدن دستگاه) انجام نمی‌شود. انتظار می‌رود که دست کم خودآزمایی‌های لازم برای حصول اطمینان از صحت و یکپارچگی نرم‌افزار و میان‌افزار و کارکرد صحیح توابع رمزنگاری انجام شوند. اگر خودآزمایی‌ها در مرحله راه‌اندازی اولیه (روشن شدن دستگاه) انجام نشوند، الزام کارکرد امنیتی حاضر چند بار و هر بار با انتخاب‌های مختلف اجرا می‌شود. **نکته کاربردی ۳۰:** اگر در خودآزمایی‌ها از گواهی‌نامه‌ها استفاده شود (مثلاً برای تأیید امضا جهت تأیید صحت و یکپارچگی)، گواهی‌نامه‌ها باید از «الزامات پروتکل X509 (۳)» انتخاب شوند و بر اساس الزام « الزامات پروتکل X509 (۱)» و الزام «الزامات پروتکل X509 (۲)» تأیید گردند. علاوه بر این، «خودآزمایی محصول مورد ارزیابی۲» باید در سند هدف امنیتی در نظر گرفته شوند.	

۲,۵,۴ به‌روزرسانی امن

عدم موفقیت سرپرست محصول در تأیید به‌روزرسانی‌های سیستم، ممکن است کل سیستم را در معرض خطر قرار دهد. برای اعتماد به منبع به‌روزرسانی‌ها، سیستم می‌تواند مجموعه‌ای از فرایندها و مکانیسم‌های رمزنگاری را مورداستفاده قرار دهد و با استفاده از آن‌ها، به‌روزرسانی‌ها را تهیه و تدارک ببیند، رمزنگاری به‌روزرسانی‌ها را از طریق مکانیسم امضای دیجیتال بررسی کند و به‌روزرسانی‌ها را روی سیستم نصب نماید. هرچند که الزامی برای انجام خودکار این فرایند وجود ندارد، اسناد راهنما و رویکرد سرپرست محصول برای حصول اطمینان از اعتبار امضا را باید مبنای کار قرار داد. (برای این خانواده، تعدادی الزام مبتنی بر انتخاب در پیوست دو ارائه شده‌اند.)

شماره الزام	نام الزام
۳۹	**به روز رسانی امن ۱**

محصول مورد ارزیابی باید این امکان را به سرپرست محصول بدهد که هم به نسخه فعلی نرم‌افزار و میان‌افزار محصول مورد ارزیابی و هم به جدیدترین نسخه نصب‌شده آن‌ها دسترسی داشته باشد.

نکته کاربردی ۳۱:

نسخه فعلی (مورداستفاده)، ممکن است جدیدترین نسخه نصب‌شده نباشد. به عنوان مثال، ممکن است تعدادی از به‌روزرسانی‌ها نصب شوند، اما پیش از اجرای آن‌ها نیاز به راه‌اندازی مجدد سیستم باشد؛ بنابراین، جستجوها[۱] باید بتواند هم به نسخه مورداستفاده و هم به آخرین نسخه نصب‌شده دسترسی داشته باشند.

شماره الزام	نام الزام
۴۰	**به روز رسانی امن ۲**

محصول مورد ارزیابی باید این امکان را برای سرپرست محصول امنیتی فراهم کندکه به‌روزرسانی نرم‌افزار و میان‌افزارمیان‌افزار محصول مورد ارزیابی را به صورت دستی انجام دهد و [انتخاب: از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند، از به‌روزرسانی‌های خودکار پشتیبانی کند، از هیچ مکانیسم به‌روزرسانی دیگری پشتیبانی نکند].

تذکر: در صورتی که نویسنده سند هدف امنیتی برای این الزام گزینه‌های به روزرسانی خودکار را انتخاب نماید لازم است الزام «مدیریت کارکرد در محصول مورد ارزیابی ۱ (۲)/به روزرسانی امن» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه نماید.

نکته کاربردی ۳۲:

عبارت «انتخاب» در این الزام، بین پشتیبانی از «جستجوی خودکار به‌روزرسانی‌ها» و «به‌روزرسانی خودکار» تمایز قائل می‌شود. جستجوی خودکار به‌روزرسانی‌ها به یک محصول مورد ارزیابی اشاره دارد که جستجو می‌کند تا ببیند به‌روزرسانی جدیدی وجود دارد یا خیر و این امر را به سرپرست محصول اطلاع می‌دهد (مثلاً از طریق یک پیام یا یک پرچم)، اما نصب به‌روزرسانی نیازمند انجام اقداماتی توسط سرپرست محصول خواهد بود، اما به‌روزرسانی خودکار به یک محصول مورد ارزیابی اشاره دارد که به‌روزرسانی‌ها را جستجو می‌کند و در صورت وجود آن‌ها را نصب می‌نماید.

[۱] Query

شماره الزام	نام الزام
۴۱	**به روز رسانی امن ۳**

محصول مورد ارزیابی باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از [انتخاب: مکانیسم امضای دیجیتال، درهم‌ساز منتشرشده]، ابزاری را برای احراز هویت میان‌افزار آن‌ها در اختیار محصول مورد ارزیابی قرار دهد.

تذکر: در صورتی که از مکانیسم امضای دیجیتال استفاده شود نیاز است الزام‌های «الزامات به روز رسانی ۴» و «الزامات به روزرسانی ۵» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه کند.

نکته کاربردی ۳۳:

مکانیسم امضای دیجیتال که در این الزام به آن اشاره شده است، یکی از الگوریتم‌هایی است که در الزام «عملیات رمزنگاری ۱ (۲)»تشریح شده است. همچنین درهم‌ساز مورد استفاده از این الزام نیز توسط یکی از توابع تشریح‌شده در الزام « عملیات رمزنگاری ۱ (۳)» تولید می‌شود. نویسنده هدف امنیتی باید مکانیسم اجرا شده توسط محصول مورد ارزیابی را تعیین نماید. لازم به ذکر است می‌توان از هر دو مکانیسم استفاده کرد.

نکته کاربردی ۳۴:

در نسخه‌های بعدی این پروفایل حفاظتی، لازم خواهد شد که برای به‌روزرسانی‌های امن، از یک مکانیسم امضای دیجیتال استفاده شود.

نکته کاربردی ۳۵:

اگر در مکانیسم تأیید به‌روزرسانی از گواهی‌نامه‌ها استفاده شود، این گواهی‌ها باید از «الزامات پروتکل X509 (۳)» انتخاب شده و بر اساس «الزامات پروتکل X509» تأیید گردند. علاوه بر این، «خودآزمایی محصول مورد ارزیابی۲» باید در سند هدف امنیتی در نظر گرفته شود.

نکته کاربردی ۳۶:

در این الزام کارکرد امنیتی، منظور از «به‌روزرسانی»، فرایند جایگزین کردن یک مؤلفه نرم‌افزاری غیر فرار (non-volatile) با یک مؤلفه دیگر است. به مؤلفه اول، تصویر غیر فرار یا تصویر NV و به مؤلفه دوم، تصویر به‌روزرسانی گفته می‌شود. هر چند که تصویر

شماره الزام	نام الزام
	به‌روزرسانی معمولاً جدیدتر از تصویر NV است، اما الزامی در این زمینه وجود ندارد. در مواردی ممکن است مالک سیستم بخواهد آن را به نسخه قدیمی‌تر برگرداند و این کار ایرادی ندارد (مثلاً هنگامی که شرکتی یک به‌روزرسانی معیوب را منتشر کند، یا هنگامی که سیستم مبتنی بر کارکرد یک ویژگی مستندسازی نشده باشد که در به‌روزرسانی جدید وجود ندارد). همچنین، ممکن است مالک سیستم بخواهد به‌روزرسانی را با تصویر NV انجام دهد تا معایب موجود را برطرف نماید. تمام مؤلفه‌های مجزای نرم‌افزار (مانند برنامه‌های کاربردی، درایورها، هسته و میان‌افزار[۱]) محصول مورد ارزیابی باید توسط تولیدکننده، امضای دیجیتال شوند و در نهایت توسط مکانیسم به‌روزرسانی تأیید گردند. از آن‌جا که ممکن است مؤلفه‌ها توسط تولیدکننده‌های مختلف امضا شوند، لازم است که فرایند به‌روزرسانی هم تصویر NV و هم تصویر به‌روزرسانی تولیدشده توسط یک تولیدکننده واحد (مثلاً تأیید از طریق مقایسه کلیدهای عمومی) یا امضاشده توسط کلیدهای امضای معتبر را تأیید کند (مثلاً تأیید گواهی‌نامه‌ها در صورت استفاده از گواهی‌نامه‌های X.509).
۴۲	**مهرهای زمانی ۱**
	محصول مورد ارزیابی باید قابلیت ارائه مهرهای زمانی معتبر را داشته باشد. **نکته کاربردی ۳۷:** محصول مورد ارزیابی به خودی خود اطلاعات معتبری را درباره زمان فعلی و مکان محصول مورد ارزیابی ارائه نمی‌کند. این اطلاعات بستگی به اطلاعات خارجی درباره زمان و تاریخ دارند که یا به صورت دستی توسط سرپرست محصول و یا توسط سرور NTP فراهم آمده‌اند. عبارت «مهر زمانی معتبر» به استفاده محدود از اطلاعات زمانی و تاریخی (که توسط موجودیت‌های خارجی ارائه شده‌اند) و تمام تغییرات ثبت‌شده در تنظیمات زمانی (شامل اطلاعات مربوط به زمان قدیم و جدید) اشاره دارد. با استفاده از این اطلاعات، می‌توان زمان واقعی تمام داده‌های ممیزی را محاسبه کرد.

۶,۴ دسترسی به محصول

این بخش به تشریح الزامات امنیتی مربوط به نشست‌های سرپرست محصول محصول مورد ارزیابی می‌پردازد. هم نشست‌های محلی و هم نشست‌های راه دور پایش می‌شوند تا در صورت غیر فعال بودن شناسایی شوند و قفل شدن یا خاتمه یافتن آن‌ها نیز در صورت رسیدن به آستانه زمانی بررسی می‌شود. راهبران باید قادر باشند

[۱] Firmware

نشست‌های تعاملی خود را خاتمه دهند. در ابتدای هر نشست باید یک اطلاعیه مشاوره‌ای برای آن‌ها نمایش داده شود.

شماره الزام	نام الزام
۴۳	**قفل‌کردن و خاتمه دادن به نشست‌ها ۷**
در مورد نشست‌های تعاملی محلی[۱]، محصول مورد ارزیابی باید پس از اتمام زمان غیر فعال بودن که توسط سرپرست محصول تعیین شده است، [انتخاب: • نشست را قفل کند – تمام فعالیت‌های مربوط به دسترسی به داده‌های کاربری و نمایش این داده‌ها، به جز فعالیت‌های مربوط به قفل‌گشایی نشست را غیر فعال کند و از سرپرست محصول بخواهد که پیش از قفل‌گشایی نشست، مجدداً احراز هویت نماید؛ • نشست را خاتمه دهد].	
۴۴	**قفل‌کردن و خاتمه دادن به نشست‌ها ۵**
در مورد نشست‌های تعاملی راه دور[۲]، درصورتی که نشست تعاملی برای مدت معینی غیرفعال باشد، محصول مورد ارزیابی باید نشست تعاملی خاتمه دهد. مدت زمان مجاز برای غیرفعال بودن توسط سرپرست محصول تعیین می‌شود.	
۴۵	**قفل‌کردن و خاتمه دادن به نشست‌ها ۶**
محصول مورد ارزیابی باید به سرپرست محصول اجازه دهد که نشست تعاملی خود را خاتمه دهد.	
۴۶	**پیغام‌های هشدار در رابطه با استفاده محصول ۱**
قبل از ایجاد نشست برای سرپرست محصول، محصول مورد ارزیابی باید توصیه‌های امنیتی مدیریتی و همچنین تاییدیه استفاده از محصول مورد ارزیابی را به سرپرست محصول نشان دهد. **نکته کاربردی ۳۸:**	

[۱] Local
[۲] Remote

شماره الزام	نام الزام
این الزام در مورد نشست‌های تعاملی بین یک کاربر انسانی و یک محصول مورد ارزیابی اعمال می‌شود. موجودیت‌های IT که اتصالاتی مانند تماس‌های راه دور از طریق شبکه را برقرار می‌کنند، نیازی به رعایت این الزام نخواهند داشت.	

۷,۴ کلاس کانال‌ها/مسیرهای مورد اعتماد

برای پرداختن به مسائل مربوط به انتقال داده‌های حساس از جایی دیگر به محصول مورد ارزیابی و از محصول مورد ارزیابی به جایی دیگر، اهداف ارزیابی مطابق با استانداردها مسیر ارتباطی بین خود و نقاط پایانی را رمزگذاری می‌کنند. این کانال‌ها با استفاده از یک یا چند مورد از این چهار پروتکل استاندارد ایجاد می‌شوند: IPsec, TLS, HTTPS و SSH. این پروتکل‌ها توسط RFC هایی تعیین می‌شوند که گزینه‌های پیاده‌سازی مختلفی را در اختیار کاربران قرار می‌دهند. در مورد برخی از این گزینه‌ها الزاماتی نیز جود دارد (مخصوصاً گزینه‌های مربوط به مقادیر اولیه رمزنگاری). هدف این است که قابلیت همکاری و مقاومت در برابر حملات رمزنگاری افزایش یابد. این پروتکل‌ها علاوه بر حفاظت در برابر افشای اطلاعات (و شناسایی تغییرات ایجادشده)، امکان احراز هویت دوطرفه را نیز برای هر یک از نقاط پایانی فراهم می‌آورند و این کار را به صورت امن و با استفاده از روش‌های رمزنگاری انجام می‌دهند. بدین معنی که حتی اگر یک مهاجم بدخواه نیز در بین دو نقطه پایانی حضور داشته باشد، هرگونه تلاش وی برای اینکه خود را به عنوان یکی از طرفین ارتباط معرفی کند، شناسایی خواهد شد.

شماره الزام	نام الزام
۴۷	**کانال امن ۱**
محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [انتخاب: IPsec, SSH, TLS, HTTPS] میان خود و دیگر موجودیت‌های IT معتبر همچون سرور ممیزی، [انتخاب: سرور احرازهویت، اختصاص: [دیگر قابلیت ها]] که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آن‌ها را احرازهویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد. **تذکر: در صورتی که هر یک از پروتکل‌های IPsec،SSH،TLS،HTTPS به عنوان پروتکل‌های ارتباطی امن استفاده شود نیاز است از پیوست دو تمامی الزامات مربوط به آن پروتکل تکمیل و به سند هدف امنیتی اضافه گردد.**	
۴۸	**کانال امن ۲**
محصول مورد ارزیابی باید اجازه داشته باشد یا به موجودیت‌های معتبرIT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	

شماره الزام	نام الزام
۴۹	**کانال امن ۳**

محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای [اختصاص: لیست خدماتی که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباطات را آغاز کند] راه‌اندازی نماید.

نکته کاربردی ۳۹:

هدف از الزام حاضر این است که ابزاری را برای استفاده از پروتکل رمزنگاری جهت حفاظت از ارتباطات خارجی با موجودیت‌های معتبر IT کارکرد فراهم آورد. منظوراز موجودیت‌های معتبر IT موجودیت‌هایی است که محصول مورد ارزیابی برای انجام کارکردهای خود با آن‌ها ارتباط برقرار می‌کند. محصول مورد ارزیابی دست کم از یکی از پروتکل‌های لیست‌شده استفاده می‌کند تا با سرور جمع‌آوری اطلاعات ممیزی ارتباط برقرار کند. اگر ارتباط با یک سرور احراز هویت (مانند RADIUS) برقرار شود، نویسنده هدف امنیتی باید عبارت «سرور احراز هویت» را در الزام شماره ۷۱ «کانال امن ۱» انتخاب کند. این اتصال باید توسط یکی از پروتکل‌های لیست‌شده حفاظت گردد. اگر سایر موجودیت‌های معتبر IT (مانند سرور NTP) مورد حفاظت قرار گیرند، نویسنده هدف امنیتی باید انتخاب‌های مقتضی را انجام دهد و موارد مناسب را در عبارت اختصاص بگنجاند. نویسنده هدف امنیتی مکانیسم یا مکانیسم‌های پشتیبانی‌شده توسط محصول مورد ارزیابی را انتخاب می‌کند و اطمینان حاصل می‌نماید که الزامات پروتکل پیوست دو متناظر با انتخاب وی، در هدف امنیتی گنجانده شده‌اند. اگر TLS انتخاب شده باشد، نویسنده هدف امنیتی به جای تمامی «الزامات پروتکلTLS Client/ احراز هویت» از تمامی «الزامات پروتکلTLS Client/ احراز هویت دو طرفه» استفاده خواهد کرد.

هر چند که هیچ الزامی در مورد طرف آغازکننده ارتباط وجود ندارد، نویسنده هدف امنیتی در عبارت اختصاص این الزام، خدماتی که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباط با موجودیت IT معتبر آغاز کند را لیست می‌نماید.

این الزام بیان می‌دارد که نه تنها ارتباطات در هنگام برقراری اولیه حفاظت می‌شوند، بلکه در حین برقراری مجدد ارتباط پس از یک قطعی نیز از آن‌ها محافظت می‌شود. ممکن است نیاز به تنظیم دستی کانال‌هایی برای حفاظت از سایر ارتباطات وجود داشته باشد. درصورتی‌که پس از یک قطعی، محصول مورد ارزیابی تلاش کند تا ارتباطات را به صورت خودکار و با دخالت عامل انسانی از سر گیرد، ممکن است پنجره‌ای باز شود که مهاجمان بتوانند از طریق آن به اطلاعات مهمی دست یابند یا ارتباط را در معرض خطر قرار دهند.

شماره الزام	نام الزام
۵۰	**مسیر امن ۱**

محصول، باید مسیر ارتباطی امنی که به طور منطقی از کانال‌های دیگر متمایز است را با استفاده از پروتکل [انتخاب: IPsec, SSH, TLS, HTTPS] فراهم نماید و نقاط پایانی را به صورت مطمئن شناسایی کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.

تذکر: در صورتی که هر یک از پروتکل‌های IPsec،SSH،TLS،HTTPS به عنوان پروتکل‌های ارتباطی امن استفاده شود نیاز است از پیوست دو تمامی الزامات مربوط به آن پروتکل تکمیل و به سند هدف امنیتی اضافه گردد.

شماره الزام	نام الزام
۵۱	**مسیر امن ۲**
محصول مورد ارزیابی باید به سرپرست محصول اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کند.	
۵۲	**مسیر امن ۳**
محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه سرپرست محصول و تمام فعالیت‌های راه دور سرپرستی الزامی کند. **نکته کاربردی ۴۰:** این الزام اطمینان حاصل می‌نماید که مدیران سیستم معتبر، تمام ارتباطات از راه دور رابا محصول مورد ارزیابی، از طریق یک مسیر امن آغاز می‌کنند و در طی ارتباط با محصول مورد ارزیابی، همچنان از مسیر امن استفاده می‌نمایند. داده‌های منتقل شده از طریق این مسیر، با استفاده از پروتکل انتخاب‌شده در عبارت انتخاب، رمزگذاری می‌شوند. نویسنده هدف امنیتی، مکانیسم یا مکانیسم‌های پشتیبانی‌شده توسط محصول مورد ارزیابی را انتخاب می‌کند و اطمینان حاصل می‌نماید که الزامات پروتکل پیوست دو متناظر با انتخاب وی، در هدف امنیتی گنجانده شده‌اند.	

۵ الزامات تضمین امنیت

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی محصول است. در این بخش الزامات EAL1 آورده می‌شود که لیست الزامات آن در جدول زیر آمده است.

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	برچسب گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

۱,۵ 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 نمی‌باشد، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه دهندگان محصول باشد.

۱,۱,۵ مشخصات کارکردی

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

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.1.1D)** **شرح مولفه:** توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.2D)** **شرح مولفه:** توسعه دهنده 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 بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه شده 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 مطرح شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی‌باشد.

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.1.1C)** **شرح مولفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی [۱]و پشتیبان کننده‌ی الزام کارکرد امنیتی[۲]توصیف نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.2C)** **شرح مولفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.3C)** **شرح مولفه:** مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.4C)** **شرح مولفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌های کارکرد امنیتی در سند مشخصات کارکردی باشد.

[۱]-SFR-enforcing TSFI
[۲]-SFR-supporting TSFI

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مولفه: (ADV_FSP.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مولفه: (ADV_FSP.1.2E)** **شرح مولفه:** 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» ارائه شده است.

۲,۵ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل مدیریتی و نحوه بررسی محیط عملیاتی توسط مدیر (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 به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگتر

دستورالعمل‌هایی که ارائه دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو می‌باشد.

۱,۲,۵ راهنمای کاربردی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.1D)** **شرح مولفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.1C)** **شرح مولفه:** 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.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.2C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه شده توسط محصول به صورت امن استفاده می‌گردد.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.3C)** **شرح مولفه:**

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های دردسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.4C)** **شرح مولفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع 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 توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.5C)** **شرح مولفه:** 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.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.6C)** **شرح مولفه:** 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.
	نام عنصر: راهنمای کاربردی ۱ **شماره مولفه: (AGD_OPE.1.7C)** **شرح مولفه:**

مولفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مولفه: (AGD_OPE.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مولفه‌های محتوایی را برآورده می‌نماید.

۲,۲,۵ راهنمای آماده‌سازی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.1.1D)** **شرح مولفه:** توسعه دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای آماده-سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.1.1C)**

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مولفه: مستندات آماده‌سازی بایدتمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مولفه: (AGD_PRE.1.2C)** **شرح مولفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

مولفه‌های اقدامات ارزیاب	
راهنمای آماده-سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مولفه: (AGD_PRE.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مولفه: (AGD_PRE.1.2E)** **شرح مولفه:** ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید نماید، محصول می‌تواند به صورت امن برای عمل نمودن آماده شود.

۳,۵ 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 براساس کارکردی که برای محصول در نظر گرفته شده 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 گرفته شده است.

۱,۳,۵ آزمون مستقل

«آزمون مستقل» برای تائید کارکرد محصول که در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و مستندات «راهنمای مدیر» ارائه شده، صورت می‌گیرند. هدف اصلی آزمون اطمینان از برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی می‌باشد. ارزیاب باید در سند «گزارش آزمون»، طرح آزمون و نتایج آن را مستند نماید.

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مولفه: (ATE_IND.1.1D)** **شرح مولفه:** توسعه دهنده باید برای آزمودن، محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مولفه: (ATE_IND.1.1C)** **شرح مولفه:** محصول باید مناسب آزمودن باشد.

مولفه‌های اقدامات ارزیاب	
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مولفه: (ATE_IND.1.1E)**

مولفه‌های اقدامات ارزیاب	
	شرح مولفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده، مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آزمون مستقل ۱ **شماره مولفه: (ATE_IND.1.2E)** **شرح مولفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را آزمون نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل می‌نمایند.

۴,۵ کلاس آسیب‌پذیری

۱,۴,۵ تحلیل آسیب‌پذیری

مولفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مولفه: (AVA_VAN.1.1D)** **شرح مولفه:** توسعه دهنده باید برای آزمودن، محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مولفه: (AVA_VAN.1.1C)** **شرح مولفه:**

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	محصول باید مناسب آزمودن باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مولفه: (AVA_VAN.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آسیب‌پذیری ۱ **شماره مولفه: (AVA_VAN.1.2E)** **شرح مولفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب‌پذیری ۱ **شماره مولفه: (AVA_VAN.1.3E)** **شرح مولفه:** ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۵,۵ کلاس پشتیبانی از چرخه حیات

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

۱,۵,۵ قابلیت‌های پیکربندی

این مولفه جهت معرفی محصول به صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه شده، می‌باشد (بدین معنی که جدا ار برچسب گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصول که توسط مرکز گواهی تائید شده است را به آسانی تشخیص دهد.

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول ۱** **شماره مولفه: (ALC_CMC.1.1D)** **شرح مولفه:** توسعه دهنده باید محصول و مرجع محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول ۱** **شماره مولفه: (ALC_CMC.1.1C)** **شرح مولفه:** محصول باید با یک مرجع یکتا برچسب زده شود.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری محصول ۱** **شماره مولفه: (ALC_CMC.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

۲,۵,۵ حوزه پیکربندی

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مولفه: (ALC_CMS.1.1D)** **شرح مولفه:** ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مولفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مولفه: (ALC_CMS.1.1C)** **شرح مولفه:** لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: پوشش پیکربندی محصول ۱ **شماره مولفه: (ALC_CMS.1.1C)** **شرح مولفه:** لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

مولفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مولفه: (ALC_CMS.1.1E)** **شرح مولفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مولفه‌های محتوایی را برآورده می‌نماید.

۶ پیوست یک: الزامات اختیاری

چنان که در مقدمه این پروفایل حفاظتی نیز گفته شد، الزامات اولیه (الزاماتی که باید توسط محصول مورد ارزیابی رعایت شوند) در این پروفایل تشریح شده‌اند. علاوه بر این، دو نوع الزامات دیگر نیز وجود دارند که در پیوست‌های یک و دو به آن‌ها پرداخته شده است. نوع اول (پیوست حاضر) از الزاماتی تشکیل شده است که می‌توان آن‌ها را در هدف امنیتی گنجاند، اما برای انطباق با این پروفایل حفاظتی ضروری نیستند. نوع دوم (پیوست دو) از الزاماتی تشکیل شده است که مبتنی بر عبارت‌های انتخاب سایر الزامات کارکرد امنیتی این پروفایل حفاظتی هستند. اگر انتخاب‌های خاصی انجام شده باشند، الزامات پیوست مربوطه نیز باید در متن هدف امنیتی گنجانده شوند (مثلاً پروتکل‌های رمزنگاری انتخاب‌شده در یک الزام کانال امن).

۱,۶ کلاس ممیزی امنیت

درصورتی‌که در محصول مورد ارزیابی فضای حافظه محلی برای داده‌های ممیزی در نظر گرفته شده باشد، محصول مورد ارزیابی می‌تواند ادعا کند که مطابق آن چه در «ذخیره سازی رویدادهای ممیزی» گفته شده است، از دستکاری غیر مجاز داده‌های ممیزی جلوگیری به عمل آورد. فضای حافظه محلی دستگاه‌های شبکه برای ذخیره‌سازی داده‌های ممیزی، محدود است. اگر این حافظه پر شود، امکان از دست رفتن داده‌های ممیزی وجود خواهد داشت. ممکن است یک سرپرست محصول بخواهد اطلاعات مربوط به تعداد داده‌های ممیزی ازدست‌رفته را داشته باشد. این تعداد می‌تواند نشان‌دهنده مشکلات سرور باشد؛ بنابراین، «محل ذخیره سازی داده‌های ممیزی» و «محل ذخیره سازی داده‌های ممیزی» تهیه شده‌اند تا این قابلیت‌های اختیاری دستگاه‌های شبکه را بیان کنند. همچنین جدول زیرمربوط به رویدادهای ممیزی مربوط به الزامات مبتنی بر انتخاب می باشد. همانطور که در بخش‌های قبلی هم مطرح شده بود، در صورت نیاز باید بهاین جدول برای ثبت اطلاعات ممیزی مراجعه کرد.

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت شده
۱	محل ذخیره سازی داده‌های ممیزی	نگرانی درباره کمبود فضای حافظه برای رویدادهای ممیزی	
۲	مدیریت کارکرد در محصول ۱ (۱)/ ممیزی	تغییر و تصحیح رفتار در انتقال داده‌های ممیزی به یک موجودیت IT خارجی	
۳	مدیریت کارکرد در محصول ۱ (۲)/ ممیزی	تغییر و تصحیح رفتار در مدیریت داده‌های ممیزی	
۴	مدیریت کارکرد در محصول ۱ (۱)/ ممیزی	تغییر و تصحیح رفتار محصول	
۵	مدیریت کارکرد در محصول ۱ (۲)/ اقدامات مدیریتی	شروع و پایان خدمت	
۶	مدیریت کارکرد در محصول ۱ / فضای ذخیره‌سازی ممیزی محلی	تغییر و تصحیح رفتار کارکرد ممیزی هنگامی که حافظه ممیزی کم است	
۷	مدیریت داده‌های محصول ۱/ اقدامات مدیریتی	تغییر و تصحیح، حذف، تولید/ ورود کلیدهای رمزنگاری شده	

شماره الزام	نام الزام
۵۳	**ذخیره سازی داده‌های ممیزی ۱**
محصول مورد ارزیابی باید از پاک شدن غیر مجاز داده‌های ممیزی جلوگیری نماید.	
۵۴	**ذخیره سازی داده‌های ممیزی ۲**
محصول مورد ارزیابی باید از دستکاری غیر مجاز داده‌های ممیزی جلوگیری نماید.	
۵۵	**محل ذخیره سازی داده‌های ممیزی ۴**
محصول مورد ارزیابی باید در صورت پر شدن حافظه محلی، اطلاعات مربوط به تعداد داده‌های ممیزی [انتخاب: از بین رفته، بازنویسی شده، [اختصاص: سایر اطلاعات]] را ارائه کند. محصول مورد ارزیابی یکی از اقدامات تعیین‌شده در «محل ذخیره سازی داده‌های ممیزی ۳» را انجام می‌دهد. **نکته کاربردی ۴۱:** این گزینه در صورتی باید انتخاب شود که محصول مورد ارزیابی از این کارکرد پشتیبانی کند. درصورتی‌که حافظه محلی داده‌های ممیزی توسط سرپرست محصول خالی شود، شمارنده‌های مربوط به انتخاب انجام‌شده باید به مقادیر اولیه خود برگردند (این مقدار در اکثر موارد صفر است). اسناد راهنما باید به سرپرست محصول هشدار دهند که خالی کردن حافظه ممکن است سبب از دست رفتن داده‌ها شود.	
۵۶	**محل ذخیره سازی داده‌های ممیزی ۵**
محصول مورد ارزیابی باید در هنگام نیاز به کاربر هشدار دهد که حافظه ذخیره‌سازی داده‌های ممیزی در حال اتمام است و/یا محصول، داده‌های ممیزی را در اثر کم بودن حافظه ذخیره‌سازی از دست خواهد داد. **نکته کاربردی ۴۲:** درصورتی‌که محصول مورد ارزیابی امکان تولید پیام مربوطه را داشته باشد این گزینه انتخاب می‌شود. درصورتی‌که داده‌های مربوط به رویدادهای قابل‌ممیزی تنها در حافظه محلی ذخیره شده باشند، این هشدار می‌تواند اهمیت بسیار زیادی داشته باشد. باید اطمینان حاصل نمود که هشدار مورد اشاره در «محل ذخیره سازی داده‌های ممیزی ۳» را می‌توان به اطلاع کاربر رساند. ارتباط باید از طریق سوابق ممیزی صورت گیرد، زیرا ممکن است در هنگام رخ دادن اتفاق، نشست فعالی برای مدیریت این کار وجود نداشته باشد.	

۲،۴ کلاس مدیریت امنیت

شماره الزام	نام الزام
۵۷	**مدیریت کارکرد در محصول ۱ (۱)/ ممیزی**
محصول مورد ارزیابی باید امکان تعیین یا تغییر رفتار در مورد انتقال داده‌های ممیزی به یک موجودیت IT خارجی را به سرپرست محصول محدود کند. **نکته کاربردی ۴۳:** اگر پروتکل انتقال داده‌های ممیزی به یک موجودیت IT خارجی برطبق «محل ذخیره سازی داده‌های ممیزی ۱» قابل پیکربندی باشد، باید همواره الزام «مدیریت کارکرد در محصول ۱ (۱)/ ممیزی» را انتخاب کرد.	
۵۸	**مدیریت کارکرد در محصول ۱ (۲)/ ممیزی**
محصول مورد ارزیابی باید امکان تعیین یا تغییر رفتار در مورد مدیریت داده‌های ممیزی را به سرپرست محصول محدود کند. **نکته کاربردی ۴۴:** این الزام تنها در صورتی باید انتخاب شود که مدیریت داده‌های ممیزی، قابل پیکربندی باشند. عبارت «مدیریت داده‌های ممیزی» به گزینه‌های مختلف «انتخاب» و «اختصاص» در «محل ذخیره سازی داده‌های ممیزی ۲» و «محل ذخیره سازی داده‌های ممیزی ۳» و «محل ذخیره سازی داده‌های ممیزی ۴» اشاره دارد.	
۵۹	**مدیریت کارکرد در محصول ۱ (۱)/ اقدامات مدیریتی**
محصول مورد ارزیابی باید امکان تغییر رفتار در مورد ارائه خدمات امنیتی محصول را به سرپرست محصول محدود کند. **نکته کاربردی ۴۵:** این الزام تنها در صورتی باید انتخاب شود که رفتار محصول درزمینه ارائه خدمات امنیتی، قابل پیکربندی باشد.	
۶۰	**مدیریت کارکرد در محصول ۱ (۲)/ اقدامات مدیریتی**

محصول مورد ارزیابی باید امکان فعال و غیر فعال کردن توابع «ارائه خدمات» را به سرپرست محصول محدود کند.

نکته کاربردی ۴۶:

«مدیریت کارکرد در محصول ۱ (۲)/ اقدامات مدیریتی» تنها در صورتی باید انتخاب شود که سرپرست محصول امکان شروع و متوقف کردن خدمات را داشته باشد.

۶۱	**مدیریت کارکرد در محصول ۱ (۱)/ فضای ذخیره‌سازی ممیزی محلی**

محصول مورد ارزیابی باید امکان تعیین و تغییر رفتار در مورد کارکرد ممیزی در هنگام پر شدن حافظه محلی داده‌های ممیزی را به سرپرست محصول محدود کند.

نکته کاربردی ۴۷:

این الزام تنها در صورتی باید انتخاب شود که رفتار «کارکرد ممیزی در هنگام پر شدن حافظه محلی داده‌های ممیزی»، قابل پیکربندی باشد.

۶۲	**مدیریت داده‌های محصول ۱/ اقدامات مدیریتی**

محصول مورد ارزیابی باید امکان تغییر، پاک کردن، تولید کردن و وارد کردن کلیدهای رمزنگاری را به سرپرست محصول محدود کند.

نکته کاربردی ۴۸:

این الزام تنها در صورتی باید انتخاب شود که کلیدهای رمزنگاری قابل تغییر، پاک کردن، تولید کردن و وارد کردن توسط سرپرست محصول باشند.

۲,۶ کلاس حفاظت از محصول مورد ارزیابی

شماره الزام	نام الزام
۶۳	حفظ وضعیت امن در زمان شکست ۱/ فضای ذخیره‌سازی ممیزی محلی

محصول مورد ارزیابی باید به‌هنگام شکست به‌دلیل «پر شدن حافظه محلی داده‌های ممیزی»، در حالت کارکرد امن باقی بماند.

نکته کاربردی ۴۹:

اگر محصول مورد ارزیابی به گونه‌ای پیکربندی شده باشد که در صورت عدم وجود هیچ حافظه دیگری برای ذخیره کردن داده‌های ممیزی، تمام کارکردهای امنیتی را متوقف کند (در حالت کارکرد امن باقی بماند)، این الزام را باید به محصول مورد ارزیابی اضافه کرد. بدین ترتیب، مهاجم نمی‌تواند داده‌های ممیزی دیگری را تولید کند و اقدامات خود را پنهان نماید. انتظار می‌رود که این رفتار در بخش «گزینه‌های دیگر»). مربوط به الزام «محل ذخیره سازی داده‌های ممیزی ۳» مدل‌سازی شود (در بخش «اختصاص» موجود در «انتخاب»).

۷ پیوست دو: الزامات مبتنی بر انتخاب

چنان که در مقدمه این پروفایل حفاظتی نیز گفته شد، الزامات اولیه (الزاماتی که باید توسط محصول مورد ارزیابی یا پلت‌فرم‌های مربوطه رعایت شوند) در متن این پروفایل حفاظتی گنجانده شده‌اند. بر اساس انتخاب‌هایی که در بخش‌های مختلف این پروفایل حفاظتی انجام می‌شوند، الزامات دیگری نیز مطرح خواهند شد. الزامات زیر به همین منظور ارائه شده‌اند.

همچنین جدول زیرمربوط به رویدادهای ممیزی مربوط به الزامات مبتنی بر انتخاب می‌باشد. همانطور که در بخش‌های قبلی هم مطرح شده بود، در صورت نیاز باید به این جدول برای ثبت اطلاعات ممیزی مراجعه کرد.

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت شده
۱	الزامات پروتکل HTTPS	شکست درایجاد یک نشست HTTPS	دلایل شکست
۲	الزامات پروتکل IPSEC	شکست در ایجاد یک SA مربوطبه پروتکل IPSEC	دلایل شکست

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت شده
۳	الزامات پروتکل SSH Client	شکست درایجاد یک نشست SSH	دلایل شکست
		موفقیت در کلید دهی مجدد SSH	ارتباط با نقاط پایانی غیر محصول (آدرس IP)
۴	الزامات پروتکل SSH Server	شکست درایجاد یک نشست SSH	دلایل شکست
		موفقیت در کلید دهی مجدد SSH	ارتباط با نقاط پایانی غیر محصول (آدرس IP)
۵	الزامات پروتکل TLS Client/ احراز هویت	شکست در ایجاد یک نشست TLS	دلایل شکست
۶	الزامات پروتکل TLS Client/ احراز هویت دو طرفه	شکست در ایجاد یک نشست TLS	دلایل شکست
۷	الزامات پروتکل TLS Server/ احراز هویت	شکست در ایجاد یک نشست TLS	دلایل شکست
۸	الزامات پروتکل TLS Server/ احراز هویت دو طرفه	شکست در ایجاد یک نشست TLS	دلایل شکست
۹	خودآزمایی محصول مورد ارزیابی۲	شکست در خودآزمایی	دلایل شکست (شامل شناساگرگواهی‌نامه‌های غیر معتبر)
۱۰	الزامات به روز رسانی امن	شکست در به روز رسانی	دلایل شکست (شامل شناساگرگواهی‌نامه‌های غیر معتبر)
۱۱	مدیریت کارکرد در محصول ۱ (۲)/ به روز رسانی امن	فعال سازی و غیر فعال سازی جستجوی خودکار بروزرسانی یا بروز رسانی خودکار	

۱,۷ الزامات پروتکل HTTPS

شماره الزام	نام الزام
۶۴	**الزامات پروتکل HTTPS (۱)**
محصول مورد ارزیابی باید پروتکل HTTPS مطابق با RFC 2818 را اجرا کنند. **نکته کاربردی ۵۰:** نویسنده سند هدف امنیتی باید اطلاعات کافی را فراهم آورد و مشخص کند که پیاده‌سازی این پروتکل، مطابق استانداردهای تعریف‌شده است. برای انجام این کار می‌توان عناصری را به این مؤلفه افزود یا اطلاعاتی را به خلاصه مشخصات محصول(فصل آخر سند هدف امنیتی) اضافه کرد.	
۶۵	**الزامات پروتکل HTTPS (۲)**
محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	
۶۶	**الزامات پروتکل HTTPS (۳)**
درصورتی‌که گواهی‌نامه همتا[۱] نامعتبر باشد، محصول مورد ارزیابی باید [انتخاب: اتصال را برقرار ننماید، برای برقراری اتصال درخواست احراز هویت نماید، هیچ اقدام دیگری انجام ندهد]. **نکته کاربردی ۵۱:** اعتبار بر اساس مسیر گواهی‌نامه، تاریخ انقضا و وضعیت لغو بر اساس RFC 5280 تعیین می‌شود.	

۲,۷ الزامات پروتکل IPsec

نقاط پایانی ارتباطات دستگاه‌های شبکه ممکن است با یکدیگر فاصله منطقی یا جغرافیایی داشته باشند، یا ممکن است مسیر ارتباط از تعداد زیادی سیستم غیر قابل‌اعتماد دیگر بگذرد. کارکرد امنیتی دستگاه شبکه باید این قابلیت را داشته باشد که از ترافیک حساس منتقل‌شده حفاظت نماید (مانند ترافیک سرپرست محصول، ترافیک احراز هویت، ترافیک ممیزی و موارد دیگری از این دست). یکی از راه‌های ایجاد کانال ارتباطی بین دستگاه شبکه و یک موجودیت IT خارجی، به گونه‌ای که این ارتباط را بتوان از هر دو طرف احراز هویت کرد، استفاده از IPsec است.

[۱] Peer certificate

IPsec جزء مؤلفه‌های ضروری این پروفایل حفاظتی به شمار نمی‌آید. اگر یک محصول مورد ارزیابی از پروتکل IPsec استفاده کند و انتخاب مربوطه را در «کانال امن» و/یا «مسیر امن» انجام دهد. نیاز است الزامات این پروتکل به سند هدف امنیتی اضافه گردد.

IPsec یک پروتکل همتا به همتا است و بنابراین نیازی به تفکیک الزامات کلاینت و سرور وجود ندارد.

شماره الزام	نام الزام
۶۷	**الزامات پروتکل IPSEC (۱)**
در محصول مورد ارزیابی باید پروتکل IPsec را بر اساس آن چه در RFC 4301 مشخص شده است، پیاده‌سازی شود. **نکته کاربردی ۵۲:** بر اساس RFC 4301 برای پیاده سازی IPSEC جهت محافظت از ترافیک IP باید از یک پایگاه‌داده خط‌مشی امنیتی (SPD) استفاده کرد. با استفاده از SPD می‌توان تعیین کرد که بسته‌های IP چگونه باید مدیریت شوند: ۱- «PROTECT» از بسته‌ها (مثلاً رمزگذاری آن‌ها) ۲- «BYPASS» از سرویس IPSEC (مثلاً عدم رمزگذاری) ۳- «DISCARD» بسته (مثلاً دور ریختن بسته). پایگاه‌داده مذکور را می‌توان به روش‌های مختلفی پیاده‌سازی کرد که از آن جمله می‌توان به لیست‌های کنترل دسترسی به مسیریاب، مجموعه قوانین فایروال، استفاده از یک پایگاه داده SPD سنتی و مواردی از این دست اشاره کرد. صرف نظر از روشی که به کار گرفته می‌شود، قوانینی وجود دارند که بسته‌ها باید از آن‌ها پیروی کنند و اقدامات باید بر اساس آن‌ها انجام شوند. باید ابزارهایی برای تنظیم این قوانین وجود داشته باشند، اما رویکردی عمومی و کلی در این زمینه وجود ندارد. قاعده کلی این است که SPD باید بتواند بسته‌های IP را از یکدیگر تمایز دهد و قوانین مربوطه را در مورد آن‌ها اعمال نماید. ممکن است چند SPD وجود داشته باشند (یک پایگاه داده برای هر واسط شبکه)، اما الزامی در این زمینه وجود ندارد.	
۶۸	**الزامات پروتکل IPSEC (۲)**
محصول مورد ارزیابی باید خط‌مشی در پایگاه داده SPD داشته باشد که تمام موارد غیر منطبق را دور بریزد.	
۶۹	**الزامات پروتکل IPSEC (۳)**
محصول مورد ارزیابی باید مد انتقال و [انتخاب: مد تونل، هیچ مد دیگر] پیاده‌سازی کند.	
۷۰	**الزامات پروتکل IPSEC (۴)**

محصول مورد ارزیابی باید بر اساس آنچه در RFC 4303 گفته شده است فریمورک ESP از پروتکل IPSEC را با استفاده از الگوریتم‌های رمزنگاری AES-CBC-128, AES-CBC-256 و [انتخاب: AES-GCM-128، AES-GCM-256، هیچ الگوریتم دیگر] و همچنین الگوریتم درهم‌سازی امن (SHA) مبتنی بر HMAC، پیاده‌سازی کند. الگوریتم‌های رمزنگاری AES-CBC-128, AES-CBC-256 در RFC 3602 تشریح شده‌اند. همچنین AES-GCM-128 و AES-GCM-256 در RFC 4106 تشریح شده اند.)
۷۱ **الزامات پروتکل IPSEC (۵)**
محصول مورد ارزیابی باید یکی از این پروتکل‌ها را به کار گیرد: [انتخاب: • IKEv1، با استفاده از مد اصلی برای انتقال در فاز اول، طبق آنچه که در RFC 4109, RFCs 2407,2408,2409، [انتخاب: هیچ RFC دیگر برای اعداد متوالی بسط‌یافته، RFC4304 برای اعداد متوالی بسط‌یافته] و [انتخاب: هیچ RFC دیگر برای توابع درهم‌ساز، RFC 4868 برای توابع درهم‌ساز] • IKEv2، مطابق با آنچه که در RFC 5996 تشریح شده است و [انتخاب: بدون پشتیبانی از پیمایش NAT[۱]، با پشتیبانی اجباری از پیمایش NAT چنان که در بخش ۲,۲۳ از RFC 5996 تشریح شده است] و [انتخاب: هیچ RFC دیگر برای توابع درهم‌ساز، RFC 4868 برای توابع درهم‌ساز]].
نکته کاربردی ۵۳: اگر محصول مورد ارزیابی برای دو پروتکل IKEv1 یا IKEv2 از الگوریتم درهم‌ساز SHA-2 استفاده کند، نویسنده سند هدف امنیتی باید RFC 4868 را انتخاب نماید.
۷۲ **الزامات پروتکل IPSEC (۶)**
محصول مورد ارزیابی باید اطمینان حاصل کند که برای رمزگذاری پی‌آیند[۲] در [انتخاب: IKEv1،IKEv2]، از الگوریتم‌های رمزنگاری AES-CBC-128 و AES-CBC-256 (طبق آنچه که در RFC 3602 تشریح شده است) و [انتخاب: AES-GCM-128, AES-GCM-256 مطابق آنچه که درRFC 5282 تشریح شده است، هیچ الگوریتم دیگر] استفاده شده است.
نکته کاربردی ۵۴:

[۱] NAT traversal

[۲] Payload

AES-GCM-128 و AES-GCM-256 تنها در صورتی انتخاب می‌شوند که IKEv2 نیز انتخاب شده باشد، همچنین هیچ RFC ای وجود ندارد که AES-GCM را برای IKEv1 تعریف کرده باشد.
۷۳ **الزامات پروتکل IPSEC (۷)**
محصول مورد ارزیابی باید اطمینان حاصل کند که [انتخاب: • سرپرست محصول می‌تواند طول عمر SA فاز اول IKEv1 را بر اساس [انتخاب: o تعداد بایت‌ها، o مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد.] پیکر بندی کند. • سرپرست محصول می‌تواند طول عمر IKEv2 SA را بر اساس [انتخاب: o تعداد بایت‌ها، o مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد.] پیکر بندی کند. **نکته کاربردی ۵۵:** نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در «الزامات پروتکل IPSEC (۵)» صورت گرفته است) را انتخاب می‌کند. نویسنده سند هدف امنیتی همچنین طول عمر را بر اساس مقادیر یا بر اساس زمان (ترکیبی از این دو) انتخاب می‌کند. برای رعایت این الزام، لازم است که مدت زمان توسط سرپرست محصول قابل پیکربندی باشد (بر اساس دستورالعمل‌هایی که در سند شرح محصول ذکر شده‌اند). به طور کلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SA را باید در سند شرح محصول در نظر گرفت.
۷۴ **الزامات پروتکل IPSEC (۸)**
محصول مورد ارزیابی باید اطمینان حاصل کند که [انتخاب: • سرپرست محصول می‌تواند طول عمر SA فاز دوم IKEv1 را بر اساس [انتخاب: o تعداد بایت‌ها، o مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۸] ساعت قرار داد.]

پیکربندی کند.

- سرپرست محصول می‌تواند طول عمر IKEv2 Child SA را بر اساس [انتخاب:
  - تعداد بایت‌ها،
  - مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۸] ساعت قرار داد.

]

پیکربندی کند.

نکته کاربردی ۵۶:

نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در «الزامات پروتکل IPSEC (۵)» صورت گرفته است) را انتخاب می‌کند. نویسنده سند هدف امنیتی همچنین طول عمر را بر اساس مقادیر یا بر اساس زمان (ترکیبی از این دو) انتخاب می‌کند. برای رعایت این الزام، لازم است که مدت زمان توسط سرپرست محصول قابل پیکربندی باشد (بر اساس دستورالعمل‌هایی که در سند شرح محصول ذکر شده‌اند). به طور کلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SA را باید در سند شرح محصول در نظر گرفت.

۷۵	**الزامات پروتکل IPSEC (۹)**

محصول باید مقدار x را که در تبادل کلید IKE DiffieHellman (x در $g^x \bmod p$) به کار می‌رود، با استفاده از تولیدکننده بیت تصادفی که در الزام شماره ۱۴ «تولید بیت تصادفی ۱» مشخص شده است و دست‌کم طول آن [اختصاص: تعداد بیت‌های (یک یا بیش از یک) باشد که حداقل دو برابر قدرت امنیتی گروه Diffie-Hellman مذاکره‌شده باشد] تولید نماید.

نکته کاربردی۵۷:

از آنجایی که در پیاده‌سازی ممکن است گروه‌های مختلف Diffie-Hellman در مذاکره برای استفاده در SA مجاز باشند الزام «الزامات پروتکل IPSEC (۹)» می‌تواند مقادیر متعددی داشته باشند. نویسند سند هدف امنیتی برای هر گروه DH مورد پشتیبانی، از جدول ۲ در دفترچه NIST SP 800-57 «توصیه‌هایی برای مدیریت کلید – بخش اول: عمومی» برای تعیین قدرت امنیتی («تعداد بیت‌های امنیتی») مربوط به گروه DH راهنمایی بگیرد. سپس هر ارزش منحصربه‌فرد برای پر کردن قسمت اختصاص هر مورد به کار می‌رود. برای مثال، اگر فرض کنیم در پیاده‌سازی گروه DH ۱۴ (2048-bit MODP) و گروه ۲۰ (ECDH با استفاده Curve P-384 در NIST) پشتیبانی می‌شود، با توجه به جدول ۲، تعداد بیت‌های امنیتی برای گروه ۱۴، ۱۱۲ و برای گروه ۲۰، ۱۹۲ است.

۷۶	**الزامات پروتکل IPSEC (۱۰)**

محصول باید نانس‌های مورداستفاده در تبادلات [انتخاب: IKEv1، IKEv2] با طول [انتخاب:

- [اختصاص: قدرت امنیتی مربوط به گروه Diffie-Hellman مذاکره‌شده]؛
- حداقل ۱۲۸ بیت اندازه و حداقل نصف اندازه خروجی تابع درهم‌سازی نیمه‌تصادفی مذاکره‌شده (PRF)] را تولید کند.

نکته کاربردی۵۸:

، اگر IKEv2 نیز انتخاب شده باشد (همان طور که در RFC5996 اجباری شده است)، نویسنده سند هدف امنیتی باید دومین گزینه را برای طول نانس انتخاب کند. نویسنده سند هدف امنیتی مجاز است هر یک از گزینه‌ها را برای IKEv1 انتخاب نماید.

در اولین گزینه برای طول نانس، از آنجایی که در پیاده‌سازی ممکن است مذاکره کردن برای استفاده از گروه‌های مختلف Diffie-Hellman در ساخت تضمین‌های امنیتی مجاز باشد، اختصاص «الزامات پروتکل IPSEC (۱۰)» می‌تواند مقادیر متعددی داشته باشد.

نویسنده سند هدف امنیتی برای هر گروه DH مورد پشتیبانی، از جدول ۲ در دفترچه NIST SP 800-57 «توصیه‌هایی برای مدیریت کلید – بخش اول: عمومی» برای تعیین قدرت امنیتی («تعداد بیت‌های امنیتی») مربوط به گروه DH راهنمایی بگیرد. سپس هر ارزش منحصربه‌فرد برای پر کردن قسمت اختصاص هر مورد به کار می‌رود. برای مثال، اگر فرض کنیم در پیاده‌سازی گروه DH ۱۴ (2048-bit MODP) و گروه ۲۰ (ECDH با استفاده Curve P-384 در NIST) پشتیبانی می‌شود، با توجه به جدول ۲، تعداد بیت‌های امنیتی برای گروه ۱۴، ۱۱۲ و برای گروه ۲۰، ۱۹۲ است. به این دلیل که نانس‌ها ممکن است پیش از اینکه در مورد گروه DH مذاکره شود، مبادله شوند، توصیه می‌شود نانس به‌کاررفته به اندازه کافی بزرگ باشد که همه پیشنهادهای محصول انتخاب‌شده در تبادل را پشتیبانی نماید.

۷۷	**الزامات پروتکل IPSEC (۱۱)**

محصول باید اطمینان حاصل نماید که همه پروتکل‌های IKE، گروه‌های DH ۱۴ (2048-bit MODP) و [انتخاب: گروه ۱۹ (256-bit Random ECP)، گروه ۲۰ (384-bit Random ECP)، گروه ۲۴ (2048-bit MODP به همراه 256-bit POS)، گروه ۵ (1536-bit MODP)، [اختصاص: سایر گروه‌های DH که توسط محصول پیاده‌سازی می‌شوند]، هیچ گروه DH دیگری] را پشتیبانی می‌کنند.

۷۸	**الزامات پروتکل IPSEC (۱۲)**

محصول باید به صورت پیش‌فرض بتواند اطمینان حاصل نماید که قدرت الگوریتم متقارن (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [انتخاب: فاز ۱ IKEv1، IKEv2 IKE_SA] مذاکره شده است، بیشتر یا مساوی قدرت الگوریتم متقارنی (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [انتخاب: فاز ۲ IKEv1، IKEv2 CHILD_SA] مذاکره شده است، باشد.

نکته کاربردی۵۹:

نویسنده سند هدف امنیتی یکی یا هر دوی انتخاب‌های IKE را بر اساس اینکه کدام یک توسط محصول پیاده‌سازی می‌شود، انتخاب می‌کند.	
۷۹	**الزامات پروتکل IPSEC (۱۳)**
محصول باید اطمینان حاصل نماید که همه پروتکل‌های IKE احراز هویت همتا را با استفاده از [انتخاب: RSA، ECDSA] که از گواهی‌های X.509v3 مطابق با RFC4945 و [انتخاب: کلیدهای پیش‌اشتراکی، هیچ روش دیگری] استفاده می‌کند، انجام می‌دهند.	
۸۰	**الزامات پروتکل IPSEC (۱۴)**
محصول باید کانال امن را فقط با همتاهای دارای گواهی معتبر برقرار سازد.	

۳,۷ الزامات پروتکل SSH Client

شماره الزام	نام الزام
۸۱	**الزامات پروتکل SSH Client (۱)**
محصول باید پروتکل SSH را مطابق با RFC های 4251، 4252، 4253، 4254 و [انتخاب: RFC های 5647، 5656، 6187، 6668، هیچ RFC دیگری] پیاده‌سازی نماید. **نکته کاربردی ۶۰:** نویسنده سند هدف امنیتی انتخاب می‌کند که مطابقت با کدام یک از RFC های وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً، الگوریتم‌های رمزنگاری معتبر). RFC4253 مشخص می‌کند که الگوریتم‌های رمزنگاری خاصی "REQUIRED" (موردنیاز) هستند. در نتیجه، پشتیبانی از این الگورتیم‌ها باید پیاده‌سازی شوند، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد.	
۸۲	**الزامات پروتکل SSH Client (۲)**
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، روش‌های احراز هویت زیر مطابق با آنچه که در RFC4252 توضیح داده‌شده است، پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، احراز هویت مبتنی بر کلمه عبور.	
۸۳	**الزامات پروتکل SSH Client (۳)**
همان طور که در RFC4253 توضیح داده‌شده است، محصول باید اطمینان حاصل نماید که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک ارتباطات انتقال SSH کنار گذاشته شوند.	

نکته کاربردی۶۱:

RFC4253 امکان پذیرش «بسته‌های بزرگ» را فراهم می‌کند، با این اخطار که بسته‌ها باید «طول مناسبی» داشته باشند یا اینکه کنار گذاشته می‌شوند. توصیه می‌شود این اختصاص توسط نویسنده هدف امنیتی با درنظر گرفتن بیشترین اندازه بسته که قابل پذیرش است پر شود تا به این وسیله «طول مناسب» برای محصول تعریف شود.

۸۴	**الزامات پروتکل SSH Client (۴)**
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری: aes256-cbc, aes128-cbc, [انتخابAEAD_AES_256_GCM AEAD_AES_128_GCM, هیچ الگوریتم رمزنگاری دیگری] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.	
۸۵	**الزامات پروتکل SSH Client (۵)**
محصول باید اطمینان حاصل نماید که پیاده‌سازی پروتکل انتقالSSH، از [انتخاب: ssh-rsa, ecdsa-sha2-nistp256] و [انتخاب: ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384، هیچ الگوریتم کلید عمومی دیگری] به عنوان الگوریتم‌های کلید عمومی خودش استفاده می‌کند و سایر الگوریتم‌های کلید عمومی رد می‌شوند.	
۸۶	**الزامات پروتکل SSH Client (۶)**
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقالSSH، از [انتخاب: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512] و [انتخاب: AEAD_AES_128_GCM, AEAD_AES_256_GCM، هیچ الگوریتمMAC دیگری] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند.	
۸۷	**الزامات پروتکل SSH Client (۷)**
محصول باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1 , ecdh-sha2-nistp256] و [انتخاب: ecdh-sha2-nistp384, ecdh-sha2-nistp521, هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.	
۸۸	**الزامات پروتکل SSH Client (۸)**
محصول باید اطمینان حاصل نماید که کلید اتصال SSH حتماً بعد از ارسال تعداد 2^{28} بسته با آن کلید، تجدید شود.	
۸۹	**الزامات پروتکل SSH Client (۹)**

محصول باید اطمینان حاصل نماید که کاربر SSH، سرور SSH را با استفاده از یک پایگاه داده محلی احراز هویت می‌کند و نام هر میزبان را با کلید عمومی متناظر آن یا [انتخاب: فهرستی از مراجع صدور گواهی مطمئن، هیچ روش دیگری] همان‌طور که در RFC 4251 بخش ۴,۱ تشریح شده است مطابقت می‌دهد. **نکته کاربردی۶۲:** تنها در صورتی می‌توان گزینه «لیست مراجع صدور گواهی مطمئن» را انتخاب کرد که x509v3-ecdsa-sha2-nistp256 یا x509v3-ecdsa-sha2-nistp384 در «الزامات پروتکل SSH Client (۵)» انتخاب‌شده باشد.

۴,۷ الزامات پروتکل SSH Server

شماره الزام	نام الزام
۹۰	**الزامات پروتکل SSH Server (۱)**
محصول باید پروتکل SSH مطابق با RFC های 4251، 4252، 4253، 4254 و [انتخاب: RFC های 5647، 5656، 6187، 6668، هیچ RFC دیگری] را پیاده‌سازی نماید. **نکته کاربردی۶۳:** نویسنده سند هدف امنیتی انتخاب می‌کند که مطابقت با کدام یک از RFC های وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً، الگوریتم‌های رمزنگاری معتبر). RFC4253 مشخص می‌کند که الگوریتم‌های رمزنگاری خاصی "REQUIRED" (موردنیاز) هستند. در نتیجه، پشتیبانی از این الگورتیم‌ها باید پیاده‌سازی شوند، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد.	
۹۱	**الزامات پروتکل SSH Server (۲)**

محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، همان‌طور که در RFC4252 توضیح داده‌شده است، روش‌های احراز هویت زیر پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، احراز هویت مبتنی بر کلمه عبور.	
۹۲	**الزامات پروتکل SSH Server (۳)**
همان‌طور که در RFC4253 توضیح داده‌شده است، محصول باید اطمینان حاصل نماید که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک اتصال انتقال SSH کنار گذاشته شوند. **نکته کاربردی۶۴:** RFC4253 امکان پذیرش «بسته‌های بزرگ» را فراهم می‌کند، با این اخطار که بسته‌ها باید «طول مناسبی» داشته باشند یا کنار گذاشته می‌شوند. توصیه می‌شود این اختصاص توسط نویسنده هدف امنیتی و با در نظر گرفتن بیشترین اندازه بسته که قابل‌پذیرش است پر شود تا به این وسیله «طول مناسب» برای محصول تعریف شود.	
۹۳	**الزامات پروتکل SSH Server (۴)**
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری: aes256-cbc ,aes128-cbc, [انتخاب: AEAD_AES_256_GCM AEAD_AES_128_GCM, هیچ الگوریتم رمزنگاری دیگری] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.	
۹۴	**الزامات پروتکل SSH Server (۵)**
محصول باید اطمینان حاصل نماید که پیاده‌سازی پروتکل انتقالSSH، از [انتخاب: ssh-rsa, ecdsa-sha2-nistp256] و [انتخاب: ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384، هیچ الگوریتم کلید عمومی دیگری] به عنوان الگوریتم‌های کلید عمومی خودش استفاده می‌کند و سایر الگوریتم‌های کلید عمومی رد می‌شوند.	
۹۵	**الزامات پروتکل SSH Server (۶)**
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقالSSH، از [انتخاب: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512] و [انتخاب: AEAD_AES_128_GCM, AEAD_AES_256_GCM، هیچ الگوریتمMAC دیگری] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند.	
۹۶	**الزامات پروتکل SSH Server (۷)**
محصول باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1 , ecdh-sha2-nistp256] و [انتخاب:	

ecdh-sha2-nistp384, ecdh-sha2-nistp521 , هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.
۹۷ **الزامات پروتکلSSH Server (۸)**
محصول باید اطمینان حاصل نماید که کلید اتصال SSH حتماً تا قبل از پایان ارسال تعداد2^{28} بسته با آن کلید، تجدید شود.

۵,۷ الزامات پروتکلTLS Client/ احراز هویت

شماره الزام	نام الزام
۹۸	**الزامات پروتکلTLS Client/ احراز هویت ۱**
محصول باید [انتخاب: TLS 1.2 (RFC5246)، TLS1.1 (RFC4346)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • مجموعه‌های رمز اجباری: • [TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268] • [انتخاب: مجموعه‌های رمز اختیاری: o TLS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268 o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492 o TLS_ECDHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492 o TLS_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5246 o TLS_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246 o TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256مطابق با RFC 5246 o TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289	

o TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289	
o TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289	
o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289	
o TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289	
• هیچ مجموعه رمز دیگری]].	
نکته کاربردی ۶۵: مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. توجه شود که به‌منظور اطمینان از مطابقت با RFC 5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.	
۹۹	الزامات پروتکلTLS Client/ احراز هویت ۲
محصول باید تأیید نماید که با توجه به RFC 6125، شناسه[۱] ارائه‌شده با شناسه مرجع مطابقت داشته باشد. **نکته کاربردی۶۶:** قوانین مربوط به تأیید شناسه در بخش ۶ از RFC 6125 توضیح داده‌شده‌اند. شناسه مرجع توسط کاربر (مثلاً واردکردن یک URL در مرورگر وب یا کلیک کردن روی یک لینک)، توسط پیکربندی (مثلاً پیکربندی نام یک سرور ایمیل یا سرور احراز هویت) یا توسط یک برنامه کاربردی (مثلاً یک پارامتر از یک API) بر اساس سرویس برنامه کاربردی، تعیین می‌شود. بر مبنای دامنه منبع از شناسه مرجع منحصربه‌فرد و نوع سرویس برنامه کاربردی (مثلاً HTTP، SIP، LDAP)، client همه شناسه‌های مرجعی که قابل‌قبول هستند را نظیر یک Common Namee برای قسمت Subject Name از گواهینامه و یک نام DNS (حساس به بزرگ و کوچک بودن حروف) ، نام URL و نام سرویس برای قسمت Subject Alternative Name. سپس client لیست همه شناسه‌های مرجع قابل‌قبول را با شناسه‌های ارائه‌شده در گواهی سرور TLS مقایسه می‌کند.	
۱۰۰	الزامات پروتکلTLS Client/ احراز هویت ۳
محصول باید کانال امن را فقط در صورتی برقرار سازد که گواهی همتا معتبر باشد. **نکته کاربردی۶۷:**	

[۱] Identifier

اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC5280 تعیین می‌گردد. اعتبار گواهی بر اساس «الزامات پروتکل X509» آزمودهٔ می‌شود.	
۱۰۱	الزامات پروتکلTLS Client/ احراز هویت ۴
محصول باید Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب: secp256r1, secp384r1, secp521r1, یا هیچ گزینه دیگری] در پیام ClientHello ارائه دهد. **نکته کاربردی۶۸:** اگر در «الزامات پروتکلTLS Client/ احراز هویت ۱» مجموعه‌های رمز بیضوی انتخاب‌شده باشند، انتخاب یک یا چند مورد از منحنی‌ها الزامی است. اگر در «الزامات پروتکلTLS Client/ احراز هویت ۱» هیچ‌کدام از مجموعه‌های رمز بیضوی انتخاب‌نشده باشند، هیچ‌کدام از منحنی‌ها نباید انتخاب شوند. این الزام مجموعه رمزهای بیضوی مجاز برای احراز هویت و توافق کلید را به NIST curve های « عملیات رمزنگاری ۱ (۲)» و «مدیریت کلید رمزنگاری ۱» و «مدیریت کلید رمزنگاری ۲» محدود می‌سازند. این افزونه برای کاربرانی که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.	

۶,۷ الزامات پروتکلTLS Client همراه با احراز هویت دوطرفه

شماره الزام	نام الزام
۱۰۲	**الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۱**
محصول باید [انتخاب: TLS 1.2 (RFC5246)، TLS1.1 (RFC4346)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • مجموعه‌های رمز اجباری: • [TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268] • [انتخاب: مجموعه‌های رمز اختیاری: o LS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268	

o	TLS_DHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
o	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
o	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
o	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
o	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
o	TLS_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5246
o	TLS_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
o	TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256مطابق با RFC 5246
o	TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
o	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
o	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289
o	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
o	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
o	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
o	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
•	هیچ مجموعه رمز دیگری]].

نکته کاربردی۶۹:

مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند.

مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. توجه شود که به‌منظور اطمینان از مطابقت با RFC 5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.

۱۰۳	**الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۲**

محصول باید تأیید نماید که با توجه به RFC 6125، شناسه[۱] ارائه‌شده با شناسه مرجع مطابقت داشته باشد.

نکته کاربردی۷۰:

[۱] Identifier

قوانین مربوط به تأیید شناس در بخش ۶ از RFC 6125 توضیح داده‌شده‌اند. شناسه مرجع توسط کاربر (مثلاً واردکردن یک URL در مرورگر وب یا کلیک کردن روی یک لینک)، توسط پیکربندی (مثلاً پیکربندی نام یک سرور ایمیل یا سرور احراز هویت) یا توسط یک برنامه کاربردی (مثلاً یک پارامتر از یک API) بر اساس سرویس برنامه کاربردی، تعیین می‌شود. بر مبنای دامنه منبع از شناسه مرجع منحصربه‌فرد و نوع سرویس برنامه کاربردی (مثلاً HTTP، SIP، LDAP)، client همه شناسه‌های مرجعی که قابل‌قبول هستند را نظیر یک Common Namee برای قسمت Subject Name از گواهینامه و یک نام DNS (حساس به بزرگ و کوچک بودن حروف) ، نام URL و نام سرویس برای قسمت Subject Alternative Name. سپس client لیست همه شناسه‌های مرجع قابل‌قبول را با شناسه‌های ارائه‌شده در گواهی سرور TLS مقایسه می‌کند.

۱۰۴	**الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۳**
محصول باید کانال امن را فقط در صورتی برقرار سازد که گواهی همتا معتبر باشد.	

نکته کاربردی۷۱:

اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC5280 تعیین می‌گردد.

۱۰۵	**الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۴**
محصول باید Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب: secp256r1, secp384r1, secp521r1, یا هیچ گزینه دیگری] در پیام ClientHello ارائه دهد.	

نکته کاربردی۷۲:

اگر در «الزامات پروتکلTLS Client/ احراز هویت ۱» مجموعه‌های رمز بیضوی انتخاب‌شده باشند، انتخاب یک یا چند مورد از منحنی‌ها الزامی است. اگر در «الزامات پروتکلTLS Client/ احراز هویت ۱» هیچ‌کدام از مجموعه‌های رمز بیضوی انتخاب‌نشده باشند، هیچ‌کدام از منحنی‌ها نباید انتخاب شوند. این الزام مجموعه رمزهای بیضوی مجاز برای احراز هویت و توافق کلید را به NIST curve های « عملیات رمزنگاری ۱ (۲)» و «مدیریت کلید رمزنگاری ۱» و «مدیریت کلید رمزنگاری ۲» محدود می‌سازند. این افزونه برای کاربرانی که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.

۱۰۶	**الزامات پروتکلTLS Client/ احراز هویت دوطرفه ۵**
محصول باید با استفاده از گواهینامه X.509v3، از احراز هویت دوطرفه پشتیبانی نماید.	

نکته کاربردی۷۳:

استفاده از گواهی‌های نسخه سوم X.509 برای محصول در «الزامات پروتکل X509 (۳)» توضیح داده‌شده است. با توجه به این الزام، کاربر حتماً قابلیت ارائه گواهی به سرور TLS به‌منظور احراز هویت دو طرفه را داشته باشد.

۷,۷ **الزامات پروتکل**TLS Server

شماره الزام	نام الزام
۱۰۷	**الزامات پروتکلTLS Server/ احراز هویت ۱**
محصول باید [انتخاب: TLS 1.2 (RFC5246)، TLS1.1 (RFC4346)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • مجموعه‌های رمز اجباری: • [TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268] • [انتخاب: مجموعه‌های رمز اختیاری: o LS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268 o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492 o TLS_ECDHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492 o TLS_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5246 o TLS_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246 o TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256مطابق با RFC 5246 o TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289 o TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289	

o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289 o TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289 • هیچ مجموعه رمز دیگری]]. **نکته کاربردی۷۴:** مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. توجه شود که به‌منظور اطمینان از مطابقت با RFC 5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.

۱۰۸	**الزامات پروتکلTLS Server/ احراز هویت ۲**
محصول 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 کاربردی۷۵:** تمام نسخه‌های SSL و نسخه TLS 1.0 رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در «الزامات پروتکلTLS Server/ احراز هویت ۱» انتخاب‌نشده است، در اینجا انتخاب شود.	

۱۰۹	**الزامات پروتکلTLS Server/ احراز هویت ۳**
محصول 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] ،[انتخاب: ۳۰۷۲ بیت، هیچ اندازه دیگری]] ایجاد نماید. **نکته کاربردی۷۶:** اگر در بخش « الزامات پروتکلTLS Server/ احراز هویت ۱» سند هدف امنیتی مجموعه رمزهایDHE یا ECDHE لیست شده باشند، سند هدف امنیتی باید شامل Diffie-Hellman یا منحنی‌هایNIST لیست شده در این الزام باشد.	

۸,۷ الزامات پروتکلTLS Server همراه با احراز هویت دو طرفه

شماره الزام	نام الزام

۱۱۰	**الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۱**

محصول باید [انتخاب: TLS 1.2 (RFC5246)، TLS1.1 (RFC4346)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید:

- مجموعه‌های رمز اجباری:
- [TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268]
- [انتخاب: مجموعه‌های رمز اختیاری:
  - LS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
  - TLS_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5246
  - TLS_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
  - TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256مطابق با RFC 5246
  - TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- هیچ مجموعه رمز دیگری]].

نکته کاربردی۷۷:

مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند.

مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. توجه شود که به‌منظور اطمینان از مطابقت با RFC 5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.	
الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۲	**۱۱۱**
محصول 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 کاربردی۷۸: تمام نسخه‌های SSL و نسخه ۱,۰ TLS رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در « الزامات پروتکلTLS Server/ احرازهویت دوطرفه ۱» انتخاب‌نشده است، در اینجا انتخاب شود.	
الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۳	**۱۱۲**
محصول 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] ،[انتخاب: ۳۰۷۲ بیت، هیچ اندازه دیگری]] ایجاد نماید.	
نکته کاربردی۷۹: اگر در بخش «الزامات پروتکلTLS Server/ احراز هویت ۱» سند هدف امنیتی مجموعه رمزهایDHE یا ECDHE لیست شده باشند، سند هدف امنیتی باید شامل Diffie-Hellman یا منحنی‌های NIST لیست شده در این الزام باشد.	
الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۴	**۱۱۳**
محصول باید با استفاده از گواهی‌نامه‌های X.509v3 احراز هویت دو طرفه کلاینت TLS، را پشتیبانی نماید.	
نکته کاربردی۸۰: استفاده از گواهی‌های نسخه سوم X.509 برای محصول در «الزامات پروتکل X509 (۳)» توضیح داده‌شده است. در کنار این الزام، باید در این استفاده گواهی‌های کلاینت نیز برای احراز هویت مشترک پشتیبانی شوند.	
الزامات پروتکلTLS Server/ احراز هویت دو طرفه ۵	**۱۱۴**
درصورتی‌که گواهی همتا معتبر نباشد، محصول نباید کانال امن را برقرار سازد.	
نکته کاربردی۸۱:	

اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC5280 تعیین می‌گردد. اعتبار گواهی بر اساس تمامی «الزامات پروتکل X509» آزموده می‌شود.

۱۱۵	الزامات پروتکلTLS Server/ احراز هویت دو طرفه ۶

درصورتی‌که نام مشخص‌شده[۱] (DN) یا نام مستعار موجودیت فعال[۲] (SAN) در یک گواهینامه با شناسه مورد انتظار برای همتا مطابقت نداشته باشد، محصول نباید کانال امن را برقرار سازد.

نکته کاربردی۸۲:

ممکن است شناسه همتا در قسمت Subject یا Alternative Name Extention از گواهینامه باشد. شناسه مورد انتظار ممکن است پیکربندی شود، با Domain Name، 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.

۹,۷ الزامات خودآزمایی محصول مورد ارزیابی

شماره الزام	نام الزام
۱۱۶	خودآزمایی محصول مورد ارزیابی۲

اگر برای آزمون‌های خودآزمایی از یک گواهینامه استفاده شود و آن گواهینامه غیر معتبر اعلام‌شده باشد، محصول باید در آزمون خودآزمایی ناموفق باشد.

نکته کاربردی۸۳:

گواهینامه‌ها را می‌توان به‌صورت اختیاری برای آزمون‌های خودآزمایی استفاده کرد (خودآزمایی محصول۱). اگر برای آزمون‌های خودآزمایی از گواهینامه‌ها استفاده شود، سند هدف امنیتی باید شامل این مورد باشد. اگر در «الزامات پروتکل X509 (۳)» «امضای کدها برای تأیید صحت» انتخاب‌شده باشد، سند هدف امنیتی باید شامل «خودآزمایی محصول مورد ارزیابی۲» باشد. اعتبار به‌وسیله مسیر گواهینامه، تاریخ انقضاء و وضعیت ابطال مطابق با «الزامات پروتکل X509» تعیین می‌گردد.

[۱] Distinguished name

[۲] Subject Alternative Name

۱۰,۷ الزامات به‌روزرسانی امن

شماره الزام	نام الزام
۱۱۷	**الزامات به‌روزرسانی امن ۴**
درصورتی‌که گواهینامه امضای کد آن غیر معتبر اعلام‌شده است، محصول نباید یک به‌روزرسانی را نصب نماید.	
۱۱۸	**الزامات به‌روزرسانی امن ۵**
هنگامی‌که گواهینامه به علت انقضای آن، غیر معتبر اعلام‌شده است، محصول باید [انتخاب: اجازه بدهد که در این موارد سرپرست محصول در موردپذیرش گواهی تصمیم‌گیری نماید، گواهی را بپذیرد، گواهی را نپذیرد].	
نکته کاربردی۸۴: گواهینامه‌ها را می‌توان به‌صورت اختیاری برای امضای کدها در به‌روزرسانی‌های نرم‌افزار سیستم استفاده کرد (الزامات به‌روزرسانی امن ۳). اگر برای اعتبارسنجی به‌روزرسانی‌ها از گواهینامه‌ها استفاده شود، سند هدف امنیتی باید شامل الزام شماره ۲۳ «الزامات پروتکل X509 (۳)»، الزام شماره ۱۱۷ « الزامات به‌روزرسانی امن ۴» و الزام شماره ۱۱۸ « الزامات به‌روزرسانی امن ۵» باشد اعتبار به‌وسیله مسیر گواهینامه، تاریخ انقضاء و وضعیت ابطال مطابق با تمامی «الزامات پروتکل X509» تعیین می‌گردد. برای گواهینامه‌های منقضی، نویسنده هدف امنیتی انتخاب می‌کند که گواهینامه پذیرفته شود، رد شود یا تصمیم‌گیری در خصوص پذیرش یا رد گواهینامه به سرپرست محصول واگذار شود.	
۱۱۹	**مدیریت کارکرد در محصول مورد ارزیابی ۱ (۲) / به‌روزرسانی امن**
محصول باید قابلیت فعال‌سازی و غیرفعال سازی کارکردهای [انتخاب: جستجو برای به‌روزرسانی خودکار، به‌روزرسانی خودکار]را برای سرپرست محصول فراهم آورد.	
نکته کاربردی۸۵: این الزام تنها زمانی قابل پیاده‌سازی است که محصول امکان پشتیبانی از به‌روزرسانی خودکار را فراهم کند و اجازه فعال و غیرفعال سازی این قابلیت را بدهد. فعال‌سازی و غیرفعال سازی قابلیت به‌روزرسانی خودکار به سرپرست محصول محدود می‌شود.	