به نام خدا

پروفایل حفاظتی

سامانه مدیریت رخداد و حوادث امنیتی

(SIEM)

آبان ۹۹

نسخه ۲,۲

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 را که در این سند برای برآورده کردن الزامات ارائه‌شده‌اند، در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک کنند. مرکز مدیریت راهبردی افتا با همکاری مرکز تحقیقات صنایع انفورماتیک و سازمان فناوری اطلاعات ایران این سند را در راستای این هدف تهیه کرده است. در این سند الزامات امنیتی SIEM بیان می‌شود.

این سند بر اساس سند طرح ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R5 تهیه شده است.

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

فهرست

۱ شرح محصول

اصطلاح SIEM به مجموعه‌ای از نرم‌افزار، تجهیزات و سرویس‌های مدیریت‌شده اطلاق می‌گردد که هشدارهای امنیتی که توسط سخت‌افزار شبکه و برنامه‌های کاربری تولیدشده‌اند را ازنظر امنیتی تحلیل می‌نماید.

در برخی موارد اصطلاحات SEM، SIM و SIEM به‌جای یکدیگر بکار می‌روند. بخشی از مدیریت امنیتی که با مانیتور نمودن بلادرنگ، همبستگی رویدادها، اخطارها و نمای کنسول مرتبط است معمولاً تحت عنوان مدیریت رویدادهای امنیتی شناخته می‌شوند (SEM). بخش دیگر که ارائه‌دهنده ذخیره‌سازی طولانی‌مدت، تحلیل و گزارش از داده‌های گزارش‌گیری شده[۱] است تحت عنوان مدیریت اطلاعات امنیتی مطرح می‌گردد (SIM).

اصطلاح SIEM[۲] توصیف‌کننده قابلیت‌های محصول چون جمع‌آوری، تحلیل و ارائه اطلاعات از تجهیزات امنیتی و شبکه، دسترسی برنامه‌های مدیریتی، مدیریت آسیب‌پذیری‌ها و ابزارهای خط‌مشی، سیستم‌عامل و پایگاه داده و برنامه گزارش‌گیری می‌باشد. تمرکز اصلی SIEM روی نظارت نمودن و کمک به مدیر و سرویس‌های دارای مجوز، سرویس دایرکتوری و دیگر تغییرات پیکربندی سیستم می‌باشد، همچنین ارائه‌دهنده گزارش ممیزی، بررسی و پاسخ ضمنی[۳] می‌باشد.

SIEM نوعی تجهیز شبکه است بنابراین مسائل امنیتی موجود در پروفایل تجهیز شبکه شامل می‌شود و از طرفی لازم است الزامات کارکردی تجهیز شبکه نیز برای این محصول رعایت شود. این پروفایل یک مجموعه کاملی از الزامات برای هر دستگاه SIEM می‌باشد.

۱-۱ تهدیدات

در ادامه، تهدیدات پیش روی دستگاه‌های شبکه بر اساس عملکرد این دستگاه‌ها دسته‌بندی شده‌اند. همچنین برای هر تهدید، یک توصیف منطقی از چگونگی پوشش دادن آن در الزامات اصلی، اختیاری و الزامات مبتنی بر انتخاب، ارائه شده است.

۱-۱-۱ ارتباط با دستگاه‌های شبکه

یک دستگاه شبکه با سایر دستگاه‌های شبکه و موجودیت‌های شبکه ارتباط برقرار می‌کند،SIEM نیز به عنوان یک دستگاه شبکه ممکن است نیاز به ارتباط با سایر دستگاه‌های شبکه داشته باشد. مقصد این ارتباط ممکن است از لحاظ منطقی یا جغرافیایی یک دستگاه راه‌دور 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 غیرمجازی را با دستگاه شبکه برقرار کنند یا ارتباطات مجاز را در معرض خطر قرار دهند. کارکرد امنیتی دستگاه شبکه باید این قابلیت را

---

[۱] Log Data
[۲] Security Information Evant Management (SIEM)
[۳] Incident Responce

داشته باشد که از ترافیک حساس شبکه (مانند ترافیک سرپرستی، 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 غیرمجاز.

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 سرپرستی 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 غیرمجاز به شمار می‌آیند.

تهدید اصلی علیه ارتباطات دستگاه شبکه که در این پروفایل حفاظتی به آن پرداخته می‌شود، یک موجودیت غیرمجاز 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 سرپرستی ضعیفی به کار گرفته شده باشند، یک عامل تهدید می‌تواند به صورت غیرمجاز 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[۱] دستگاه را محدود می‌کند، بلکه ضمانت و اعتماد حاصل از استانداردسازی را نیز از دستگاه می‌گیرد.

۱-۱-۱-۱ دسترسی سرپرستی غیرمجاز

ممکن است عامل تهدید تلاش کند تا با استفاده از ابزارهای بدخواهانه، به دستگاه شبکه دسترسی سرپرستی پیدا کند. به عنوان مثال، عامل تهدید خود را به عنوان سرپرست به دستگاه معرفی می‌کند، به عنوان دستگاه به سرپرست معرفی می‌نماید، نشست سرپرستی را بازپخش می‌کند (به طور کامل یا بخش‌هایی خاص از آن)، یا حملات مردی در میان را ترتیب می‌دهد تا به نشست‌های سرپرستی 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.

منطق الزام کارکرد امنیتی (SFR):

[۱] Interoperability

- نقش سرپرست در الزام FMT_SMR.2 تعریف شده است و توانایی‌های سرپرستی مربوطه نیز در الزامات FMT_SMF.1 و FMT_MTD.1/CoreData تعریف شده‌اند، و همچنین توانایی‌های اضافه اختیاری نیز در الزامات FMT_MOF.1/Services و FMT_MOF.1/Functions تعریف شده است.
- اقداماتی که قبل از احراز هویت کردن سرپرست اجازه انجام گرفتن دارند در الزام FIA_UIA_EXT.1 در نظر گرفته شده است، و شامل نمایش یک پیغام هشدار موافقت یا توجه می‌باشد که در الزام FTA_TAB.1 مشخص می‌گردد.
- الزام برای فرآیند احراز هویت سرپرست در FIA_UAU_EXT.2 توصیف شده است.
- قفل نشست‌های سرپرست به‌وسیله FTA_SSL_EXT.1 (برای نشست‌های محلی)، FTA_SSL_EXT.3 (برای نشست‌های راه‌دور)، و FTA_SSL_EXT.4 (برای تمامی نشست‌های تعاملی) تضمین می‌شود.
- کانال امن برای ارتباطات سرپرست راه‌دور از طریق FTP_TRP.1/Admin انجام می‌گیرد.
- (اقدامات بدخواهانه که توسط نشست سرپرست انجام شده است به صورت جداگانه در "فعالیت ردیابی نشده" ارائه شده است.)
- (حفاظت از اطلاعات محرمانه سرپرست به صورت جداگانه در "هک شدن گذرواژه" ارائه شده است.)

۲-۱-۱-۱ *رمزنگاری ضعیف*

ممکن است عامل تهدید از ضعیف بودن الگوریتم رمزنگاری بهره‌برداری کند یا حملات از پای درآوردن رمزنگاری[۱] را علیه فضای کلید ترتیب دهد. انتخاب نادرست الگوریتم رمزنگاری، مُدها یا اندازه کلیدها به مهاجمان اجازه می‌دهد تا به الگوریتم رمزنگاری حمله کنند یا با حملات جستجوی فراگیر[۲] علیه فضای کلید، دسترسی غیرمجاز به دست آورند و با کمترین تلاش موفق به خواندن، دست‌کاری یا کنترل ترافیک شوند.

منطق الزام کارکرد امنیتی:

- الزامات تولید و نابودی کلید در FCS_CKM.1 و FCS_CKM.2 ارائه می‌شوند.
- الزامات برای استفاده از طرح‌های رمزنگاری در FCS_COP.1/DataEncryption، FCS_COP.1/SigGen، FCS_COP.1/Hash، و FCS_COP.1/KeyedHash تعریف می‌شوند.
- الزامات تولید بیت تصادفی برای پشتیبانی از تولید کلید و پروتکل‌های امن در FCS_RBG_EXT.1 تعریف می‌شوند.
- مدیریت توابع رمزنگاری در FMT_SMF.1 مشخص می‌شود.

---

[۱] Cryptographic exhaust

[۲] Brute force

۱-۱-۱-۳ 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 پروتکل‌هایی با طراحی نامناسب یا فرایندهای ضعیف مدیریت کلید، حملات مردی در میان، 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.

منطق الزام کارکرد امنیتی:

- استفاده عمومی پروتکل‌های امن برای کانال‌های ارتباطی تعریف شده، به صورت سطح بالا در الزامات FTP_ITC.1 و FTP_TRP.1/Admin مشخص شده است؛ برای محصولات توزیع شده، الزامات ارتباطات بین مؤلفه‌ای در FPT_ITT.1 آورده شده است.
- الزامات پروتکل‌های ارتباط امن برای تمامی پروتکل‌های مجاز در FCS_DTLSC_EXT.1، FCS_DTLSC_EXT.2، FCS_DTLSS_EXT.1، FCS_DTLSS_EXT.2، FCS_HTTPS_EXT.1، FCS_IPSEC_EXT.1، FCS_SSHC_EXT.1، FCS_SSHS_EXT.1، FCS_TLSC_EXT.1، FCS_TLSC_EXT.2، FCS_TLSS_EXT.1، FCS_TLSS_EXT.2 تعریف می‌شوند.
- الزامات اختیاری و مبتنی بر انتخاب برای استفاده از گواهی‌نامه‌های کلید عمومی جهت پشتیبانی از پروتکل‌های امن، در FIA_X509_EXT.1، FIA_X509_EXT.2 و FIA_X509_EXT.3 تعریف شده‌اند.

۱-۱-۱-۴ 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 سرپرست 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.

منطق الزام کارکرد امنیتی:

- استفاده از پروتکل‌های امن مناسب برای احراز هویت کردن نقاط پایانی، به‌وسیله‌ی الزامات FTP_ITC.1 و FTP_TRP.1/Admin تضمین شده است؛ برای محصولات توزیع شده، الزامات احراز هویت برای نقاط پایانی در ارتباطات بین مؤلفه‌ای، در FPT_ITT.1 آورده شده است.

- موارد خاص اضافه احتمالی احراز هویت امن در طول ثبت‌نام مؤلفه‌های محصول توزیع‌شده، در FCO_CPC_EXT.1 و FTP_TRP.1/Join بیان شده است.

۱-۱-۲ 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 تائید کرد؛ در غیر این صورت، یک منبع غیر معتبر می‌تواند به‌روزرسانی خود را به کار گیرد و کارکرد امنیتی دستگاه شبکه را دور بزند. روش‌های تائید منبع و محتوای به‌روزرسانی نرم‌افزار یا ثابت‌افزار به‌وسیله ابزارهای رمزنگاری معمولاً جایی که هش‌های به‌روزرسانی‌ها به صورت دیجیتال امضاء شده باشند، طرح‌های امضاء دیجیتال را بکار می‌گیرند.

نسخه‌های به‌روزنشده نرم‌افزارها یا ثابت‌افزارها می‌توانند دستگاه شبکه را در معرض خطر عوامل تهدیدی قرار دهند که در پی سوءاستفاده از آسیب‌پذیری‌های شناخته‌شده آن‌ها هستند. به‌روزرسانی‌های تأیید نشده یا به‌روزرسانی‌هایی که با استفاده از ابزارهای رمزنگاری ضعیف یا غیر امن تائید 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.

۱-۱-۲-۱ به‌روزرسانی‌های مخرب

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

منطق الزام کارکرد امنیتی:

- الزامات برای حفاظت از به‌روزرسانی‌ها در FPT_TUD_EXT.1 ارائه شده است.
- استفاده اختیاری از حفاظت مبتنی بر گواهی‌نامه برای امضاها می‌تواند در FPT_TUD_EXT.2 مشخص گردد، الزامات فرآیند گواهی X509 در FIA_X509_EXT.1، FIA_X509_EXT.2 و FIA_X509_EXT.3 مشخص شده است.
- الزامات برای مدیریت به‌روزرسانی‌ها در FMT_SMF.1، برای به‌روزرسانی دستی در FMT_MOF.1/ManualUpdate و الزامات اختیاری برای به‌روزرسانی خودکار در FMT_MOF.1/AutoUpdate مشخص می‌گردد.

۱-۱-۳ فعالیت ممیزی‌شده

سرپرستان 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 سرپرست 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 سرپرست 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 غیرمجاز، 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 (مثال؛ سرور syslog) را داشته باشد.

۱-۱-۳-۱ فعالیت ردیابی‌نشده

ممکن است عامل تهدید تلاش کند تا بدون اطلاع سرپرست، به کارکرد امنیتی دستگاه شبکه دسترسی پیدا کند، آن را تغییر دهد و/یا دست‌کاری نماید. بدین ترتیب، ممکن است مهاجم راهی برای حمله به دستگاه شبکه پیدا کند (مثال؛ از طریق پیکربندی‌های نامناسب، ایراد در محصول) و سرپرست نیز آگاه نشود که دستگاه در معرض خطر قرار گرفته است.

منطق الزام کارکرد امنیتی:

- الزامات توانایی‌های ممیزی پایه در FAU_GEN.1 و FAU_GEN.2 مشخص شده است و مهرهای زمانی در FPT_STM_EXT.1 ارائه شده است.
- الزامات حفاظت از رکوردهای ممیزی ذخیره‌شده روی محصول، در FAU_STG.1 تعریف شده است.
- الزامات برای مخابره امن رکوردهای ممیزی محلی به موجودیت IT خارجی از طریق کانال امن، در FAU_STG_EXT.1 تعریف شده است.
- الزامات اضافه اختیاری که با از دست دادن داده‌های ممیزی محلی ذخیره شده سروکار دارد، در FAU_STG_EXT.2/LocSpace و FAU_STG_EXT.3/LocSpace مشخص شده است.
- اگر پیکربندی قابلیت عملکردی ممیزی (اختیاری) توسط محصول فراهم شود، الزامات آن در FMT_SMF.1 مشخص می‌گردد، و محدود کردن این قابلیت به سرپرست‌های امنیتی در FMT_MOF.1/Functions مشخص شده است.

۱-۱-۴ داده‌ها و اطلاعات محرمانه دستگاه و سرپرست

دستگاه شبکه دربردارنده 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 سرپرستی اشاره کرد. کلیدهای سرپرست و دستگاه، اطلاعات کلید و اطلاعات محرمانه احراز هویت را باید در برابر دست‌کاری و افشای غیرمجاز محافظت نمود. علاوه بر این، کارکرد امنیتی دستگاه باید تغییر اطلاعات محرمانه پیش‌فرض احراز هویت را (مانند؛ کلمه‌های عبور سرپرست) ملزم نماید.

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 غیرمجاز امکان می‌دهند تا با استفاده از اطلاعات محرمانه سرپرست امنیتی، به کارکردهای سرپرستی 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 غیرمجاز مهاجم به داده‌های دستگاه و سرپرست ادامه خواهد یافت.

۱-۱-۴-۱ به خطر افتادن کارکرد امنیتی

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

منطق الزام کارکرد امنیتی:

- حفاظت از کلیدهای سری/خصوصی در مقابل مصالحه/تراضی شدن در FPT_SKP_EXT.1 مشخص شده است.
- نابودی امن کلیدها در FCS_CKM.4 مشخص شده است.
- اگر مدیریت کلیدها (اختیاری) توسط محصول فراهم شود، الزامات آن در FMT_SMF.1 مشخص می‌گردد، و محدود کردن این قابلیت به سرپرست‌های امنیتی در FMT_MTD.1/CryptoKeys مشخص شده است.
- (حفاظت از گذرواژه‌ها به صورت جداگانه در "هک شدن گذرواژه" مشخص شده است.)

۱-۱-۴-۲ هک شدن گذرواژه

ممکن است عامل تهدید از ضعیف بودن گذرواژه‌های سرپرستی 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.

منطق الزام کارکرد امنیتی:

- الزامات طول‌های گذرواژه و کاراکترهای موجود در آن، در FIA_PMG_EXT.1 مشخص شده است.
- حفاظت از ورود گذرواژه از طریق بازخورد مبهم در FIA_UAU.7 مشخص شده است.
- اقدامات به دست آوردن تعداد حد آستانه شکست‌های متوالی گذرواژه در FIA_AFL.1 مشخص شده است.
- الزامات ذخیره‌سازی امن گذرواژه‌ها در FPT_APW_EXT.1 مشخص شده است.

۱-۱-۵ 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.

۱-۱-۵-۱ از کار افتادن کارکرد امنیتی

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

منطق الزام کارکرد امنیتی:

- الزامات برای اجرای خودآزمایی(ها) در FPT_TST_EXT.1 مشخص شده است.
- استفاده اختیاری از گواهی‌نامه‌های برای خودآزمایی(ها) در FPT_TST_EXT.2 مشخص شده است. (همچنین پشتیبانی از گواهی‌نامه‌های FIA_X509_EXT.1، FIA_X509_EXT.2 و FIA_X509_EXT.3 نیز وجود دارد.)

[۱] Roots of trust

۱-۲ 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.

۱-۲-۱ 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 ندارد که از دسترسی فیزیکی به دستگاه (که به موجودیت‌های غیرمجاز 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.

۱-۲-۲ کارکرد محدود

چنین فرض می‌شود که دستگاه کارکردهای شبکه را به عنوان کارکرد اصلی خود ارائه می‌کند و سرویس‌ها 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.

۱-۲-۳ 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 سرپرستی را در برمی‌گیرند. 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.

۱-۲-۴ سرپرست مورد اعتماد

چنین فرض می‌شود که سرپرستان 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 سرپرستان امنیتی از اطلاعات محرمانه حساب کاربری و گذرواژه‌هایی با قدرت امنیتی و

آنتروپی مناسب استفاده می‌کنند و در هنگام سرپرستی دستگاه، اهداف بدخواهانه‌ای در سر ندارند. از دستگاه شبکه انتظار نمی‌رود که در صورت انجام اقدامات بدخواهانه توسط سرپرست امنیتی، در مقابل اقدامات وی از خود محافظتی به عمل آورد.

۱-۲-۵ به‌روزرسانی منظم

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

۱-۲-۶ امنیت اطلاعات محرمانه سرپرست

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

۱-۲-۷ مؤلفه‌های در حال اجرا (فقط برای اهداف ارزیابی توزیع‌شده)

برای اهداف ارزیابی توزیع‌شده فرض می‌شود که دسترس‌پذیری همه‌ی مؤلفه‌های هدف ارزیابی، در راستای کاهش احتمال یک حمله پیش‌بینی نشده (یا یک شکست) روی یک یا چند مؤلفه‌ی هدف ارزیابی، به صورت مناسب بررسی شده است. همچنین فرض می‌شود در راستای دسترس‌پذیری، عملکرد ممیزی در حال اجرا بر روی مؤلفه‌ها، برای تمامی آن‌ها به درستی بررسی شده است.

۱-۲-۸ اطلاعات باقیمانده

سرپرست باید اطمینان یابد که برای اطلاعات باقیمانده حساس (مانند: کلیدهای رمزنگاری، اجزای سازنده کلید، PINs، رمزعبورها و غیره.) روی تجهیز شبکه، وقتی که تجهیز از محیط عملیاتی حذف یا برداشته می‌شود، امکان دسترسی غیرمجاز وجود ندارد.

۱-۳ 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.

۱-۳-۱ 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.

منطق الزام کارکرد امنیتی:

- نمایش یک پیغام هشدار موافقت یا توجه الزامی می‌باشد و در الزام FTA_TAB.1 مشخص شده است.

۲ اهداف امنیتی

۲-۱ اهداف امنیتی مربوط به محیط عملیاتی

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

۲-۱-۱ امنیت فیزیکی

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

۲-۱-۲ عدم کارکرد عمومی

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

۲-۱-۳ 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.

۲-۱-۴ سرپرست مورد اعتماد

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

۲-۱-۵ 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.

۲-۱-۶ امنیت حساب کاربری سرپرست

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

۲-۱-۷ مؤلفه‌های در حال اجرا (فقط برای اهداف ارزیابی توزیع‌شده)

برای اهداف ارزیابی توزیع‌شده سرپرست امنیتی باید اطمینان یابد که دسترس‌پذیری هر مؤلفه‌ی هدف ارزیابی، در راستای کاهش احتمال یک حمله پیش‌بینی نشده (یا یک شکست) روی یک یا چند مؤلفه‌ی هدف ارزیابی، به صورت مناسب بررسی شده است. همچنین سرپرست امنیتی باید اطمینان یابد که عملکرد ممیزی در حال اجرا بر روی مؤلفه‌ها به درستی بررسی شده است.

۲-۱-۸ اطلاعات باقیمانده

سرپرست امنیتی باید اطمینان یابد که برای اطلاعات باقیمانده حساس (مانند: کلیدهای رمزنگاری، اجزای سازنده کلید، PINs، رمزعبورها و غیره.) روی تجهیز شبکه، وقتی که تجهیز از محیط عملیاتی حذف یا برداشته می‌شود، امکان دسترسی غیرمجاز وجود ندارد.

۲-۲ مسائل امنیتی مرتبط با تجهیز SIEM

۲-۲-۱ تهدیدات

نوع تهدید	توضیحات
خطای مدیر	مدیر سیستم ممکن است با پیکربندی نادرست محصول مکانیسم‌های امنیتی را تحت تأثیر قرار دهد.
مخاطرات محرمانگی و صحت	ممکن است موجودیت غیرمجازی با دور زدن مکانیسم‌های امنیتی، صحت و محرمانگی داده‌هایی که توسط SIEM جمع‌آوری، ذخیره یا تحلیل‌شده‌اند را به خطر اندازد.
دسترسی غیرمجاز	کاربر غیرمجاز ممکن است با دور زدن مکانیسم‌های امنیتی سعی در افشاء داده‌هایی که توسط محصول جمع‌آوری، ذخیره یا تحلیل‌شده‌اند، نماید.
حذف غیرمجاز	کاربر غیرمجاز ممکن است داده‌هایی را که توسط محصول جمع‌آوری، ذخیره یا تحلیل‌شده‌اند را با دور زدن مکانیسم‌های امنیتی از بین ببرد.
تزریق لاگ	کاربر غیرمجاز ممکن است با وارد نمودن داده‌ای که محصول نتواند آن را بکار برد، سبب بدعمل نمودن محصول گردد.
مخاطرات دسترس‌پذیری	کاربر غیرمجاز ممکن است با متوقف نمودن اجرای محصول، سعی در به خطر انداختن پیوستگی عملکرد تحلیل محصول نماید.

نوع تهدید	توضیحات
مخاطرات افزایش حق دسترسی	کاربر غیرمجاز ممکن است با دستیابی به محصول و با استفاده از مجوزهای سیستمی به عملکرد امنیتی محصول و داده‌های آن دستیابی پیدا نماید.
مخاطرات پیکربندی	محصول ممکن است توسط افراد مجاز یا غیرمجاز به‌صورت نامناسبی پیکربندی گردد و سبب نفوذ بالقوه‌ای گردد که تشخیص داده نمی‌شود.
واکنش آسیب‌پذیری	محصول ممکن است در واکنش نشان دادن به آسیب‌پذیری‌های شناسایی‌شده یا مورد ظن یا فعالیت‌های نامناسب با شکست روبرو گردد.
تشخیص آسیب‌پذیری	محصول ممکن است در تشخیص آسیب‌پذیری‌ها یا فعالیت‌های نامناسب بر اساس داده‌هایی که SIEM دریافت نموده با شکست مواجه گردد.

۲-۲-۲ فرضیات

نوع	توضیحات
دسترسی	محصول برای انجام عملکرد خود به تمام منابع موجود در زیرساخت IT که به آن‌ها نیاز داشته، دسترسی دارد.
محافظت	سخت‌افزار و نرم‌افزار محصول که به اجرای خط‌مشی‌های امنیتی حساس هستند، از هرگونه تغییرات فیزیکی غیرمجاز محافظت می‌گردند.
محل استقرار	منابع پردازشی محصول در داخل فضایی قرار می‌گیرند که ازنظر دسترسی کنترل‌شده هستند تا از دسترسی فیزیکی غیرمجاز جلوگیری شود.
مدیریت	یک یا بیش از یک فرد دارای صلاحیت برای مدیریت محصول و امنیت اطلاعات آن به محصول اختصاص داده می‌شود.
سرپرست مورد اعتماد	سرپرست[۱] مجاز فردی بی‌دقت یا متخاصم نیست و دستورات ارائه‌شده توسط مستندات محصول را دنبال می‌نماید.
دسترسی امن	محصول تنها توسط کاربران مجاز قابل‌دسترسی است.

۲-۲-۳ خط‌مشی‌های سازمانی

نوع	توضیحات
مسئولیت‌پذیری	تمام کاربران مجاز محصول باید مسئول اقداماتشان باشند.

[۱] Administrator

نوع	توضیحات
اهداف مجاز	تمام داده‌های جمع‌آوری‌شده، ذخیره‌شده و تحلیل‌شده توسط محصول باید برای اهداف مجاز استفاده گردد.
تجزیه‌وتحلیل	پردازش‌های تحلیلی و اطلاعاتی که از استنتاج‌های صورت گرفته در رابطه بانفوذها (گذشته، حال، آینده) ناشی شده‌اند باید به داده SIEM اعمال گردد و اقدام مناسبی صورت گیرد.
تشخیص	اطلاعات پیکربندی ایستا باید جمع‌آوری گردد زیرا ممکن است از پتانسیل برای نفوذ در آینده یا رویداد مجدد نفوذ قبلی در یک سیستم IT حکایت نماید.
مدیریت	محصول باید توسط کاربران مجاز مدیریت گردد.
محافظت از تغییرات	داده‌های تحلیل‌شده و تولیدشده توسط محصول باید از تغییرات محافظت گردند.
جلوگیری از ورود غیرمجاز	محصول باید از ورود غیرمجاز همچون قطع اجرای برنامه‌های معمولی محافظت نماید.

۳ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول ۳-۱ هستند و در ادامه هریک از الزامات شرح و بسط داده‌شده‌اند. همچنین الزامات مربوط به پیوست این سند نیز در ادامه جدول ۳-۱ 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 ۳-۱ 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	نابودی کلید رمزنگاری ۴	FCS_CKM.4.1
۱۰	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1/DataEncryption
۱۱	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1/SigGen
۱۲	عملیات رمزنگاری ۱ (۳)	FCS_COP.1.1/Hash
۱۳	عملیات رمزنگاری ۱ (۴)	FCS_COP.1.1/KeyedHash
۱۴	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۱۵	تولید بیت تصادفی ۲	FCS_RBG_EXT.1.2
۱۶	مدیریت احراز هویت ناموفق ۱	FIA_AFL.1.1
۱۷	مدیریت احراز هویت ناموفق ۲	FIA_AFL.1.2
۱۸	مدیریت رمز عبور ۱	FIA_PMG_EXT.1.1
۱۹	شناسایی و احراز هویت کاربر ۱	FIA_UIA_EXT.1.1
۲۰	شناسایی و احراز هویت کاربر ۲	FIA_UIA_EXT.1.2
۲۱	سازوکار احراز هویت بر اساس رمز عبور ۲	FIA_UAU_EXT.2.1
۲۲	احراز هویت کاربر ۱۰	FIA_UAU.7.1
۲۳	مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی دستی	FMT_MOF.1.1(1)/ManualUpdate
۲۴	مدیریت داده‌های محصول ۱	FMT_MTD.1.1/CoreData
۲۵	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۲۶	نقش‌های امنیتی ۳	FMT_SMR.2.1
۲۷	نقش‌های امنیتی ۴	FMT_SMR.2.2
۲۸	نقش‌های امنیتی ۵	FMT_SMR.2.3
۲۹	محافظت از داده‌های محصول (کلیدهای متقارن) ۱	FPT_SKP_EXT.1.1
۳۰	حفاظت از کلمه عبور سرپرست محصول ۱	FPT_APW_EXT.1.1

شماره الزام	نام الزام	عنصر متناظر با الزام
۳۱	حفاظت از کلمه عبور سرپرست محصول ۲	FPT_APW_EXT.1.2
۳۲	خودآزمایی محصول ۱	FPT_TST_EXT.1.1
۳۳	به‌روزرسانی امن ۱	FPT_TUD_EXT.1.1
۳۴	به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۳۵	به‌روزرسانی امن ۳	FPT_TUD_EXT.1.3
۳۶	مهرهای زمانی معتبر ۱	FPT_STM_EXT.1.1
۳۷	مهرهای زمانی معتبر ۲	FPT_STM_EXT.1.2
۳۸	قفل‌کردن و خاتمه دادن به نشست‌ها ۷	FTA_SSL_EXT.1.1
۳۹	قفل‌کردن و خاتمه دادن به نشست‌ها ۵	FTA_SSL.3.1
۴۰	قفل‌کردن و خاتمه دادن به نشست‌ها ۶	FTA_SSL.4.1
۴۱	پیغام‌های هشدار در رابطه با استفاده محصول ۱	FTA_TAB.1.1
۴۲	کانال امن ۱	FTP_ITC.1.1
۴۳	کانال امن ۲	FTP_ITC.1.2
۴۴	کانال امن ۳	FTP_ITC.1.3
۴۵	مسیر امن ۱	FTP_TRP.1.1/Admin
۴۶	مسیر امن ۲	FTP_TRP.1.2/Admin
۴۷	مسیر امن ۳	FTP_TRP.1.3/Admin
۴۸	تجزیه‌وتحلیل تحلیل‌گر ۱	SIEM_ANL.1.1
۴۹	تجزیه‌وتحلیل تحلیل‌گر ۲	SIEM_ANL.1.2
۵۰	تجزیه‌وتحلیل تحلیل‌گر ۳	SIEM_ANL.1.3(1)
۵۱	واکنش تحلیل‌گر ۱	SIEM_RCT.1.1
۵۲	بازبینی داده‌های محدودشده ۱ (۱)	SIEM_RDR.1.1(1)
۵۳	بازبینی داده‌های محدودشده ۱ (۲)	SIEM_RDR.1.1(2)
۵۴	بازبینی داده‌های محدودشده ۲	SIEM_RDR.1.2
۵۵	بازبینی داده‌های محدودشده ۳	SIEM_RDR.1.3
۵۶	تضمین در دسترس بودن داده‌های سیستم-حذف ۱ (۱)	SIEM_STG.1.1(1)
۵۷	تضمین در دسترس بودن داده‌های سیستم-حذف ۱ (۲)	SIEM_STG.1.1(2)
۵۸	تضمین در دسترس بودن داده‌های سیستم-تغییر ۱ (۱)	SIEM_STG.1.2(1)
۵۹	تضمین در دسترس بودن داده‌های سیستم-تغییر ۱ (۲)	SIEM_STG.1.2(2)
۶۰	تضمین در دسترس بودن داده‌های سیستم ۲	SIEM_STG.2.1

شماره الزام	نام الزام	عنصر متناظر با الزام
الزامات کارکرد امنیتی برای پیاده‌سازی ارتباطات سلسله مراتبی		
۶۱	خروج داده‌های کاربری از محصول ۱	FDP_ETC.2.1
۶۲	خروج داده‌های کاربری از محصول ۲	FDP_ETC.2.2
۶۳	خروج داده‌های کاربری از محصول ۳	FDP_ETC.2.3
۶۴	خروج داده‌های کاربری از محصول ۴	FDP_ETC.2.4
۶۵	ورود داده‌های کاربری به محصول ۱	FDP_ITC.2.1
۶۶	ورود داده‌های کاربری به محصول ۲	FDP_ITC.2.2
۶۷	ورود داده‌های کاربری به محصول ۳	FDP_ITC.2.3
الزامات مربوط به پیوست یک		
۶۸	ذخیره‌سازی رویدادهای ممیزی ۱	FAU_STG.1.1
۶۹	ذخیره‌سازی رویدادهای ممیزی ۲	FAU_STG.1.2
۷۰	محل ذخیره‌سازی داده‌های ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی	FAU_STG_EXT.2.1/LocSpace
۷۱	ذخیره‌سازی رویدادهای ممیزی ۶/ فضای ذخیره‌سازی ممیزی محلی	FAU_STG.3.1/LocSpace
۷۲	الزامات پروتکل X509 (۱)/ تبادل داده کاربردی داخل محصول	FIA_X509_EXT.1.1/ITT
۷۳	الزامات پروتکل X509 (۲)/ تبادل داده کاربردی داخل محصول	FIA_X509_EXT.1.2/ITT
۷۴	مدیریت کارکرد در محصول ۱ (۱)/ سرویس‌ها	FMT_MOF.1.1(1)/Services
۷۵	مدیریت داده‌های محصول ۱/ کلیدهای رمزنگاری	FMT_MTD.1.1/CryptoKeys
۷۶	انتقال داده امنیتی در داخل محصول ۱	FPT_ITT.1.1
۷۷	مسیر امن ۱/ پیوند زدن	FPT_TRP.1.1/Join
۷۸	مسیر امن ۲ / پیوند زدن	FPT_TRP.1.2/Join
۷۹	مسیر امن ۳ / پیوند زدن	FPT_TRP.1.3/Join
۸۰	تعریف کانال ثبت‌نام مؤلفه ۱	FCO_CPC_EXT.1.1
۸۱	تعریف کانال ثبت‌نام مؤلفه ۲	FCO_CPC_EXT.1.2
۸۲	تعریف کانال ثبت‌نام مؤلفه ۳	FCO_CPC_EXT.1.3
۸۳	تولید داده ممیزی ۱	FAU_GEN_EXT.1.1
۸۴	محل ذخیره‌سازی داده‌های ممیزی حفاظت شده	FAU_STG_EXT.3.1/LocSpace

شماره الزام	نام الزام	عنصر متناظر با الزام
۸۵	محل ذخیره‌سازی داده ممیزی ۴	FAU_STG_EXT.4.1
الزامات مربوط به پیوست دو		
۸۶	الزامات پروتکل DTLS Client (۱)	FCS_DTLSC_EXT.1.1
۸۷	الزامات پروتکل DTLS Client (۲)	FCS_DTLSC_EXT.1.2
۸۸	الزامات پروتکل DTLS Client (۳)	FCS_DTLSC_EXT.1.3
۸۹	الزامات پروتکل DTLS Client (۴)	FCS_DTLSC_EXT.1.4
۹۰	الزامات پروتکل DTLS Client/ احراز هویت ۱	FCS_DTLSC_EXT.2.1
۹۱	الزامات پروتکل DTLS Client/ احراز هویت ۲	FCS_DTLSC_EXT.2.2
۹۲	الزامات پروتکل DTLS Client/ احراز هویت ۳	FCS_DTLSC_EXT.2.3
۹۳	الزامات پروتکل DTLS Server (۱)	FCS_DTLSS_EXT.1.1
۹۴	الزامات پروتکل DTLS Server (۲)	FCS_DTLSS_EXT.1.2
۹۵	الزامات پروتکل DTLS Server (۳)	FCS_DTLSS_EXT.1.3
۹۶	الزامات پروتکل DTLS Server (۴)	FCS_DTLSS_EXT.1.4
۹۷	الزامات پروتکل DTLS Server (۵)	FCS_DTLSS_EXT.1.5
۹۸	الزامات پروتکل DTLS Server (۶)	FCS_DTLSS_EXT.1.6
۹۹	الزامات پروتکل DTLS Server (۷)	FCS_DTLSS_EXT.1.7
۱۰۰	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۱	FCS_DTLSS_EXT.2.1
۱۰۱	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۲	FCS_DTLSS_EXT.2.2
۱۰۲	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۳	FCS_DTLSS_EXT.2.3
۱۰۳	الزامات پروتکل HTTPS (۱)	FCS HTTPS_EXT.1.1
۱۰۴	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2
۱۰۵	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۱۰۶	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1
۱۰۷	الزامات پروتکل IPSEC (۲)	FCS_IPSEC_EXT.1.2
۱۰۸	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
۱۰۹	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
۱۱۰	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.1.5
۱۱۱	الزامات پروتکل IPSEC (۶)	FCS_IPSEC_EXT.1.6
۱۱۲	الزامات پروتکل IPSEC (۷)	FCS_IPSEC_EXT.1.7
۱۱۳	الزامات پروتکل IPSEC (۸)	FCS_IPSEC_EXT.1.8

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۱۴	الزامات پروتکل IPSEC (۹)	FCS_IPSEC_EXT.1.9
۱۱۵	الزامات پروتکل IPSEC (۱۰)	FCS_IPSEC_EXT.1.10
۱۱۶	الزامات پروتکل IPSEC (۱۱)	FCS_IPSEC_EXT.1.11
۱۱۷	الزامات پروتکل IPSEC (۱۲)	FCS_IPSEC_EXT.1.12
۱۱۸	الزامات پروتکل IPSEC (۱۳)	FCS_IPSEC_EXT.1.13
۱۱۹	الزامات پروتکل IPSEC (۱۴)	FCS_IPSEC_EXT.1.14
۱۲۰	الزامات پروتکل NTP (۱)	FCS_NTP_EXT.1.1
۱۲۱	الزامات پروتکل NTP (۲)	FCS_NTP_EXT.1.2
۱۲۲	الزامات پروتکل NTP (۳)	FCS_NTP_EXT.1.3
۱۲۳	الزامات پروتکل NTP (۴)	FCS_NTP_EXT.1.4
۱۲۴	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.1.1
۱۲۵	الزامات پروتکل SSH Client (۲)	FCS_SSHC_EXT.1.2
۱۲۶	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.1.3
۱۲۷	الزامات پروتکل SSH Client (۴)	FCS_SSHC_EXT.1.4
۱۲۸	الزامات پروتکل SSH Client (۵)	FCS_SSHC_EXT.1.5
۱۲۹	الزامات پروتکل SSH Client (۶)	FCS_SSHC_EXT.1.6
۱۳۰	الزامات پروتکل SSH Client (۷)	FCS_SSHC_EXT.1.7
۱۳۱	الزامات پروتکل SSH Client (۸)	FCS_SSHC_EXT.1.8
۱۳۲	الزامات پروتکل SSH Client (۹)	FCS_SSHC_EXT.1.9
۱۳۳	الزامات پروتکل SSH Server (۱)	FCS_SSHS_EXT.1.1
۱۳۴	الزامات پروتکل SSH Server (۲)	FCS_SSHS_EXT.1.2
۱۳۵	الزامات پروتکل SSH Server (۳)	FCS_SSHS_EXT.1.3
۱۳۶	الزامات پروتکل SSH Server (۴)	FCS_SSHS_EXT.1.4
۱۳۷	الزامات پروتکل SSH Server (۵)	FCS_SSHS_EXT.1.5
۱۳۸	الزامات پروتکل SSH Server (۶)	FCS_SSHS_EXT.1.6
۱۳۹	الزامات پروتکل SSH Server (۷)	FCS_SSHS_EXT.1.7
۱۴۰	الزامات پروتکل SSH Server (۸)	FCS_SSHS_EXT.1.8
۱۴۱	الزامات پروتکل TLS Client (۱)	FCS_TLSC_EXT.1.1
۱۴۲	الزامات پروتکل TLS Client (۲)	FCS_TLSC_EXT.1.2
۱۴۳	الزامات پروتکل TLS Client (۳)	FCS_TLSC_EXT.1.3

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۴۴	الزامات پروتکل TLS Client (۴)	FCS_TLSC_EXT.1.4
۱۴۵	الزامات پروتکل TLS Client/ احراز هویت ۱	FCS_TLSC_EXT.2.1
۱۴۶	الزامات پروتکل TLS Server (۱)	FCS_TLSS_EXT.1.1
۱۴۷	الزامات پروتکل TLS Server (۲)	FCS_TLSS_EXT.1.2
۱۴۸	الزامات پروتکل TLS Server (۳)	FCS_TLSS_EXT.1.3
۱۴۹	الزامات پروتکل TLS Server ۴	FCS_TLSS_EXT.1.4
۱۵۰	الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۱	FCS_TLSS_EXT.2.1
۱۵۱	الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۲	FCS_TLSS_EXT.2.2
۱۵۲	الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۳	FCS_TLSS_EXT.2.3
۱۵۳	الزامات پروتکل X509 (۱)/ ابطال	FIA_X509_EXT.1.1/Rev
۱۵۴	الزامات پروتکل X509 (۱)/ ابطال	FIA_X509_EXT.1.2/Rev
۱۵۵	الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1
۱۵۶	الزامات پروتکل X509 (۴)	FIA_X509_EXT.2.2
۱۵۷	الزامات پروتکل X509 (۵)	FIA_X509_EXT.3.1
۱۵۸	الزامات پروتکل X509 (۶)	FIA_X509_EXT.3.2
۱۵۹	الزامات به‌روزرسانی امن ۴	FPT_TUD_EXT.2.1
۱۶۰	الزامات به‌روزرسانی امن ۵	FPT_TUD_EXT.2.2
۱۶۱	الزامات به‌روزرسانی امن ۶	FPT_TUD_EXT.2.3
۱۶۲	الزامات به‌روزرسانی امن ۷	FPT_TUD_EXT.2.4
۱۶۳	مدیریت کارکرد در محصول مورد ارزیابی ۱/ به‌روزرسانی خودکار	FMT_MOF.1.1/AutoUpdate
۱۶۴	مدیریت کارکرد در محصول مورد ارزیابی ۱/ توابع	FMT_MOF.1.1/Functions

۳-۱ کلاس ممیزی امنیت

برای حصول اطمینان از این‌که سرپرست محصول، اطلاعات لازم برای شناسایی مشکلات عمدی و غیرعمدی موجود در زمینه 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 سرپرستان مسئول بازبینی این اطلاعات را دچار سردرگمی کند. محصول مورد ارزیابی باید بتواند اطلاعات ممیزی را به یک موجودیت مورد اعتماد 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**	**FAU_GEN.1.1**

محصول 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 نیاز به حساب کاربری شخصی داشته باشند، نام حساب کاربری آن‌ها نیز باید ثبت شود)
- تغییرات امنیتی در پیکربندی (علاوه بر اطلاعات حاکی از تغییرات رخداده ، باید ثبت 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)
- [انتخاب: هیچ اقدام دیگر، اختصاص: [لیست سایر کاربردهای ویژه]]؛

ت) اختصاصاً لیست رویدادهای قابل ممیزی تعریف شده در جدول زیر

نام خانواده	رویدادهای قابل ممیزی	موارد اضافی تر
FAU_GEN.1	هیچ	
FAU_GEN.2	هیچ	
FAU_STG_EXT.1	هیچ	
FCS_CKM.1	هیچ	
FCS_CKM_EXT.4	هیچ	
FCS_COP.1(1)	هیچ	
FCS_COP.1(2)	هیچ	
FCS_COP.1(3)	هیچ	
FCS_COP.1(4)	هیچ	
FCS_RBG_EXT.1	هیچ	
FDP_RIP.2	هیچ	
FIA_PMG_EXT.1	هیچ	
FIA_UIA_EXT.1	همه مواردی که از سازوکار شناسایی و احراز هویت استفاده می‌کنند.	ارائه کردن شناسه کاربری، مبدا تلاش(به طور مثال IP address)
FIA_UAU_EXT.2	همه مواردی که از ساز و کارهای احراز هویت استفاده می‌کنند.	مبدا تلاش (به طور مثال IPaddress)
FIA_UAU.7	هیچ	
FIA_X509_EXT.1	تلاش ناموفق برای اعتبار سنجی یک گواهینامه	دلیل ناموفق بودن و شکست خوردن
FIA_X509_EXT.2	هیچ	
FIA_X509_EXT.3	هیچ	
FMT_MOF.1(1)/ TrustedUpdate	هر گونه تلاش برای شروع یک به‌روزرسانی دستی	هیچ
FMT_MTD.1	هیچ	
FMT_SMF.1	هیچ	
FMT_SMR.2	هیچ	
FPT_SKP_EXT.1	هیچ	
FPT_APW_EXT.1	هیچ	
FPT_TST_EXT.1	هیچ	

FPT_TUD_EXT.1	شـــروع به‌روزرســـانی؛ نتیجه تلاش به‌روزرسانی (موفقیت یا شکست)	هیچ اطلاعات اضافه دیگری
FPT_STM.1	تغییرات زمانی	مقادیر جدید و قدیم برای زمان مبدا تلاش (به طور مثال IP address)
FPT_TST_EXT.1	هیچ	
FTA_SSL_EXT.1	هرگونه تلاش در باز کردن یک نشست تعاملی	بدون هیچ اطلاعات اضافه
FTA_SSL.3	پایان دادن به نشست راه دور توسط سازوکارهای قفل نمودن نشست	بدون هیچ اطلاعات اضافه
FTA_SSL.4	پایان دادن یک نشست تعاملی	بدون هیچ اطلاعات اضافه
FTA_TAB.1	هیچ	
FTP_ITC.1	راه اندازی یک کانال امن پایان کانال امن شکست در عملکرد کانال امن	شناسایی راه‌انداز و مقصد تلاشی که در برقراری یک کانال امن، با شکست مواجه شده است.
FTP_TRP.1	راه اندازی یک کانال امن پایان کانال امن شکست در عملکرد مسیر امن	شناسایی، شناسه کاربری ادعا شده

۲	**تولید داده ممیزی ۲**	**FAU_GEN.1.2**

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 مؤلفه‌های کارکردی ارائه‌شده در پروفایل حفاظتی یا هدف امنیتی، اطلاعات در ستون سوم از جدول الزام **FAU_GEN.1.1** مشخص‌شده است.

۳	**تولید داده ممیزی ۳**	**FAU_GEN.2.1**

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.

نکته کاربردی:

زمانی که یک رویداد ممیزی توسط مؤلفه دیگری triggered شده باشد، مؤلفه‌ای که رویدادها را ثبت می‌کند باید رویداد را با آن شناسه آغازگر مؤلفه که باعث رویداد شده است، مرتبط کند. (فقط برای اهداف ارزیابی توزیع شده اعمال می‌شود.)

[۱] Subject

۴	محل ذخیره‌سازی داده‌های ممیزی ۱	FAU_STG_EXT.1.1

محصول باید قادر به ارسال داده ممیزی تولید شده به یک موجودیت IT خارجی با استفاده از کانال مورد اعتماد مطابق با FTP_ITC.1 باشد.

نکته کاربردی:

برای انتخاب گزینه انتقال داده‌های ممیزی تولیدشده به یک موجودیت IT خارجی، ذخیره‌سازی و بازبینی سوابق ممیزی از یک سرور ممیزی به‌جز سرور محصول مورد ارزیابی متکی است. در این مورد ذخیره‌سازی، توسط محیط عملیاتی صورت می‌گیرد.

تا زمانی که سرور ممیزی خارجی بخشی از هدف ارزیابی نباشد، به جز قابلیت‌های انتقال داده ممیزی FTP_ITC.1، هیچ الزامی برای آن وجود ندارد. هیچ الزامی برای قالب یا اساس پروتکل داده‌های ممیزی که منتقل می‌شوند وجود ندارد. هدف ارزیابی باید قادر به پیکربندی برای انتقال داده‌های ممیزی به موجودیت IT خارجی بدون مداخله مدیر باشد. انتقال دستی نیازمندی‌ها را برآورده نخواهد کرد. انتقال می‌تواند در زمان واقعی یا به صورت دوره‌ای انجام شود. اگر انتقال در زمان واقعی انجام نشود، TSS شرح می‌دهد که باید چه رویدادی برای انتقال ایجاد شود و چه محدوده‌ای از فرکانس‌های هدف ارزیابی برای ایجاد انتقال داده‌های ممیزی به سرور ممیزی پشتیبانی می‌شود. همچنین TSS فرکانس‌های قابل قبولی برای انتقال پیشنهاد می‌دهد.

برای هدف‌های ارزیابی توزیع‌شده، هر مؤلفه باید به طور مناسبی قادر به استخراج داده ممیزی از طریق کانال محافظت شده خارجی (FTP_ITC.1) یا بین مؤلفه‌ای (FPT_ITT.1 یا FTP_ITC.1) باشد. حداقل یک مؤلفه از هدف ارزیابی باید قادر به استخراج سوابق ممیزی از طریق FTP_ITC.1 باشد تا تمامی سوابق ممیزی هدف ارزیابی را بتوان برای موجودیت IT خارجی استخراج کرد.

۵	محل ذخیره‌سازی داده‌های ممیزی ۲	FAU_STG_EXT.1.2

محصول مورد ارزیابی باید بتواند داده‌های ممیزی تولیدشده را در خود ذخیره کند.

[انتخاب:

- هدف ارزیابی شامل تنها یک جزء مستقل است که داده‌های ممیزی را به‌صورت محلی ذخیره می‌کند .
- هدف ارزیابی باید یک هدف ارزیابی توزیع شده باشد که داده‌های ممیزی را روی اجزاء هدف ارزیابی زیر ذخیره می‌کند: [اختصاص: شناسایی اجزاء هدف ارزیابی
- هدف ارزیابی یک هدف ارزیابی توزیع شده با ذخیره داده‌های ممیزی است که به صورت خارجی برای اجزای هدف ارزیابی زیر ارائه شده است. [اختصاص: لیستی از مؤلفه‌های هدف ارزیابی که داده‌های ممیزی را به‌صورت محلی ذخیره نمی‌کنند و سایر اجزای هدف ارزیابی که داده‌های ممیزی تولید شده خود را به آن‌ها منتقل می‌کنند].

۶	محل ذخیره‌سازی داده‌های ممیزی ۳	FAU_STG_EXT.1.3

درصورتی‌که فضای حافظه محلی داده ممیزی پرشده 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:

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

برای اهداف ارزیابی توزیع شده، ذخیره محلی داده ممیزی تولید شده برای هر مؤلفه الزامی نیست ولی لازم است هدف ارزیابی کلی بتواند داده‌های ممیزی را به صورت محلی ذخیره کند. برای اطمینان از حفاظت سوابق ممیزی در موارد خطای ارتباط شبکه، هر مؤلفه باید حداقل بتواند اطلاعات ممیزی محلی را به طور موقت بافر کند. (برای جزئیات بیشتر به بخش ۶,۳,۳ مراجعه کنید). بافر محلی اطلاعات ممیزی لزوماً شامل حافظه غیرفرار نیست و اطلاعات ممیزی را می‌توان در حافظه فرار ذخیره نمود. هرچند، مفهوم ذخیره‌سازی محلی اطلاعات ممیزی در FAU_STG_EXT.1.3 نیازمند ذخیره‌سازی در حافظه غیرفرار است. رفتار هر مؤلفه‌ای که ذخیره‌سازی اطلاعات ممیزی را انجام می‌دهد، در زمانی که حافظه محلی در آستانه پر شدن باشد باید شرح داده شود. لازم است برای تمامی مؤلفه‌هایی که اطلاعات ممیزی را به جای ذخیره‌سازی محلی در خود، بافر می‌کنند شرح داده شود که در صورت رسیدن فضای بافر به آستانه پر شدن چه اتفاقی می‌افتد.

۳-۲ 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، تائید 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.

شماره الزام	نام الزام	
۷	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1

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

شماره الزام	نام الزام	
محصول مورد ارزیابی باید بر اساس الگوریتم‌های تولید کلید رمزنگاری مشخص‌شده، 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. رویه‌های FFC از Diffie-Hellman گروه ۱۴ استفاده می‌کند که موارد زیر را برآورده می‌کند:(RFC 3526 ، بخش ۳) **نکته کاربردی:** نویسنده هدف امنیتی، تمام الگوهای تولید کلید مورد استفاده برای استقرار کلید و احراز هویت دستگاه‌ها را انتخاب می‌کند. درصورتی‌که برای استقرار کلید از تولید کلید استفاده شود، الگوی در «مدیریت کلید رمزنگاری ۲» و پروتکل‌های رمزنگاری انتخاب‌شده باید مطابق با انتخاب باشند. درصورتی‌که برای احراز هویت دستگاه‌ها از تولید کلید استفاده شود، به غیر از *ssh-rsa*، *ecdsa-sha2-nistp256*، *ecdsasha2-nistp384* و*ecdsa-sha2-nistp521*، انتظار می‌رود که کلید عمومی مرتبط با یک گواهی‌نامه X.509v3 باشد. اگر محصول مورد ارزیابی به‌عنوان یک دریافت‌کننده در الگوی استقرار کلید عمل کند و برای پشتیبانی از احراز هویت دوطرفه پیکربندی نشده باشد، نیازی نیست که هدف ارزیابی، تولید کلید را پیاده‌سازی نماید. در اهداف ارزیابی توزیع‌شده، اگر کامپوننت هدف ارزیابی به عنوان یک دریافت‌کننده در الگوی استقرار کلید عمل کند، نیازی نیست که هدف ارزیابی تولید کلید را پیاده‌سازی نماید.		
۸	**مدیریت کلید رمزنگاری ۲**	**FCS_CKM.2.1**
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، مرور ۱ «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری فاکتورگیری عدد صحیح»[۲]؛		

[۱] Key establishment
[۲] Integer factorization cryptography

شماره الزام	نام الزام

- الگوهای استقرار کلید منحنی بیضوی [۱]که این الزامات را رعایت کنند: شماره ویژه NIST 800-56A، مرور۲ «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته»[۲]؛
- الگوهای استقرار کلید میدانی[۳] که این الزامات را رعایت کنند: شماره ویژه NIST 800-56A، مرور ۲ «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته».
- الگوی استقرار کلید با استفاده از گروه ۱۴ Diffie-Hellman مطابق RFC 3526 بخش ۳.

نکته کاربردی:

این عنصر در واقع نسخه اصلاح شده الزام «مدیریت کلید رمزنگاری۲[۴]» 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. برای گروه ۱۴ *Diffie-Hellman*، نویسنده هدف امنیتی باید به جای استفاده از انتخاب استقرار کلید میدانی محدود، از SFR به طور متناظر انتخاب کند.

الگوهای استقرار کلید مبتنی بر RSA در بخش ۹ از نسخه ۱ NIST SP 800-56B تشریح شده‌اند؛ اما این بخش وابسته به پیاده‌سازی موارد مذکور در سایر بخش‌های نسخه ۱ SP 800-56B است. اگر محصول مورد ارزیابی در الگوی استقرار کلید RSA به‌عنوان گیرنده عمل کند، نیازی نخواهد بود که محصول، 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، توسط تولید کلید مورداشاره در «مدیریت کلید رمزنگاری ۱» مشخص‌شده‌اند.

۹	نابودی کلید رمزنگاری ۴	FCS_CKM.4.1

توابع امنیتی مورد ارزیابی باید کلیدهای رمزنگاری را بر اساس یک روش خاص برای نابودی کلیدهای رمزنگاری، از بین ببرد: [اختصاص:

- در مورد کلیدهای با متن ساده در ذخیره‌سازی فرار[۵]، نابودی باید از طریق [انتخاب: یک بازنویسی ساده و مستقیم شامل [انتخاب: الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی، صفرها، یک‌ها، مقدار جدیدی از کلید، [اختصاص:

[۱] Elliptic curve-based
[۲] Discrete logarithm cryptography
[۳] Finite filed-based
[۴] FCS_CKM.2
[۵] Volatile memory

شماره الزام	نام الزام

مقداری ایستا یا پویا که شامل هیچ CSP نباشد.]]، از بین بردن ارجاع مستقیم به کلید پس از درخواست جمع‌آوری مقادیر باقی مانده] انجام شود

- در مورد کلیدهای با متن ساده در ذخیره‌سازی غیر فرار، نابودی باید از طریق فراخوانی یک رابط ارائه شده توسط بخشی از توابع امنیتی هدف امنیتی که [انتخاب:
  - به طور منطقی محل ذخیره‌سازی کلید را تعیین کرده و [انتخاب: تنها، [اختصاص: تعداد انجام]-بار] بازنویسی شامل [انتخاب: یک الگوی شبه تصادفی با استفاده از RBG محصول، صفرها، یک‌ها، مقدار جدیدی از کلید، [اختصاص: یک مقدار استاتیک یا پویا که شامل هیچ CSP نباشد]] انجام دهد.
  - آموزش بخشی از محصول برای تخریب انتزاعی که نشان‌دهنده کلید است.

  ] باشد.

نکته کاربردی:

در بخش‌هایی از انتخاب‌ها که کلیدهای تخریب شده توسط "بخشی از TSF" شناسایی شده‌اند؛ TSS بخش مربوطه و رابط درگیر را تشخیص می‌دهد. رابطی که در این الزام مورد ارجاع قرار می‌گیرد، می‌تواند اشکال مختلفی برای اهداف ارزیابی داشته باشد، که بیشتر مانند رابط برنامه‌نویسی برنامه کاربردی برای هسته سیستم عامل است. ممکن است سطوح مختلفی از abstraction مشاهده شود. برای مثال، در یک پیاده‌سازی داده شده، برنامه ممکن است به جزئیات فایل سیستم دسترسی داشته باشد و ممکن است بتواند به طور منطقی محل حافظه خاصی را آدرس‌دهی نماید. در پیاده‌سازی دیگری، برنامه ممکن است مدیریت ساده‌ای روی منبعی داشته باشد و فقط بتواند از بخش دیگری از محصول مانند مترجم[۱] یا سیستم‌عامل درخواست حذف منبع کند.

در صورتی که برای کلیدهای مختلف و/یا وضعیت‌های تخریب مختلف، از روش‌های مختلف تخریب کلید استفاده شود، وضعیت‌های متفاوت و کلیدها/روش‌های اعمال آن‌ها در TSS شرح داده می‌شود. (و ممکن است سند هدف امنیتی برای کمک به وضوح بیشتر از تکرارهای مجزایی از SFR ها استفاده کند. TSS تمامی کلیدهای مرتبط مورد استفاده در پیاده‌سازی SFRها، از جمله مواردی که کلیدها در فرم غیر متنی ذخیره می‌شوند را شرح می‌دهد. در مورد ذخیره‌سازی غیر متنی، روش رمزنگاری و کلید مرتبط- کلید رمزنگاری در TSS شناسایی می‌شوند.

برخی انتخاب‌ها اجازه اختصاص "مقداری که شامل هیچ CSP نیست" می‌دهند. به این معنی است که، هدف ارزیابی از برخی داده‌های مشخصی استفاده می‌کند که توسط RBG برای برآورده کردن نیازمندی‌های FCS_RBG_EXT در نظر گرفته نشده است، و هیچ کدام از مقادیر خاص ذکر شده در گزینه‌های دیگر انتخاب نیست. عبارت "شامل هیچ CSP" برای اطمینان از انتخاب با دقت داده‌ها است و از منبعی عمومی که ممکن است شامل داده‌های حاضر یا قبلی که خود نیازمند حفظ محرمانگی هستند، گرفته نشده است.

[۱] interpreter

شماره الزام	نام الزام	
برای اجتناب از تردید: "کلیدهای رمزنگاری" در این SFR شامل کلیدهای نشست است. تخریب کلید بر روی مؤلفه‌های عمومی جفت کلید نامتقارن اعمال نمی‌شود.		
۱۰	**عملیات رمزنگاری ۱ (۱)**	FCS_COP.1.1/DataEncryption
توابع امنیتی مورد ارزیابی باید رمزگذاری و رمزگشایی را بر اساس الگوریتم‌های رمزنگاری خاص AES که در حالت [انتخاب: CBC، CTR، GCM] استفاده می‌شوند و در اندازه‌های کلید رمزنگاری [اختصاص: ۱۲۸ بیتی، ۱۹۲ بیتی، ۲۵۶ بیتی] و با توجه به استاندارد AES که در ISO 18033-3 تعریف شده است، [انتخاب: CBC همان‌طور که در ISO 10116 مشخص‌شده است، CTR مشخص شده در ISO 10116، GCM همان‌طور که در ISO 19772 مشخص‌شده است]. انجام دهد. **نکته کاربردی:** در مورد نخستین انتخاب عملیات رمزنگاری ۱(۱)/رمزنگاری داده، نویسنده هدف امنیتی باید حالت یا حالت‌های کارکردی AES را انتخاب 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)**	FCS_COP.1.1/SigGen

[۱] Cipher suite

شماره الزام	نام الزام	
توابع امنیتی مورد ارزیابی باید خدمات امضای رمزنگاری (تولید و تائید) را بر اساس الگوریتم‌های رمزنگاری خاص ارائه کند: [انتخاب: • الگوریتم امضای دیجیتال RSA و اندازه کلیدهای رمزنگاری(ماژول‌ها) [اختصاص: ۲۰۴۸ بیتی یا بزرگ‌تر] • الگوریتم امضای دیجیتال منحنی بیضوی و اندازه کلیدهای رمزنگاری [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 RSASSA_PKCS1v1_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال ۲ یا الگوی امضای دیجیتال ۳، • در مورد الگوهای ECDSA: FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۶ و پیوست D، با اجرای منحنی‌های NIST [انتخاب: P-384، P-256، P-521، هیچ منحنی دیگر]؛ ISO/IEC 14888-3، بخش ۶,۴] **نکته کاربردی:** نویسنده هدف امنیتی باید الگوریتم پیاده‌سازی شده برای اجرای امضای دیجیتال را انتخاب کند.. نویسنده هدف امنیتی باید انتخاب‌ها/اختصاص‌های مناسبی به منظور مشخص نمودن پارامترهایی که برای الگوریتم پیاده‌سازی می‌شوند، ایجاد کند. نویسنده هدف امنیتی باید اطمینان حاصل نماید که اختصاص‌ها و انتخاب‌های این SFR شامل تمامی مقادیر پارامترهای ضروری برای مجموعه رمزهای منتخب در سند هدف امنیتی برای پروتکل SFRها می‌باشد. (پیوست B.2.1 را ببینید) نویسنده سند هدف امنیتی انطباق انتخاب‌ها با سایر الزامات SFR، مخصوصاً زمانی که از منحنی‌های بیضوی پشتیبانی می‌شود بررسی می‌کند.		
۱۲	**عملیات رمزنگاری ۱ (۳)**	FCS_COP.1.1/Hash

شماره الزام	نام الزام	
توابع امنیتی مورد ارزیابی باید خدمات درهم‌سازی رمزنگاری را بر اساس یک الگوریتم رمزنگاری مشخص [انتخاب: SHA-1, SHA-256, SHA-384, SHA-512] و اندازه پیام هشدار [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیت با رعایت استاندارد ISO/IEC 10118-3:2004. ارائه نماید **نکته کاربردی:** به تولیدکنندگان اکیداً توصیه می‌شود که از پروتکل‌های به‌روزرسانی شده‌ای که از خانواده SHA-2 پشتیبانی می‌نمایند، پیاده‌سازی کنند. تا زمانی که پروتکل‌های به‌روز شده پشتیبانی شوند، این پروفایل حفاظتی اجازه پشتیبانی از پیاده‌سازی‌های SHA-1 را بر اساس SP 800-131A فراهم می‌کند. در نسخه بعدی این پروفایل حفاظتی، SHA-256 حداقل نیازمندی برای تمامی اهداف امنیتی خواهد بود. 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)**	FCS_COP.1.1/KeyedHash
محصول مورد ارزیابی باید احراز هویت پیام مبتنی بر کلید درهم‌سازی شده[1] را بر اساس الگوریتم رمزنگاری خاص [انتخاب:HMAC-SHA-1, HMAC-SHA-256,HMAC-SHA-384, HMAC-SHA-512] و اندازه کلید رمزنگاری [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 [اختصاص: بخش هفتم ISO/IEC 9797-2:2011 با نام «الگوریتم MAC ۲»] انجام دهد. **نکته کاربردی ۱۵:** 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**	FCS_RBG_EXT.1.1
محصول مورد ارزیابی باید تمامی خدمات تولید بیت تصادفی قطعی را بر اساس ISO/IEC 18031:2011 و با استفاده از [انتخاب: Hash_DRBG(هر)، HMAC_DRBG (هر)، CTR_DRBG (AES)] ارائه دهد.		
۱۵	**تولید بیت تصادفی ۲**	FCS_RBG_EXT.1.2

[1] Keyed-hash message authentication

شماره الزام	نام الزام

RBG قطعی باید دست کم توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی را از [انتخاب: [اختصاص: تعداد منابع مبتنی بر نرم‌افزار] منبع نویز مبتنی بر نرم‌افزار، [اختصاص: تعداد منابع مبتنی بر سخت‌افزار] 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 مورد اشاره در ISO/IEC 18031:2011 از کلیدها و CSPهایی که تولید خواهد کرد، باشد.

نکته کاربردی ۱۶:

در مورد نخستین عبارت انتخاب در «تولید بیت تصادفی ۲» ، هدف امنیتی باید حداقل به یکی از انواع منابع نویز اشاره کند. اگر محصول مورد ارزیابی شامل چندین منابع نویز از یک نوع باشد، نویسنده هدف امنیتی عبارت اختصاص را با تعداد مناسبی برای 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 برای این عنصر، باید تکرار شود تا تمام منابع مورد اشاره 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 نوبه خود، به عناصر اولیه رمزنگاری اساسی (توابع درهم‌ساز و رمزها) بستگی دارد. نویسنده هدف امنیتی، تابع مورداستفاده را انتخاب خواهد کرد و شامل عناصر اولیه رمزنگاری اساسی خاص مورد استفاده در الزام است با اینکه هریک از توابع درهم‌ساز تعیین‌شده (SHA-1, , SHA-256, SHA-384, SHA-512) را می‌توان در Hash_DRBG یا HMAC_DRBG مورداستفاده قرار داد، تنها اجازه پیاده‌سازی‌های مبتنی بر AES در CTR_DRBG وجود دارد.

اگر اندازه کلید برای پیاده‌سازی AES متفاوت از اندازه کلید مورداستفاده برای رمزگذاری داده‌های کاربری باشد، ممکن است نیاز به تنظیم یا تکرار «عملیات رمزنگاری» باشد تا اندازه کلید مختلف در آن لحاظ گردد. برای انتخاب در «تولید بیت تصادفی ۲»، نویسنده هدف امنیتی حداقل تعداد بیت‌های آنتروپی تزریق‌شده به RBG را تعیین می‌کند. که باید برابر با، یا بیشتر از قدرت امنیتی هر کلید تولید شده توسط هدف ارزیابی باشد.

۳-۳ کلاس شناسایی و احراز هویت

محصول، یک مکانیسم ورود مبتنی بر گذرواژه را به عنوان ابزاری امن در اختیار سرپرستان قرار می‌دهد تا بتوانند با استفاده از آن با محصول مورد ارزیابی ارتباط برقرار کنند. سرپرست محصول باید یک گذرواژه قدرتمند را تهیه کند و مکانیسمی را برای تغییر منظم آن در نظر گیرد. برای جلوگیری از حملاتی که در آن‌ها فرد مهاجم نوشتن/ورود گذرواژه به‌وسیله سرپرست، را می‌بیند، گذرواژه را باید در هنگام ورود به حالت محو و ناخوانا درآورد. قفل‌کردن و خاتمه دادن نشست را نیز می‌توان برای جلوگیری از ورود غیرمجاز به حساب کاربری استفاده شده

قرار داد. گذرواژه‌ها 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 احراز هویت ناموفق ۱**	FIA_AFL.1.1
محصول، باید هنگامی که یک عدد صحیح مثبت قابل تنظیم توسط سرپرست در [اختصاص: بازه عددی قابل‌قبول] از تلاش‌های ناموفق احراز هویت مربوط به تلاش سرپرست برای احراز هویت راه دور رخ داد، مشخص نمایند		
۱۷	**مدیریت احراز هویت ناموفق ۲**	FIA_AFL.1.2
زمانی که تعداد تعیین شده از تلاش‌های احراز هویت ناموفق صورت گرفت، محصول باید انتخاب: [○ احراز هویت موفق سرپرست راه دور متخلف را تا [اختصاص: اقدام] توسط سرپرست محلی انجام شود، محدود کند. ○ احراز هویت موفق سرپرست راه دور متخلف را تا اتمام زمان تعیین شده توسط مدیر، محدود کند. [**نکته کاربردی:** این الزام برای تعداد مشخصی از تلاش‌های احراز هویت ناموفق پیوسته اعمال می‌شود و برای مدیر در کنسول محلی تا زمانی که حساسیتی برای قفل کردن حساب مدیر به این شکل نباشد؛ اعمال نمی‌شود. این مورد می‌تواند (برای مثال) با نیاز به حساب جداگانه برای مدیران محلی یا وجود مکانیسم احراز هویت پیاده‌سازی شده‌ای که تلاش ورود محلی و راه دور را تشخیص می‌دهد مورد توجه قرار گیرد. "اقدام" که توسط مدیر محلی انجام می‌شود، به طور خاص پیاده‌سازی شده و در راهنما مدیر تعریف می‌شود. (برای مثال؛ تنظیم مجدد تحریم، تنظیم مجدد رمز عبور). نویسنده سند هدف امنیتی با توجه به نحوه پیاده‌سازی و مدیریت هدف ارزیابی، یکی از گزینه‌ها را برای مدیریت شکست احراز هویت انتخاب می‌کند. در TSS شرح داده شده است که هدف ارزیابی چگونه تضمین کند که شکست احراز هویت توسط مدیران راه دور، نمی‌توانند منجر به حالتی شوند که هیچ دسترسی مدیریتی چه به طور دائم و چه به طور موقت وجود نداشته باشد. (برای مثال: با ارائه ورود محلی که مسدود نباشد.) دستورالعمل عملیاتی توصیف و شناسایی اهمیت هر اقدامی که برای اطمینان از حفظ دائمی دسترسی مدیر مورد نیاز است را ارائه می‌دهد، حتی اگر مدیر راه دور در نتیجه FIA_AFL.1 به دلیل مسدود شدن حساب‌ها، به طور دائمی یا موقت در دسترس نباشد.		
۱۸	**مدیریت رمز عبور ۱**	FIA_PMG_EXT.1.1
توابع امنیتی 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 بین [اختصاص: حداقل تعداد کاراکترهای پشتیبانی شده توسط هدف ارزیابی] و [اختصاص: تعداد کاراکترهای بزرگ‌تر یا مساوی ۱۵]قابل پیکربندی باشد.

نکته کاربردی:

نویسنده هدف امنیتی کاراکترهای ویژه که توسط هدف ارزیابی پشتیبانی می‌شوند را تعیین می‌کند. وی می‌تواند با استفاده از عبارت اختصاص، کاراکترهای ویژه دیگری را به لیست اختیاری بیفزاید. منظور از «کلمه‌های عبور سرپرستی »، کلمه‌های عبوری هستند که توسط مدیران سیستم در کنسول محلی مورد استفاده 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 هدف امنیتی پشتیبانی می‌کنند.

اختصاص دوم باید با حداقل طول بزرگ‌ترین کلمه عبور توسط مدیر امنیتی پیکربندی شود.

۱۹	**شناسایی و احراز هویت کاربر ۱**	FIA_UIA_EXT.1.1

توابع امنیتی 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:

- نمایش بنر هشدار مطابق با FTA_TAB.1
- [انتخاب: هیچ اقدامات دیگری ،تولید خودکار کلیدهای رمزنگاری [اختصاص: لیست خدمات، اقدامات انجام‌شده توسط محصول مورد ارزیابی در پاسخ به درخواست‌های غیر از هدف ارزیابی]]

۲۰	**شناسایی و احراز هویت کاربر ۲**	FIA_UIA_EXT.1.2

پیش از آن که توابع امنیتی مورد ارزیابی امکان انجام هر اقدامات میانی دیگری از طرف کاربر مدیریتی سیستم را فراهم آورد، باید مدیر سیستم را با موفقیت شناسایی و احراز هویت نماید.

نکته کاربردی:

این الزام برای کاربران خدماتی که به طور مستقیم توسط محصول مورد ارزیابی در دسترس قرار می‌گیرند (چه مدیران سیستم و چه موجودیت‌های IT خارجی) اعمال می‌شود و در مورد خدماتی که از طریق ارتباطات محصول مورد ارزیابی در دسترس قرار می‌گیرند ، 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.

اگر از تولید خودکار کلیدهای رمزنگاری بدون تائید سرپرست پشتیبانی شود ، گزینه "تولید خودکار کلیدهای رمزنگاری" باید انتخاب شود .

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) این ارتباطات باید بر اساس الزام‌های «کانال امن» انجام شوند که پروتکل‌ها تعیین و احراز هویت را انجام می‌دهند. 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 "counts" به معنی آغاز فرایند تعیین و احراز هویت است.

مطابق نکته کاربردی ۲۴، برای اهداف امنیتی توزیع شده، حداقل یک مؤلفه باید از احراز هویت مدیران امنیتی مطابق FIA_UIA_EXT.1 و FIA_UAU_EXT.2 پشتیبانی کند. ولی تمامی مؤلفه‌های هدف ارزیابی ضروری نیست. در صورتی که تمامی مؤلفه‌های هدف ارزیابی از این روش احراز هویت مدیران امنیتی پشتیبانی نکنند، TSS باید نحوه شناسایی و احراز هویت مدیران امنیتی را شرح دهد.

۲۱	**سازوکار احراز هویت بر اساس رمزعبور ۲**	FIA_UAU_EXT.2.1

توابع امنیتی مورد ارزیابی باید یک مکانیسم احراز هویت مبتنی بر کلمه عبور محلی، [انتخاب: [اختصاص: سایر مکانیسم‌های احراز هویت]، هیچ مکانیسم احراز هویتی] را برای احراز هویت کاربر مدیر محلی فراهم آورد.

نکته کاربردی:

عبارت اختصاص باید تمام مکانیسم‌های احراز هویت پشتیبانی‌شده محلی اضافی را شناسایی کند. مکانیسم‌های احراز هویت محلی از طریق کنسول محلی تعریف می‌شوند. نشست‌های مدیریتی از راه دور (و مکانیسم‌های احراز هویت مربوط به آن‌ها) در « *FTP_TRP.1/Admin* » مشخص شده‌اند.

مطابق نکته کاربردی ۲۴، برای اهداف امنیتی توزیع شده، حداقل یک مؤلفه باید از احراز هویت مدیران امنیتی مطابق FIA_UIA_EXT.1 و FIA_UAU_EXT.2 پشتیبانی کند. ولی تمامی مؤلفه‌های هدف ارزیابی ضروری نیست. در صورتی که تمامی مؤلفه‌های هدف ارزیابی از این روش احراز هویت مدیران امنیتی پشتیبانی نکنند، TSS باید نحوه شناسایی و احراز هویت مدیران امنیتی را شرح دهد.

۲۲	**احراز هویت کاربر ۱۰**	FIA_UAU.7.1

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

نکته کاربردی:

«بازخورد مبهم» به معنی بازخوردی است که در آن محصول مورد ارزیابی هر داده‌ی احراز هویت وارد شده توسط کاربر را به صورت واضح و قابل خواندن نشان نمی‌دهد(مانند انعکاس کلمه‌عبور) ؛ البته ممکن است روند پیشرفت به شکل مبهم نشان داده شود (مانند

[۱] Obscured feedback

یک ستاره برای هر کاراکتر). بازخورد مبهم همچنین نشان می‌دهد که محصول مورد ارزیابی در جریان احراز هویت کاربر هیچ اطلاعاتی را که ممکن است نشان‌دهنده داده‌های احراز هویت باشد، نمایش نمی‌دهد.

۳-۴ کلاس مدیریت امنیت

توابع مدیریتی مورد نیاز در این بخش، شامل قابلیت‌های مورد نیاز برای پشتیبانی از نقش سرپرست امنیتی محصول و همچنین مجموعه‌ای از توابع مدیریتی امنیت مورد نیاز برای مدیریت بخش‌های قابل پیکربندی الزامات کارکرد امنیتی (FMT_SMF.1)، مدیریت کلی داده‌های توابع امنیتی محصول (FMT_MTD.1/CoreData) و فعال کردن به‌روزرسانی‌های محصول (FMT_MOF.1/ManualUpdate) هستند.

برای محصولات توزیع‌شده، مدیریت امنیتی مؤلفه‌های محصول باید برای هر مؤلفه به صورت مستقیم یا از طریق دیگر مؤلفه‌های تحقق بخشیده شود. خلاصه مشخصات محصول باید مشخص نماید که کدام الزامات کارکردی امنیتی مدیریتی و توابع مدیریتی برای هر مؤلفه اعمال می‌گردد (فقط در محصولات توزیع‌شده).

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	
۲۳	**مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی دستی**	FMT_MOF.1.1/ManualUpdate
توابع امنیتی مورد ارزیابی باید توانایی فعال کردن توابع به‌منظور به‌روزرسانی دستی را به سرپرست امنیتی محدود نماید. **نکته کاربردی:** این الزام امکان آغاز به‌روزرسانی دستی را به سرپرستان امنیتی محدود می‌کند.		
۲۴	**مدیریت داده‌های محصول ۱**	FMT_MTD.1.1/CoreData
توابع امنیتی مورد ارزیابی باید امکان «مدیریت» داده‌های محصول را به سرپرست‌های امنیتی محدود کند. **نکته کاربردی:** منظور از «مدیریت» می‌تواند هر یک از این اقدامات و موارد دیگری از این دست باشد: تولید، آغاز، بازدید، تغییر پیش‌فرض، تغییر، حذف، پاک کردن و اضافه نمودن. الزام کارکرد امنیتی حاضر همچنین شامل بازگرداندن کلمه عبورکاربری به حالت پیش‌فرض توسط سرپرست امنیتی است. در اینجا شناسه "CoreData" برای تفکیک الزام FMT_MTD.1 از الزام اختیاری FMT_MTD.1 تعریف شده در پیوست A.4.2.1 (FMT_MTD.1/CryptoKeys) می‌باشد.		

شماره الزام	نام الزام	
۲۵	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1

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

[اختصاص:

- توانایی مدیریت محصول به‌صورت محلی و از راه دور
- توانایی پیکربندی بنر دسترسی
- توانایی پیکربندی زمان غیرفعال بودن نشست پیش از قفل‌کردن یا خاتمه دادن آن
- توانایی به‌روزرسانی محصول مورد ارزیابی و تائید به‌روزرسانی‌ها با استفاده از قابلیت [انتخاب: امضای دیجیتال، مقایسه درهم‌سازی] پیش از نصب شدن این به‌روزرسانی‌ها
- توانایی پیکربندی پارامترهای احرازهویت ناموفق برای FIA_AFL.1
- [انتخاب:
- توانایی شروع و متوقف کردن سرویس‌ها .
  - توانایی پیکربندی رفتار ممیزی
  - توانایی تغییر رفتار انتقال داده ممیزی به یک موجودیت فناوری اطلاعات خارجی، بررسی داده‌های ممیزی، عملکرد ممیزی وقتی که فضای ذخیره‌سازی محلی پر است.
  - توانایی پیکربندی لیست خدمات ارائه‌شده در دسترس توسط محصول مورد ارزیابی پیش از شناسایی و احراز هویت یک موجودیت، چنان که در «شناسایی و احراز هویت کاربر[۱]» تشریح شده است.
  - توانایی مدیریت کلیدهای رمزنگاری
  - توانایی پیکربندی کارکرد رمزنگاری
  - توانایی پیکربندی آستانه[۲] برای تجدید کلید SSH
  - توانایی پیکربندی مدت زمان برای SA در IPsec
  - توانایی پیکربندی اثر متقابل بین اجزای هدف ارزیابی
  - توانایی فعال یا غیرفعال کردن بررسی خودکار برای به‌روزرسانی ها یا به‌روزرسانی های خودکار
  - توانایی فعال‌سازی مجدد حساب کاربری مدیر
  - توانایی تنظیم زمانی که برای مهرهای زمانی استفاده می‌شود.
  - توانایی پیکربندی NTP

[۱] FIA_UIA_EXT.1

[۲] Threshold

شماره الزام	نام الزام

- توانایی پیکربندی مرجع شناسایی همتا
- توانایی مدیریت انبار اطمینان هدف ارزیابی و تعیین گواهی‌های X509.v3 به عنوان لنگر اطمینان
- توانایی وارد کردن گواهی X509.v3 به انبار اطمینان هدف ارزیابی
- هیچ قابلیت دیگری]

[

نکته کاربردی:

محصول مورد ارزیابی باید کارکردهای لازم برای مدیریت سیستم به‌صورت محلی و مدیریت از راه دور را فراهم آورد.

به طور کلی، این پروفایل حفاظتی، تابع مدیریت امنیتی خاصی که از طریق رابط مدیر محلی یا رابط مدیر از راه دور یا هر دو قابل دسترسی باشد را الزام نمی‌کند. TSS باید با جزئیات مشخص کند که کدام توابع مدیریت امنیتی از طریق کدام رابط‌ها قابل دسترسی هستند. هدف ارزیابی باید قابلیت پیکربندی بنر دسترسی را برای FTA_TAB.1 و قابلیت پیکربندی زمان غیرفعال بودن نشست را برای FTA_SSL_EXT.1 و FTA_SSL.3 ارائه دهد. آیتم "توانایی به‌روزرسانی هدف ارزیابی و تائید به‌روزرسانی‌هایی که از قابلیت امضای دیجیتال استفاده می‌کنند قبل از نصب این به‌روزرسانی‌ها" شامل توابع مدیریتی مربوطه از FMT_MOF.1/ManualUpdate ، FMT_MOF.1/AutoUpdate (اگر در ST باشد) FIA_X509_EXT.2.2 و FPT_TUD_EXT.1.2 و FPT_TUD_EXT.2.2 (اگر در ST باشند و اگر شامل اقدام قابل پیکربندی توسط مدیر باشند) می‌باشند

به طور مشابه، انتخاب "توانایی پیکربندی رفتار ممیزی" شامل توابع امنیتی مربوطه از FMT_MOF.1/Services و FMT_MOF.1/Functions (برای تمام این SFRهایی که در سند ST هستند) می‌باشند. اگر هدف ارزیابی توانایی غیرفعال کردن حساب کاربری مدیر از راه دور را از طریق FIA_AFL.1 ارائه کند، نویسنده سند هدف امنیتی باید گزینه "توانایی فعال‌سازی مجدد حساب مدیر" را برای مجوز فعال‌سازی مجدد حساب توسط مدیر محلی، انتخاب کند. اگر هدف ارزیابی برای مدیر توانایی پیکربندی رفتار ممیزی، قبل از شناسایی یا احراز هویت ارائه کند، یا اگر هرکدام از عملکردهای رمزنگاری در هدف ارزیابی قابل پیکربندی باشد، یا اگر ST هدف ارزیابی توزیع شده‌ای را شرح دهد، نویسنده هدف امنیتی باید انتخاب مناسبی انجام دهد یا در انتخاب دوم، گزینه در غیر این صورت "هیچ قابلیت دیگری" را انتخاب کند. (انتخاب دوم ممکن است متناوباً در ST خالی بماند)

اگر هدف ارزیابی از پیکربندی آستانه برای مکانیسم‌های مورد استفاده برای FCS_SSHC_EXT.1.8 یا FCS_SSHS_EXT.1.8 (لازم است برای این تنظیمات FMT_MOF.1/Functions در ST باشد.) پشتیبانی می‌کند، گزینه "توانایی پیکربندی آستانه برای تجدید کلید SSH" باید در سند هدف امنیتی انتخاب شده باشد. اگر هدف ارزیابی محدودیتی برای مقادیر قابل قبول آستانه قرار داده است، باید در TSS بیان شود.

شماره الزام	نام الزام	
اگر هدف ارزیابی از ارتباط امن از طریق IPsec پشتیبانی کند و الزامات FCS_IPSEC_EXT.1 در سند هدف امنیتی باشد، باید در سند هدف امنیتی گزینه "توانایی تنظیم طول عمر IPsec SAs" انتخاب شود. تنظیمات طول عمر برای IPsec SAs لازم است از طریق انتخاب در FCS_IPSEC_EXT.1.7 باشد. (لازم است برای این تنظیمات FMT_MOF.1/Functions در ST باشد.) اگر هدف ارزیابی به مدیر اجازه تنظیم زمان دستگاهی که در مهرهای زمانی استفاده می‌شود داده باشد، گزینه "توانایی تنظیم زمانی که برای مهرهای زمانی استفاده می‌شود" باید در ST انتخاب شود. اگر هدف ارزیابی اجازه تنظیمات دستی زمان را نداده و فقط متکی به هماهنگی با منابع خارجی زمان مانند سرورهای NTP می‌باشد، این گزینه نباید انتخاب شود. اگر هدف ارزیابی از ارتباطات امن از طریق پروتکل IPsec پشتیبانی می‌کند و الزامات FCS_IPSEC_EXT.1 در ST باشد، گزینه "توانایی پیکربندی مرجع شناسایی همتا" باید در ST انتخاب شود. ممکن است پیکربندی مرجع شناسایی برای اهداف امنیتی که فقط از آدرس IP و انواع شناسه FQDN پشتیبانی می‌کنند، همانند پیکربندی نام‌های همتا برای اهداف ارتباط باشد. برای اهداف ارزیابی توزیع‌شده، تعامل بین مؤلفه‌های هدف امنیتی قابل تنظیم خواهد بود (FCO_CPC_EXT.1 را ببینید). بنابراین، نویسنده هدف امنیتی گزینه "توانایی پیکربندی اثر متقابل بین اجزای هدف ارزیابی" را برای اهداف ارزیابی توزیع‌شده انتخاب می‌کند. یک مثال ساده، "تغییر پروتکل ارتباطی مطابق FPT_ITT.1 " است. مثال دیگر، "تغییر مدیریت مؤلفه هدف ارزیابی از مدیریت مستقیم از راه دور، به مدیریت از راه دور از طریق یک مؤلفه دیگری از هدف ارزیابی"، می‌باشد. یک مورد استفاده پیچیده‌تر، "اگر تحقق یک SFR از طریق دو مؤلفه یا بیشتر از هدف ارزیابی به دست آید و مسئولیت‌ها بین دو مؤلفه یا بیشتر قابل‌تغییر باشد"، است. برای اهداف ارزیابی که کانال registration را پیاده‌سازی کرده‌اند (همان‌طور که در FCO_CPC_EXT.1.2 شرح داده شده است)، نویسنده هدف امنیتی از گزینه "توانایی پیکربندی کارکرد رمزنگاری" در این SFR استفاده می‌کند، و به طور متناظر در TSS برای تشریح پیکربندی هر منظر رمزنگاری کانال registration که برای بهبود امنیتی کانال، توسط محیط عملیاتی قابل‌تغییر است نگاشت می‌شود. (cf. توصیف محتوای رویه‌های آمادگی در [SD, 3.6.1.2])		
۲۶	**نقش‌های امنیتی ۳**	FMT_SMR.2.1
محصول باید نقش‌های زیر را نگهداری کند. • سرپرست امنیتی		
۲۷	**نقش‌های امنیتی ۴**	FMT_SMR.2.2
توابع امنیتی مورد ارزیابی باید بتواند بین کاربران و نقش‌ها ارتباط برقرار نماید.		
۲۸	**نقش‌های امنیتی ۵**	FMT_SMR.2.3

شماره الزام	نام الزام

توابع امنیتی مورد ارزیابی باید از برقرار بودن شرایط زیر اطمینان حاصل کند:

- نقش سرپرست امنیتی باید بتواند محصول مورد ارزیابی را به صورت محلی مدیریت کند.
- نقش سرپرست امنیتی باید بتواند محصول مورد ارزیابی را از راه دور مدیریت کند.

نکته کاربردی:

بر اساس این الزام سرپرست امنیتی باید بتواند محصول مورد ارزیابی را از طریق یک کنسول محلی و یک مکانیسم راه دور مدیریت کند. نویسنده هدف امنیتی باید برای نشان دادن نحوه دستیابی به ارتباط امن FTP_ITC.1، FPT_ITT.1 و/یا FTP_TRP.1/Admin را انتخاب کند.

در این SFR، پیاده‌سازی مدیریت کاربر خود، برای تمامی مؤلفه‌های هدف ارزیابی، در اهداف ارزیابی توزیع شده، الزامی نیست. حداقل یک مؤلفه باید از احراز هویت و شناسایی مدیران امنیتی مطابق با FIA_UIA_EXT.1 و FIA_UAU_EXT.2 پشتیبانی کند. احراز هویت سایر مؤلفه‌های هدف ارزیابی به عنوان مدیر امنیتی، می‌تواند از طریق کانال امن (یا مطابق با FTP_ITC.1 یا FPT_ITT.1) با استفاده از مؤلفه‌ای که احراز هویت مدیران را مطابق FIA_UIA_EXT.1 و FIA_UAU_EXT.2 پشتیبانی می‌کند محقق شود. شناسایی کاربران مطابق با FIA_UIA_EXT.1.2 و وابستگی کاربران با قوانین مطابق FMT_SMR.2.2، از طریق مؤلفه‌هایی که احراز هویت مدیران امنیتی را مطابق با FIA_UIA_EXT.1 وFIA_UAU_EXT.2 پشتیبانی می‌کنند انجام می‌شود. پشتیبانی از مدیریت[1] محلی مؤلفه‌های تعریف شده در FMT_SMR.2.3، توسط مؤلفه‌های هدف ارزیابی که مدیران امنیتی را از طریق استفاده از کانال امن احراز هویت می‌کنند الزامی نیست.

۳-۵ کلاس حفاظت از محصول مورد ارزیابی

در این بخش، الزامات مربوط به محصول مورد ارزیابی برای حفاظت از داده‌های امنیتی حساس مانند کلیدها و گذرواژه‌ها، 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
۲۹	محافظت از داده‌های محصول (کلیدهای متقارن) ۱

[1] administration

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:** هدف از الزام حاضر این است که دستگاه بتواند مانع از دسترسی غیرمجاز 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 از مشخص 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.	
۳۰	**حفاظت از گذرواژه سرپرست محصول ۱**
محصول مورد ارزیابی نباید کلمه‌های عبور را به شکل متن ساده ذخیره کند.	
۳۱	**حفاظت از گذرواژه سرپرست محصول ۲**
محصول مورد ارزیابی باید از خوانده شدن گذرواژه‌هایی که به‌صورت متن ساده[۱] هستند، جلوگیری کند. **نکته کاربردی:** 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 گذرواژه متن ساده را از طریق واسط «عادی» بخواند. البته سرپرست محصول که تمام دسترسی‌ها را داشته باشد می‌تواند گذرواژه را بخواند؛ اما به وی اعتماد می‌شود و فرض می‌گردد که وی این کار را نخواهد کرد. گذرواژه‌ها باید مطابق با الزام FIA_UAU.7 هنگام ورود در کنسول محلی، به صورت مبهم باشد.	

۳-۵-۱ تست 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 مؤلفه در پیوست دو ارائه شده‌اند.

[۱] Plaintext

شماره الزام	نام الزام
۳۲	خودآزمایی محصول ۱

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:

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.

محصولات توزیع‌نشده ممکن است به صورت داخلی شامل چند مؤلفه توزیع شده در راستای اجرای الزامات کارکرد امنیتی باشند. خودآزمایی‌ها باید تمام مؤلفه‌هایی که برای اجرای الزامات کارکرد امنیتی توزیع شده‌اند را پوشش دهد، و اگرچه ممکن است در راستای اجرایی شدن الزامات کارکرد امنیتی، این الزامات روی مؤلفه‌ها توزیع شده باشند، ولی بررسی/تائید جامعیت شدن باید تمام نرم‌افزار را پوشش دهد.

برای محصولات توزیع‌شده هر مؤلفه ملزم به اجرای خودآزمایی می‌باشد. ولی الزامی وجود ندارد که همه مؤلفه‌ها خودآزمایی یکسانی را اجرا نمایند. نویسنده هدف امنیتی انتخاب‌های ممکن و سپس اختصاص‌های نهایی را برای هر مؤلفه توصیف می‌نماید.

نکته کاربردی:

اگر در خودآزمایی‌ها از گواهی‌نامه‌ها استفاده شود (مثلاً برای تائید امضا جهت تائید 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)» تائید گردند. علاوه بر این، «خودآزمایی محصول مورد ارزیابی۲» باید در سند هدف امنیتی در نظر گرفته شوند.

۳-۵-۲ به‌روزرسانی امن

عدم موفقیت سرپرست محصول در تائید 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.

تعدادی الزام مبتنی بر انتخاب برای این خانواده در پیوست دو ارائه شده‌اند.

شماره الزام	نام الزام
۳۳	**به‌روزرسانی امن ۱**
محصول مورد ارزیابی باید این امکان را به سرپرستان امنیتی محصول بدهد که به نسخه فعلی نرم‌افزار/میان‌افزار محصول و [انتخاب: جدیدترین نسخه نصب‌شده نرم‌افزار/میان‌افزار محصول، هیچ نسخه دیگری از نرم‌افزار/میان‌افزار محصول] دسترسی داشته باشد. **نکته کاربردی:** اگر امکان نصب یک به‌روزرسانی مورد اعتماد که همان لحظه فعال نمی‌گردد یعنی فعال‌سازی آن دارای تأخیر می‌باشد، در محصول وجود داشته باشد، آنگاه باید هر دو نسخه محصول: نسخه مورد استفاده و نسخه نصب شده (به صورت تصویری از غیرفعال بودن آن) فراهم گردد. در این گونه موارد، گزینه " جدیدترین نسخه نصب‌شده نرم‌افزار/میان‌افزار محصول " در انتخاب این الزام، باید منتخب گردد و همچنین در خلاصه مشخصات محصول باید مشخص گردد که چگونه و چه زمانی نسخه غیرفعال، فعال می‌گردد. اگر تمامی به‌روزرسانی‌ها هم‌زمان با نصب فعال می‌گردند، آنگاه فقط نسخه فعلی در حال اجرای محصول باید فراهم گردد و گزینه " هیچ نسخه دیگری از نرم‌افزار/میان‌افزار محصول " برای انتخاب این الزام برگزیده خواهد شد. برای محصولات توزیع‌شده، نحوه تصمیم‌گیری در رابطه با نسخه‌های نصب شده روی هر مؤلفه در سند راهنمای عملیاتی توضیح داده شده است.	
۳۴	**به‌روزرسانی امن ۲**
محصول مورد ارزیابی باید این امکان را برای سرپرستان امنیتی محصول فراهم کند که به‌روزرسانی نرم‌افزار/میان‌افزار 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].	

شماره الزام	نام الزام

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

نکته کاربردی:

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.

خلاصه مشخصات محصول باید بیان کند که چه اقداماتی برای پشتیبانی محصول از گزینه‌های "از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند" یا "از به‌روزرسانی‌های خودکار پشتیبانی کند" در قسمت "انتخاب" این الزام، دخیل هستند.

وقتی که برای حفاظت از مکانیسم به‌روزرسانی مورداعتماد، مقادیر هش‌شده منتشر شده است، محصول نباید به صورت خودکار فایل(ها) به‌روزرسانی به همراه مقدار هش را (ممکن است همراه فایل یا به صورت جدا از فایل باشد) دانلود کند و به صورت خودکار بدون هیچ‌گونه مجوز فعال[۱] از سرپرست امنیتی نصب کند، حتی برای مواردی که مقادیر محاسبه شده هش با مقادیر منتشر شده منطبق باشد. در این مورد نباید گزینه "از به‌روزرسانی‌های خودکار پشتیبانی کند" استفاده گردد (بررسی خودکار برای وجود به‌روزرسانی مانعی ندارد). در این گونه موارد باید همیشه یک مجوز فعال از سرپرست امنیتی وجود داشته باشد و گزینه "به‌روزرسانی دستی" باید انتخاب گردد، اگرچه ممکن است فایل(ها) به طور خودکار دانلود شده باشند.

به‌روزرسانی‌های کاملاً خودکار فقط باید در حالتی که از مکانیسم امضاء دیجیتال استفاده شده باشد، انتخاب گردد.

۳۵	به‌روزرسانی 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 به‌روزرسانی ۴» و «الزامات به‌روزرسانی ۵» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه کند.

[۱] active authorization

شماره الزام	نام الزام

نکته کاربردی:

مکانیسم امضاء 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 در 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، هر دو مکانیسم نیز می‌تواند مورد استفاده قرار گیرد.

وقتی که از مقادیر هش منتشر شده برای امن کردن مکانیسم به‌روزرسانی مورداعتماد استفاده می‌شود، یک "مجوز فعال" برای فرآیند به‌روزرسانی، از طرف سرپرست امنیتی نیاز است. به علاوه، مخابره امن مقدار هش موثق[۱] از توسعه‌دهنده/تولیدکننده محصول به سرپرست امنیتی، یکی از فاکتورهای کلیدی برای حفاظت از مکانیسم به‌روزرسانی مورداعتماد است و سند راهنما باید چگونگی انجام این انتقال/مخابره را توضیح دهد. برای تصدیق[۲] مقدار هش مورداعتماد توسط سرپرست امنیتی، چندین روش امکان‌پذیر می‌باشد. سرپرست امنیتی می‌تواند مقدار هش را مانند فایل(ها) به‌روزرسانی به دست آورد و در حالی که هش کردن فایل(ها) در درون محصول در حال انجام است، تصدیق هش را خارج از محصول انجام دهد.

وقتی تصدیق هش موفق باشد، محصول می‌تواند بدون هیچ گام اضافه دیگری از طرف سرپرست امنیتی، به‌روزرسانی را انجام دهد. احراز هویت شدن به عنوان سرپرست امنیتی و فرستادن مقدار هش به محصول معادل با "مجوز فعال" برای به‌روزرسانی امن، در نظر گرفته می‌شود (وقتی تصدیق هش با موفقیت انجام شود)، زیرا انتظار می‌رود وقتی که به‌روزرسانی مدنظر باشد، سرپرست مقدار هش را روی محصول بارگذاری کند.

اگر مکانیسم امضاء دیجیتال انتخاب گردد، تصدیق امضاء به‌وسیله خود محصول انجام می‌گیرد. برای مکانیسم هش منتشرشده، تصدیق هم به‌وسیله سرپرست امنیتی و هم محصول قابل انجام است.

برای محصولات توزیع شده، همه مؤلفه‌ها باید از به‌روزرسانی امن پشتیبانی کنند. تصدیق امضاء یا هش به‌روزرسانی، باید به‌وسیله هر مؤلفه محصول (تصدیق امضاء) یا برای هر مؤلفه محصول (تصدیق هش) انجام گیرد.

نکته کاربردی:

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

نکته کاربردی:

[۱] Authentic hash value
[۲] Verification

شماره الزام	نام الزام
	اگر در مکانیسم تائید به‌روزرسانی از گواهی‌نامه‌ها استفاده شود، این گواهی‌ها باید از «الزامات پروتکل X509 (۳)» انتخاب شده و بر اساس «الزامات پروتکل X509» تائید گردند. علاوه بر این، «خودآزمایی محصول مورد ارزیابی۲» باید در سند هدف امنیتی در نظر گرفته شود. **نکته کاربردی:** 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 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 تائید 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 تائید از طریق مقایسه کلیدهای عمومی) یا امضاشده توسط کلیدهای امضای معتبر را تائید کند (مثلاً تائید گواهی‌نامه‌ها در صورت استفاده از گواهی‌نامه‌های X.509).
۳۶	**مهرهای زمانی ۱**
	توابع امنیتی مورد ارزیابی باید قابلیت ارائه مهرهای زمانی معتبر را برای استفاده خود داشته باشد.
۳۷	**مهرهای زمانی ۲**
	توابع امنیتی هدف ارزیابی باید [انتخاب: به مدیر امنیتی اجازه تنظیم زمان بدهد، زمان را با یک سرور NTP هماهنگ کند] **نکته کاربردی:** مهرهای زمانی قابل‌اطمینان جهت استفاده با دیگر توابع امنیتی محصول، مورد نظر می‌باشند؛ به عنوان مثال، برای تولید داده ممیزی جهت اجازه دادن به سرپرست امنیتی که بتواند با بررسی کردن ترتیب رویدادها، وقایع را بازنگری کند و زمان واقعی که وقایع رخ داده است را تعیین نماید. تصمیم در مورد سطح دقت اطلاعات (از لحاظ میزان دقیق بودن زمان رویدادها) به عهده سرپرست می‌باشد. محصول به اطلاعات خارجی زمان و تاریخ وابسته است، این اطلاعات می‌تواند به صورت دستی توسط سرپرست امنیتی تهیه گردند

[۱] Firmware

شماره الزام	نام الزام

یا به وسیله استفاده از یک یا چند منبع خارجی مانند سرور NTP به دست آورده شوند. بنابراین گزینه مناسب در "انتخاب" این الزام باید برگزیده شود. استفاده از یک ساعت بلادرنگ محلی با قابلیت همگام‌سازی خودکار با یک منبع خارجی (مثلاً؛ سرور NTP) توصیه می‌گردد، ولی الزام نمی‌باشد. همچنین برای ارتباط با یک منبع خارجی، استفاده از الزام FTP_ITC.1 اختیاری می‌باشد ولی نویسنده سند هدف امنیتی باید مشخص سازد که چگونه اطلاعات زمان و تاریخ به‌وسیله محصول دریافت و نگهداری می‌گردد.

عبارت «مهرهای زمانی قابل‌اطمینان» به استفاده محدود از اطلاعات زمانی و تاریخی (که توسط موجودیت‌های خارجی ارائه شده‌اند) و تمام تغییرات ناپیوسته ثبت‌شده در تنظیمات زمانی (شامل اطلاعات مربوط به زمان قدیم و جدید) اشاره دارد. با استفاده از این اطلاعات، می‌توان زمان واقعی تمام داده ممیزی را محاسبه کرد.

توجه شود که تمامی تغییرات ناپیوسته زمان؛ به‌وسیله سرپرست یا به صورت خودکار توسط فرآیند، باید ممیزی گردد. اگر زمان به‌وسیله هسته یا خود سیستم تغییر کند، نیاز به ممیزی نمی‌باشد، این تغییرات دیگر در حوزه تغییرات ناپیوسته زمان، قرار نمی‌گیرند.

۳-۶ دسترسی به محصول

این بخش به تشریح الزامات امنیتی مربوط به نشست‌های سرپرست محصول مورد ارزیابی می‌پردازد. هم نشست‌های محلی و هم نشست‌های راه‌دور پایش می‌شوند تا در صورت غیرفعال بودن شناسایی شوند و قفل شدن یا خاتمه یافتن آن‌ها نیز در صورت رسیدن به آستانه زمانی بررسی می‌شود. سرپرستان باید قادر باشند نشست‌های تعاملی خود را خاتمه دهند. در ابتدای هر نشست باید یک اطلاعیه مشاوره‌ای برای آن‌ها نمایش داده شود.

شماره الزام	نام الزام
۳۸	**قفل‌کردن و خاتمه دادن به نشست‌ها ۷**

در مورد نشست‌های تعاملی محلی[۱]، محصول مورد ارزیابی باید پس از اتمام زمان غیرفعال 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 غیرفعال کند و از سرپرست محصول بخواهد که پیش از قفل‌گشایی نشست، مجدداً احراز هویت نماید؛
- نشست را خاتمه دهد].

[۱] Local interactive sessions

شماره الزام	نام الزام
۳۹	**قفل‌کردن و خاتمه دادن به نشست‌ها ۵**
در مورد نشست‌های تعاملی راه‌دور[۱]، 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.	
۴۰	**قفل‌کردن و خاتمه دادن به نشست‌ها ۶**
محصول مورد ارزیابی باید به سرپرست محصول اجازه دهد که نشست تعاملی خود را خاتمه دهد.	
۴۱	**پیغام‌های هشدار در رابطه با استفاده محصول ۱**
قبل از ایجاد یک نشست کاربری سرپرست اجرایی[۲]، محصول مورد ارزیابی باید توصیه‌های مشخص شده توسط سرپرست امنیتی و همچنین تأییدیه استفاده از محصول مورد ارزیابی را نشان دهد. **نکته کاربردی:** این الزام در مورد نشست‌های تعاملی بین یک کاربر انسانی و یک محصول مورد ارزیابی اعمال می‌شود. موجودیت‌های IT که اتصالاتی مانند تماس‌های راه‌دور از طریق شبکه را برقرار می‌کنند، نیازی به رعایت این الزام نخواهند داشت.	

۳-۷ کلاس کانال‌ها/مسیرهای مورداعتماد

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 پنج پروتکل استاندارد ایجاد می‌شوند: IPsec, TLS, HTTPS , DTLS 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.

---

[۱] Remote

[۲] Administrative user

شماره الزام	نام الزام
۴۲	**کانال امن ۱**
محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [انتخاب: IPsec, SSH, TLS, DTLS, HTTPS] میان خود و دیگر موجودیت‌های IT معتبر همچون سرور ممیزی، [انتخاب: سرور احراز هویت، اختصاص: [دیگر قابلیت‌ها]، هیچ قابلیت‌های دیگری] که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آن‌ها را احراز هویت 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، DTLS،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.**	
۴۳	**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.	
۴۴	**کانال امن ۳**
محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای [اختصاص: لیست سرویس‌های که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباطات را آغاز کند] راه‌اندازی نماید. **نکته کاربردی:** هدف از الزام حاضر فراهم کردن روشی است که جهت حفاظت ارتباطات خارجی با موجودیت‌های معتبر IT، از پروتکل رمزنگاری استفاده گردد. منظور از 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 ذکر شده در الزام «کانال امن ۱» 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 دومین "انتخاب" الزام «کانال امن ۱» انتخاب کند. این اتصال باید توسط یکی از پروتکل‌های ذکر شده حفاظت گردد. اگر سایر موجودیت‌های معتبر IT 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 در پیوست دو متناظر با انتخاب وی، در هدف امنیتی گنجانده شده‌اند. هر چند که هیچ الزامی در مورد طرف آغازکننده ارتباط وجود ندارد، نویسنده هدف امنیتی در عبارت اختصاص این الزام، سرویس‌های که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباط با موجودیت IT معتبر آغاز کند را لیست می‌نماید.	

شماره الزام	نام الزام
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.	
۴۵	**مسیر امن ۱**
توابع امنیتی هدف ارزیابی، باید قادر باشد مسیر ارتباطی بین خود و مدیران از راه دور مجاز که به طور منطقی از مسیرهای ارتباطی دیگر متمایز است را با استفاده از [انتخاب: IPsec، SSH، DTLS، TLS، HTTPS] فراهم نماید و نقاط پایانی را به صورت مطمئن شناسایی کرده و از داده‌های ارتباطی در برابر افشاء محافظت نموده و تغییرات داده‌های کانال را تشخیص دهد. **تذکر: در صورتی که هر یک از پروتکل‌های HTTPS،TLS،DTLS،SSH،IPsec 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.**	
۴۶	**مسیر امن ۲**
محصول مورد ارزیابی باید به سرپرست‌های راه‌دور محصول اجازه دهد که ارتباطات را از طریق کانال امن آغاز کند.	
۴۷	**مسیر امن ۳**
محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه سرپرست محصول و تمام فعالیت‌های راه‌دور سرپرستی الزامی کند. **نکته کاربردی:** این الزام اطمینان حاصل می‌نماید که سرپرست‌های راه‌دور مجاز، تمام ارتباطات با محصول مورد ارزیابی را، 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 سند 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.	

۳-۸ کلاس مدیریت رویدادها

در این بخش الزامات مربوط به کارکرد امنیتی محصول SIEM بیان می‌شود. این الزامات مربوط به عملیات یک SIEM شامل تجزیه و تحلیل و واکنش تحلیلگراست. علاوه بر این بازبینی و دسترس‌پذیری لاگ های خام،رویدادها و هشدارهای تحلیل شده نیز به عنوان دیگر کارکردهای امنیتی بررسی خواهند شد.

شماره الزام	نام الزام
۴۸	**تجزیه‌وتحلیل تحلیل‌گر ۱**
محصول باید عملکرد تجزیه‌وتحلیل همبستگی و فیلترینگ را بر روی تمام داده‌های دریافت شده اجرا نماید.	
۴۹	**تجزیه‌وتحلیل تحلیل‌گر ۲**
محصول باید عملکرد تجزیه‌وتحلیل زیر را بر روی تمام داده‌های دریافت شده‌ی SIEM، اجرا کند: • [انتخاب: تحلیل‌های آماری، تطابق با امضا] و[اختصاص: دیگر عملکردهای تحلیلی]	
۵۰	**تجزیه‌وتحلیل تحلیل‌گر ۳**
محصول باید در درون هر یک از داده SIEM جمع‌آوری‌شده حداقل اطلاعات زیر را ثبت نماید: • زمان و تاریخ نتیجه، نوع نتیجه، شناسایی منبع داده • [اختصاص: سایر اطلاعات مرتبط امنیتی در مورد نتیجه] **نکته کاربردی SIEM 1:** نتایج تحلیلی به‌دست‌آمده توسط تحلیل‌گر، باید هم نتایج را توصیف نماید و هم‌چنین تعیین نماید بر اساس چه اطلاعاتی به این نتایج رسیده است.	
۵۱	**واکنش تحلیل‌گر ۱**
محصول باید در زمان تشخیص هر هشدار یا حادثه [اختصاص: اقدامات مناسب] را برای [اختصاص: مقصد هشدار] انجام دهد.	
۵۲	**بازبینی داده‌های محدودشده ۱ (۱)**
محصول باید [اختصاص: کاربرانی مجاز] باقابلیت خواندن [اختصاص: فهرستی از داده‌های جمع‌آوری‌شده‌ی SIEM] از داده‌های دریافت شده‌ی SIEM فراهم نماید.	

شماره الزام	نام الزام
نکته کاربردی: این الزام به کاربران مجاز سیستم اعمال می‌گردد. الزام برای نویسنده هدف امنیتی باز گذاشته‌شده است تا تعریف نماید که چه کاربران مجازی ممکن است به داده‌های سیستم دستیابی داشته باشند.	
۵۳	**بازبینی داده‌های محدودشده ۱ (۲)**
توابع امنیتی هدف ارزیابی باید [اختصاص: کاربرانی مجاز] باقابلیت خواندن [اختصاص: فهرستی از داده‌های تحلیل‌گر] از داده‌های تحلیل‌گر فراهم نماید.	
۵۴	**بازبینی داده‌های محدودشده ۲**
محصول باید داده‌های جمع‌آوری‌شده‌ی SIEM را به شیوه‌ای مناسب ارائه نماید تا کاربر بتواند اطلاعات را تفسیر کند.	
۵۵	**بازبینی داده‌های محدودشده ۳**
محصول باید دسترسی خواندن[۱] داده‌های جمع‌آوری‌شده‌ی SIEM را برای تمام کاربران، به‌جز آن دسته از کاربرانی که مجوز دسترسی خواندن به آن‌ها اعطاشده، منع نماید.	
۵۶	**تضمین در دسترس بودن داده‌های سیستم-حذف ۱ (۱)**
محصول باید از حذف غیرمجاز داده‌های جمع‌آوری‌شده و ذخیره‌شده‌ی SIEM، محافظت نماید.	
۵۷	**تضمین در دسترس بودن داده‌های سیستم-حذف ۱ (۲)**
محصول باید از حذف غیرمجاز داده‌های ذخیره‌شده‌ی تحلیل‌گر، محافظت نماید.	
۵۸	**تضمین در دسترس بودن داده‌های سیستم-تغییر ۱ (۱)**
محصول باید از تغییر غیرمجاز داده‌های جمع‌آوری‌شده و ذخیره‌شده‌ی SIEM، محافظت نماید.	
۵۹	**تضمین در دسترس بودن داده‌های سیستم-تغییر ۱ (۲)**
محصول باید از تغییر غیرمجاز داده‌های ذخیره‌شده‌ی تحلیل‌گر، محافظت نماید.	
۶۰	**تضمین در دسترس بودن داده‌های سیستم ۲**
محصول باید درصورتی‌که ظرفیت ذخیره‌سازی به حد پر شدن رسید [انتخاب: *اقدام به‌صرف‌نظر نمودن از داده‌های جمع‌آوری‌شده‌ی SIEM نماید، از ذخیره‌سازی داده‌های جمع‌آوری‌شده‌ی SIEM به‌جز داده‌هایی که توسط کاربر مجاز تعیین می*	

[۱] Read Access

شماره الزام	نام الزام
شوند جلوگیری نماید ، یا اقدام به بازنویسی بر روی قدیمی‌ترین داده‌های جمع‌آوری‌شده‌ی SIEM ذخیره‌شده نماید] و یک هشدار ارسال نماید. **نکته کاربردی:** در سند هدف امنیتی باید مشخص گردد که محصول درزمانی که ظرفیت ذخیره‌سازی به حد پر شدن رسید، چه اقداماتی انجام می‌دهد. هر چیزی که سبب متوقف شدن جمع‌آوری استاتیک اطلاعات گردد، راه‌حل خوبی نیست	

۹-۳ الزامات کارکرد امنیتی برای پیاده‌سازی ارتباطات سلسله مراتبی

الزامات زیر در ارتباطات سلسله مراتبی برای داده‌های کاربری کاربرد دارد. داده‌های کاربری اطلاعاتی هستند که در منابع محصول ذخیره‌شده‌اند و بر اساس الزامات کارکرد امنیتی توسط کاربران به‌کاربرده شوند. رویدادها یا بسته‌های یک شبکه نمونه‌هایی از داده‌های کاربری می‌باشند.

شماره الزام	نام الزام
۶۱	**خروج داده‌های کاربری از محصول ۱**
محصول باید در زمان صدور داده‌ی کاربری تحت کنترل خط‌مشی‌های کارکرد امنیتی به خارج از محصول[اختصاص: خط‌مشی‌های کارکرد امنیتی کنترل دسترسی و/یا خط‌مشی‌های کارکرد امنیتی کنترل جریان اطلاعات] را اجرا نماید.	
۶۲	**خروج داده‌های کاربری از محصول ۲**
محصول باید اطمینان دهد که مشخصه‌های امنیتی زمانی که به خارج از محصول صادر می‌شود به‌صورت صریحی به داده‌های کاربری صادرشده، مرتبط شده‌اند.	
۶۳	**خروج داده‌های کاربری از محصول ۳**
محصول باید اطمینان دهد که مشخصه‌های امنیتی زمانی که به خارج از محصول صادر می‌شود به‌صورت صریحی به داده‌های کاربری صادرشده، مرتبط شده‌اند.	
۶۴	**خروج داده‌های کاربری از محصول ۴**
محصول باید ملزم نماید که قوانین زیر در زمان صدور داده از محصول اجرا گردند: [اختصاص: قوانین کنترل صدور]	
۶۵	**ورود داده‌های کاربری به محصول ۱**

محصول باید[اختصاص: خط‌مشی کارکرد امنیتی کنترل دسترسی و یا خط‌مشی کارکرد امنیتی کنترل جریان اطلاعات] در زمان ورود داده‌ی کاربری تحت کنترل خط‌مشی از خارج به محصول اعمال نماید.	
ورود داده‌های کاربری به محصول ۲	**۶۶**
محصول باید از مشخصه‌های امنیتی همراه با داده‌های کاربری ورودی استفاده نماید.	
ورود داده‌های کاربری به محصول ۳	**۶۷**
محصول باید قوانین زیر را در زمان ورود داده کاربری تحت کنترل خط‌مشی کارکرد امنیتی از خارج محصول اجرا نماید: [اختصاص: قوانین کنترل ورودی]	

۴ 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	برچسب‌گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

۴-۱ کلاس توسعه

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

۴-۱-۱ 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.

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده‌سازی (AGD_PRE) و اطلاعاتی که در 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.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1C)** **شرح مؤلفه:**

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

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1E)** **شرح مؤلفه:**

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

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.2E)** **شرح مؤلفه:** 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»، «تست» و «آسیب‌پذیری» ارائه شده است.

۴-۲ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل 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 ارائه‌دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو می‌باشد.

۴-۲-۱ راهنمای کاربردی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی	**نام عنصر: راهنمای کاربردی ۱**

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
(AGD_OPE)	**شماره مؤلفه: (AGD_OPE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** 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 مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** 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 مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های در دسترس، 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 مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.5C)** **شرح مؤلفه:** 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 مؤلفه: (AGD_OPE.1.6C)** **شرح مؤلفه:** 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 مؤلفه: (AGD_OPE.1.7C)** **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	ارزیاب باید تائید نماید که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۴-۲-۲راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای آماده-سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه‌دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2C)** **شرح مؤلفه:** 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.

مؤلفه‌های اقدامات ارزیاب	
راهنمای آماده-سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2E)** **شرح مؤلفه:** 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.

۴-۳ کلاس تست

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

۴-۳-۱ تست مستقل

«تست 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 تست اطمینان از برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی می‌باشد. ارزیاب باید در سند «گزارش تست»، طرح تست و نتایج آن را مستند نماید.

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل	**نام عنصر: آزمون مستقل ۱**

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
(ATE_IND)	**شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.

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

مؤلفه‌های اقدامات ارزیاب	
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: تست مستقل ۱ **شماره مؤلفه: (ATE_IND.1.2E)** **شرح مؤلفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را تست نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل می‌نمایند.

۴-۴ کلاس آسیب‌پذیری

۴-۴-۱ تحلیل آسیب‌پذیری

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

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1C)** **شرح مؤلفه:** محصول باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.2E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.3E)** **شرح مؤلفه:** ارزیاب باید بر اساس 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.

۴-۵ کلاس پشتیبانی از چرخه حیات

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

۴-۵-۱ قابلیت‌های پیکربندی

این مؤلفه جهت معرفی محصول به صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه شده، می‌باشد (بدین معنی که جدا از برچسب‌گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب‌گذاری 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.

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید محصول و مرجع محصول را ارائه نماید.

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

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

۴-۵-۲حوزه پیکربندی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1D)** **شرح مؤلفه:** ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:**

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

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

۵ 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).

اگر محصول هر کدام از الزامات اختیاری را انجام دهد، توصیه شده است که فروشنده محصول قابلیت‌های عملکردی مرتبط را به سند هدف امنیتی اضافه نماید. بنابراین در نکات کاربردی مطرح شده در ادامه، عبارت "این گزینه باید انتخاب گردد..." تکرار شده است. اما این عبارت همچنین برای تأکید کردن روی این موضوع است که الزام وقتی انتخاب می‌گردد که قابلیت‌های عملکردی مرتبط توسط محصول فراهم شده باشد و نیاز نمی‌باشد که جهت

انطباق با این پروفایل حفاظتی، محصول حتماً قابلیت‌های عملکردی را پیاده‌سازی نماید. نویسندگان سند هدف امنیتی آزاد هستند که؛ هیچ، برخی یا تمامی الزامات مطرح شده در این بخش را انتخاب نمایند. این واقعیت که محصول از یک قابلیت عملکردی مشخص پشتیبانی می‌نماید، به معنی اضافه کردن تمامی الزامات این بخش به سند هدف امنیتی نمی‌باشد.

۲-۵ 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 آنچه در «ذخیره‌سازی رویدادهای ممیزی» گفته شده است، از دست‌کاری غیرمجاز 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 ذخیره‌سازی داده‌های ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی» و «ذخیره‌سازی رویدادهای ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی» تهیه شده‌اند تا این قابلیت‌های اختیاری دستگاه‌های شبکه را بیان کنند.

همچنین جدول زیر مربوط به رویدادهای ممیزی الزامات اختیاری 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.	ذخیره‌سازی رویدادهای ممیزی ۱ و ۲		
۲.	محل ذخیره‌سازی داده‌های ممیزی ۳ / فضای ذخیره‌سازی ممیزی محلی		
۳.	ذخیره‌سازی رویدادهای ممیزی ۶/ فضای ذخیره‌سازی ممیزی محلی	کم بودن فضای ذخیره‌سازی برای رویدادهای ممیزی.	
۴.	الزامات پروتکل X509 (۱) و (۲)/ تبادل داده کاربردی داخل محصول	تلاش‌های ناموفق برای اعتبارسنجی یک گواهی‌نامه.	دلیل/دلایل شکست
۵.	مدیریت کارکرد در محصول ۱ (۱)/ سرویس‌ها	آغاز و توقف سرویس‌ها.	
۶.	مدیریت داده‌های محصول ۱/ کلیدهای رمزنگاری	مدیریت کلیدهای رمزنگاری.	

۷.	انتقال داده امنیتی در داخل محصول ۱	راه‌اندازی اولیه و خاتمه دادن به کانال مورداعتماد. شکست توابع کانال مورداعتماد.	شناسایی آغازکننده و هدفی که تلاش در برقراری کانال‌های مورداعتماد با آن/برای آن شکست خورده است
۸.	مسیر امن ۱، ۲ و ۳/ پیوند زدن	راه‌اندازی اولیه و خاتمه دادن به مسیر مورداعتماد. شکست توابع مسیر مورداعتماد.	
۹.		فعال‌سازی و غیر فعال‌سازی ارتباطات مابین یک جفت از مؤلفه‌ها.	هویت‌های جفت نقاط انتهایی[۱] فعال یا غیرفعال شده

نکته کاربردی:

رویداد ممیزی «الزامات پروتکل X509 (۱) و (۲)/ تبادل داده کاربردی داخل محصول» در صورتی رخ می‌دهد که محصول مورد ارزیابی نتواند از موارد زیر اطمینان حاصل نماید و گواهی‌نامه‌ها را تائید کند:

- وجود افزونه basicConstraints و تائید اینکه پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم‌شده است
- تائید امضای دیجیتال CA سلسله مراتبی مورداعتماد
- 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.

[۱] Endpoints pairs

شماره الزام	نام الزام	
۶۸	**ذخیره‌سازی داده‌های ممیزی محافظت شده ۱**	FAU_STG.1.1
توابع امنیتی مورد ارزیابی باید از پاک شدن غیرمجاز داده‌های ممیزی ذخیره شده در دنباله ممیزی محافظت نماید.		
۶۹	**ذخیره‌سازی داده‌های ممیزی محافظت شده ۲**	FAU_STG.1.2
توابع امنیتی مورد ارزیابی باید قادر باشد از تغییرات غیرمجاز داده‌های ممیزی ذخیره شده در دنباله ممیزی جلوگیری نماید.		
۷۰	**شمارش داده‌های ممیزی از دست رفته**	FAU_STG_EXT.2.1/LocSpace
محصول 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 یکی از اقدامات تعیین‌شده در «محل ذخیره‌سازی داده‌های ممیزی ۳[۱]» را انجام می‌دهد. **نکته کاربردی:** این گزینه در صورتی باید انتخاب شود که هدف مورد ارزیابی از این کارکرد پشتیبانی کند. درصورتی‌که حافظه محلی داده‌های ممیزی توسط سرپرست محصول خالی شود، شمارنده‌های مربوط به انتخاب انجام شده 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. برای اهداف ارزیابی توزیع شده، هر کامپوننتی که شمارش داده‌های ممیزی از دست رفته را پیاده‌سازی کرده است، باید مکانیسم دسترسی و مدیریت این اطلاعات برای مدیر را فراهم نماید. اگر این الزام به سند هدف امنیتی اضافه شود، سند هدف امنیتی باید هر وضعیتی که داده ممیزی از دست رفته شمارش نمی‌شود را مشخص نماید.		
۷۱	**نمایش هشدار برای فضای ذخیره‌سازی محلی**	FAU_STG.3.1/LocSpace

[۱] FAU_STG_EXT.1.3

توابع امنیتی هدف ارزیابی باید در صورتی که دنباله ممیزی بیش از ظرفیت ذخیره‌سازی دنباله ممیزی باشد، برای اطلاع‌رسانی به مدیر هشداری ایجاد نماید.

نکته کاربردی:

درصورتی‌که هدف ارزیابی امکان تولید پیام مربوطه را داشته باشد این گزینه انتخاب می‌شود. درصورتی‌که داده‌های مربوط به رویدادهای قابل ممیزی 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 ذخیره‌سازی داده‌های ممیزی ۳» را می‌توان به اطلاع مدیر 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.

پیام هشدار باید هنگامی که فضای محلی برای ذخیره داده ممیزی در حال پر شدن بود و/یا ممکن باشد هدف ارزیابی به علت فضای محلی ناکافی داده‌های ممیزی را از دست بدهد، مدیر را مطلع نماید.

برای اهداف ارزیابی توزیع شده‌ای که در زمان پر شدن فضای حافظه محلی داده ممیزی هشداری نمایش می‌دهند، باید مشخص شود که کدام مؤلفه‌های هدف ارزیابی از این ویژگی پشتیبانی می‌کنند (اگر به عنوان هدف ارزیابی کلی انتخاب شده باشد، پشتیبانی تمامی مؤلفه‌های هدف ارزیابی از این ویژگی الزامی نیست.). هر مؤلفه‌ای که از این ویژگی پشتیبانی می‌کند باید هشداری را خودش یا از طریق مؤلفه دیگری تولید کند.

اگر FAU_STG.3/LocSpace به سند هدف امنیتی اضافه شده باشد، سند هدف امنیتی باید هر حالتی که ممکن است سوابق ممیزی "به طور مخفی از دست روند" را مشخص نماید.

۵-۳ کلاس شناسایی و احراز هویت

شماره الزام	نام الزام	
۷۲	تائید گواهینامه X509 (۱)	FIA_X509_EXT.1.1/ITT

توابع امنیتی مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تائید کند:

- تائید گواهی‌نامه RFC 5280 و تائید مسیر گواهی‌نامه با پشتیبانی از حداقل طول مسیر دو گواهی‌نامه
- مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد
- توابع امنیتی مورد ارزیابی باید برای تائید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است.
- توابع امنیتی مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) چنان که در RFC 6960 تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در RFC 5759 بخش ۵ تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در RFC5280 بخش ۶,۳ تعریف شده است، هیچ روش فسخی] تائید کند
- توابع امنیتی مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تائید کند:
  - 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.
  - گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف "Client Authentication" (id-kp2 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.
  - گواهی‌نامه‌های OCSP ارائه شده 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.

نکته کاربردی:

این الزام باید زمانی انتخاب شود که هدف ارزیابی توزیع شده باشد و پروتکل‌های انتخاب شده در FPT_ITT.1 از گواهینامه‌های X509 برای احراز هویت دوطرفه استفاده نمایند. در این مورد، به دلیل وجود الزامات اضافی شامل فعال‌سازی و غیرفعال سازی کانال ITT در FCO_CPC_EXT.1، استفاده از چک لیست فسخ اختیاری می‌باشد. اگر بررسی فسخ پشتیبانی نشده باشد، نویسنده هدف امنیتی نباید هیچ روش فسخ را انتخاب کند. هرچند، اگر بررسی فسخ گواهینامه پشتیبانی شده باشد، نویسنده هدف امنیتی باید استفاده از OCSP یا CRLها را انتخاب کند.

هدف ارزیابی باید قادر به پشتیبانی از حداقل طول مسیر دو گواهینامه باشد. به این معنی که، باید از سلسله مراتب گواهینامه شامل حداقل یک گواهینامه اصلی امضا شده توسط خودش و یک گواهینامه شناسایی هدف ارزیابی را پشتیبانی کند.

TSS باید زمان اجرا شدن بررسی لغو را شرح دهد. انتظار می‌رود زمانی که یک گواهینامه در مرحله احراز هویت استفاده می‌شود، بررسی فسخ انجام شود. تائید وضعیت گواهینامه X509 فقط زمانی که در دستگاه بارگذاری می‌شود، کافی نیست.

در صورتی که هدف ارزیابی از عملکردهایی پشتیبانی کند که از هیچ‌کدام از انواع گواهینامه‌های لیست شده در قوانین extendedKeyUsage در FIA_X509_EXT.1.1 پشتیبانی نکند، باید در TSS تعیین شود و بخش مربوط به SFR به طور کلی

عملکردهای مورد پذیرش را در نظر می‌گیرد. هر چند، اگر هدف ارزیابی از عملکردهایی پشتیبانی کند که از هرکدام از انواع این گواهینامه‌ها استفاده می‌کند، باید قوانین متناظر همانند SFR رعایت شوند.		
۷۳	**تائید گواهینامه X509 (۲)**	FIA_X509_EXT.1.2/ITT
توابع امنیتی 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:** 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.		

۴-۵ کلاس مدیریت امنیت

۷۴	**مدیریت رفتار توابع امنیتی/خدمات ۱**	FMT_MOF.1.1/Services
توابع امنیتی هدف ارزیابی باید قابلیت شروع و متوقف کردن سرویس‌ها را به سرپرست امنیتی محدود سازد.		
۷۵	**مدیریت رفتار توابع امنیتی/کلیدهای رمزنگاری ۱**	FMT_MTD.1.1/CryptoKeys
توابع امنیتی هدف ارزیابی باید توانایی مدیریت کلیدهای رمزنگاری را به سرپرست امنیتی محدود کند.		

۵-۵ کلاس حفاظت از محصول مورد ارزیابی

شماره الزام	نام الزام	
۷۶	**حفاظت از انتقال داخلی داده‌های اساسی محصول**	FPT_ITT.1.1
محصول باید از افشای داده‌های محصول محافظت نموده و زمانی که با استفاده از [انتخاب: IPsec، SSH، TLS، DTLS، HTTPS] بین بخش‌های جداگانه هدف ارزیابی فرستاده شود، تغییرات را تشخیص دهد. **نکته کاربردی:** این الزام فقط برای اهداف ارزیابی توزیع شده و اطمینان از این که تمامی ارتباطات بین مؤلفه‌های هدف ارزیابی توزیع شده از طریق استفاده از کانال ارتباطی رمز شده محافظت می‌شوند، تکرار شده است. داده‌های ارسال شده در این کانال ارتباطی امن توسط پروتکل انتخاب شده رمز می‌شوند. نویسنده هدف امنیتی باید کانال‌ها و پروتکل‌های استفاده شده توسط هر جفت مؤلفه ارتباطی در هدف ارزیابی توزیع شده را، مناسب با تکرار این الزام، مشخص نماید. همچنین این کانال ممکن است به عنوان کانال ثبت برای فرآیند ثبت، همان طور که در بخش ۳,۳ و FCO_CPC_EXT.1.2 شرح داده شده است، استفاده شود. اگر TLS انتخاب شود، الزامات داشتن شناسه مرجع پیاده‌سازی شده توسط کاربر (FCS_TLSC_EXT.1.2)، برقرار شده است و شناسه ممکن است توسط فرآیند کشف "Gatekeeper" ایجاد شود. TSS باید فرآیند کشف را شرح داده و نحوه تأمین مؤلفه "joining" برای شناسه مرجع مشخص شود.		
۷۷	**مسیر امن ۱/** Join	FTP_TRP.1.1/Join
محصول باید یک مسیر ارتباطی بین خود و یکی از مؤلفه‌های متصل که به طور منطقی از سایر مسیرهای ارتباطی متمایز است برقرار نماید و شناسایی مطمئنی از [انتخاب: نقطه پایانی محصول، مؤلفه متصل و نقطه پایانی محصول] ارائه دهد و از تغییر [انتخاب: و افشای، هیچ] داده‌های تبادل شده محافظت نماید.		
۷۸	**مسیر امن ۲/** Join	FTP_TRP.1.2/Join
محصول باید به [انتخاب: محصول، کاربران محلی مؤلفه متصل، کاربران راه دور] اجازه آغاز ارتباط توسط مسیر امن را بدهد.		
۷۹	**مسیر امن ۳/** Join	FTP_TRP.1.3/Join

محصول باید برای اتصال مؤلفه‌ها به محصول تحت محدودیت‌های محیطی مشخص شده در مرجع راهنمای عملیاتی، از مسیر امن استفاده کند.

نکته کاربردی:

این الزام یکی از انواع شناسایی کانال در انتخاب اصلی الزام FCO_CPC_EXT.1.2 را برقرار می‌کند. در FTP_TRP.1.1/Join، "مؤلفه joining"، موجودیت IT است که برای پیوستن به هدف ارزیابی توزیع شده توسط فرآیند ثبت تلاش می‌کند.

این الزام نیازمند توانایی مؤلفه‌ها برای برقراری ارتباط امن در طول ایجاد محصول توزیع شده (یا زمانی که مؤلفه‌ای به محصول توزیع شده موجود اضافه می‌شود) می‌باشد. در این الزام، زمانی که محصول از جفت مؤلفه‌های اولیه ایجاد می‌شوند، ممکن است هرکدام از این مؤلفه‌ها به عنوان محصول شناسایی شوند.

انتخاب موجود در انتهای FTP_TRP.1.1/Join تشخیص می‌دهد که در برخی موارد ممکن است محرمانگی توسط کانال ارائه نشود (به عنوان مثال، حفاظت از افشای داده‌ها). در این مورد، نویسنده هدف امنیتی باید در TSS، هدف ارزیابی مربوط به محیط برای ارائه محرمانگی را (به عنوان بخشی از محدودیت‌های اشاره شده در FTP_TRP.1.3/Join) مشخص نماید یا تعیین کند که ثبت داده تبادل شده نیازمند محرمانگی نمی‌باشد (در کدام مورد این ادعا صدق می‌کند). اگر "هیچ" انتخاب شود، ممکن است در سند هدف امنیتی برای بهبود خوانایی این عبارت حذف شود.

اختصاص موجود در FTP_TRP.1.3/Join، اطمینان حاصل می‌کند که سند هدف امنیتی هر جزئیات خاص مورد نیاز برای محافظت از محیط ثبت را مشخص کرده است.

توجه داشته باشید زمانی که سند هدف امنیتی از FTP_TRP.1/Join برای کانال ثبت استفاده می‌کند، این کانال نمی‌تواند مجدداً به عنوان کانال ارتباطی طبیعی بین مؤلفه‌ای استفاده شود (کانال بعدی باید FTP_ITC.1 یا FPT_ITT.1 را رعایت کند).

الزامات خاص برای فرآیندهای مقدماتی مربوط به FTP_TRP.1/Join در فعالیت‌های ارزیابی در [SD] تعریف شده‌اند.

۵-۶ کلاس ارتباطات

شماره الزام	نام الزام
۸۰	**تعریف کانال ثبت‌نام مؤلفه ۱**
محصول باید از مدیر امنیتی درخواست فعال‌سازی ارتباطات بین هر جفت مؤلفه‌های هدف ارزیابی کند، قبل از این که چنین ارتباطی قابل انجام باشد.	
۸۱	**تعریف کانال ثبت‌نام مؤلفه ۲**
محصول باید فرآیند ثبتی که در آن مؤلفه‌ها ایجاد می‌شوند را پیاده‌سازی کند و برای حداقل داده‌های محصول از کانال ارتباطی استفاده کند که: [انتخاب:	

- کانالی که الزامات کانال امن را در [انتخاب: FTP_ITC.1، FPT_ITT.1] برآورده می‌کند.
- کانالی که الزامات کانال ثبت را در FTP_TRP.1/Join برآورده می‌کند.
- هیچ کانالی

]

۸۲	تعریف کانال ثبت‌نام مؤلفه ۳

محصول باید یک سرپرست امنیتی را فعال نماید که بتواند کانال ارتباطات میان هر جفت مؤلفه از محصول را غیرفعال نماید.

نکته کاربردی:

این الزام (FCO_CPC_EXT.1) فقط وقتی که محصول توزیع‌شده باشد و در نتیجه چند مؤلفه داشته باشد که نیاز به ارتباط از طریق کانال داخلی داشته باشند، قابل اعمال می‌باشد.

انتخاب کانال در الزام « تعریف کانال ثبت‌نام مؤلفه ۲» اساساً یک انتخاب است بین اینکه از یک کانال امن معمولی که معادل است با الف) کانالی که برای ارتباط با موجودیت‌های خارجی (FTP_ITC.1) یا مؤلفه‌های محصول (FPT_ITT.1) استفاده می‌شود، یا ب) کانالی که برای ثبت‌نام بکار می‌رود (FTP_TRP.1/Join)، استفاده شود. در صورتی که محصول به دلیل امکان اقدامات پیکربندی قابل انجام توسط سرپرست محصول، نیاز به کانال ثبت‌نام نداشته باشد، آنگاه گزینه "هیچ کانالی" برای انتخاب الزام « تعریف کانال ثبت‌نام مؤلفه ۲» برگزیده می‌شود.

اگر نویسنده سند هدف امنیتی، کانال FPT_ITT.1/FTP_ITC.1 را برگزیند، آنگاه سند خلاصه مشخصات محصول باید تکرارهایی از الزام را که برای مشخص کردن استفاده محصول لازم است، تشریح نماید. درصورتی که FTP_TRP.1/Join انتخاب گردد، سند خلاصه مشخصات محصول (در صورت امکان با کمک سند راهنمای عملیاتی) باید جزییات کانال و مکانیسم‌هایی را که استفاده می‌کند تشریح نماید.

اگر نویسنده سند هدف امنیتی، کانال FPT_ITT.1/FTP_ITC.1 را برگزیند، آنگاه در سند هدف امنیتی باید کانال ثبت‌نام به عنوان یکی از تکرارهای الزام FPT_ITT.1 یا FTP_ITC.1 با یک نام مشخص (مثال؛ FPT_ITT.1/Join)، در قالب نکته کاربردی به الزام «تعریف کانال ثبت‌نام مؤلفه ۱» اضافه و اجرا گردد.

۶ 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 زیر 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	لیست سوابق ممیزی اضافی
۱.	FCS_DTLSC_EXT.1	شکست در برقراری یک نشست DTLS	دلیل شکست
۲.	FCS_DTLSC_EXT.2	شکست در برقراری یک نشست DTLS	دلیل شکست
۳.	FCS_DTLSC_EXT.2	تشخیص حملات replay	هویت (به عنوان مثال، آدرس IP منبع) منبع حمله replay
۴.	FCS_DTLSS_EXT.1	شکست در برقراری یک نشست DTLS	دلیل شکست
۵.	FCS_DTLSS_EXT.1	تشخیص حملات replay	هویت (به عنوان مثال، آدرس IP منبع) منبع حمله replay
۶.	FCS_DTLSS_EXT.2	شکست در برقراری یک نشست DTLS	دلیل شکست
۷.	FCS_DTLSS_EXT.2	تشخیص حملات replay	هویت (به عنوان مثال، آدرس IP منبع) منبع حمله replay
۸.	FCS_HTTPS_EXT.1	شکست در برقراری یک نشست HTTPS	دلیل شکست
۹.	FCS_IPSEC_EXT.1	شکست در برقراری یک IPsec SA	دلیل شکست
۱۰.	FCS_NTP_EXT.1	پیکربندی time server جدید حذف time server پیکربندی شده	هویت سرور زمانی جدید/حذف شده
۱۱.	FCS_SSHC_EXT.1	شکست در برقراری یک نشست SSH	دلیل شکست
۱۲.	FCS_SSHS_EXT.1	شکست در برقراری یک نشست SSH	دلیل شکست
۱۳.	FCS_TLSC_EXT.1	شکست در برقراری یک نشست TLS	دلیل شکست
۱۴.	FCS_TLSC_EXT.2	شکست در برقراری یک نشست TLS	دلیل شکست
۱۵.	FCS_TLSS_EXT.1	شکست در برقراری یک نشست TLS	دلیل شکست
۱۶.	FCS_TLSS_EXT.2	شکست در برقراری یک نشست TLS	دلیل شکست

ردیف	الزام	رویدادهای ممیزی	لیست سوابق ممیزی اضافی
.۱۷	FIA_X509_EXT.1/Rev	تلاش ناموفق برای تائید یک گواهینامه	دلیل شکست
.۱۸	FIA_X509_EXT.2	هیچ	هیچ
.۱۹	FIA_X509_EXT.3	هیچ	هیچ
.۲۰	FPT_TST_EXT.2	شکست در خودآزمایی	دلیل شکست (شامل شناسه گواهینامه نامعتبر)
.۲۱	FPT_TUD_EXT.2	شکست در به‌روزرسانی	دلیل شکست (شامل شناسه گواهینامه نامعتبر)
.۲۲	FMT_MOF.1/AutoUpdate	فعال‌سازی یا غیرفعال سازی بررسی خودکار برای به‌روزرسانی‌ها یا به‌روزرسانی‌های خودکار	هیچ
.۲۳	FMT_MOF.1/Functions	تغییر رفتار انتقال داده ممیزی به موجودیت IT خارجی، مدیریت داده ممیزی، عملکرد ممیزی زمانی که فضای ذخیره‌سازی ممیزی محل پر شده باشد.	هیچ

نکته کاربردی:

رویداد ممیزی «الزامات پروتکل X509 (۱) و (۲)/ ابطال» در صورتی رخ می‌دهد که محصول مورد ارزیابی نتواند از موارد زیر اطمینان حاصل نماید و گواهی‌نامه‌ها را تائید کند:

- وجود افزونه basicConstraints و تائید اینکه پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم‌شده است
- تائید امضای دیجیتال CA سلسله مراتبی مورداعتماد
- 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.

۶-۲ کلاس ممیزی امنیت

شماره الزام	نام الزام

۸۳	تولید داده ممیزی ۱	FAU_GEN_EXT.1.1
توابع امنیت هدف ارزیابی قادر به تولید سوابق حسابرسی برای هر مؤلفه هدف ارزیابی است. سوابق حسابرسی ایجاد شده توسط توابع امنیت هدف ارزیابی از هر مؤلفه محصول مورد ارزیابی شامل زیرمجموعه رویدادهای مربوط به ممیزی امنیت است که می‌توانند روی مؤلفه هدف ارزیابی اتفاق بیفتند.		
۸۴	**محل ذخیره‌سازی داده‌های ممیزی حفاظت شده**	FAU_STG_EXT.3.1/LocSpace
توابع امنیتی هدف ارزیابی باید قبل از اینکه ممیزی از ظرفیت ذخیره‌سازی ردیابی ممیزی محلی بیشتر شود، اخطار لازم را به مدیر ارائه دهد.		
۸۵	محل ذخیره‌سازی داده ممیزی ۴	FAU_STG_EXT.4.1
هر مؤلفه هدف ارزیابی که داده‌های ممیزی امنیتی را به صورت محلی ذخیره نمی‌کند ، می‌تواند داده‌های ممیزی امنیتی را به‌صورت محلی بافر کند تا زمانی که به یک مؤلفه دیگر هدف ارزیابی که آن را ذخیره یا انتقال می‌دهد ، انتقال داده شود. [انتخاب: FPT_ITT.1 ، FPT_ITC.1] .		

۶-۳ الزامات پروتکل DTLS Client

شماره الزام	نام الزام	
۸۶	الزامات پروتکل DTLS Client (۱)	FCS_DTLSC_EXT.1.1
توابع امنیتی هدف ارزیابی باید [انتخاب: DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید: [انتخاب: ○ TLS_RSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 3268 ○ TLS_RSA_WITH_AES_256_CBC_SHA**مطابق با** RFC 3268 ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA**مطابق با** RFC 3268 ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA**مطابق با** RFC 3268 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA**مطابق با** RFC 4492		

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 **مطابق با** RFC 5289

[

نکته کاربردی:

توسط این الزام مجموعه رمزهای مورد آزمایش در تنظیمات ارزیابی محدود می‌شوند. نویسنده سند هدف امنیتی باید مجموعه رمزهایی که پشتیبانی می‌شوند را انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با نسخه دوم ND cPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 6347 وجود داشته باشد، الزامی است.

به علت اینکه نسخه‌های جدید DTLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند.

در نسخه آینده این cPP، نسخه DTLS ۱,۲ برای تمامی اهداف ارزیابی الزامی خواهد بود.

۸۷	الزامات پروتکل DTLS Client (۲)	FCS_DTLSC_EXT.1.2

توابع امنیتی هدف ارزیابی باید تائید کند که [انتخاب: شناسه ارائه شده با شناسه مرجع طبق RFC 6125 بخش ۶، آدرس IPv4 در CN یا SAN، آدرس IPv6 در CN یا SAN، آدرس IPv4 در SAN، آدرس IPv6 در SAN، شناسه در RFC 5280 پیوست A [انتخاب: id-at-commonName، id-at-countryName، id-at-dnQualifier، idat-generationQualifier، id-at-givenName، id-at-initials، id-at-localityName، id-at-name، id-atorganizationalUnitName، id-at-organizationName، id-at-pseudonym، id-at-serialNumber، idat-stateOrProvinceName، id-at-surname، id-at-title] و نه انواع خصوصیات دیگر] مطابقت داشته باشد.

نکته کاربردی:

قوانین تائید هویت در بخش ۶ از RFC 6125 شرح داده شده است. شناسه مرجع از طریق پیکربندی (به عنوان مثال، تنظیم نام یک سرور پست الکترونیکی یا سرور احراز هویت) توسط مدیر (به عنوان مثال، در یک URL در مرورگر وب یا کلیک بر روی یک لینک) یا توسط یک کاربرد وابسته به سرویس کاربردی (به عنوان مثال، یک پارامتر از API) برقرار می‌شود. کلاینت بر اساس دامنه منبع شناسه مرجع مجزا و نوع سرویس کاربردی (مانند HTTP، SIP، LDAP)، تمامی شناسه‌های مرجعی که قابل قبول هستند را برقرار می‌کند، مانند یک "نام عمومی" برای فیلد "Subject Name" یک گواهینامه و یک نام DNS (case-insensitive)، نام URL، و نام سرویس برای فیلد "Subject Alternative Name ". سپس کلاینت این لیست تمامی شناسه‌های مرجع قابل قبول را با شناسه‌های ارائه شده در گواهینامه سرور DTLS مقایسه می‌کند.

روش مورد ترجیح برای تائید این است که Subject Alternative Name از نام DNS، نام URL، یا نام سرویس استفاده کند. برای هدف پس‌سازگاری[۱] تائید با استفاده از نام عمومی مورد نیاز است. علاوه بر این، ممکن است استفاده از آدرس IP در Subject Name یا Subject Alternative Name پشتیبانی شود ولی برای بهترین روش، ممنوع است. در نهایت، کلاینت باید از ایجاد شناسه‌های مرجع با استفاده از wildcards اجتناب نماید. هرچند، اگر شناسه‌های ارائه شده حاوی wildcards باشند، کلاینت باید از بهترین روش منطبق پیروی کند؛ این بهترین شیوه‌ها در فعالیت ارزیابی به دست می‌آیند.

۸۸	الزامات پروتکل DTLS Client (۳)	FCS_DTLSC_EXT.1.3

توابع امنیتی هدف ارزیابی باید فقط در صورتی که گواهینامه سرور معتبر باشد کانال امن را برقرار سازد.

همچنین توابع امنیتی هدف ارزیابی باید [انتخاب:

- هیچ مکانیسم لغو سرپرستی پیاده‌سازی نشود.

[۱] backwards compatibility

	– در صورت شکست توابع امنیتی هدف ارزیابی، به مجوز مدیریت برای ایجاد ارتباط به [انتخاب: مطابقت با شناسه مرجع، تائید مسیر گواهی، تائید تاریخ انقضا، تعیین وضعیت لغو] از گواهی سرور ارائه شده نیاز دارید.	
۸۹	الزامات پروتکل DTLS Client (۴)	FCS_DTLSC_EXT.1.4
توابع امنیتی هدف ارزیابی باید در Client Hello، [انتخاب: Supported Elliptic Curves Extension را ارائه ندهد، Supported Elliptic Curves Extension را به همراه NIST curve های[انتخاب: secp256r1، secp384r1، secp521r1، ffdhe2048، ffdhe3072، ffdhe4096، ffdhe6144، ffdhe8192] ارائه دهد و هیچ منحنی دیگری] **نکته کاربردی:** اگر مجموعه رمزهای با منحنی elliptic در FCS_DTLSC_EXT.1.1 انتخاب شده باشد، انتخاب یک یا چند منحنی الزامی است. اگر هیچ مجموعه رمزی با منحنی elliptic در FCS_DTLSC_EXT.1.1 انتخاب نشده باشد، باید گزینه "Supported Elliptic Curves Extension را ارائه ندهد " انتخاب شود. این الزام منحنی‌های elliptic مجاز را برای احراز هویت و پذیرش کلید منحنی‌های NIST از FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌کند. این تعمیم برای کلاینت‌هایی که از Elliptic Curve ciphersuites پشتیبانی می‌کنند، می‌باشد.		

۴-۶ الزامات پروتکل DTLS Clint /احراز هویت

۹۰	الزامات پروتکل DTLS Client / احراز هویت (۱)	FCS_DTLSC_EXT.2.1
توابع امنیتی هدف ارزیابی باید احراز هویت متقابل را با استفاده از گواهینامه X.509 نسخه ۳، پشتیبانی کند.		
۹۱	الزامات پروتکل DTLS Client / احراز هویت (۲)	FCS_DTLSC_EXT.2.2
توابع امنیتی هدف ارزیابی باید در صورت دریافت پیامی حاوی invalid MAC [انتخاب: نشست DTLS را خاتمه دهد، رکورد را بی سروصدا دور بیندازد.]		
۹۲	الزامات پروتکل DTLS Client / احراز هویت (۳)	FCS_DTLSC_EXT.2.3

توابع امنیتی هدف ارزیابی باید پیام‌هایreplayed را برای موارد زیر شناسایی کرده و بدون پاسخ دور بریزد:

- سوابق DTLS قبلاً دریافت شده
- سوابق DTLS آن‌قدر قدیمی‌باشند که متناسب پنجره لغزان نباشند.

شناسایی کرده و بی‌صدا از بین ببرد.

۶-۵ الزامات پروتکل DTLS Server

۹۳	الزامات پروتکل DTLS Server (۱)	FCS_DTLSS_EXT.1.1

توابع امنیتی هدف ارزیابی باید [انتخاب: DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید:

[انتخاب:

- TLS_RSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA**مطابق با** RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA**مطابق با** RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA**مطابق با** RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA**مطابق با** RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA **مطابق با** RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA **مطابق با** RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 **مطابق با** RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 **مطابق با** RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 **مطابق با** RFC 5289

[

نکته کاربردی:

مجموعه رمزهای آزمایش شده در تنظیمات ارزیابی توسط این الزام محدود می‌شوند. نویسنده هدف امنیتی باید مجموعه رمزهایی را که پشتیبانی می‌شوند انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با نسخه دوم ND cPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 6347 و RFC 5246 وجود داشته باشد، الزامی است.

به علت اینکه نسخه‌های جدید DTLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند.

در نسخه آینده این cPP، نسخه DTLS ۱,۲ برای تمامی اهداف ارزیابی الزامی خواهد بود.

۹۴	الزامات پروتکل DTLS Server (۲)	FCS_DTLSS_EXT.1.2

توابع امنیتی هدف ارزیابی باید اتصال کلاینت‌هایی که درخواست [لیست نسخه‌های پروتکل] دارند، رد نماید.

نکته کاربردی:

این نسخه از cPP، هدف ارزیابی را الزام به رد نسخه DTLS ۱ نمی‌کند. در نسخه آینده این cPP، تمامی اهداف ارزیابی الزام به رد نسخه DTLS ۱ خواهند بود.

۹۵	الزامات پروتکل DTLS Server (۳)	FCS_DTLSS_EXT.1.3

در صورتی که اعتبار کلاینت DTLS تائید نشود، توابع امنیتی هدف ارزیابی نباید برای اتصال handshake اقدام به تلاش نماید.

نکته کاربردی:

فرآیند تائید کلاینت DTLS، در بخش ۴,۲,۱ از RFC 6347 (DTLS 1.2) و RFC 4347 (DTLS 1.0) شرح داده شده است. هدف ارزیابی کلاینت DTLS را طی برقراری ارتباط (Handshaking) و قبل از اینکه توابع امنیتی هدف ارزیابی پیام Server Hello ارسال نماید، تائید کند. پس از دریافت ClientHello، سرور DTLS، به همراه کوکی[۱] HelloVerifyRequest ارسال می‌کند. کوکی، پیام امضا شده‌ای است که از توابع درهم‌سازی کلید شده مشخص شده در FCS_COP.1/KeyedHash استفاده می‌کند. سپس کلاینت DTLS یک ClientHello دیگری به پیوست کوکی ارسال می‌کند. اگر سرور DTLS با موفقیت کوکی امضا شده را تائید کند، کلاینت از آدرس IP جعلی استفاده نمی‌کند.		
۹۶	الزامات پروتکل DTLS Server (۴)	FCS_DTLSS_EXT.1.4
توابع امنیتی هدف ارزیابی باید برای TLS از [انتخاب: کلید RSA را با اندازه [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت]، پارامترهای Diffie-Hellman با اندازه[انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت، ۶۱۴۴ بیت ، ۸۱۹۲ بیت] گروه‌های Diffie-Hellman [انتخاب: ffdhe2048 ، ffdhe3072، ffdhe4096، ffdhe6144، ffdhe8192 ، هیچ گروه دیگری]، منحنی‌های ECDHE [انتخاب: secp256r1 ، secp384r1 ، secp521r1] و هیچ منحنی دیگری] استفاده کند.		
۹۷	الزامات پروتکل DTLS Server (۵)	FCS_DTLSS_EXT.1.5
در صورت دریافت پیامی شامل MAC نامعتبر، توابع امنیتی هدف ارزیابی باید [انتخاب: نشست DTLS را خاتمه دهد، سوابق را بدون پاسخ دور بریزد[۲]] . **نکته کاربردی:** Message Authentication Code (MAC) تابع درهم‌ساز کلیدشده مشخص شده در FCS_COP.1/KeyedHash می‌باشد. MAC، در مرحله DTLS handshake تبادل می‌شود و برای حفظ صحت پیام‌های دریافت شده از فرستنده در طول تبادل داده DTLS استفاده می‌شود. در صورتی که MAC تائید نشود، باید نشست خاتمه یابد یا باید سوابق بدون پاسخ رها شوند.		
۹۸	الزامات پروتکل DTLS Server (۶)	FCS_DTLSS_EXT.1.6
توابع امنیتی هدف ارزیابی باید پیام‌های replayed را برای موارد زیر شناسایی کرده و بدون پاسخ دور بریزد: ○ سوابق DTLS قبلاً دریافت شده ○ سوابق DTLS آن‌قدر قدیمی‌باشند که متناسب پنجره لغزان نباشند. **نکته کاربردی:**		

[۱] cookie
[۲] Silently discard the record

شناسایی Replay در بخش ۴,۱,۲,۶ از DTLS 1.2 (RFC 6347) و بخش ۴,۱,۲,۵ از DTLS 1.0 (RFC 4347) شرح داده شده است. برای هر سوابق دریافت شده، دریافت‌کننده سوابق حاوی دنباله شماره‌ای که در پنجره دریافت لغزان قرار دارد را تائید می‌کند و دنباله شماره هر سوابق دریافت شده دیگر را در طول نشست تکرار نمی‌کند. "Silently Discard" به این معنی است که هدف ارزیابی بسته‌ها را بدون پاسخ دور بریزد.		
۹۹	الزامات پروتکل DTLS Server (۷)	FCS_DTLSS_EXT.1.7
توابع امنیتی هدف ارزیابی باید از [انتخاب: هیچ از سرگیری جلسه یا بلیت‌های جلسه، از سرگیری نشست بر مبنای session ID بر اساس RFC 4346(TLS1.1) یا RFC5246(TLS1.2)، از سرگیری نشست بر مبنای بلیت‌های نشست با توجه به RFC 5077] پشتیبانی کند.		

۶-۶ الزامات پروتکل DTLS Server /احراز هویت دوطرفه

۱۰۰	الزامات پروتکل DTLS Server / احراز هویت متقابل (۱)	FCS_DTLSS_EXT.2.1
توابع امنیتی هدف ارزیابی باید احراز هویت متقابل DTLS Client را با استفاده از گواهینامه X.509 نسخه ۳، پشتیبانی کند.		
۱۰۱	الزامات پروتکل DTLS Server / احراز هویت متقابل (۲)	FCS_DTLSS_EXT.2.2
زمانی که کانال مورد اعتماد ایجاد می‌شود، اگر گواهینامه کلاینت معتبر نباشد به صورت پیش‌فرض توابع امنیتی هدف ارزیابی نباید یک کانال مورد اعتماد را ایجاد کند. همچنین توابع امنیتی هدف ارزیابی باید: [انتخاب: – هیچ مکانیسم لغو سرپرستی را اجرا نکند. – در صورت عدم موفقیت توابع امنیتی هدف ارزیابی در [انتخاب: تطابق با شناسه مرجع، تائید مسیر گواهینامه، تائید تاریخ انقضا، تعیین وضعیت ابطال] گواهینامه مشتری ارائه شده، به مجوز سرپرست برای برقراری ارتباط نیاز دارد.]		
۱۰۲	الزامات پروتکل DTLS Server / احراز هویت متقابل (۳)	FCS_DTLSS_EXT.2.3
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 برای کلاینت برقرار سازد.		

[۱] Distinguished name
[۲] Subject Alternative Name

۶-۷ الزامات پروتکل HTTPS

شماره الزام	نام الزام	
۱۰۳	**الزامات پروتکل HTTPS (۱)**	FCS_HTTPS_EXT.1.1
توابع امنیتی هدف ارزیابی باید پروتکل HTTPS مطابق با RFC 2818 را اجرا کنند. **نکته کاربردی:** 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 جزئیات بیشتری را به TSS اضافه کرد.		
۱۰۴	**الزامات پروتکل HTTPS (۲)**	FCS_HTTPS_EXT.1.2
توابع امنیتی هدف ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.		
۱۰۵	**الزامات پروتکل HTTPS (۳)**	FCS_HTTPS_EXT.1.3
درصورتی‌که گواهی‌نامه همتا[1] اراده شده باشد، توابع امنیتی هدف ارزیابی باید [انتخاب: نیاز به احراز هویت کلاینت نداشته باشد، اتصال را برقرار ننماید، برای برقراری اتصال درخواست احراز هویت نماید، [اختصاص: اقدام دیگر]].		

۶-۸ 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.

IPsec جزء مؤلفه‌های ضروری این پروفایل حفاظتی به شمار نمی‌آید. اگر یک محصول مورد ارزیابی از پروتکل IPsec استفاده کند، آنگاه باید انتخاب مربوطه را در «کانال امن» و/یا «مسیر امن» انجام دهد. همچنین 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

[1] Peer certificate

۱۰۶	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1
در توابع امنیتی هدف ارزیابی باید معماری IPsec را بر اساس آنچه در RFC 4301 مشخص شده است، پیاده‌سازی شود. **نکته کاربردی:** بر اساس RFC 4301 برای پیاده‌سازی IPSEC جهت محافظت از ترافیک IP باید از یک پایگاه داده 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). پایگاه داده 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. صرف‌نظر 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.		

۱۰۷	الزامات پروتکل IPSEC (۲)	FCS_IPSEC_EXT.1.2
توابع امنیتی هدف ارزیابی باید اسمی داشته باشد خط‌مشی پایانی موجود در SPD با هر چیز مطابقت داشته باشد. در غیر این‌صورت غیرمنطبق است، و دور انداخته می‌شود.		

۱۰۸	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
توابع امنیتی هدف ارزیابی باید [انتخاب: مد انتقال، مد تونل] پیاده‌سازی کند. **نکته کاربردی:** نویسنده هدف امنیتی باید حالت‌های پشتیبانی شده برای عملکرد IPsec را انتخاب نماید.		

۱۰۹	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
توابع امنیتی هدف ارزیابی باید بر اساس آنچه در RFC 4303 گفته شده است، پروتکل ESP مربوط به IPSEC را با استفاده از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128 (RFC 3602), AES-CBC-192 (RFC 3602), AES-CBC-256 (RFC 3602), AES-GCM-128 (RFC 4106), AES-GCM-192 (RFC 4106), AES-GCM-256 (RFC 4106)] به همراه الگوریتم درهم‌سازی امن HMAC مبتنی بر SHA، [انتخاب: HMAC-SHA-1، HMAC-SHA-256، HMAC-SHA-384، HMAC-SHA-512، هیچ الگوریتم دیگری] پیاده‌سازی کند. **نکته کاربردی:**		

زمانی که یک الگوریتم AES-CBC انتخاب شود، باید حداقل یک HMAC مبتنی بر SHA نیز انتخاب شود. اگر فقط یک الگوریتم AES-GCM انتخاب شده باشد، HMAC مبتنی بر SHA، تا زمانی که AES-GCM هر دو عملکرد محرمانگی و یکپارچگی را برآورده می‌کند، الزامی نیست. ممکن است Ipsec از یک نسخه کوتاه توابع HMAC مبتنی بر SHA موجود در انتخاب‌ها، استفاده کند. در صورت استفاده از خروجی کوتاه، باید در TSS مشخص شود.		
۱۱۰	**الزامات پروتکل IPSEC (۵)**	FCS_IPSEC_EXT.1.5
توابع امنیتی هدف ارزیابی باید یکی از این پروتکل‌ها را پیاده‌سازی کند: [انتخاب: • IKEv1، با استفاده از مد اصلی برای تبادلات[۱] در فاز اول، طبق آنچه 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 در RFC 5996 تشریح شده است و [انتخاب: بدون پشتیبانی از پیمایش NAT[۲]، 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:** 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. اگر هدف ارزیابی از HMAC های کوتاه شده مبتنی بر SHA، همان‌طور که در RFC 4868 شرح داده شده است، استفاده کند، باید در TSS مشخص شود.		
۱۱۱	**الزامات پروتکل IPSEC (۶)**	FCS_IPSEC_EXT.1.6
توابع امنیتی هدف ارزیابی باید اطمینان حاصل کند که برای رمزگذاری پی‌آیند[۳] در پروتکل [انتخاب: IKEv1، IKEv2]، از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128، AES-CBC-192، AES-CBC-256، AES-GCM-128، AES-GCM-192، AES-GCM-256] استفاده شده است. الگوریتم‌های رمزنگاری AES-CBC-128، AES-CBC-192 و AES-CBC-256 در RFC 3602 تشریح شده‌اند. همچنین AES-GCM-128، AES-GCM-192 و AES-GCM-256 در RFC5282 تشریح شده‌اند.) **نکته کاربردی:**		

[۱] exchanges
[۲] NAT traversal
[۳] Payload

AES-GCM-128، AES-GCM-192 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.		
۱۱۲	**الزامات پروتکل IPSEC (۷)**	FCS_IPSEC_EXT.1.7

توابع امنیتی هدف ارزیابی باید اطمینان حاصل کند که [انتخاب:

- سرپرست امنیتی می‌تواند طول عمر SA فاز اول IKEv1 را بر اساس [انتخاب:
  - تعداد بایت‌ها،
  - مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد.

[

پیکربندی کند.

- سرپرست امنیتی می‌تواند طول عمر IKEv2 SA را بر اساس [انتخاب:
  - تعداد بایت‌ها،
  - مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد.

[

پیکربندی کند.

نکته کاربردی:

نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در FCS_IPSEC_EXT.1.5 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). محدودیت‌های Hardcoded این الزام را برآورده نمی‌کند. به طور کلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SA را باید در سند شرح محصول در نظر گرفت.

۱۱۳	**الزامات پروتکل IPSEC (۸)**	FCS_IPSEC_EXT.1.8

توابع امنیتی هدف ارزیابی باید اطمینان حاصل کند که [انتخاب:

- سرپرست امنیتی می‌تواند طول عمر SA فاز دوم IKEv1 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.

- سرپرست امنیتی 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:	
نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در FCS_IPSEC_EXT.1.5 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). محدودیت‌های Hardcoded این الزام را برآورده نمی‌کند. به طور کلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SA را باید در سند شرح محصول در نظر گرفت.	
۱۱۴	**الزامات پروتکل IPSEC (۹)**	FCS_IPSEC_EXT.1.9
توابع امنیتی هدف ارزیابی 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 FCS_RBG_EXT.1مشخص 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 کاربردی:	
از آنجایی که در پیاده‌سازی ممکن است گروه‌های مختلف Diffie-Hellman در مذاکره برای استفاده در SA مجاز باشند الزام FCS_IPSEC_EXT.1.9 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.	
۱۱۵	**الزامات پروتکل IPSEC (۱۰)**	FCS_IPSEC_EXT.1.10

توابع امنیتی هدف ارزیابی 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 کاربردی:

، 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 FCS_IPSEC_EXT.1.10 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.

۱۱۶	**الزامات پروتکل IPSEC (۱۱)**	FCS_IPSEC_EXT.1.11

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که همه پروتکل‌های IKE، گروه‌های DH [انتخاب:

- [انتخاب: ۱۴ (2048-bit MODP) ، ۱۵ (3072-bit MODP)، ۱۶ (4096-bit MODP)، ۱۷ (6144-bit MODP)، ۱۸ (8192-bit MODP)] با توجه به RFC 3526
- [انتخاب: ۱۹ (2048-bit Random ECP) ، ۲۰ (384-bit Random ECP) ، ۲۱ (521-bit Random ECP)، ۲۴ (256-bit POS)] با توجه به RFC 5114 همراه با 2048-bit MODP

] را پشتیبانی می‌کنند.

۱۱۷	**الزامات پروتکل IPSEC (۱۲)**	FCS_IPSEC_EXT.1.12

توابع امنیتی هدف ارزیابی 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 کاربردی:** نویسنده سند هدف امنیتی یکی یا هر دوی انتخاب‌های IKE را بر اساس اینکه کدام یک توسط محصول پیاده‌سازی می‌شود، انتخاب می‌کند.		
۱۱۸	**الزامات پروتکل IPSEC (۱۳)**	FCS_IPSEC_EXT.1.13
توابع امنیتی هدف ارزیابی 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. **نکته کاربردی:** حداقل یک روش احرازهویت همتا مبتنی بر کلید عمومی مطابق با این پروفایل حفاظتی مورد نیاز است؛ یک یا چند طرح کلید عمومی توسط نویسنده هدف امنیتی انتخاب می‌شود تا مشخص شود چه چیزی پیاده‌سازی شده‌است. نویسنده هدف امنیتی همچنین اطمینان حاصل می‌کند که الزامات FCS الگوریتم‌های مورد استفاده به منظور پشتیبانی از آن روش‌ها را لیست کرده است (قابلیت‌های تولید کلید ، اگر فراهم شده‌است). قابل ذکر است TSS شرح خواهد داد کدام یک از این الگوریتم‌ها استفاده شده است (برای مثال، RFC2409 سه روش احرازهویت با استفاده از کلیدهای عمومی؛هر یک از پشتیبانی‌شده ها در TSS شرح داده خواهد شد).		
۱۱۹	**الزامات پروتکل IPSEC (۱۴)**	FCS_IPSEC_EXT.1.14
توابع امنیتی هدف ارزیابی باید کانال امن را فقط در صورتی که شناسه ارائه شده در گواهینامه دریافت شده با شناسه پیکربندی شده مرجع تطابق داشته، و شناسه ارائه شده و مرجع یکی از انواع [انتخاب: SAN: آدرس IP، SAN: نام کامل واجد شرایط دامنه (FQDN)[۱]، SAN: کاربر FQDN، CN: آدرس IP، CN: نام کامل واجد شرایط دامنه (FQDN) نام مشخص‌شده[۲] (DN)] و [انتخاب: هیچ نوع شناسه مرجع دیگری، [اختصاص: سایر انواع شناسه مرجع پشتیبانی شده]] باشد، برقرار سازد. **نکته کاربردی:** زمانی که از گواهینامه‌های RSA یا ECDSA برای احرازهویت همتا استفاده شود، شناسه و گواهینامه‌های ارائه شده به شکل DN، آدرس IP، FQDN یا FQDN کاربر می‌باشند. شناسه مرجع، شناسه‌ای است که هدف ارزیابی انتظار دارد در طول احراز		

[۱] Fully Qualified Domain Name
[۲] Distinguished name

هویت IKE از همتا دریافت شود. شناسه ارائه شده، شناسه‌ای است که در گواهینامه همتا قرار دارد. نویسنده هدف امنیتی باید انواع شناسه ارائه شده و مرجع پشتیبانی شده را انتخاب کند و ممکن است به صورت اختیاری انواع پشتیبانی شده بیشتری را نیز در انتخاب دوم اختصاص دهد. به جز نوع شناسه DN، ممکن است هدف ارزیابی شناسه را در نام عمومی یا Subject Alternative Name (SAN) یا هردو، پشتیبانی کند. Subject Alternative Name با استفاده از نام‌های DNS، نام‌های URI یا نام‌های Service، روش ترجیحی برای تائید است. تائید با استفاده از نام عمومی برای هدف پس‌سازگاری[۱] مورد نیاز است. علاوه بر این، ممکن است استفاده از آدرس IP در Subject Name یا Subject Alternative Name پشتیبانی شود ولی برای بهترین روش، ممنوع است. الگوریتم‌های گواهینامه همتای پشتیبانی شده همانند FCS_IPSEC_EXT.1.13 هستند.

۹-۶ الزامات پروتکل NTP

شماره الزام	نام الزام	
۱۲۰	**الزامات پروتکل NTP (۱)**	FCS_NTP_EXT.1.1
توابع امنیتی هدف ارزیابی باید تنها از نسخه‌های NTP زیر استفاده کند: [انتخاب : NTP v3 ((RFC 1305) ، NTP v4 (RFC 5905)		
۱۲۱	**الزامات پروتکل NTP (۲)**	FCS_NTP_EXT.1.2
توابع امنیتی هدف ارزیابی باید زمان سیستم را با استفاده از [انتخاب: • احراز هویت با استفاده از [انتخاب: SHA1, SHA256, SHA384, SHA512، AES-CBC-128، AES-CBC-256] به عنوان الگوریتم(های) Digest پیام • [انتخاب: IPsec, DTLS] برای فراهم کردن ارتباط امن بین خودش و منبع زمانی NTP] به‌روزرسانی کند.		
۱۲۲	**الزامات پروتکل NTP (۳)**	FCS_NTP_EXT.1.3
توابع امنیتی هدف ارزیابی نباید مهر زمانی NTP را از آدرس‌های Broadcast و/یا Multicast به‌روزرسانی کند.		
۱۲۳	**الزامات پروتکل NTP (۴)**	FCS_NTP_EXT.1.4
توابع امنیتی هدف ارزیابی باید پیکربندی حداقل سه منابع زمانی NTP را پشتیبانی کند. **نکته کاربردی:**		

[۱] backwards compatibility

هدف ارزیابی باید از پیکربندی حداقل ۳ منبع زمانی پشتیبانی کند، اگرچه الزامی نیست هدف ارزیابی پیکربندی شده، همیشه از این حداقل ۳ منبع زمانی استفاده کند.

۶-۱۰ الزامات پروتکل SSH Client

شماره الزام	نام الزام	
۱۲۴	**الزامات پروتکل SSH Client (۱)**	FCS_SSHC_EXT.1.1
توابع امنیتی هدف ارزیابی باید پروتکل SSH را مطابق با RFC های [انتخاب: 4251، 4252، 4253، 4254، 5647، 5656، 6187، 8332،6668] پیاده‌سازی نماید. **نکته کاربردی:** 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 الگوریتم‌ها باید پیاده‌سازی شوند، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. اطمینان حاصل نمایید الگوریتم‌های اجراشده‌ای که با عنوان "REQUIRED" مشخص شده‌اند ولی در عناصر بعد از این بخش لیست نشده‌اند، خارج از محدوده فعالیت ارزیابی برای این الزام باشند. RFC 5647 only applies to the RFC compliant implementation of GCM; a TOE that only implements the "@openssh.com" variant of GCM should not select 5647. aes*- gcm@openssh.com is specified in Section 1.6 of the OpenSSH Protocol Specification (https://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/PROTOCOL?rev=1.31).		
۱۲۵	**الزامات پروتکل SSH Client (۲)**	FCS_SSHC_EXT.1.2
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، روش‌های احراز هویت زیر مطابق با آنچه در RFC4252 توضیح داده‌شده است، پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، [انتخاب: احراز هویت مبتنی بر کلمه عبور، هیچ روش دیگری].		
۱۲۶	**الزامات پروتکل SSH Client (۳)**	FCS_SSHC_EXT.1.3
همان طور که در RFC4253 توضیح داده‌شده است، توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک ارتباطات انتقال SSH کنار گذاشته شوند. **نکته کاربردی:** 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 در نظر گرفتن بیشترین اندازه بسته که قابل پذیرش است پر شود تا به این وسیله «طول مناسب» برای محصول تعریف شود.		

۱۲۷	الزامات پروتکل SSH Client (۴)	FCS_SSHC_EXT.1.4

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی انتقال SSH، از الگوریتم‌های رمزنگاری[انتخاب: aes128-cbc، aes128-ctr،aes256-cbc، aes256-ctr، AEAD_AES_128_GCM، AEAD_AES_256_GCM، aes128-gcm@openssh.com, aes256-gcm@openssh.com]استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند.

نکته کاربردی:

RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM وAEAD_AES_256_GCM را در SSH مشخص می‌کند. همان‌طور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم MAC استفاده شده باشد، الگوریتم‌های AEAD_AES_128_GCM وAEAD_AES_256_GCM فقط به عنوان الگوریتم‌های رمزنگاری قابل انتخاب هستند. در سند هدف امنیتی، ورودی‌های متناظر FCS_COP برای الگوریتم‌های انتخاب شده در اینجا هستند.

۱۲۸	الزامات پروتکل SSH Client (۵)	FCS_SSHC_EXT.1.5

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که پیاده‌سازی احراز هویت مبتنی بر کلید عمومی SSH، از انتخاب-ssh [rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, x509v3-ssh-rsa، x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384، x509v3-ecdsa-sha2-nistp521، nistp521 x509v3-rsa2048-sha256] به عنوان الگوریتم‌های کلید عمومی خودش استفاده می‌کند و سایر الگوریتم‌های کلید عمومی رد می‌شوند.

نکته کاربردی:

اگر x509v3-ssh-rsa x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384 یا x509v3-rsa2048-sha256 - انتخاب شده باشند، باید لیستی از گواهینامه‌های معتبر مجاز از FCS_SSHC_EXT.1.9 انتخاب شوند و SFRهای FIA_X509_EXT در پیوست B، کاربردی هستند.

It is recommended to configure the TOE to reject presented RSA keys with a key length below 2048 bit. RFC 8332 specifies the use of rsa-sha2-256 or rsa-sha2-512 in SSH.

۱۲۹	الزامات پروتکل SSH Client (۶)	FCS_SSHC_EXT.1.6

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: hmac-sha1، hmac-sha1-96، hmac-sha2-256، hmac-sha2-512، AEAD_AES_128_GCM، AEAD_AES_256_GCM، ضمنی] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC رد می‌شوند.

نکته کاربردی ۹۹:

RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM وAEAD_AES_256_GCM را در SSH مشخص می‌کند. همان‌طور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم‌های رمزنگاری استفاده شده باشد، الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM فقط به عنوان الگوریتم MAC قابل انتخاب هستند. در

سند هدف امنیتی، ورودی‌های متناظر FCS_COP برای الگوریتم‌های انتخاب شده در اینجا هستند. RFC 6668 استفاده از الگوریتم‌های sha2 در SSH را مشخص می‌کند.		
۱۳۰	**الزامات پروتکل SSH Client (۷)**	FCS_SSHC_EXT.1.7
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1, diffie-hellman-group15-sha512, ecdh-sha2-nistp256] و [انتخاب: diffie-hellman-group14- sha256, diffie-hellman-group16-sha512, diffie-hellman-group17-sha512, diffie-hellmangroup18-sha512, ecdh-sha2-nistp384, ecdh-sha2-nistp521, هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.		
۱۳۱	**الزامات پروتکل SSH Client (۸)**	FCS_SSHC_EXT.1.8
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در اتصالات SSH کلیدهای یکسان برای آستانه بیشتر از یک ساعت و بیشتر از یک گیگابایت تبادل داده، استفاده نشود. لازم است پس از رسیدن به هر یک از آستانه‌ها، تجدید کلید انجام شود. **نکته کاربردی:** این الزام، دو آستانه تعریف می‌کند. یکی برای حداکثر فاصله زمانی که کلیدهای همان نشست می‌توانند استفاده شوند، و دیگری برای حداکثر مقدار داده‌ای که می‌توان با کلیدهای همان نشست انتقال داد. هر دو آستانه باید اجرا شوند و تجدید کلید باید روی هرکدام از آستانه‌ها که زودتر رسید، انجام شود. برای آستانه حداکثر داده منتقل شده، باید مجموع داده‌های ورودی و خروجی محاسبه شود. تجدید کلید بر روی تمامی کلیدها (رمزنگاری، حفظ صحت) برای ترافیک ورودی و خروجی اعمال می‌شود. برای هدف ارزیابی، اجرای آستانه‌های کمتر از حداکثر مقادیر تعریف شده در الزام قابل قبول است. برای هر آستانه قابل تنظیم مربوط به این الزام، باید سند راهنما نحوه تنظیم آستانه را مشخص کند. مقادیر مجاز باید هم در سند راهنما مشخص شوند و هم باید کمتر یا برابر آستانه‌های مشخص شده در این الزام باشند، یا هدف ارزیابی نباید مقادیر خارج از آستانه‌های تعریف شده در این الزام را بپذیرد.		
۱۳۲	**الزامات پروتکل SSH Client (۹)**	FCS_SSHC_EXT.1.9
توابع امنیتی هدف ارزیابی 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 کاربردی:** تنها در صورتی می‌توان گزینه «لیست مراجع صدور گواهی مطمئن» را انتخاب کرد که x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384 یا x509v3-ecdsa-sha2-nistp521 در FCS_SSHC_EXT.1.5 انتخاب‌شده باشد.		

۶-۱۱ الزامات پروتکل SSH Server

شماره الزام	نام الزام	
۱۳۳	**الزامات پروتکل SSH Server (۱)**	FCS_SSHS_EXT.1.1
توابع امنیتی هدف ارزیابی باید پروتکل SSH مطابق با RFC های ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، [انتخاب: ۴۲۵۶، ۴۳۴۴، ۵۶۴۷، ۵۶۵۶، ۶۱۸۷، ۶۶۶۸، ۸۲۶۸،۸۳۰۸ بخش ۳,۱، ۸۳۳۲] پیاده‌سازی نماید. **نکته کاربردی:** 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 الگوریتم‌ها باید پیاده‌سازی شوند، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. اطمینان حاصل نمایید الگوریتم‌های اجراشده‌ای که با عنوان "REQUIRED" مشخص شده‌اند ولی در عناصر بعد از این بخش لیست نشده‌اند، خارج از محدوده فعالیت ارزیابی برای این الزام باشند.		
۱۳۴	**الزامات پروتکل SSH Server (۲)**	FCS_SSHS_EXT.1.2
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، همان‌طور که در RFC4252 توضیح داده‌شده است، روش‌های احراز هویت زیر پشتیبانی می‌شوند: مبتنی بر کلید عمومی، مبتنی بر کلمه عبور.		
۱۳۵	**الزامات پروتکل SSH Server (۳)**	FCS_SSHS_EXT.1.3
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 کاربردی:** 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.		
۱۳۶	**الزامات پروتکل SSH Server (۴)**	FCS_SSHS_EXT.1.4

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری [انتخاب: aes128- cbc, aes256-cbc, aes128-ctr, aes256-ctr, AEAD_AES_128_GCM, AEAD_AES_256_GCM, aes128-gcm@openssh.com, aes256-gcm@openssh.com] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند. **نکته کاربردی:** RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM وAEAD_AES_256_GCM را در SSH مشخص می‌کند. همان‌طور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم MAC استفاده شده باشد، الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM فقط به عنوان الگوریتم‌های رمزنگاری قابل انتخاب هستند. در سند هدف امنیتی، ورودی‌های متناظر FCS_COP برای الگوریتم‌های انتخاب شده در اینجا هستند.		
۱۳۷	**الزامات پروتکل SSH Server (۵)**	FCS_SSHS_EXT.1.5
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که پیاده‌سازی احراز هویت مبتنی بر کلید عمومی SSH، از [انتخاب: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256] به عنوان الگوریتم‌های کلید عمومی خودش استفاده می‌کند و سایر الگوریتم‌های کلید عمومی رد می‌شوند. **نکته کاربردی:** اگر x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384 یا x509v3-ecdsa-sha2-nistp521 انتخاب شده باشند، SFRهای FIA_X509_EXT در پیوست B، کاربردی هستند. It is recommended to configure the TOE to reject presented RSA keys with a key length below 2048 bit. RFC 8332 specifies the use of rsa-sha2-256 or rsa-sha2-512 in SSH		
۱۳۸	**الزامات پروتکل SSH Server (۶)**	FCS_SSHS_EXT.1.6
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256، ضمنی] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند. **نکته کاربردی:** RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM وAEAD_AES_256_GCM را در SSH مشخص می‌کند. همان‌طور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم‌های رمزنگاری استفاده شده باشد، الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM فقط به عنوان الگوریتم MAC قابل انتخاب هستند. در سند هدف امنیتی، ورودی‌های متناظر FCS_COP برای الگوریتم‌های انتخاب شده در اینجا هستند. RFC 6668 استفاده از الگوریتم‌های sha2 در SSH را مشخص می‌کند.		
۱۳۹	**الزامات پروتکل SSH Server (۷)**	FCS_SSHS_EXT.1.7

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1, diffie-hellman-group15-sha512, ecdh-sha2-nistp256] و [انتخاب: diffie-hellman-group16-sha512, diffie-hellman-group14- sha256, diffie-hellman-group17-sha512, diffie-hellmangroup18-sha512, ecdh-sha2-nistp384, ecdh-sha2-nistp521, هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.		
۱۴۰	**الزامات پروتکل SSH Server (۸)**	FCS_SSHS_EXT.1.8
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که اتصالات SSH کلیدهای یکسان برای آستانه بیشتر از یک ساعت و بیشتر از یک گیگابایت تبادل داده، استفاده نشود. لازم است پس از رسیدن به هر یک از آستانه‌ها، تجدید کلید انجام شود. **نکته کاربردی:** این الزام، دو آستانه تعریف می‌کند. یکی برای حداکثر فاصله زمانی که کلیدهای همان نشست می‌توانند استفاده شوند، و دیگری برای حداکثر مقدار داده‌ای که می‌توان با کلیدهای همان نشست انتقال داد. هر دو آستانه باید اجرا شوند و تجدید کلید باید روی هرکدام از آستانه‌ها که زودتر رسید، انجام شود. برای آستانه حداکثر داده منتقل شده، باید مجموع داده‌های ورودی و خروجی محاسبه شود. تجدید کلید بر روی تمامی کلیدها (رمزنگاری، حفظ صحت) برای ترافیک ورودی و خروجی اعمال می‌شود. برای هدف ارزیابی، اجرای آستانه‌های کمتر از حداکثر مقادیر تعریف شده در الزام قابل قبول است. برای هر آستانه قابل تنظیم مربوط به این الزام، باید سند راهنما نحوه تنظیم آستانه را مشخص کند. مقادیر مجاز باید هم در سند راهنما مشخص شوند و هم باید کمتر یا برابر آستانه‌های مشخص شده در این الزام باشند، یا هدف ارزیابی نباید مقادیر خارج از آستانه‌های تعریف شده در این الزام را بپذیرد.		

۶-۱۲ الزامات پروتکل TLS Client

شماره الزام	نام الزام	
۱۴۱	**الزامات پروتکل TLS Client**	FCS_TLSC_EXT.1.1
توابع امنیتی هدف ارزیابی باید [انتخاب: TLS 1.2 (RFC5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کرده و تمامی نسخه‌های TLS و SSL را رد نماید. پیاده‌سازی توابع امنیتی هدف ارزیابی باید با پشتیبانی از مجموعه‌های رمز زیر باشد: ○ [انتخاب: ○ TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268] ○ TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق 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_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق 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
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289

]].

نکته کاربردی:

مجموعه رمزهای آزمایش شده در تنظیمات ارزیابی توسط این الزام محدود می‌شوند. نویسنده هدف امنیتی باید مجموعه رمزهایی که پشتیبانی می‌شوند را انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات

		ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با نسخه دوم ND cPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 5246 وجود داشته باشد، الزامی است. به علت اینکه نسخه‌های جدید TLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند. در نسخه آینده این cPP، نسخه TLS ۱,۲ برای تمامی اهداف ارزیابی الزامی خواهد بود.
۱۴۲	الزامات پروتکل TLS Client	FCS_TLSC_EXT.1.2
		توابع امنیتی هدف ارزیابی باید تائید کند که [انتخاب: شناسه ارائه شده با شناسه مرجع طبق RFC 6125 بخش ۶، آدرس IPv4 در CN یـا SAN، آدرس IPv6 در CN یا SAN، آدرس IPv4 در SAN، آدرس IPv6 در SAN، شناسه در RFC 5280 پیوست A [انتخاب: id-at-commonName، id-at-countryName، id-at-dnQualifier، id-at-generationQualifier، id-at-givenName، id-at-initials، id-at-localityName، id-at-name، id-at-organizationName، id-at-organizationalUnitName، id-at-pseudonym، id-at-serialNumber، id-at-stateOrProvinceName، id-at-surname، id-at-title] و نه انواع خصوصیات دیگر] مطابقت داشته باشد. **نکته کاربردی:** قوانین مربوط به تائید شناسه در بخش ۶ از RFC 6125 توضیح داده‌شده‌اند. شناسه مرجع توسط مدیر (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. روش مورد ترجیح برای تائید این است که Subject Alternative Name از نام DNS، نام URL، یا نام سرویس استفاده کند. برای هدف پس‌سازگاری[۱] تائید با استفاده از نام عمومی مورد نیاز است. علاوه بر این، ممکن است استفاده از آدرس IP در Subject Name یا Subject Alternative Name پشتیبانی شود ولی برای بهترین روش، ممنوع است. در نهایت، کلاینت باید از ایجاد شناسه‌های مرجع با استفاده از wildcards اجتناب نماید. هرچند، اگر شناسه‌های ارائه شده حاوی wildcards باشند، کلاینت باید از بهترین روش منطبق پیروی کند؛ این بهترین شیوه‌ها در فعالیت ارزیابی به دست می‌آیند.
۱۴۳	الزامات پروتکل TLS Client	FCS_TLSC_EXT.1.3

[۱] backwards compatibility

توابع امنیتی هدف ارزیابی باید فقط در صورتی که گواهینامه سرور معتبر باشد کانال امن را برقرار سازد.
همچنین توابع امنیتی هدف ارزیابی باید [انتخاب:
- هیچ مکانیسم لغو سرپرستی پیاده‌سازی نشود.
- در صورت شکست توابع امنیتی هدف ارزیابی، به مجوز مدیریت برای ایجاد ارتباط به [انتخاب: مطابقت با شناسه مرجع، تائید مسیر گواهی، تائید تاریخ انقضا، تعیین وضعیت لغو] از گواهی سرور ارائه شده نیاز دارید.]

نکته کاربردی:

اگر TLS در FTP_ITC یا FTP_TRP.1/Admin انتخاب شده باشد، اعتبار توسط تائید شناسه، مسیر گواهینامه، تاریخ انقضاء، و وضعیت لغو مطابق با RFC 5280، تعیین می‌شود. اعتبار گواهینامه بر اساس آزمون اجرا شده برای FIA_X509_EXT.1/Rev ارزیابی می‌شود. اگر TLS در FPT_ITT انتخاب شده باشد، اعتبار گواهینامه بر اساس آزمون اجرا شده برای FIA_X509_EXT.1/ITT ارزیابی می‌شود.

۱۴۴	الزامات پروتکل TLS Client	FCS_TLSC_EXT.1.4

توابع امنیتی هدف ارزیابی باید در Client Hello، [انتخاب: Supported Elliptic Curves Extension را ارائه ندهد، Supported Elliptic Curves Extension را به همراه NIST curve های[انتخاب: secp256r1، secp384r1، secp521r1، ffdhe2048، ffdhe3072، ffdhe4096، ffdhe6144، ffdhe8192] ارائه دهد و هیچ منحنی دیگری]

نکته کاربردی:

اگر در FCS_TLSC_EXT.1.1 مجموعه‌های رمز بیضوی انتخاب‌شده باشند، انتخاب یک یا چند مورد از منحنی‌ها الزامی است.
اگر در FCS_TLSC_EXT.1.1 هیچ‌کدام از مجموعه‌های رمز بیضوی انتخاب‌نشده باشند، سپس "عدم نمایش افزونه پشتیبانی منحنی‌های بیضوی" باید انتخاب شود.
این الزام مجموعه رمزهای بیضوی مجاز برای احراز هویت و توافق کلید را به NIST curve های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازند. این افزونه برای کاربرانی که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.

۶-۱۳ الزامات پروتکل TLS Client/ احراز هویت

شماره الزام	نام الزام	
۱۴۵	**الزامات پروتکل TLS Client/ احراز هویت ۱**	FCS_TLSC_EXT.2.1
توابع امنیتی هدف ارزیابی باید با استفاده از گواهینامه X.509v3، از احراز هویت دوطرفه پشتیبانی نماید.		

۶-۱۴ الزامات پروتکل TLS Server

شماره الزام	نام الزام	
۱۴۶	**الزامات پروتکل TLS Server ۱**	FCS_TLSS_EXT.1.1

توابع امنیتی هدف ارزیابی باید [انتخاب: TLS 1.2 (RFC5246)، TLS1.1 (RFC4346)] را پیاده‌سازی نماید و تمامی نسخه‌های TLS و SSL دیگر را رد نماید. پیاده‌سازی توابع امنیتی هدف ارزیابی باید از مجموعه‌های رمز زیر پشتیبانی نماید:

[انتخاب:

- TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
- TLS_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_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 **مطابق با** RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 **مطابق با** RFC 5288
- 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_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289

].

نکته کاربردی:

مجموعه‌های رمز که باید در پیکربندی ارزیابی تست شوند، توسط این الزام محدود شده‌اند. نویسنده هدف امنیتی باید مجموعه رمزهایی را که پشتیبانی می‌شوند، انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با نسخه دوم ND cPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 5246 وجود داشته باشد، الزامی است.

به علت اینکه نسخه‌های جدید TLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند.

در نسخه آینده این cPP، نسخه TLS ۱,۲ برای تمامی اهداف ارزیابی الزامی خواهد بود.

۱۴۷	الزامات پروتکل TLS Server ۲	FCS_TLSS_EXT.1.2

توابع امنیتی هدف ارزیابی باید اتصال‌های کاربرانی را که درخواست SSL2.0، SSL3.0، TLS1.0 و [انتخاب: TLS1.1، TLS1.2، هیچ‌کدام] دارند، رد نماید.

نکته کاربردی:

تمام نسخه‌های SSL و نسخه TLS 1.0 رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در FCS_TLSS_EXT.1.1 انتخاب‌نشده است، در اینجا انتخاب شود. در صورتی که گزینه هیچ‌کدام انتخاب شود، عبارت هیچ کدام توسط نویسنده سند هدف امنیتی قابل حذف است.

۱۴۸	الزامات پروتکل TLS Server ۳	FCS_TLSS_EXT.1.3

توابع امنیتی هدف ارزیابی باید [انتخاب: کلید RSA با اندازه کلید [انتخاب: ۲۰۴۸ بیت و ۳۰۷۲ بیت، ۴۰۹۶ بیت] پیاده‌سازی کند، پارامترهای EC Diffie-Hellman را بر روی منحنی‌های NIST [انتخاب: secp256r1، secp384r1، secp521r1] و هیچ منحنی دیگری تولید کند، پارامترهای Diffie-Hellman را با اندازه [انتخاب: ۳۰۷۲ بیت، ۲۰۴۸ بیت،۴۰۹۶ بیت، ۶۱۴۴ بیت، ۸۱۹۲ بیت] همچنین گروه‌های Diffie-Hellman را با [انتخاب : ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192] ایجاد نماید.]

نکته کاربردی:

اگر در بخش FCS_TLSS_EXT.1.1 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. FMT_SMF.1 تنظیمات پارامترهای پذیرش کلید برای برقراری قدرت امنیتی ارتباط TLS، الزامی می‌کند.		
۱۴۹	**الزامات پروتکلTLS Server ۴**	FCS_TLSS_EXT.1.4
توابع امنیتی هدف ارزیابی باید از [انتخاب: بدون از سرگیری نشست یا بلیت نشست، از سرگیری نشست بر اساس شناسه‌های نشست با توجه به RFC4346(TLS1.1) یا RFC 5246(TLS1.2)، از سرگیری نشست مبتنی بر بلیت‌های با توجه به RFC 5077] پشتیبانی کنند.		

۶-۱۵ الزامات پروتکل TLS Server/ احراز هویت دوطرفه

شماره الزام	نام الزام	
۱۵۰	**الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۱**	FCS_TLSS_EXT.2.1
توابع امنیتی هدف ارزیابی باید در ارتباط TLS با احرازهویت دوطرفه TLS کلاینت‌ها، از گواهینامه‌های X509v3 استفاده کند.		
۱۵۱	**الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۲**	FCS_TLSS_EXT.2.2
زمانی که کانال مورد اعتماد ایجاد می‌شود، اگر گواهینامه کلاینت معتبر نباشد به صورت پیش‌فرض توابع امنیتی هدف ارزیابی نباید یک کانال مورد اعتماد را ایجاد کند. همچنین توابع امنیتی هدف ارزیابی باید: [انتخاب: – هیچ مکانیسم لغو سرپرستی را اجرا نکند. – در صورت عدم موفقیت توابع امنیتی هدف ارزیابی در [انتخاب: تطابق با شناسه مرجع، تائید مسیر گواهینامه، تائید تاریخ انقضا، تعیین وضعیت ابطال] گواهینامه مشتری ارائه شده، به مجوز سرپرست برای برقراری ارتباط نیاز دارد.]		
۱۵۲	**الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۳**	FCS_TLSS_EXT.2.3
اگر شناسه مندرج در یک گواهینامه با شناسه مورد انتظار کلاینت مطابقت نداشته باشد، توابع امنیتی هدف ارزیابی نباید یک کانال قابل اعتماد ایجاد کند. اگر شناسه یک FQDN باشد آنگاه توابع امنیتی هدف ارزیابی باید شناسه‌ها را با توجه به RFC		

6125 با هم انطباق دهد، در غیر این صورت توابع امنیتی هدف ارزیابی باید شناسه را از گواهینامه parse کرده آن را با شناسه مورد انتظار کلاینت که در شرح خلاصه محصول، توصیف شده است، انطباق دهد.

۶-۱۶ الزامات شناسایی و احراز هویت

شماره الزام	نام الزام	
۱۵۳	**اعتبارسنجی گواهینامه X509 (۱)**	FIA_X509_EXT.1.1

توابع امنیتی مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تائید کند:

- تائید گواهی‌نامه RFC 5280 و تائید مسیر گواهی‌نامه با پشتیبانی از حداقل طول مسیر از سه گواهینامه
- مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.
- توابع امنیتی مورد ارزیابی باید برای تائید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است.
- توابع امنیتی مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) چنان که در RFC 6960 تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در بخش ۵ از RFC 5759 تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در بخش ۶,۳ از RFC 5280 تعریف شده است] را تائید کند
- توابع امنیتی مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تائید کند:
  - گواهی‌نامه‌های مورد استفاده برای 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
  - گواهی‌نامه‌های سرور ارائه شده 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.
  - گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف "Client Authentication" (id-kp2 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.
  - 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.

شماره الزام	نام الزام	
۱۵۴	**اعتبارسنجی گواهینامه X509 (۲)**	FIA_X509_EXT.1.2

توابع امنیتی مورد ارزیابی تنها درصورتی‌که افزونه مربوط به basicConstraints ارائه شده باشد و پرچم CA به حالت «TRUE» تنظیم‌شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA می‌پذیرد.

نکته کاربردی:

الزام FIA_X509_EXT.1.1/Rev قوانین تائید گواهینامه‌ها را لیست کرده است. نویسنده سند هدف امنیتی وضعیت لغوی که با استفاده از OCSP یا CRL ها تائید می‌شود، را انتخاب می‌کند. ممکن است پروتکل‌های کانال/مسیر امن استفاده از آن گواهینامه‌ها را الزام کند. این استفاده مستلزم آن است که قوانین extendedKeyUsage تائید شده باشد. اگر هدف ارزیابی عملکردی را که از هر نوع گواهینامه لیست شده در قوانین extendedKeyUsage از FIA_X509_EXT.1.1 استفاده می‌کند، پشتیبانی نکند؛ باید در TSS مشخص شده باشد و بخش مربوط به SFR به طور کلی عملکردهای مورد پذیرش را در نظر می‌گیرد. هرچند، اگر هدف ارزیابی از عملکردهایی پشتیبانی کند که از هرکدام از انواع این گواهینامه‌ها استفاده می‌کند، باید قوانین متناظر همانند SFR رعایت شوند.

هدف ارزیابی باید قادر به پشتیبانی از حداقل طول مسیر سه گواهینامه باشد. به این معنی که، باید از سلسله مراتبی حاوی حداقل یک گواهینامه اصلی self-signed، گواهینامه CA فرعی و گواهینامه هویت هدف ارزیابی باشد، پشتیبانی کند.

انتظار می‌رود اعتبارسنجی در یک گواهینامه CA اصلی امن؛ در ذخیره اصلی مدیریت شده توسط پلتفرم، به پایان برسد. TSS باید زمان اجرای بررسی لغو را شرح دهد. انتظار می‌رود بررسی لغو، زمانی که گواهینامه در یک مرحله احراز هویت استفاده می‌شود و زمان انجام به‌روزرسانی‌های امن (اگر انتخاب شده باشد)، انجام شود. تائید وضعیت گواهینامه X.509 فقط زمانی که در دستگاه بارگذاری می‌شود کافی نیست.

تائید وضعیت لغو گواهینامه‌های X.509 در طول شروع به کار خودآزمایی‌ها الزامی نیست. (اگر گزینه استفاده گواهینامه‌های X.509 برای خودآزمایی انتخاب شده باشد)

FIA_X509_EXT.1.2/Rev بر روی گواهینامه‌هایی که توسط توابع امنیتی هدف ارزیابی استفاده یا پردازش شده‌اند اعمال می‌شود و گواهینامه‌هایی که ممکن است به عنوان گواهینامه‌های CA امن اضافه شوند را محدود می‌کند.

سند هدف امنیتی باید شامل FIA_X509_EXT.2 در همه موارد باشد، به جز زمانی که فقط SSH در FTP_ITC.1 یا FPT_ITT.1 و ssh-rsa، ecdsa-sha2-nistp256 یا ecdsa-sha2-nistp384 انتخاب شده باشد و/یا احراز هویت محدود به ssh-rsa، ecdsa-sha2-nistp256، ecdsa-sha2-nistp384 و/یا ecdsa-sha2-nistp521 باشد. علاوه بر این، اگر FPT_TUD_EXT یا FPT_TST_EXT برای استفاده از گواهینامه‌های X509 انتخاب شده باشد، باید FIA_X509_EXT.1/Rev در سند هدف امنیتی باشد.

۱۵۵	**احراز هویت گواهینامه X509 (۱)**	FIA_X509_EXT.2.1
توابع امنیتی مورد ارزیابی باید برای پشتیبانی از احراز هویت در [انتخاب: IPsec، TLS، HTTPS، SSH، DTLS] و همچنین برای [انتخاب: امضای کد برای به‌روزرسانی نرم‌افزار سیستم، امضای کد برای تائید اعتبارسنجی، [اختصاص: سایر کاربردها]، هیچ کاربرد اضافی دیگر] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.		
۱۵۶	**احراز هویت گواهینامه X509 (۲)**	FIA_X509_EXT.2.2

اگر توابع امنیتی مورد ارزیابی نتواند اتصال مورد نیاز برای تعیین اعتبار یک گواهی‌نامه را برقرار کند، توابع امنیتی هدف ارزیابی باید [انتخاب: به سرپرست محصول اجازه دهد که در این مورد تصمیم‌گیری کند، گواهی‌نامه را بپذیرد، گواهی‌نامه را نپذیرد]. **نکته کاربردی:** انتخاب نویسنده هدف امنیتی در FIA_X509_EXT.2.1 شامل IPsec، TLS، HTTPS می‌باشد؛ اگر این پروتکل‌ها در FTP_ITC.1.1 یا FPT_ITT.1 باشند. اگر احراز هویتی غیر از ssh-rsa، ecdsa-sha2-nistp256، ecdsa-sha2-nistp384 و/یا ecdsasha2-nistp521 در FCS_SSHC_EXT.1.5 یا FCS_SSHS_EXT.1.5 انتخاب شده باشد، باید ST حاوی SSH باشد. ممکن است گواهینامه‌ها به صورت اختیاری برای به‌روزرسانی‌های امن نرم‌افزار سیستم (FPT_TUD_EXT.2) و برای تائید صحت (FPT_TST_EXT.2) استفاده شوند. معمولاً باید برای بررسی وضعیت لغو یک گواهینامه، دانلود یک CRL یا جستجو با استفاده از OCSP ارتباطی برقرار شود. انتخاب موجود در FIA_X509_EXT.2.2 برای شرح رفتار رویدادی در حالتی است که چنین ارتباطی برقرار نشده باشد (برای مثال، به علت خطای شبکه). اگر هدف ارزیابی، گواهینامه معتبری مطابق تمام قوانین دیگر موجود در FIA_X509_EXT.1 تعیین کرده باشد، رفتار مربوط به انتخاب، اعتبار را تعیین می‌کند. هدف ارزیابی باید گواهینامه را در صورتی که هر قانون اعتبارسنجی دیگری را در FIA_X509_EXT.1 نفی می‌کند، نپذیرد. اگر گزینه‌های تنظیمات مدیر توسط نویسنده هدف امنیتی انتخاب شده باشد، باید عملکردهای متناظر در FMT_SMF.1 را نیز انتخاب کند. انتخاب باید شامل الزامات اعتبارسنجی FCS_IPSEC_EXT.1.14 ، FCS_TLSC_EXT.1.3 و FCS_TLSC_EXT.2.3 باشد. اگر هدف ارزیابی توزیع شده باشد و FIA_X509_EXT.1/ITT انتخاب شده باشد، گواهینامه بررسی لغو اختیاری است. این مورد ناشی از اقدامات احراز هویت اضافی برای فعال‌سازی و غیرفعال سازی کانال امن داخلی هدف ارزیابی است؛ همان‌طور که در FCO_CPC_EXT.1 تعریف شده است. در این مورد، ارتباطی برای تائید اعتبار گواهینامه مورد نیاز نیست و این الزام به طور قطعی رعایت می‌شود. سند هدف امنیتی باید شامل FIA_X509_EXT.2 در همه موارد باشد، به جز زمانی که فقط SSH در FTP_ITC.1 یا FPT_ITT.1 و ssh-rsa، ecdsa-sha2-nistp256 یا ecdsa-sha2-nistp384 انتخاب شده باشد و/ یا احراز هویت -ecdsa-sha2 nistp521 نیز انتخاب شده باشد. علاوه بر این، اگر FPT_TUD_EXT یا FPT_TST_EXT گواهینامه‌های X509 را انتخاب کرده باشد، باید FIA_X509_EXT.2 در سند هدف امنیتی باشد.		
۱۵۷	**درخواست‌های گواهینامه X509 (۱)**	FIA_X509_EXT.3.1

توابع امنیتی مورد ارزیابی باید مطابق با آنچه در RFC 2986 تشریح شده است، یک Certificate Request Message تولید کند و بتواند این اطلاعات را در درخواست ارائه کند: کلید عمومی[۱] و [انتخاب: اطلاعات مخصوص به دستگاه[۲]، Common Name، Orgsnization، Organization Unit، Country]. **نکته کاربردی:** کلید عمومی در واقع بخش کلید عمومی از جفت کلیدهای عمومی-خصوصی است که بر اساس آنچه در FCS_CKM.1 شرح داده‌شده است، توسط هدف ارزیابی تولید می‌شود.		
۱۵۸	**درخواست‌های گواهینامه X509 (۲)**	FIA_X509_EXT.3.2
توابع امنیتی مورد ارزیابی باید زنجیره گواهی‌نامه‌ها از Root CA را بر اساس پاسخ گواهینامه‌های CA دریافت شده اعتبارسنجی کند.		

۶-۱۷ الزامات به‌روزرسانی امن

۱۵۹	**الزامات به‌روزرسانی امن ۴**	FPT_TUD_EXT.2.1
توابع امنیتی مورد ارزیابی قبل از نصب هر به‌روزرسانی ، اعتبار گواهی امضای کد را بررسی کند.		
۱۶۰	**الزامات به‌روزرسانی امن ۵**	FPT_TUD_EXT.2.2
اگر اطلاعات لغو برای گواهی در زنجیره اعتماد موجود نباشد، گواهینامه معتبری نیست تا به عنوان مهار مطمئن تعیین شده باشد، توابع امنیتی هدف ارزیابی باید [انتخاب: update را نصب نکند، اجازه بدهد که در این موارد سرپرست محصول در مورد پذیرش update تصمیم بگیرد.]		
۱۶۱	**الزامات به‌روزرسانی امن ۶**	FPT_TUD_EXT.2.3
هنگامی‌که گواهینامه به علت انقضای آن، غیر معتبر اعلام‌شده است، توابع امنیتی هدف ارزیابی باید [انتخاب: اجازه بدهد که در این موارد سرپرست محصول در مورد پذیرش گواهی تصمیم‌گیری نماید، گواهی را بپذیرد، گواهی را نپذیرد].		
۱۶۲	**الزامات به‌روزرسانی امن ۷**	FPT_TUD_EXT.2.4
هنگامی‌که گواهینامه به علتی غیر از انقضای آن، غیر معتبر اعلام‌شده است، یا اطلاعات ابطال آن در دست نباشد توابع امنیتی هدف ارزیابی نباید اجازه update دهند.		

[۱] Public Key
[۲] Device-specific information

۱۸-۶ الزامات مدیریت امنیت

۱۶۳	مدیریت رفتار توابع امنیتی/به‌روزرسانی خودکار ۱	FMT_MOF.1.1/AutoUpdate

توابع امنیتی هدف ارزیابی باید قابلیت [انتخاب: فعال‌سازی،غیرفعال سازی] کارکردهای [انتخاب: جستجو برای به‌روزرسانی خودکار، به‌روزرسانی خودکار] را برای سرپرست امنیتی فراهم آورد.

نکته کاربردی:

این الزام تنها زمانی قابل پیاده‌سازی است که محصول امکان پشتیبانی از بررسی به‌روزرسانی خودکار و به‌روزرسانی خودکار را فراهم کند و اجازه فعال و غیرفعال سازی این قابلیت را بدهد. فعال‌سازی و غیرفعال سازی قابلیت بررسی به‌روزرسانی خودکار و/یا به‌روزرسانی خودکار به سرپرست امنیتی محدود می‌شود. گزینه "به‌روزرسانی خودکار" فقط زمانی ممکن است انتخاب شود که از امضاهای دیجیتال برای اعتبار به‌روزرسانی امن استفاده شده باشد.

۱۶۴	مدیریت رفتار توابع امنیتی/به‌روزرسانی خودکار ۲	FMT_MOF.1.1/Functions

توابع امنیتی هدف ارزیابی باید توانایی [انتخاب: تعیین رفتار، تغییر رفتار] توابع [انتخاب: انتقال داده‌های ممیزی به موجودیت IT خارجی، مدیریت داده‌های ممیزی، عملکرد ممیزی زمانی که فضای حافظه محلی ممیزی پر شده باشد] را به سرپرست امنیتی محدود کند.

نکته کاربردی:

این الزام تنها در صورتی باید انتخاب شود که یک یا چند مورد از سناریوهای زیر اعمال شده باشد:

- اگر پروتکل انتقال برای انتقال داده‌های ممیزی به یک موجودیت IT خارجی، مطابق آنچه در FAU_STG_EXT.1.1 تعریف شده است قابل تنظیم باشد، گزینه "انتقال داده ممیزی به موجودیت IT خارجی" باید انتخاب شود.
- اگر مدیریت داده‌های ممیزی قابل تنظیم باشد، "مدیریت داده ممیزی" باید انتخاب شود. اصطلاح "مدیریت داده ممیزی" به گزینه‌های مختلف برای انتخاب و اختصاص در الزامات FAU_STG_EXT.1.2، FAU_STG_EXT.1.3 و FAU_STG_EXT.2/LocSpace اشاره می‌کند.
- اگر رفتار عملکرد ممیزی زمان پر شدن فضای ذخیره‌سازی ممیزی محلی قابل تنظیم باشد، گزینه "عملکرد ممیزی زمانی که فضای ذخیره‌سازی ممیزی محلی پر شده باشد" باید انتخاب شود.

انتخاب اول برای "تعیین رفتار" و "تغییر رفتار" باید به صورت مناسب انتخاب شود. ممکن است بر اساس انتخاب دوم، لازم به انتخاب‌های مختلفی برای انتخاب اول باشد (برای مثال، "مدیریت داده ممیزی" ممکن است "تعیین رفتار" و "تغییر رفتار" را برای انتخاب اول الزام کند و از طرف دیگر "توابع امنیتی هدف ارزیابی" ممکن است فقط "تغییر رفتار" را الزام کند.). در آن صورت، FMT_MOF.1/Functions باید با افزایش شماره پیوست تکرار شود. (به عنوان مثال، FMT_MOF.1/Functions1، FMT_MOF.1/Functions2، غیره).

۷ مراجع

- **collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020**
- **Intrusion Detection System Protection Profile V 1.7 Published by U.S. Government Protection Profile**