به نام خدا

پروفایل حفاظتی

سامانه مدیریت رخداد و حوادث امنیتی

(SIEM)

اسفند ۹۶

نسخه ۲,۱

پیشگفتار

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی که در این سند برای برآورده نمودن الزامات ارائه‌شده‌اند را در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد نمود. مرکز افتا با مشارکت سازمان فناوری اطلاعات این سند را در راستای این هدف تهیه نموده است. در این سند الزامات امنیتی SIEM بیان می‌شود.

این سند بر اساس سند طرح ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 تهیه گردیده است. در بخش پایانی «الزامات تضمین امنیتی» که از ساختاری مشابه بخش قبلی برخوردار است مطرح گردیده است، این بخش الزامات لازم جهت ارزیابی محصول را عنوان می‌نماید.

فهرست

1 شرح محصول ۷
۱,۱ تهدیدات ۷
۱,۱,۱ ارتباط با دستگاه‌های شبکه ۷
۱,۱,۲ به‌روزرسانی‌های معتبر ۱۱
۱,۱,۳ فعالیت ممیزی‌شده ۱۲
۱,۱,۴ داده‌ها و اطلاعات محرمانه دستگاه و سرپرست ۱۳
۱,۱,۵ از کار افتادن کارکردهای امنیتی دستگاه ۱۴
۱,۲ فرضیات ۱۵
۱,۲,۱ حفاظت فیزیکی ۱۵
۱,۲,۲ کارکرد محدود ۱۵
۱,۲,۳ عدم محافظت از ترافیک ۱۶
۱,۲,۴ سرپرست مورد اعتماد ۱۶
۱,۲,۵ به‌روزرسانی منظم ۱۶
۱,۲,۶ امنیت اطلاعات محرمانه سرپرست ۱۶
۱,۲,۷ مؤلفه‌های در حال اجرا (فقط برای اهداف ارزیابی توزیع‌شده) ۱۶
۱,۲,۸ اطلاعات باقیمانده ۱۷
۱,۳ خط‌مشی امنیتی سازمان ۱۷
۱,۳,۱ بنر دسترسی ۱۷
۲ اهداف امنیتی ۱۷
۲,۱ اهداف امنیتی مربوط به محیط عملیاتی ۱۷
۲,۱,۱ امنیت فیزیکی ۱۷

۲,۱,۲ عدم کارکرد عمومی ۱۷
۲,۱,۳ محافظت از ترافیک ۱۷
۲,۱,۴ سرپرست مورد اعتماد ۱۸
۲,۱,۵ به‌روزرسانی ۱۸
۲,۱,۶ امنیت حساب کاربری سرپرست ۱۸
۲,۱,۷ مؤلفه‌های در حال اجرا (فقط برای اهداف ارزیابی توزیع‌شده) ۱۸
۲,۱,۸ اطلاعات باقیمانده ۱۸
۲,۲ مسائل امنیتی مرتبط با دستگاه SIEM ۱۹
۲,۲,۱ تهدیدات ۱۹
۲,۲,۲ فرضیات ۲۰
۲,۲,۳ خط‌مشیهای سازمانی ۲۰
۳ الزامات کارکرد امنیتی ۲۱
۳,۱ کلاس ممیزی امنیت ۳۰
۳,۲ پشتیبانی رمزنگاری (FCS) ۳۵
۳,۳ کلاس شناسایی و احراز هویت ۴۲
۳,۴ کلاس مدیریت امنیت ۴۵
۳,۵ کلاس حفاظت از محصول مورد ارزیابی ۴۹
۳,۵,۱ آزمون محصول مورد ارزیابی ۵۱
۳,۵,۲ به‌روزرسانی امن ۵۲
۳,۶ دسترسی به محصول ۵۷
3.7 کلاس کانال‌ها/مسیرهای مورداعتماد ۵۸
۳,۸ کلاس مدیریت رویدادها ۶۰

۳,۹ الزامات کارکرد امنیتی برای پیاده‌سازی ارتباطات سلسله مراتبی ۶۳
4 الزامات تضمین امنیت ۶۴
4.1 کلاس توسعه..... ۶۴
4.1.1 مشخصات کارکردی..... ۶۵
4.2 کلاس راهنمای کاربر ۶۷
۴,۲,۱ راهنمای کاربردی ۶۸
۴,۲,۲ راهنمای آماده‌سازی ۷۰
4.3 کلاس آزمون..... ۷۱
4.3.1 آزمون مستقل ۷۲
4.4 کلاس آسیب‌پذیری..... ۷۳
۴,۴,۱ تحلیل آسیب‌پذیری..... ۷۳
4.5 کلاس پشتیبانی از چرخه حیات..... ۷۴
4.5.1 قابلیتهای پیکربندی ۷۴
۴,۵,۲ حوزه پیکربندی ۷۶
۵ پیوست یک: الزامات اختیاری ۷۷
۵,۱ کلاس ممیزی امنیت..... ۷۷
۵,۲ کلاس شناسایی و احراز هویت..... ۸۰
۵,۳ کلاس مدیریت امنیت..... ۸۲
۵,۴ کلاس حفاظت از محصول مورد ارزیابی ۸۳
۵,۵ کلاس ارتباطات..... ۸۴
۶ پیوست دو: الزامات مبتنی بر انتخاب ۸۵
6.1 الزامات پروتکل DTLS Client..... ۸۷

۶,۲ الزامات پروتکل DTLS Clint /احراز هویت ۹۰
6.3 الزامات پروتکل DTLS Server ۹۴
۶,۴ الزامات پروتکل DTLS Server /احراز هویت دوطرفه ۹۷
۶,۵ الزامات پروتکل HTTPS ۱۰۱
۶,۶ الزامات پروتکل IPsec ۱۰۲
۶,۷ الزامات پروتکل SSH Client ۱۰۹
۶,۸ الزامات پروتکل SSH Server ۱۱۲
۶,۹ الزامات پروتکل TLS Client ۱۱۴
6.10 الزامات پروتکل TLS Client/ احراز هویت ۱۱۷
۶,۱۱ الزامات پروتکل TLS Server ۱۲۰
۶,۱۲ الزامات پروتکل TLS Server/ احراز هویت دو طرفه ۱۲۳
۶,۱۳ الزامات شناسایی و احراز هویت ۱۲۶
۶,۱۴ الزامات خودآزمایی محصول مورد ارزیابی ۱۲۹
۶,۱۵ الزامات به‌روزرسانی امن ۱۳۰
۷ مراجع ۱۳۱

۱ شرح محصول

اصطلاح SIEM به مجموعه‌ای از نرم‌افزار، تجهیزات و سرویس‌های مدیریت‌شده اطلاق می‌گردد که هشدارهای امنیتی را که توسط سخت‌افزار شبکه و برنامه‌های کاربری تولیدشده‌اند، از نظر 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 است. تمرکز اصلی SIEM روی نظارت نمودن و کمک به مدیر و سرویس‌های دارای مجوز، سرویس دایرکتوری و دیگر تغییرات پیکربندی سیستم است، همچنین ارائه‌دهنده گزارش ممیزی، بررسی و پاسخ ضمنی[۳] است.

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 است.

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

---

[۱] Log Data

[۲] Security Information Evant Management (SIEM)

[۳] Incident Responce

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 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 غیراستاندارد 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 غیراستاندارد 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.

[۱] Interoperability

منطق الزام کارکرد امنیتی (SFR):

- 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 است 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.)

۱,۱,۱,۲ 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.

---

[۱] Cryptographic exhaust

[۲] Brute force

- مدیریت توابع رمزنگاری در FMT_SMF.1 مشخص می‌شود.

۱,۱,۱,۳ کانال‌های ارتباطی غیرقابل‌اعتماد

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 تأییدنشده 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 تأییدنشده 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] Roots of trust

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.)

۱,۲ 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 انتروپی 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، رمز عبورها 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 است 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، رمز عبورها 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 سازوکارهای امنیتی را تحت تأثیر قرار دهد.
مخاطرات محرمانگی و صحت	ممکن است موجودیت غیرمجازی با دور زدن سازوکارهای 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 سازوکارهای 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 سازوکارهای 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.
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.
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.

[۱] Administrator

نوع	توضیحات
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

شماره الزام	نام الزام	عنصر متناظر با الزام
۲	تولید داده ممیزی ۲	FAU_GEN.1.2
۳	تولید داده ممیزی ۳	FAU_GEN.2.1
۴	محل ذخیره‌سازی داده‌های ممیزی ۱	FAU_STG_EXT.1.1
۵	محل ذخیره‌سازی داده‌های ممیزی ۲	FAU_STG_EXT.1.2
۶	محل ذخیره‌سازی داده‌های ممیزی ۳	FAU_STG_EXT.1.3
۷	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1
۸	مدیریت کلید رمزنگاری ۲	FCS_CKM.2.1
۹	مدیریت کلید رمزنگاری ۴	FCS_CKM.4.1
۱۰	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1(1)
۱۱	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1(2)
۱۲	عملیات رمزنگاری ۱ (۳)	FCS_COP.1.1(3)
۱۳	عملیات رمزنگاری ۱ (۴)	FCS_COP.1.1(4)
۱۴	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۱۵	تولید بیت تصادفی ۲	FCS_RBG_EXT.1.2
۱۶	مدیریت 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 امن	FMT_MOF.1.1(1)/TrustedUpdate
۲۴	مدیریت داده‌های محصول ۱	FMT_MTD.1.1
۲۵	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1

شماره الزام	نام الزام	عنصر متناظر با الزام
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 گذرواژه سرپرست محصول ۱	FPT_APW_EXT.1.1
۳۱	حفاظت از گذرواژه 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 ۱	FPT_STM_EXT.1.1
۳۷	مهرهای زمانی 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 محصول۱	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
۴۶	مسیر امن ۲	FTP_TRP.1.2
۴۷	مسیر امن ۳	FTP_TRP.1.3
۴۸	تجزیه‌وتحلیل تحلیل‌گر ۱	SIEM_ANL.1.1

شماره الزام	نام الزام	عنصر متناظر با الزام
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
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

شماره الزام	نام الزام	عنصر متناظر با الزام
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
الزامات مربوط به پیوست دو		
۸۳	الزامات پروتکل DTLS Client (۱)	FCS_DTLSC_EXT.1.1
۸۴	الزامات پروتکل DTLS Client (۲)	FCS_DTLSC_EXT.1.2

شماره الزام	نام الزام	عنصر متناظر با الزام
۸۵	الزامات پروتکل DTLS Client (۳)	FCS_DTLSC_EXT.1.3
۸۶	الزامات پروتکل DTLS Client (۴)	FCS_DTLSC_EXT.1.4
۸۷	الزامات پروتکل DTLS Client/ احراز هویت ۱	FCS_DTLSC_EXT.2.1
۸۸	الزامات پروتکل DTLS Client/ احراز هویت ۲	FCS_DTLSC_EXT.2.2
۸۹	الزامات پروتکل DTLS Client/ احراز هویت ۳	FCS_DTLSC_EXT.2.3
۹۰	الزامات پروتکل DTLS Client/ احراز هویت ۴	FCS_DTLSC_EXT.2.4
۹۱	الزامات پروتکل DTLS Client/ احراز هویت ۵	FCS_DTLSC_EXT.2.5
۹۲	الزامات پروتکل DTLS Client/ احراز هویت ۶	FCS_DTLSC_EXT.2.6
۹۳	الزامات پروتکل DTLS Client/ احراز هویت ۷	FCS_DTLSC_EXT.2.7
۹۴	الزامات پروتکل DTLS Server (۱)	FCS_DTLSS_EXT.1.1
۹۵	الزامات پروتکل DTLS Server (۲)	FCS_DTLSS_EXT.1.2
۹۶	الزامات پروتکل DTLS Server (۳)	FCS_DTLSS_EXT.1.3
۹۷	الزامات پروتکل DTLS Server (۴)	FCS_DTLSS_EXT.1.4
۹۸	الزامات پروتکل DTLS Server (۵)	FCS_DTLSS_EXT.1.5
۹۹	الزامات پروتکل DTLS Server (۶)	FCS_DTLSS_EXT.1.6
۱۰۰	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۱	FCS_DTLSS_EXT.2.1

شماره الزام	نام الزام	عنصر متناظر با الزام
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 DTLS Server/ احراز هویت دوطرفه ۴	FCS_DTLSS_EXT.2.4
۱۰۴	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۵	FCS_DTLSS_EXT.2.5
۱۰۵	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۶	FCS_DTLSS_EXT.2.6
۱۰۶	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۷	FCS_DTLSS_EXT.2.7
۱۰۷	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۸	FCS_DTLSS_EXT.2.8
۱۰۸	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۹	FCS_DTLSS_EXT.2.9
۱۰۹	الزامات پروتکل HTTPS (۱)	FCS HTTPS_EXT.1.1
۱۱۰	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2
۱۱۱	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۱۱۲	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1
۱۱۳	الزامات پروتکل IPSEC (۲)	FCS_IPSEC_EXT.1.2
۱۱۴	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
۱۱۵	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
۱۱۶	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.1.5
۱۱۷	الزامات پروتکل IPSEC (۶)	FCS_IPSEC_EXT.1.6

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

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۴۳	الزامات پروتکل TLS Client (۱)	FCS_TLSC_EXT.1.1
۱۴۴	الزامات پروتکل TLS Client (۲)	FCS_TLSC_EXT.1.2
۱۴۵	الزامات پروتکل TLS Client (۳)	FCS_TLSC_EXT.1.3
۱۴۶	الزامات پروتکل TLS Client (۴)	FCS_TLSC_EXT.1.4
۱۴۷	الزامات پروتکلTLS Client/ احراز هویت ۱	FCS_TLSC_EXT.2.1
۱۴۸	الزامات پروتکلTLS Client/ احراز هویت ۲	FCS_TLSC_EXT.2.2
۱۴۹	الزامات پروتکلTLS Client/ احراز هویت ۳	FCS_TLSC_EXT.2.3
۱۵۰	الزامات پروتکلTLS Client/ احراز هویت ۴	FCS_TLSC_EXT.2.4
۱۵۱	الزامات پروتکلTLS Client/ احراز هویت ۵	FCS_TLSC_EXT.2.5
۱۵۲	الزامات پروتکل TLS Server (۱)	FCS_TLSS_EXT.1.1
۱۵۳	الزامات پروتکل TLS Server (۲)	FCS_TLSS_EXT.1.2
۱۵۴	الزامات پروتکل TLS Server (۳)	FCS_TLSS_EXT.1.3
۱۵۵	الزامات پروتکلTLS Server/ احراز هویت دوطرفه ۱	FCS_TLSS_EXT.2.1
۱۵۶	الزامات پروتکلTLS Server/ احراز هویت دو طرفه ۲	FCS_TLSS_EXT.2.2
۱۵۷	الزامات پروتکلTLS Server/ احراز هویت دو طرفه ۳	FCS_TLSS_EXT.2.3
۱۵۸	الزامات پروتکلTLS Server/ احراز هویت دو طرفه ۴	FCS_TLSS_EXT.2.4

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۵۹	الزامات پروتکلTLS Server/ احراز هویت دو طرفه ۵	FCS_TLSS_EXT.2.5
۱۶۰	الزامات پروتکلTLS Server/ احراز هویت دو طرفه ۶	FCS_TLSS_EXT.2.6
۱۶۱	الزامات پروتکل X509(۱)/ ابطال	FIA_X509_EXT.1.1/Rev
۱۶۲	الزامات پروتکل X509(۱)/ ابطال	FIA_X509_EXT.1.2/Rev
۱۶۳	الزامات پروتکل X509(۳)	FIA_X509_EXT.2.1
۱۶۴	الزامات پروتکل X509(۴)	FIA_X509_EXT.2.2
۱۶۵	الزامات پروتکل X509(۵)	FIA_X509_EXT.3.1
۱۶۶	الزامات پروتکل X509(۶)	FIA_X509_EXT.3.2
۱۶۷	خودآزمایی محصول مورد ارزیابی ۲	FPT_TST_EXT.2.1
۱۶۸	الزامات به‌روزرسانی امن ۴	FPT_TUD_EXT.2.1
۱۶۹	الزامات به‌روزرسانی امن ۵	FPT_TUD_EXT.2.2
۱۷۰	مدیریت کارکرد در محصول مورد ارزیابی ۱/ به‌روزرسانی خودکار	FMT_MOF.1.1/AutoUpdate
۱۷۱	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**
محصول مورد ارزیابی باید بتواند سوابق ممیزی را برای رویدادهای قابل ممیزی زیر تهیه کند: الف) آغاز و اتمام توابع ممیزی؛ ب) تمامی رویدادهای قابل ممیزی برای سطوح ممیزی. پ) تمام اقدامات مدیریتی شامل موارد زیر: • ورود و خروج مدیریتی به سیستم (درصورتی‌که مدیران سیستم نیاز به حساب کاربری شخصی داشته باشند، نام حساب کاربری آن‌ها نیز باید ثبت شود) • تغییرات در داده‌های توابع امنیتی هدف ارزیابی مرتبط با تغییرات پیکربندی (علاوه بر اطلاعات حاکی از ایجاد تغییرات، باید تعیین شود که چه مواردی تغییر کرده‌اند) • تولید/واردکردن، تغییر، یا پاک کردن کلیدهای رمزنگاری (علاوه بر این کار، نام کلید اختصاصی یا یک مرجع کلید نیز باید ثبت شود)	

- تغییر گذرواژه (نام حساب کاربری مربوطه نیز باید ثبت شود)
- [انتخاب: [آغاز و توقف سرویس‌ها، هیچ اقدام دیگر، اختصاص:[لیست سایر کاربردهای ویژه]]]

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

نکته کاربردی ۱:

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

برای اهداف ارزیابی توزیع‌شده، هر مؤلفه باید یک رکورد ممیزی برای الزامات کارکرد امنیتی که پیاده می‌کند، بیان نماید. اگر زمانی که یک رویداد ممیزی برقرار می‌گردد، بیش از یک مؤلفه‌ی هدف ارزیابی درگیر باشد، آنگاه باید این رویداد برای تمامی مؤلفه‌های درگیر، ممیزی گردد (برای مثال، رد شدن یک ارتباط وقتی که یک مؤلفه قصد برقراری یک کانال ارتباط امن با مؤلفه‌ی دیگری را دارد، باید رویداد ممیزی آن توسط هر دو مؤلفه ثبت گردد). همچنین این فعالیت فقط محدود به پیغام‌های خطا نمی‌شود، بلکه عملیات موفق را نیز شامل می‌گردد.

نکته کاربردی ۲:

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

۲	**تولید داده ممیزی ۲**

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

الف) تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت[۱] فعال و نتیجه رویداد (موفقیت یا شکست)؛ و

ب) در مورد هر یک از انواع رویدادهای ممیزی و بر اساس تعریف رویدادهای قابل ممیزی ارائه‌شده در پروفایل حفاظتی یا هدف امنیتی، اطلاعات در نکته کاربردی ۳ مشخص‌شده است.

نکته کاربردی ۳:

نویسنده هدف امنیتی با توجه به رویدادهای ممیزی ثبت‌شده برای هر یک از الزامات زیر باید اطلاعات مناسب دیگر علاوه بربند الف این الزام فراهم نماید. برای نمونه توسعه‌دهنده با توجه به الزام شماره ۲۰ «شناسایی و احراز هویت کاربر ۲» برای ثبت رکورد

[۱] Subject

ممیزی علاوه بر اطلاعات بند الف این الزام باید آدرس IP منشأ احراز هویت را در رکورد ممیزی (به‌عنوان نمونه در قسمت توضیحات رکورد) ثبت نماید؛ بنابراین این اطلاعات توسط نویسنده سند هدف امنیتی در این قسمت قرار داده می‌شود.

- برای الزام شماره ۱۶ و ۱۷ «مدیریت احراز هویت ناموفق» اطلاعات ممیزی تلاش‌های ناموفق که از تعداد مجاز بیشتر بوده است، ثبت می‌شود. این اطلاعات باید شامل منشأ تلاش صورت گرفته (مانند آدرس IP) باشد.
- برای الزام شماره ۲۱ «سازوکار احراز هویت بر اساس رمز عبور» اطلاعات ممیزی تمام کاربردهای سازوکار تعیین هویت و احراز هویت ثبت می‌شود. این اطلاعات باید شامل منشأ تلاش صورت گرفته (مانند آدرس IP) باشد. برای الزام شماره ۲۹ «مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن» اطلاعات ممیزی مربوط به هرگونه تلاش برای آغاز یک به‌روزرسانی، دستی ثبت می‌شود.
- برای الزام شماره ۲۴ «مدیریت داده‌های محصول» اطلاعات ممیزی تمام فعالیت‌های مدیریتی داده‌های محصول ثبت می‌شود.
- برای الزامات شماره ۳۳ الی ۳۵ «به‌روزرسانی امن» اطلاعات ممیزی مربوط به آغاز به‌روزرسانی، نتیجه تلاش‌های به‌روزرسانی (موفقیت یا شکست) ثبت می‌شود.
- برای الزام شماره ۳۶ «مهرهای زمانی[۱]» اطلاعات ممیزی مربوط به تغییرات صورت گرفته در زمان ثبت می‌شود. این اطلاعات باید شامل زمان‌های جدید و قدیم، منشأ تلاش (مانند آدرس IP) برای تغییر زمان موفق یا ناموفق باشد.
- برای الزام ۳۸ «قفل‌کردن و خاتمه دادن به نشست‌ها ۷» اگر «قفل کردن» انتخاب شود، اطلاعات ممیزی تمام تلاش‌های صورت گرفته برای باز کردن قفل یک نشست تعاملی ثبت می‌شود. در صورتی که «خاتمه دادن» انتخاب شود، اطلاعات ممیزی مربوط به خاتمه دادن یک نشست محلی از طریق یک سازوکار قفل‌کردن نشست ثبت می‌شود
- برای الزام ۳۹ «قفل‌کردن و خاتمه دادن به نشست‌ها ۵» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست راه‌دور از طریق یک سازوکار قفل‌کردن نشست ثبت می‌شود.
- برای الزام ۴۰ «قفل‌کردن و خاتمه دادن به نشست‌ها ۶» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست تعاملی ثبت می‌شود.
- برای الزامات ۴۲ الی ۴۴ «کانال امن» اطلاعات ممیزی مربوط به آغاز کردن کانال امن / خاتمه دادن کانال امن / شکست توابع کانال امن ثبت می‌شود. این اطلاعات باید شامل شناسایی دلیل و هدف تلاش ناموفق برای ایجاد کانال امن باشد.
- برای الزامات ۴۵ الی ۴۷ «مسیر امن» اطلاعات ممیزی مربوط به آغاز کردن مسیر امن / خاتمه دادن مسیر امن / شکست توابع مسیر امن ثبت می‌شود.

[۱] Time stamps

نکته کاربردی ۴:

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

۳	**تولید داده ممیزی ۳**

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

نکته کاربردی ۵:

مؤلفه‌ای که رویداد ممیزی را ثبت می‌نماید، وقتی که یک رویداد قابل ممیزی توسط مؤلفه‌ی دیگری برقرار می‌گردد، باید رویداد را با هویت مؤلفه‌ی که برقرارکننده آن رویداد است، مرتبط سازد.

۴	**محل ذخیره‌سازی داده‌های ممیزی ۱**

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

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.

نکته کاربردی ۶:

محصول مورد ارزیابی برای انتقال داده‌های ممیزی تولیدشده به یک موجودیت IT خارجی، ذخیره‌سازی و بازبینی سوابق ممیزی از یک سرور ممیزی به‌جز سرور محصول مورد ارزیابی استفاده می‌کند. ذخیره‌سازی این سوابق ممیزی و اجازه دادن به سرپرست محصول جهت بازبینی این سوابق، توسط محیط عملیاتی صورت می‌گیرد. از آنجایی که سرور ممیزی خارجی قسمتی از محصول مورد ارزیابی نیست، به جزء توانایی‌های انتقال داده‌های ممیزی، الزاماتی برای آن تعریف نمی‌شود. همچنین برای قالب و پروتکل زیرساختی داده‌های ممیزی که باید انتقال یابند، الزاماتی تعیین نمی‌شود. محصول باید توانایی پیکربندی انتقال داده ممیزی به سرور خارجی را بدون مداخله سرپرست داشته باشد. انتقال دستی، نمی‌تواند الزامات را برآورده نماید. ارسال باید به صورت بلادرنگ یا دوره‌ای انجام گیرد. اگر ارسال به صورت بلادرنگ انجام نشود، خلاصه مشخصات محصول چگونگی صورت گرفتن ارسال و بازه‌ی تکرار که محصول برای ارسال پشتیبانی می‌کند را توصیف می‌نماید. خلاصه مشخصات محصول همچنین بازه‌ی تکرار قابل‌قبول را پیشنهاد می‌نماید.

برای محصولات توزیع‌شده، هر مؤلفه باید قادر باشد که داده‌های ممیزی را از طریق یک کانال خارجی حفاظت شده، به صورت مناسبی خارج نماید. حداقل یک مؤلفه باید توانایی خارج کردن رکوردهای ممیزی به سرور IT خارجی را داشته باشد.	
۵	**محل ذخیره‌سازی داده‌های ممیزی ۲**
محصول مورد ارزیابی باید بتواند داده‌های ممیزی تولیدشده را در خود ذخیره کند.	
۶	**محل ذخیره‌سازی داده‌های ممیزی ۳**
درصورتی‌که حافظه محلی محصول پرشده باشد و ظرفیتی برای ذخیره‌سازی داده‌های ممیزی نداشته باشد، محصول مورد ارزیابی باید [انتخاب: داده‌های ممیزی جدید را کنار بگذارد، سوابق ممیزی گذشته را بر اساس این قوانین بازنویسی[۱] کند: [اختصاص: قوانین بازنویسی سوابق ممیزی گذشته]، [اختصاص: اقدامات دیگر]]. **نکته کاربردی ۷:** درصورتی‌که حافظه محلی پرشده باشد، سرور خارجی ثبت رویدادها[۲] می‌تواند به‌عنوان فضای ذخیره‌سازی جایگزین مورداستفاده قرار گیرد. «اقدامات دیگر» که در بخش «اختصاص» ذکرشده است، می‌تواند مواردی ازجمله «ارسال داده‌های ممیزی جدید به یک موجودیت IT خارجی» را شامل شود. برای هر محصولات توزیع‌شده، نیاز نیست که هر مؤلفه داده‌های ممیزی را به صورت محلی ذخیره نماید ولی به طور کلی محصول باید توانایی ذخیره‌ی محلی داده‌های ممیزی را داشته باشد. هر مؤلفه حداقل باید توانایی ذخیره موقت اطلاعات ممیزی برای مواردی را که ارتباط شبکه دچار مشکل می‌شود، داشته باشد. نیاز نیست که ذخیره موقت بر روی حافظه ثابت صورت گیرد، این ذخیره محلی می‌تواند روی حافظه فرار انجام گیرد. برای هر مؤلفه که اطاعات را به صورت محلی ذخیره می‌نماید یا اطلاعات ممیزی را به صورت موقت ذخیره می‌کند، باید مشخص شود هنگام پر شدن حافظه، چه اقدامی صورت گیرد.	

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]

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

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**
محصول مورد ارزیابی باید بر اساس الگوریتم‌های تولید کلید رمزنگاری، کلیدهای رمزنگاری نامتقارن را تولید کند: [انتخاب: • الگوهای RSA با استفاده از کلیدهای رمزنگاری با اندازه‌های ۲۰۴۸ بیت یا بزرگ‌تر که این الزامات را رعایت کنند: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.3؛ • الگوهای ECC با استفاده از «منحنی‌های NIST» [انتخاب: P-256, P-384, P-521] بر اساس این الزامات: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.4. • الگوهای FFC با استفاده از کلیدهای رمزنگاری با اندازه‌های ۲۰۴۸ بیت یا بزرگ‌تر که این الزامات را رعایت کنند: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.1. **نکته کاربردی ۸:** نویسنده هدف امنیتی، تمام الگوهای تولید کلید مورداستفاده برای استقرار کلید و احراز هویت دستگاه‌ها را انتخاب می‌کند. درصورتی‌که برای استقرار کلید از الگوهای تولید کلید استفاده شود، الگوهای لیست‌شده در «مدیریت کلید رمزنگاری ۲» و پروتکل‌های رمزنگاری انتخاب‌شده باید مطابق با انتخاب باشند. درصورتی‌که برای احراز هویت دستگاه از الگوهای تولید کلید، غیر از ssh-rsa، ecdsa-sha2-nistp256، ecdsa-sha2-nistp384 و ecdsa-sha2-nistp521 استفاده شود، انتظار می‌رود که کلید عمومی مرتبط با یک گواهی‌نامه X.509v3 باشد. اگر محصول مورد ارزیابی به‌عنوان یک دریافت‌کننده در الگوهای استقرار کلید عمل کند و برای پشتیبانی از احراز هویت مشترک پیکربندی نشده باشد، محصول نیاز به پیاده‌سازی تولید کلید ندارد. در محصول مورد ارزیابی توزیع‌شده، اگر مؤلفه محصول به‌عنوان یک دریافت‌کننده در الگوی استقرار کلید عمل کند، محصول نیاز به پیاده‌سازی تولید کلید ندارد.	
۸	**مدیریت کلید رمزنگاری ۲**
محصول مورد ارزیابی باید استقرار کلید[۱] رمزنگاری را بر اساس یک روش خاص استقرار کلید رمزنگاری انجام دهد: [انتخاب:	

[۱] Key establishment

شماره الزام	نام الزام

- الگوهای استقرار کلید RSA که این الزامات را رعایت کنند: انتشار ویژه NIST 800-56B بازبینی ۱، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری فاکتورگیری عدد صحیح»[۱]؛
- الگوهای استقرار کلید منحنی بیضوی[۲] که این الزامات را رعایت کنند: انتشار ویژه NIST 800-56A بازبینی ۲، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته»[۳]؛
- الگوهای استقرار کلید میدانی[۴] که این الزامات را رعایت کنند: انتشار ویژه NIST 800-56A بازبینی ۲، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته».
- الگوی استقرار کلید با استفاده از دیفی-هلمن گروه ۱۴ که این الزامات را رعایت کنند: RFC 3526، بخش۳؛

نکته کاربردی ۹:

این عنصر درواقع نسخه اصلاح‌شده الزام «مدیریت کلید رمزنگاری۲»[۵] در استاندارد ISO 15408 است که به‌جای توزیع کلید، به استقرار کلید می‌پردازد.

نویسنده هدف امنیتی، تمام الگوهای استقرار کلید مورداستفاده برای پروتکل‌های رمزنگاری منتخب را انتخاب می‌کند. برای دیفی-هلمن گروه ۱۴، نویسنده هدف امنیتی باید به جای انتخاب استقرار کلید میدانی، از الزام کارکردی امنیتی یک انتخاب مناسب انجام دهد.

الگوهای استقرار کلید مبتنی بر RSA در بخش ۹، بازبینی ۱، مربوط به NIST SP 800-56B تشریح شده‌اند؛ اما این بخش وابسته به پیاده‌سازی موارد مذکور در سایر بخش‌های بازبینی ۱ مربوط به SP 800-56B است.

توجه: اگر محصول مورد ارزیابی در الگوی استقرار کلید به‌عنوان گیرنده عمل کند، نیازی نخواهد بود که محصول، الگوی تولید کلید RSA را اجرا نماید.

منحنی‌های بیضوی مورداستفاده در الگوهای استقرار کلید، با منحنی‌های مشخص‌شده در الزام شماره‌ی ۷ «مدیریت کلید رمزنگاری ۱» ارتباط دارند.

پارامترهای دامنه مورداستفاده در الگوهای استقرار کلید میدانی، به الگوهای تولید کلید مورداشاره در «مدیریت کلید رمزنگاری ۱» وابسته هستند.

---

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

شماره الزام	نام الزام
۹	**مدیریت کلید رمزنگاری ۴**

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

- برای کلیدهای متن-آشکار در ذخیره‌ساز فرار[۱]، نابودی باید از طریق یک [انتخاب: بازنویسی ساده شامل [انتخاب: الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی، صفرها، یک‌ها، یک مقدار جدید از کلید، [اختصاص: یک مقدار ثابت یا پویا که شامل هیچ CSP نباشد]]، نابودی مرجع کلید که مستقیماً با درخواست زباله‌روبی همراه باشد] انجام شود.
- برای کلیدهای متن-آشکار در ذخیره‌ساز غیرفرار، نابودی باید از طریق فراخوان[۲] یک واسط مهیا شده توسط محصول مورد ارزیابی که [انتخاب:
  - بصورت منطقی مکان ذخیره‌سازی کلید را آدرس می‌دهد و یک بازنویسی [انتخاب: ساده، [اختصاص: تعداد عبورها]-عبور] شامل [انتخاب: الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی، صفرها، یک‌ها، یک مقدار جدید از کلید، [اختصاص: یک مقدار ثابت یا پویا که شامل هیچ CSP نباشد]] را انجام می‌دهد.
  - یک بخشی از توابع امنیتی محصول را برای نابودی انتزاع معرف کلید، می‌سازد]

انجام شود.]

نکته کاربردی ۱۰:

در قسمت مربوط به انتخاب در گزینه دوم از اولین اختصاص، جاییکه کلیدها برای نابودی به‌وسیله «یک بخشی از توابع امنیتی محصول» شناسایی می‌شوند، خلاصه مشخصات محصول باید «بخش» مربوطه و واسط مرتبط با آن را تعریف نماید. واسط اشاره شده در الزام می‌تواند در محصولات مختلف، شکل متفاوتی داشته باشد. شاید مشهودترین شکل آن یک برنامه کاربردی روی یک سیستم عامل باشد.

وقتی که روش‌های تخریب مختلفی برای کلیدهای مختلف و/یا موقعیت‌های تخریب مختلف استفاده می‌شود، این روش‌ها و کلیدها/موقعیت‌های متفاوت بکار گرفته شده، در خلاصه مشخصات محصول توصیف می‌شوند. خلاصه مشخصات محصول همه کلیدهای مرتبط استفاده شده در پیاده‌سازی الزامات کارکرد امنیتی را توصیف می‌نماید، همچنین مواردی که محل ذخیره شدن کلیدها بصورت متن آشکار است را شامل می‌شود.

در بعضی از اختصاص‌های بالا، از «شامل هیچ CSP نباشد» استفاده شده است. این جمله به این معنی است که محصول از برخی داده خاص استفاده می‌کند که شامل هیچ کدام از مقادیر تولید شده توسط تولیدکننده بیت تصادفی موجود در الزام

[۱] Volatile Storage

[۲] Invocation

شماره الزام	نام الزام
FCS_RBG_EXT یا مقادیر مشخص لیست شده در این الزام، مثلا موارد لیست شده در اولین انتخاب از اولین اختصاص این الزام نیست. در واقع وجود عبارت «شامل هیچ CSP نباشد» برای مطمئن شدن از این موضوع است که حتما بازنویسی داده با دقت انتخاب شده است. لازم به ذکر است که کلیدهای رمزنگاری در این الزام، شامل کلیدهای نشست نیز می‌شود. همچنین تخریب کلید برای مؤلفه عمومی در جفت کلید نامتقارن، اعمال نمی‌شود.	
۱۰	**عملیات رمزنگاری ۱ (۱)**
محصول مورد ارزیابی باید رمزگذاری و رمزگشایی را بر اساس الگوریتم‌های رمزنگاری خاص [اختصاص: الگوریتم AES که در حالت [انتخاب: CBC، GCM، CTR] و در اندازه‌های کلید [انتخاب: ۱۲۸ بیتی، ۱۹۲ بیتی، ۲۵۶ بیتی] استفاده می‌شوند] و با توجه به [اختصاص: استاندارد AES که در ISO 18033-3 تعریف‌شده است، [انتخاب: CBC که در ISO 10116 تعریف‌شده است، GCM که در ISO 19772 تعریف‌شده است، CTR که در ISO 10116 تعریف شده است]] انجام دهد. **نکته کاربردی ۱۱:** در مورد نخستین انتخاب این الزام، نویسنده هدف امنیتی حالت یا حالت‌های کارکردی AES را انتخاب می‌کند. در مورد دومین انتخاب، نویسنده هدف امنیتی اندازه کلیدهای پشتیبانی شده توسط این کارکرد را انتخاب می‌کند. حالت‌ها و اندازه کلیدهای انتخاب‌شده در این مرحله، متناظر با انتخاب مجموعه رمز[۱] در الزامات کانال امن هستند.	
۱۱	**عملیات رمزنگاری ۱ (۲)**
محصول مورد ارزیابی باید سرویس‌ها امضای رمزنگاری (تولید و تائید) را بر اساس الگوریتم‌های رمزنگاری زیر ارائه کند: [انتخاب: • الگوریتم امضای دیجیتال RSA و کلید رمزنگاری با اندازه‌های (ماژول‌ها) [اختصاص: ۲۰۴۸ بیتی یا بزرگ‌تر] • الگوریتم امضای دیجیتال بیضوی و کلید رمزنگاری با اندازه‌های [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،	

[۱] Cipher suite

شماره الزام	نام الزام
• در مورد الگوهای ECDSA: FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۶ و پیوست D، با اجرای منحنی‌های [انتخاب: P-256، P-384، P-521]؛ ISO/IEC 14888-3، بخش ۶,۴ [**نکته کاربردی ۱۲:** نویسنده هدف امنیتی الگوریتم(های) مورد استفاده برای اجرای امضای دیجیتال را انتخای می‌کند. برای الگوریتم‌های انتخاب‌شده، نویسنده هدف امنیتی انتخاب‌ها و اختصاص‌های مناسب را انجام می‌دهد و پارامترهای الگوریتم‌ها را به شکل مناسب تعیین می نماید. نویسنده هدف امنیتی، با استفاده از انتخاب‌ها و اختصاص‌های این الزام، از شامل شدن تمامی مقادیر پارامترهای ضروری برای مجموعه رمز انتخاب شده به‌وسیله الزامات سند هدف امنیتی، اطمینان پیدا می‌نماید. نویسنده هدف امنیتی همچنین سازگار بودن انتخاب‌های انجام گرفته شده با دیگر الزامات رمزنگاری را بررسی می‌کند، خصوصاً زمانی که از منحنی‌های بیضوی پشتیبانی شود.	
۱۲	**عملیات رمزنگاری ۱ (۳)**
محصول مورد ارزیابی باید سرویس‌ها درهم‌سازی رمزنگاری را بر اساس یک الگوریتم رمزنگاری مشخص [انتخاب: SHA-1، SHA-256، SHA-384، SHA-512] و اندازه‌های خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیتی که [اختصاص: ISO/IEC 10118-3:2004] را رعایت کند، ارائه نماید. **نکته کاربردی ۱۳:** به تولیدکنندگان اکیداً توصیه می‌شود که از پروتکل‌های به‌روزرسانی شده‌ای که از خانواده SHA-2 پشتیبانی می‌نمایند، استفاده کنند. تا زمانی که پروتکل‌های به‌روز شده پشتیبانی شوند، این پروفایل حفاظتی اجازه پشتیبانی از SHA-1 را بر اساس SP 800-131A فراهم می‌کند. توجه: طبق SP 800-131 A الگوریتم SHA-1 فقط می‌تواند برای عملیات‌های غیر از امضای دیجیتال همچون درهم سازی پسورد و ... استفاده شود. در نسخه‌های آتی این پروفایل حفاظتی، SHA-256 کمینه الزام برای محصولات خواهد بود. انتخاب درهم‌ساز باید بر اساس قدرت کلی الگوریتم مورداستفاده برای الزام «عملیات رمزنگاری ۱(۱)» و الزام «عملیات رمزنگاری ۱(۲)» انجام شود (مثلاً SHA 256 برای کلیدهای ۱۲۸ بیتی).	
۱۳	**عملیات رمزنگاری ۱ (۴)**

شماره الزام	نام الزام
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 با استفاده از اندازه‌های کلید [اختصاص: اندازه کلید مورداستفاده در HMAC (بر حسب بیت)] و اندازه‌های 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 ۱۴:** اندازه کلید k در عبارت «اختصاص» بین L1 و L2 خواهد بود (که در ISO/IEC 10118 مربوط به توابع درهم‌ساز تعریف شده است). به عنوان مثال، در مورد SHA-256 داریم: L1=512, L2=256 که L2<=k<=L1.	
۱۴	**تولید بیت تصادفی ۱**
محصول مورد ارزیابی باید سرویس‌ها تولید بیت تصادفی را بر اساس ISO/IEC 18031:2011 و با استفاده از [انتخاب: Hash_DRBG، HMAC_DRBG، CTR_DRBG (AES)] ارائه دهد.	
۱۵	**تولید بیت تصادفی ۲**
RBG قطعی باید دست کم توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی را از [انتخاب: [اختصاص: تعداد منابع مبتنی بر نرم افزار] منبع نویز مبتنی بر نرم‌افزار، [اختصاص: تعداد منابع مبتنی بر سخت افزار] منبع نویز مبتنی بر سخت‌افزار] گردآوری کند. این آنتروپی باید دست کم [انتخاب: ۱۲۸ بیت، ۱۹۲ بیت، ۲۵۶ بیت] و حداقل معادل بالاترین قدرت امنیتی کلیدها و CSPs که تولید می‌کند، مطابق باISO/IEC 18031:2011، باشد. **نکته کاربردی ۱۵:** در مورد نخستین عبارت این الزام، نویسنده هدف امنیتی حداقل یکی از انواع منابع نویز را انتخاب می‌کند. اگر محصول مورد ارزیابی شامل چند منبع نویز از یک نوع باشد، نویسنده هدف امنیتی عبارت اختصاص را با تعداد مناسبی از هر یک از انواع منابع پر می‌کند (مثلاً دو منبع نویز مبتنی بر نرم‌افزار و یک منبع نویز مبتنی بر سخت‌افزار). مستندات و آزمون‌های مورد نیاز در فعالیت‌های ارزیابی، باید تکرار گردند تا تمام منابع مشخص شده در هدف امنیتی را پوشش دهند. سند ISO/IEC 18031:2011 شامل سه روش مختلف تولید اعداد تصادفی است که هر یک از آن‌ها به عناصر اولیه فرایند رمزنگاری (توابع درهم‌ساز و مجموعه‌های رمز) بستگی دارد. نویسنده هدف امنیتی، تابع استفاده شده و شامل عناصر اولیه فرایند رمزنگاری را که در الزام بکار گرفته شده است، انتخاب خواهد کرد. با اینکه تمام توابع درهم‌ساز تعیین‌شده (SHA-1، SHA-256، SHA-384، SHA-512) را می‌توان در	

[1] Keyed-hash message authentication

شماره الزام	نام الزام
Hash_DRBG یا HMAC_DRBG مورداستفاده قرار داد، در پیاده‌سازی‌های CTR_DRBG تنها موارد مبتنی بر AES اجازه استفاده دارند. اگر اندازه کلید برای پیاده‌سازی AES متفاوت با اندازه کلید مورداستفاده برای رمزگذاری داده‌های کاربری باشد، ممکن است نیاز به تغییر یا تکرار «عملیات رمزنگاری» باشد تا تفاوت اندازه کلید در آن لحاظ گردد. در قسمت انتخاب تعداد بیت آنتروپی مربوط به این الزام، نویسنده هدف امنیتی حداقل تعداد بیت‌های انتروپی تزریق‌شده به RBG را انتخاب می‌کند که این مقدار باید بزرگتر یا مساوی طول هر کلید امنیتی باشد که توسط محصول تولید می‌شود.	

۳,۳ کلاس شناسایی و احراز هویت

محصول، یک سازوکار 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 سازوکاری 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**
محصول مورد ارزیابی باید وقتی که یک عدد مثبت قابل تنظیم توسط سرپرست در [اختصاص: بازه مقادیر قابل‌قبول]، از تلاش‌های ناموفق احراز هویت مرتبط با تلاش‌های سرپرستان برای احراز هویت راه‌دور اتفاق میافتد را تشخیص دهد.	
۱۷	**مدیریت احراز هویت ناموفق ۲**
زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده برسد، محصول مورد ارزیابی باید [انتخاب: سرپرست راه‌دور تخطی‌کننده را از احراز هویت موفق جلوگیری نماید تا وقتی که یک [اختصاص: اقدام] توسط یک سرپرست محلی صورت گیرد، سرپرست راه‌دور تخطی‌کننده را از احراز هویت موفق جلوگیری نماید تا وقتی که یک دوره زمانی تعریف شده توسط سرپرست سپری شود.] انجام دهد. **نکته کاربردی ۱۶:**	

این الزام روی یک تعداد تلاش پی‌درپی احراز هویت ناموفق اعمال می‌شود و برای یک سرپرست در کنسول محلی اعمال نمی‌گردد، زیرا قفل کردن یک سرپرست محلی، مد نظر نیست. نیل به این مهم نیازمند وجود حساب‌های سرپرستی محلی و راه‌دور جداگانه یا داشتن سازوکار احرازهویتی است که بتواند تلاش‌های ورود سرپرست محلی و راه‌دور را بصورت متمایز پیاده‌سازی نماید. عبارت «اقدام» در اختصاص این الزام، توسط یک سرپرست محلی اتخاذ می‌گردد و در واقع یک پیاده‌سازی خاص است که توسط راهنمای سرپرست[۱] تعریف می‌شود (مثل بازنشاندن رمزعبور[۲]، بازنشاندن قفل[۳]). نویسنده هدف امنیتی یک از گزینه‌های انتخاب در این الزام را برای کنترل کردن شکست‌های احراز هویت، بسته به نوع پیاده‌سازی کنترل‌کننده در محصول، گزینش می‌نماید.

خلاصه مشخصات محصول باید توصیف نماید که محصول چگونه این اطمینان را ایجاد می‌کند که مسدود شدن موقت یا دائم یک سرپرست راه‌دور بدلیل شکست‌های احراز هویت، باعث بوجود آمدن عدم دسترس‌پذیری سرپرست نمی‌گردد (مثال: با تعریف کردن یک ورود محلی که مسدود سازی برای آن اعمال نمی‌شود). راهنمای محیط عملیاتی مشخص می‌سازد که چگونه همیشه یک دسترسی سرپرست نگه‌داری می‌شود حتی در صورتی که یک سرپرست راه‌دور در اثر موارد مطرح شده در این الزام، مسدود گردد.

۱۸	**مدیریت رمز عبور ۱**

محصول مورد ارزیابی باید قابلیت‌های مدیریت گذرواژه زیر را برای کلمه‌ی عبور سرپرست اجرایی محصول فراهم آورد:

الف) گذرواژه را باید بتوان با هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای ویژه مطرح شده در این بخش ساخت: [انتخاب: "(", ")", "*", "&", "^", "%", "$", "#", "@", "!"، [اختصاص: سایر کارکترها]]؛

ب) حداقل طول گذرواژه باید قابل پیکربندی به [اختصاص: کمترین تعداد کاراکترهای قابل پشتیبانی توسط محصول] و [اختصاص: تعداد کاراکترهای بزرگتر مساوی با ۱۵]باشد.

نکته کاربردی ۱۷:

نویسنده هدف امنیتی کاراکترهای ویژه قابل استفاده در گذرواژه را انتخاب می‌کند. وی می‌تواند با استفاده از عبارت اختصاص در بند الف، کاراکترهای دیگری را به لیست اضافه کند. منظور از «کلمه‌ی عبور سرپرست اجرایی»، گذرواژه‌هایی هستند که توسط مدیران سیستم در کنسول محلی روی پروتکل‌هایی که از آن‌ها پشتیبانی می‌کنند مانند، SSH و HTTPS، مورد استفاده قرار می‌گیرند. این گذرواژه‌ها گاهی نیز برای ارائه آن دسته از داده‌های پیکربندی که از دیگر الزامات کارکرد امنیتی در محصول پشتیبانی می‌کنند، مورد استفاده قرار می‌گیرند.

اختصاص مطرح شده در بند ب، باید به بزرگترین مقداری که می‌تواند برای کمینه طول رمزعبور توسط سرپرست پیکربندی شود، تنظیم گردد.

---

[۱] Administrator guidance

[۲] Password reset

[۳] Lockout reset

۱۹	شناسایی و احراز هویت کاربر ۱

محصول مورد ارزیابی پیش از آن که از دیگر موجودیت‌های خارج از محصول بخواهد که فرایند تعیین و احراز هویت را انجام دهد، باید اجازه انجام فعالیت‌های زیر را بدهد:

- نمایش بنر اخطار با توجه به الزام FTA_TAB.1
- [انتخاب: هیچ اقدامی، [اختصاص: لیست سرویس‌ها، اقدامات انجام‌شده توسط محصول مورد ارزیابی در پاسخ به درخواست‌های خارجی]]

۲۰	شناسایی و احراز هویت کاربر ۲

پیش از آن که محصول مورد ارزیابی امکان انجام اقدامات مدیریتی سیستم را فراهم آورد، باید هر مدیرسیستم را ملزم نماید که به صورت موفق شناسایی و احراز هویت گردد.

نکته کاربردی ۱۸:

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

احراز هویت می‌تواند مبتنی بر گذرواژه باشد و از طریق کنسول محلی و یا از طریق پروتکلی صورت گیرد که از گذرواژه‌ها پشتیبانی می‌کند (مانند SSH)، یا اینکه بر اساس گواهی‌نامه انجام شود (مانند SSH و TLS).

در مورد ارتباط با موجودیت‌های IT خارجی (مانند یک سرور ممیزی یا سرور NTP) این ارتباطات باید بر اساس الزام‌های FTP_ITC.1 انجام شوند که پروتکل آن از شناسایی و احراز هویت پشتیبانی می‌کند. این امر بدین معنی است که نیازی نیست ارتباطاتی از قبیل ایجاد ارتباط IPsec با سرور احراز هویت، در عبارت اختصاص ذکر شوند، زیرا ایجاد ارتباط به معنی آغاز فرایند شناسایی و احراز هویت است.

با توجه به نکته کاربردی مطرح شده در الزام FMT_SMR.2، برای محصولات توزیع‌شده، حداقل یکی از مؤلفه‌های محصول باید شناسایی و احراز هویت را برای سرپرست‌های امنیتی، مطابق با الزامات FIA_UIA_EXT.1 و FIA_UAU_EXT.2، اجرا نماید. این امر برای تمامی مؤلفه‌ها ضروری نیست. در مواردی که هیچ کدام از مؤلفه‌های این امر را پشتیبانی نمی‌کنند، خلاصه مشخصات محصول باید توضیح دهد که چگونه شناسایی و احراز هویت را برای سرپرست‌های امنیتی انجام می‌دهد.

۲۱	سازوکار احراز هویت بر اساس رمزعبور ۲

محصول مورد ارزیابی باید یک سازوکار محلی احراز هویت مبتنی بر گذرواژه و [انتخاب: [اختصاص: سایر سازوکارهای احراز هویت]، هیچ سازوکار دیگری] را برای احراز هویت کاربر محلی مدیر سیستم فراهم آورد.

نکته کاربردی ۱۹:

عبارت اختصاص باید برای مشخص کردن تمام سازوکارهای محلی احراز هویت پشتیبانی‌شده، اضافه بر موارد ذکر شده را نشان دهد. سازوکارهای احراز هویت محلی در واقع آن‌هایی هستند که از طریق کنسول محلی انجام می‌شوند. نشست‌های مدیریتی از راه‌دور (و سازوکارهای احراز هویت مربوط به آن‌ها) در الزام FTP_TRP.1/Admin مشخص شده‌اند.

با توجه به نکته کاربردی مطرح شده در الزام FMT_SMR.2، برای محصولات توزیع‌شده، حداقل یکی از مؤلفه‌های محصول باید شناسایی و احراز هویت را برای سرپرست‌های امنیتی، مطابق با الزامات FIA_UIA_EXT.1 و FIA_UAU_EXT.2، اجرا نماید. این امر برای تمامی مؤلفه‌ها ضروری نیست. در مواردی که هیچ کدام از مؤلفه‌های این امر را پشتیبانی نمی‌کنند، خلاصه مشخصات محصول باید توضیح دهد که چگونه شناسایی و احراز هویت را برای سرپرست‌های امنیتی انجام می‌دهد.

۲۲	احراز هویت کاربر ۱۰

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

نکته کاربردی ۲۰:

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

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

[۱] Obscured feedback

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)/ به روزرسانی امن**
محصول مورد ارزیابی باید توانایی فعال کردن توابع به‌منظور به‌روزرسانی دستی را به سرپرست‌های امنیتی محدود نماید. **نکته کاربردی ۲۱:** این الزام امکان آغاز به‌روزرسانی دستی را به سرپرست محصول امنیتی محدود می‌کند.	
۲۴	**مدیریت داده‌های محصول ۱**
محصول مورد ارزیابی باید امکان «مدیریت» داده‌های توابع امنیتی محصول را به سرپرست‌های امنیتی محدود کند. **نکته کاربردی ۲۲:** منظور از «مدیریت» می‌تواند هر یک از این اقدامات و موارد دیگری از این دست باشد: تولید، آغاز، بازدید، تغییر پیش‌فرض، تغییر، پاک کردن و اضافه نمودن. الزام حاضر همچنین شامل بازگرداندن گذرواژهکاربری به حالت پیش‌فرض توسط سرپرست محصول امنیتی است. عبارت "CoreData" در نام این الزام برای جداسازی آن با الزام ذکر شده در قسمت الزامات اختیاری با نام FMT_MTD.1/CryptoKeys است.	
۲۵	**کارکرد مدیریتی محصول ۱**
محصول مورد ارزیابی باید قابلیت انجام کارکردهای مدیریتی زیر را داشته باشد: [اختصاص: • اداره کردن محصول به‌صورت محلی و راه‌دور • پیکربندی بنر دسترسی	

شماره الزام	نام الزام

- پیکربندی زمان غیرفعال بودن نشست پیش از قفل‌کردن یا خاتمه دادن آن
- به‌روزرسانی محصول مورد ارزیابی و تائید به‌روزرسانی‌ها با استفاده از[انتخاب: امضای دیجیتال، مقایسه درهم‌سازی] پیش از نصب شدن این به‌روزرسانی‌ها
- پیکربندی پارامترهای شکست احراز هویت برای الزام FIA_AFL.1
- [انتخاب:
  - پیکربندی رفتار ممیزی
  - پیکربندی لیست سرویس‌ها ارائه‌شده توسط محصول مورد ارزیابی پیش از شناسایی یا احراز هویت یک موجودیت، مشخص شده در الزام FIA_UIA_EXT.1
  - پیکربندی کارکرد رمزنگاری
  - پیکربندی حد آستانه برای ایجاد مجدد کلید در پروتکل SSH
  - پیکربندی طول عمر برای IPSec SAs
  - پیکربندی تعامل بین مؤلفه‌های محصول
  - فعال‌سازی مجدد حساب سرپرست
  - تنظیم زمان برای مهرهای زمانی
  - پیکربندی شناساننده مرجع برای همتا
  - هیچ قابلیت دیگری]

نکته کاربردی ۲۳:

محصول مورد ارزیابی باید به طور کلی، قابلیت کارکردی را برای سرپرستی محلی و راه‌دور فراهم آورد. این پروفایل حفاظتی کارکرد مدیریت امنیتی خاصی را برای واسط سرپرستی محلی یا راه‌دور، مشخص نمی‌نماید، بلکه خلاصه مشخصات محصول باید این کار را برای هر واسط معرفی نماید. این کارکردها شامل پیکربندی بنر دسترسی برای الزام FTA_TAB.1 و زمان غیر فعال بودن نشست برای الزام FTA_SSL_EXT.1 و FTA_SSL.3 هستند.

- آیتم «به‌روزرسانی محصول مورد ارزیابی و تائید به‌روزرسانی‌ها با استفاده از امضای دیجیتال پیش از نصب شدن این به‌روزرسانی‌ها»، شامل توابع مدیریتی مربوطه در الزامات FMT_MOF.1/ManualUpdate و FMT_MOF.1/AutoUpdate (در صورت ذکر شدن در سند هدف ارزیابی) و الزامات FIA_X509_EXT.2.2 و FPT_TUD_EXT.1.2 و FPT_TUD_EXT.2.2 (اگر شامل اقدام قابل‌پیکربندی توسط سرپرست باشد و در صورت ذکر شدن در سند هدف ارزیابی)

شماره الزام	نام الزام

است. به‌طور مشابه، گزینه «پیکربندی رفتار ممیزی»، شامل توابع مدیریتی مربوطه در الزامات FMT_MOF.1/Services و FMT_MOF.1/Functions (در صورت وجود آن‌ها در سند هدف ارزیابی)، است.

- اگر محصول امکان مسدودسازی شدن به صورت inline را برای حساب سرپرست راه‌دور قرار داده باشد، آنگاه نویسنده هدف ارزیابی باید گزینه «فعال سازی مجدد حساب سرپرست» را انتخاب کند تا به سرپرست محلی امکان فعال‌سازی مجدد داده شود.
- اگر محصول مورد ارزیابی پیش از شناسایی و احراز هویت، امکان پیکربندی رفتار ممیزی و سرویس‌ها موجود را برای سرپرست محصول فراهم کند، یا امکان پیکربندی هر یک از کارکردهای رمزنگاری محصول مورد ارزیابی وجود داشته باشد، نویسنده هدف امنیتی باید گزینه یا گزینه‌های مناسب را در دومین عبارت «انتخاب» برگزیند و در غیر این صورت گزینه «هیچ قابلیت دیگری» را انتخاب کند.
- اگر محصول، پیکربندی حدآستانه‌ها برای سازوکارهای استفاده شده در الزامات FCS_SSHC_EXT.1.8 و FCS_SSHS_EXT.1.8 (چنین پیکربندی‌هایی نیازمند وجود الزام FMT_MOF.1/Functions در سند هدف ارزیابی است) را پشتیبانی کند، آنگاه باید گزینه «پیکربندی حد آستانه برای ایجاد مجدد کلید در پروتکل SSH» در سند هدف ارزیابی آورده شود. همچنین اگر محصول محدودیت‌هایی را در مقادیر قابل‌قبول برای آستانه‌ها اعمال می‌نماید، این محدودیت‌ها باید در خلاصه مشخصات محصول ذکر گردد.
- اگر محصول به سرپرست اجازه تنظیم زمان دستگاه که در مهرهای زمانی استفاده می‌شود را بدهد، آنگاه باید گزینه «تنظیم زمان برای مهرهای زمانی» در سند هدف ارزیابی آورده شود. زمانی که محصول اجازه تنظیم دستی زمان را نمی‌دهد و با یک سرور خارجی مانند سرور NTP، هماهنگی را انجام می‌دهد، گزینه ذکر شده نباید انتخاب گردد.
- اگر محصول از ارتباطات امن به‌وسیله پروتکل IPSec پشتیبانی می‌کند و الزامات FCS_IPSEC_EXT.1 در سند هدف ارزیابی بیان شده است، آنگاه باید گزینه «پیکربندی شناساننده مرجع برای همتا» در سند هدف ارزیابی آورده شود. برای محصولات که فقط از شناسانندهایی مانند آدرس IP و FQDN پشتیبانی می‌کنند، پیکربندی شناساننده مرجع ممکن است با پیکربندی نام همتا برای ارتباط، یکسان باشد.
- برای محصولات توزیع‌شده، تعامل بین مؤلفه‌های محصول قابل پیکربندی خواهد بود (باتوجه به الزام FCO_CPC_EXT.1). بنابراین، نویسنده سند هدف ارزیابی باید گزینه «پیکربندی تعامل بین مؤلفه‌های محصول» را برای محصولات توزیع‌شده انتخاب نماید. تغییر در مدیریت محصول، از «مستقیماً توسط سرپرستی راه‌دور» به «سرپرستی راه‌دور از طریق مؤلفه‌ی دیگر» می‌تواند به عنوان یک مثال برای پیکربندی تعاملات باشد.

شماره الزام	نام الزام
۲۶	**نقش‌های امنیتی ۳**
محصول باید نقش‌های زیر را نگهداری کند. • سرپرست امنیتی	
۲۷	**نقش‌های امنیتی ۴**
محصول مورد ارزیابی باید بتواند بین کاربران و نقش‌ها ارتباط برقرار نماید.	
۲۸	**نقش‌های امنیتی ۵**
محصول مورد ارزیابی باید از برقرار بودن شرایط زیر اطمینان حاصل کند: • نقش سرپرست امنیتی، باید بتواند محصول مورد ارزیابی را به صورت محلی اداره کند. • نقش سرپرست امنیتی، باید بتواند محصول مورد ارزیابی را از راه‌دور اداره کند. **نکته کاربردی ۲۴:** بر اساس این الزام سرپرست امنیتی باید بتواند محصول مورد ارزیابی را از طریق یک کنسول محلی و یک سازوکار راه‌دور اداره کند. نویسنده سند هدف ارزیابی باید الزامات FTP_ITC.1، FPT_ITT.1 و/یا FTP_TRP.1/Admin را برای اثبات چگونگی به دست آمدن یک ارتباط امن، انتخاب نماید. برای محصولات توزیع‌شده، نیاز نیست که هر مؤلفه مدیریت خود برای این الزام را پیاده‌سازی کند. حداقل یک مؤلفه باید احراز هویت و شناسایی سرپرستان امنیتی را بر اساس الزامات FIA_UIA_EXT.1 و FIA_UIA_EXT.2 پشتیبانی نماید. برای اعمال شدن احراز هویت در دیگر مؤلفه‌ها، سرپرست امنیتی باید از طریق یک کانال امن (مطابق با الزامات FTP_ITC.1 یا FPT_ITT.1) و مؤلفه‌ای که احراز هویت و شناسایی را پشتیبانی می‌کند، با مؤلفه‌های دیگر ارتباط برقرار نماید. شناسایی کاربرها و ارتباط بین کاربران و نقش‌ها نیز از طریق مؤلفه‌ای که احراز هویت و شناسایی را پشتیبانی می‌کند، انجام می‌گیرد. برای دیگر مؤلفه‌ها نیاز نیست که از سرپرستی محلی مؤلفه (ذکر شده در الزام FMT_SMR.2.3) پشتیبانی کنند.	

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**
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 ۲۵:** 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 ۲۶:** 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.	

[۱] Plaintext

۳,۵,۱ آزمون محصول مورد ارزیابی

محصول مورد ارزیابی، برای اینکه برخی شکست‌های سازوکارهای 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.

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 سازوکار 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 ۲۷:

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.

شماره الزام	نام الزام
برای محصولات توزیع‌شده هر مؤلفه ملزم به اجرای خودآزمایی است. ولی الزامی وجود ندارد که همه مؤلفه‌ها خودآزمایی یکسانی را اجرا نمایند. نویسنده هدف امنیتی انتخاب‌های ممکن و سپس اختصاص‌های نهایی را برای هر مولفه توصیف می‌نماید. **نکته کاربردی ۲۸:** 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 سازوکارهای رمزنگاری را مورداستفاده قرار دهد و با استفاده از آن‌ها، به‌روزرسانی‌ها را تهیه و تدارک ببیند، رمزنگاری به‌روزرسانی‌ها را از طریق سازوکار 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	**به روز رسانی 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 ۲۹:** اگر امکان نصب یک به‌روزرسانی مورد اعتماد که همان لحظه فعال نمی‌گردد یعنی فعال‌سازی آن دارای تاخیر است، 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	

شماره الزام	نام الزام
	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	**به روز رسانی 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 سازوکار به‌روزرسانی دیگری پشتیبانی نکند]. **تذکر: در صورتی که نویسنده سند هدف امنیتی برای این الزام گزینه‌های به روزرسانی خودکار را انتخاب نماید لازم است الزام «مدیریت کارکرد در محصول مورد ارزیابی ۱ (۲)/به‌روزرسانی امن» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه نماید.** **نکته کاربردی ۳۰:** 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 سازوکار 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

[۱] active authorization

شماره الزام	نام الزام
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 کاملا خودکار فقط باید در حالتی که از سازوکار امضاء دیجیتال استفاده شده باشد، انتخاب گردد.	
۳۵	**به روز رسانی امن ۳**
محصول مورد ارزیابی باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از [انتخاب: سازوکار امضای دیجیتال، درهم‌ساز منتشرشده]، ابزاری را برای احراز هویت میان‌افزار آن‌ها در اختیار محصول مورد ارزیابی قرار دهد. **تذکر: در صورتی که از سازوکار امضای دیجیتال استفاده شود نیاز است الزام‌های «الزامات به روز رسانی ۴» و «الزامات به روزرسانی ۵» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه کند.** **نکته کاربردی ۳۱:** سازوکار 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 سازوکار اجرا شده توسط محصول مورد ارزیابی را تعیین نماید، هر دو سازوکار نیز می‌تواند مورد استفاده قرار گیرد. وقتی که از مقادیر هش منتشر شده برای امن کردن سازوکار 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/تولید کننده محصول به سرپرست امنیتی، یکی از فاکتورهای کلیدی برای حفاظت از سازوکار 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 است. 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.	

[۱] Authentic hash value

[۲] Verification

شماره الزام	نام الزام

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، درنظر گرفته می‌شود (وقتی تصدیق هش باموفقیت انجام شود)، زیرا انتظار می‌رود وقتی که به‌روزرسانی مد نظر باشد، سرپرست مقدار هش را روی محصول بارگذاری کند.

اگر سازوکار امضاء دیجیتال انتخاب گردد، تصدیق امضاء به‌وسیله خود محصول انجام می‌گیرد. برای سازوکار 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 ۳۲:

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

نکته کاربردی ۳۳:

اگر در سازوکار 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 ۳۴:

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 سازوکار 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

[۱] Firmware

شماره الزام	نام الزام
(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**
محصول مورد ارزیابی باید قابلیت ارائه مهرهای زمانی قابل‌اطمینان[۱] برای استفاده خودش را داشته باشد.	
۳۷	**مهرهای زمانی ۲**
محصول باید [انتخاب: به سرپرست امنیتی اجازه دهد که زمان را تنظیم نماید، زمان را با منابع خارجی زمان همگام سازد].	

نکته کاربردی ۳۵:

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 است. محصول به اطلاعات خارجی زمان و تاریخ وابسته است، این اطلاعات می‌تواند به صورت دستی توسط سرپرست امنیتی تهیه گردند 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 باید برگزیده شود. استفاده از یک ساعت بلادرنگ محلی با قابلیت همگام‌سازی خودکار با یک منبع خارجی (مثلا؛ سرور NTP) توصیه می‌گردد، ولی الزام نیست. همچنین برای ارتباط با یک منبع خارجی، استفاده از الزام FTP_ITC.1 اختیاری است 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 نیست، این تغییرات دیگر در حوزه تغییرات ناپیوسته زمان، قرار نمی‌گیرند.

[۱] Reliable time stamps

۳,۶ دسترسی به محصول

این بخش به تشریح الزامات امنیتی مربوط به نشست‌های سرپرست محصول محصول مورد ارزیابی می‌پردازد. هم نشست‌های محلی و هم نشست‌های راه‌دور پایش می‌شوند تا در صورت غیر فعال بودن شناسایی شوند و قفل شدن یا خاتمه یافتن آن‌ها نیز در صورت رسیدن به آستانه زمانی بررسی می‌شود. 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 غیر فعال بودن که توسط سرپرست محصول تعیین شده است، [انتخاب: • نشست را قفل کند – تمام فعالیت‌های مربوط به دسترسی به داده‌های کاربری و نمایش این داده‌ها، به جز فعالیت‌های مربوط به قفل‌گشایی نشست را غیر فعال کند و از سرپرست محصول بخواهد که پیش از قفل‌گشایی نشست، مجدداً احراز هویت نماید؛ • نشست را خاتمه دهد].	
۳۹	**قفل‌کردن و خاتمه دادن به نشست‌ها ۵**
در مورد نشست‌های تعاملی راه‌دور[۲]، درصورتی که نشست تعاملی برای مدت معینی غیرفعال باشد، محصول مورد ارزیابی باید نشست تعاملی خاتمه دهد. مدت زمان مجاز برای غیرفعال بودن توسط سرپرست محصول تعیین می‌شود.	
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**

[۱] Local interactive sessions

[۲] Remote

شماره الزام	نام الزام
قبل از ایجاد یک نشست کاربری سرپرست اجرایی[۱]، محصول مورد ارزیابی باید توصیه‌های مشخص شده توسط سرپرست امنیتی و همچنین تاییدیه استفاده از محصول مورد ارزیابی را نشان دهد. **نکته کاربردی ۳۶:** 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.

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.	

[۱] Administrative user

شماره الزام	نام الزام
	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 ۳۷:** هدف از الزام حاضر فراهم کردن روشی است که جهت حفاظت ارتباطات خارجی با موجودیت‌های معتبر IT، از پروتکل رمزنگاری استفاده گردد. منظوراز موجودیت‌های معتبر IT، موجودیت‌هایی است که محصول مورد ارزیابی برای انجام کارکردهای خود با آن‌ها ارتباط برقرار می‌کند. محصول مورد ارزیابی دست کم از یکی از پروتکل‌های 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 سازوکار یا سازوکارهای 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. 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**

شماره الزام	نام الزام
محصول، باید با استفاده از پروتکل [انتخاب: IPsec, SSH, TLS, DTLS, HTTPS] مسیر ارتباطی امنی را میان خود و سرپرست‌های راه‌دور مجاز که به طور منطقی از مسیرهای ارتباطی دیگر متمایز است را فراهم نماید و نقاط پایانی را به صورت مطمئن شناسایی کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات در داده کانال 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.**	
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 ۳۸:** 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، سازوکار یا سازوکارهای 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 دسترس پذیری 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.	

شماره الزام	نام الزام
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. **نکته کاربردی SIEM 2:** 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.	

شماره الزام	نام الزام
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 به‌صرف نظر نمودن از داده‌های جمع‌آوری‌شده‌ی SIEM نماید، از ذخیره‌سازی داده‌های جمع‌آوری‌شده‌ی SIEM به‌جز داده‌هایی که توسط کاربر مجاز تعیین می شوند جلوگیری نماید ، یا اقدام به بازنویسی بر روی قدیمی‌ترین داده‌های جمع‌آوری‌شده‌ی SIEMذخیره‌شده نماید*] و یک هشدار ارسال نماید. **نکته کاربردی SIEM 3:**	

[۱] Read Access

شماره الزام	نام الزام
در سند هدف امینتی 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	

۳,۹ 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.	

۶۶	ورود داده‌های کاربری به محصول ۲
محصول باید از مشخصه‌های امنیتی همراه با داده‌های کاربری ورودی استفاده نماید.	
۶۷	ورود داده‌های کاربری به محصول ۳
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	برچسب گذاری 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 توسعه دهندگان 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 توسعه دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده‌سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی‌باشد.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: مشخصات کارکرد ابتدایی۱

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**شماره مؤلفه: (ADV_FSP.1.1C)** **شرح مؤلفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی [۱]و پشتیبان کننده‌ی الزام کارکرد امنیتی[۲]توصیف نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.2C)** **شرح مؤلفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره 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.

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

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1E)** **شرح مؤلفه:** 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»، «آزمون» 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 ارائه دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو است.

۴,۲,۱ راهنمای کاربردی

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **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 دردسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.

مؤلفه‌های محتوایی	
نام خانواده	عنصر امنیتی
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ **شماره 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:** ارزیاب باید تائید نماید که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۴,۲,۲ راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)** **شرح مؤلفه:** توسعه دهنده 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 بایدتمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2C)**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	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 آزمون

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

۴,۳,۱ آزمون مستقل

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

مؤلفه‌های اقدامات توسعه دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** توسعه دهنده 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: آزمون مستقل ۱ **شماره مؤلفه: (ATE_IND.1.2E)**

مؤلفه‌های اقدامات ارزیاب	
	شرح مؤلفه: ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را آزمون 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:** توسعه دهنده 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:** 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 براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

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 توسعه دهنده 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، است (بدین معنی که جدا ار برچسب گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به تنهایی،

برچسب گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصول که توسط مرکز گواهی تائید شده است را به آسانی تشخیص دهد.

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

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

۴,۵,۲ حوزه پیکربندی

مؤلفه‌های اقدامات توسعه دهنده	
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:** 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 الزمات 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 تاکید کردن روی این موضوع است که الزام وقتی انتخاب می‌گردد که قابلیت‌های عملکردی مرتبط توسط محصول فراهم شده باشد و نیاز نیست که جهت انطباق با این پروفایل حفاظتی، محصول حتما 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 نیست.

۵,۱ کلاس ممیزی امنیت

درصورتی‌که در محصول مورد ارزیابی فضای حافظه محلی برای داده‌های ممیزی در نظر گرفته شده باشد، محصول مورد ارزیابی می‌تواند ادعا کند که مطابق آن چه در «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 است. 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 غیرفعال‌سازی ارتباطات مابین یک جفت از مؤلفه‌ها.	هویت‌های جفت نقاط انتهایی[۱] فعال یا غیرفعال شده

[۱] Endpoints pairs

نکته کاربردی ۳۹:

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.

شماره الزام	نام الزام
۶۸	**ذخیره‌سازی داده‌های ممیزی ۱**
محصول مورد ارزیابی باید از پاک شدن غیرمجاز داده‌های ممیزی جلوگیری نماید.	
۶۹	**ذخیره‌سازی داده‌های ممیزی ۱**
محصول مورد ارزیابی باید از دست‌کاری غیرمجاز داده‌های ممیزی جلوگیری نماید.	
۷۰	**محل ذخیره‌سازی داده‌های ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی**
محصول مورد ارزیابی باید در صورت پر شدن حافظه محلی، اطلاعات مربوط به تعداد داده‌های ممیزی [انتخاب: از بین رفته، بازنویسی شده را، [اختصاص: سایر اطلاعات]] ارائه کند. محصول مورد ارزیابی یکی از اقدامات تعیین‌شده در «محل ذخیره‌سازی داده‌های ممیزی ۳» را انجام می‌دهد. **نکته کاربردی ۴۰:** این گزینه باید انتخاب گردد، در صورتی که محصول مورد ارزیابی از این کارکرد پشتیبانی کند. درصورتی‌که حافظه محلی داده‌های ممیزی توسط سرپرست محصول خالی شود، شمارنده‌های مربوط به انتخاب انجام‌شده باید به مقادیر اولیه خود برگردند (این مقدار در اکثر موارد صفر است). سند راهنما باید به سرپرست محصول هشدار دهد که خالی کردن حافظه ممکن است سبب از دست رفتن داده‌ها شود. برای محصولات توزیع‌شده، هر مؤلفه که از دست رفتن داده ممیزی را شمارش می‌کند باید سازوکاری را برای سرپرست فراهم آورد که امکان دسترسی به اطلاعات و مدیریت اطلاعات داشته باشد.	

اگر این الزام در سند هدف امنیتی بیان گردد آنگاه نویسنده سند هدف امنیتی باید به صورت واضح هر شرایطی را که در آن شمارش از دست رفتن ممیزی انجام نمی‌گیرد، توضیح دهد.

۷۱	**ذخیره‌سازی رویدادهای ممیزی ۶/ فضای ذخیره‌سازی ممیزی محلی**

در صورتی که حجم داده‌های ممیزی از ظرفیت ذخیره‌سازی محلی داده‌های ممیزی فراتر رود/سرریز کند، محصول مورد ارزیابی باید با تولید اخطار، سرپرست را اگاه نماید.

نکته کاربردی ۴۱:

این گزینه باید انتخاب گردد، درصورتی‌که محصول مورد ارزیابی امکان تولید پیام برای سرپرست را وقتی حافظه محلی در نظر گرفته شده برای داده ممیزی پر می‌شود، داشته باشد. درصورتی‌که داده‌های مربوط به رویدادهای قابل‌ممیزی تنها در حافظه محلی ذخیره شده باشند، این هشدار می‌تواند اهمیت بسیار زیادی داشته باشد.

باید اطمینان حاصل نمود که هشدار مورد اشاره در «محل ذخیره‌سازی داده‌های ممیزی ۳» را می‌توان به اطلاع سرپرست رساند. از آنجایی که نمی‌توان تضمین کرد که در هنگام رخ دادن این رویداد (پر شدن حافظه)، نشست فعالی برای سرپرست اجرایی وجود داشته باشد، ارتباط باید از طریق سوابق ممیزی صورت گیرد.

وقتی که حافظه محلی برای ذخیره‌سازی داده ممیزی پر شد یا محصول به دلیل حافظه ناکافی با خطر از دست دادن داده مواجه شد، پیغام هشدار باید سرپرست را آگاه نماید.

برای محصولات توزیع‌شده که امکان نمایش پیغام هشدار را پیاده‌سازی می‌کنند، باید توضیح داده شود که کدام مؤلفه این ویژگی را پشتیبانی می‌نماید (وقتی که این ویژگی برای یک محصول انتخاب می‌گردد، نیاز نیس که تمامی مؤلفه‌های محصول آن را پشتیبانی نمایند). در نهایت هر مؤلفه‌ای که این ویژگی را پشتیبانی می‌کند، باید یک پیغام هشدار را به‌وسیله خودش یا از طریق دیگر مؤلفه‌ها تولید نماید.

اگر این الزام در سند هدف امنیتی آورده شود، آنگاه نویسنده سند هدف امنیتی باید شرایطی را که تحت آن داده به صورت غیرقابل مشاهده حذف می‌شود، ذکر نماید.

۵,۲ کلاس شناسایی و احراز هویت

شماره الزام	نام الزام
۷۲	**الزامات پروتکل X509 (۱)/ تبادل داده کاربردی داخل محصول**

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

- تائید گواهی‌نامه RFC 5280 و تائید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.

- مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.
- محصول 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
- محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC 6960، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۶,۳، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵، هیچ روش فسخ] تائید کند.
- محصول 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-kp1 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.

نکته کاربردی ۴۲:

این الزام باید انتخاب گردد، در صورتی که محصول توزیع‌شده باشد و پروتکل(های) انتخاب شده در الزام FPT_ITT.1 از گواهی‌نامه‌های X.509 برای احراز هویت نظیر استفاده نمایند. در این مورد، از آنجایی که الزامات اضافه‌ای در الزام FCO_CPC_EXT.1 در رابطه با فعال و غیرفعال‌سازی کانال ITT وجود دارد، استفاده از لیست فسخ اختیاری است. در صورتی که بررسی لیست فسخ پشتیبانی نمی‌شود، نویسنده سند هدف امنیتی باید گزینه "هیچ روش فسخ" را انتخاب نماید. به هر حال، درصورت پشتیبانی، نویسنده سند هدف امنیتی باید مشخص نماید که از OCSP یا RCL استفاده می‌گردد.

محصول باید از حداقل طول مسیر برای دو گواهی‌نامه پشتیبانی کند. بدین معنی که محصول باید از یک سلسله مراتب گواهی‌نامه که حداقل از گواهی‌نامه ریشه خود-امضاء[۱] و گواهی‌نامه هویت محصول تشکیل شده باشد، پشتیبانی نماید.

سند خلاصه مشخصات محصول باید مشخص نماید که چه مواقعی بررسی وضعیت فسخ انجام می‌گیرد. انتظار می‌رود که وقتی از گواهی‌نامه در احراز هویت استفاده می‌گردد، وضعیت فسخ نیز بررسی گردد. بررسی وضعیت یک گواهی‌نامه X509 فقط وقتی که روی دستگاه بارگذاری می‌شود، کافی نیست.

[۱] Self-signed root certificate

اگر محصول از هیچ کدام از موارد مطرح شده در قوانین extendedKeyUsage پشتیبانی نمی‌کند، این وضعیت باید در سند خلاصه مشخصات محصول شرح داده شود.

۷۳	**الزامات پروتکل X509 (۲)/ تبادل داده کاربردی داخل محصول**

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

نکته کاربردی ۴۳:

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.

۵,۳ کلاس مدیریت امنیت

شماره الزام	نام الزام
۷۴	**مدیریت کارکرد در محصول ۱ (۱)/ سرویس‌ها**

محصول مورد ارزیابی باید توانایی فعال و غیرفعال کردن سرویس‌ها و توابع را به سرپرست امنیتی محدود نماید.

نکته کاربردی ۴۴:

این گزینه فقط زمانی باید انتخاب گردد که سرپرست امنیتی محصول توانایی آغاز و توقف سرویس‌ها را داشته باشد. در این مورد گزینه "آغاز و توقف سرویس‌ها" باید در "انتخاب" الزام FAU_GEN.1.1 انتخاب گردد.

همچنین عبارت "سرویس" نیز در نکته کاربردی دوم مطرح شده در الزام FAU_GEN.1.1 توضیح داده شده است.

۷۵	**مدیریت داده‌های محصول ۱/ کلیدهای رمزنگاری**

محصول مورد ارزیابی باید توانایی مدیریت کردن کلیدهای رمزنگاری را به سرپرست امنیتی محدود نماید.

نکته کاربردی ۴۵:

این گزینه زمانی باید انتخاب گردد که سرپرست امنیتی امکان مدیریت کلیدهای رمزنگاری (برای مثال؛ اصلاح، حذف، تولید/واردکردن) را داشته باشد. این الزام مدیریت کلیدهای رمزنگاری را به سرپرست‌های امنیتی محدود می‌نماید. عبارت "CryptoKeys" برای جداسازی این تکرار الزام FMT_MTD.1 از تکرار اجباری آن با نام FMT_MTD.1/CoreData است.

۵,۴ کلاس حفاظت از محصول مورد ارزیابی

شماره الزام	نام الزام
۷۶	**انتقال داده امنیتی در داخل محصول ۱**
محصول باید از آشکارسازی داده توابع امنیتی محصول حفاظت کند و دست‌کاری/اصلاح در داده را وقتی که بین قسمت‌های مختلف محصول از طریق [انتخاب: IPsec، SSH، TLS، DTLS، HTTPS] مخابره می‌شود، تشخیص دهد. **نکته کاربردی ۴۶:** این الزام فقط برای محصولات توزیع‌شده قابل اعمال است و اطمینان پیدا می‌کند که تمام ارتباطات میان مؤلفه‌های محصول از طریق یک کانال ارتباطی رمزگذاری شده، حفاظت می‌گیرد. داده‌ای که از طریق این کانال ارتباطی مورداعتماد عبور داده می‌شود، به‌وسیله پروتکل انتخاب شده در عبارت "انتخاب" این الزام، رمزگذاری می‌گردد. نویسنده هدف امنیتی باید کانال‌ها و پروتکل‌های مورد استفاده توسط هر کدام از مؤلفه‌های یک ارتباط را مشخص نماید. این کانال ممکن است به عنوان کانال ثبت‌نام (داخل فرآیند ثبت‌نام در الزام FCO_CPC_EXT.1.2، توضیح داده شده است) استفاده گردد.	
۷۷	**مسیر امن ۱/ پیوند زدن**
محصول مورد ارزیابی باید مسیر ارتباطی میان خود و یک مؤلفه پیوندی[۱] که به طور منطقی از مسیرهای ارتباطی دیگر متمایز است را فراهم نماید و [انتخاب: نقطه‌پایانی توابع امنیتی محصول، هر دو مورد (مؤلفه پیوندی و نقطه‌پایانی توابع امنیتی محصول)] را به صورت مطمئن شناسایی کرده و داده‌های تبادلی را در برابر تغییر [انتخاب: و افشاء، هیچ مورد دیگری] محافظت نماید.	
۷۸	**مسیر امن ۲/ پیوند زدن**
محصول مورد ارزیابی باید به [انتخاب: توابع امنیتی محصول، مؤلفه پیوندی] اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	
۷۹	**مسیر امن ۳/ پیوند زدن**
محصول مورد ارزیابی باید برای پیوند مؤلفه‌ها به توابع امنیتی تحت شرایط/قیدهای محیط عملیاتی تعریف شده که در راهنمای عملیاتی مورد اشاره قرار گرفته است، استفاده از کانال امن را الزامی کند. **نکته کاربردی ۴۷:** این الزام (FTP_TRP.1/Join)، یکی از انواع کانال را که در اولین "انتخاب" در الزام FCO_CPC_EXT.1.2 بیان شده است، پیاده‌سازی می‌کند. عبارت "مؤلفه پیوندی" در الزام «مسیر امن ۱/پیوند زدن» در واقع یک موجودیت IT است که تلاش می‌کند از طریق فرآیند ثبت‌نام، به محصول توزیع‌شده بپیوندد.	

[۱] Joining

هدف از الزام این است که برای مؤلفه‌ها امکان ارتباط با یک شیوه امن در زمان تشکیل توابع امنیتی فراهم گردد.
دومین "انتخاب" در الزام «مسیر امن ۱/پیوند زدن» در واقع بیان می‌کند که در برخی موارد، کانال ممکن است محرمانگی (حفاظت از آشکارسازی داده) را فراهم نکند. بنابراین، نویسنده هدف امنیتی باید در خلاصه مشخصات محصول بیان کند که در این مورد آیا محصول محرمانگی را روی محیط الزام می‌کند (از طریق "شرایط/قیدهای محیط عملیاتی تعریف شده" در همین الزام) یا اینکه داده تبادل شده نیاز به محرمانگی ندارد.
توجه شود که وقتی از FTP_TRP.1/Join برای کانال ثبت‌نام استفاده شود، سپس این کانال نمی‌تواند به عنوان یک کانال عادی ارتباطات میان مؤلفه‌ای مورد استفاده قرار گیرد. باید از FPT_ITT.1 یا FTP_ITC.1 استفاده شود.

۵,۵ کلاس ارتباطات

شماره الزام	نام الزام
۸۰	**تعریف کانال ثبت‌نام مؤلفه ۱**
محصول باید سرپرست امنیتی را ملزم کند که قبل از اتفاق افتادن ارتباط میان هر جفت مؤلفه از محصول، برای آن‌ها یک ارتباط فعال نماید.	
۸۱	**تعریف کانال ثبت‌نام مؤلفه ۲**
محصول باید یک فرآیند ثبت‌نام را پیاده‌سازی کند که در آن مؤلفه‌ها یک کانال ارتباطات را منتشر و استفاده کنند که این کانال حداقل برای داده توابع امنیتی محصول از [انتخاب: • یک کانال که الزامات کانال امن را مطابق [انتخاب: FTP_ITC.1، FPT_ITT.1] رعایت کند. • یک کانال که الزامات کانال ثبت‌نام امن را مطابق FTP_TRP.1/Join رعایت کند. • هیچ کانالی] استفاده نماید.	
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 ۴۸:** 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 است. 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 بدلیل 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 سازوکارهایی 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 است. همانطور که در بخش‌های قبلی هم مطرح شده بود، در صورت نیاز باید به این جدول برای ثبت اطلاعات ممیزی مراجعه کرد.

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت شده
۱.	الزامات پروتکل DTLS Client	شکست درایجاد یک نشست DTLS	دلایل شکست
۲.	الزامات پروتکل DTLS Client/ احراز هویت	شکست درایجاد یک نشست DTLS	دلایل شکست
		تشخیص حملات تکرار	هویت منبع حمله تکرار (مثلا؛ آدرس IP)
۳.	الزامات پروتکل DTLS Server	شکست درایجاد یک نشست DTLS	دلایل شکست
		تشخیص حملات تکرار	هویت منبع حمله تکرار (مثلا؛ آدرس IP)

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت شده
۴.	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه	شکست درایجاد یک نشست DTLS	دلایل شکست
		تشخیص حملات تکرار	هویت منبع حمله تکرار (مثلا؛ آدرس IP)
۵.	الزامات پروتکل HTTPS	شکست درایجاد یک نشست HTTPS	دلایل شکست
۶.	الزامات پروتکل IPSEC	شکست در ایجاد یک SA مربوط به پروتکل IPSEC	دلایل شکست
۷.	الزامات پروتکل SSH Client	شکست درایجاد یک نشست SSH	دلایل شکست
		موفقیت در کلید دهی مجدد SSH	ارتباط با نقاط پایانی غیر محصول (آدرس IP)
۸.	الزامات پروتکلSSH Server	شکست درایجاد یک نشست SSH	دلایل شکست
		موفقیت در کلید دهی مجدد SSH	ارتباط با نقاط پایانی غیر محصول (آدرس IP)
۹.	الزامات پروتکل TLS Client/ احراز هویت	شکست در ایجاد یک نشست TLS	دلایل شکست
۱۰.	الزامات پروتکل TLS Client/ احراز هویت دو طرفه	شکست در ایجاد یک نشست TLS	دلایل شکست
۱۱.	الزامات پروتکل TLS Server/ احراز هویت	شکست در ایجاد یک نشست TLS	دلایل شکست
۱۲.	الزامات پروتکل TLS Server/ احراز هویت دو طرفه	شکست در ایجاد یک نشست TLS	دلایل شکست
۱۳.	الزامات پروتکل X509(۱) و (۲)/ ابطال	تلاش‌های ناموفق برای اعتبارسنجی یک گواهی‌نامه.	دلایل شکست
۱۴.	الزامات پروتکل X509(۳) و (۴)	-	-
۱۵.	الزامات پروتکل X509(۵) و (۶)	-	-
۱۶.	خودآزمایی محصول مورد ارزیابی ۲	شکست در خودآزمایی	دلایل شکست (شامل شناساننده گواهی‌نامه‌های غیرمعتبر)

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت شده
.۱۷	الزامات به روز رسانی امن ۴ و ۵	شکست در به‌روزرسانی	دلایل شکست (شامل شناساننده گواهی‌نامه‌های غیرمعتبر)
.۱۸	مدیریت کارکرد در محصول ۱/ به روزرسانی خودکار	فعال‌سازی و غیر فعال‌سازی جستجوی خودکار به‌روزرسانی‌ها یا به روزرسانی‌های خودکار	-
.۱۹	مدیریت کارکرد در محصول ۱/ توابع	اصلاح یا تغییر رفتار؛ مخابره داده ممیزی به موجودیت IT خارجی، کنترل داده ممیزی، قابلیت عملکردی ممیزی وقتی که فضای محلی ذخیره‌سازی ممیزی پر باشد.	-

نکته کاربردی ۴۹:

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.

۶,۱ الزامات پروتکل DTLS Client

شماره الزام	نام الزام
۸۳	**الزامات پروتکل DTLS Client (۱)**
محصول باید [انتخاب: DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • [انتخاب: ○ TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	

- TLS_RSA_WITH_AES_192_CBC_SHAمطابق 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_192_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_192_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_192_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_192_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_192_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_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با5289 RFC
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289

- TLS_ECDHE_RSA_WITH_AES_192_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_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384 مطابق با RFC 5289

-].

نکته کاربردی ۵۰:

مجموعه‌های رمز که باید در پیکربندی ارزیابی‌شده آزمون شوند، توسط این الزام محدود شده‌اند.

نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 6347، الزامی است.

در نسخه‌های آتی این پروفایل حفاظتی، DTLS v1.2 برای همه محصولات الزامی می‌گردد.

۸۴	**الزامات پروتکل DTLS Client (۲)**

محصول باید مطابقت شناسه[۱] ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تائید نماید.

نکته کاربردی ۵۱:

قوانین مربوط به تائید شناسه در بخش ۶ از RFC 6125 توضیح داده شده‌اند. شناسه مرجع توسط سرپرست (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. کلاینت بر مبنای دامنه منبع و نوع سرویس برنامه کاربردی (مثلاً؛ HTTP، SIP، LDAP) مربوط به یک شناسه مرجع منحصربه‌فرد، همه شناسه‌های مرجع قابل‌قبول؛ نظیر یک Common Name برای قسمتName Subject از گواهی‌نامه و نام (حساس به بزرگ و کوچک بودن حروف) DNS، URI و سرویس برای قسمت Subject Alternative Name را منتشر می‌نماید. سپس کلاینت لیست همه شناسه‌های مرجع قابل‌قبول را با شناسه‌های ارائه‌شده در گواهی سرور DTLS مقایسه می‌کند.

روش ترجیحی برای تائید شناسه، Subject Alternative Name است که از نام‌های DNS، URI، یا سرویس‌ها استفاده می‌کند. تائید شناسه با استفاده از Common Name برای اهدافی مانند سازگاری پس‌زمینه[۲]، الزامی است. به علاوه، استفاده از آدرس‌های IP در

[۱] Identifier

[۲] Background

هرکدام از دو روش ذکر شده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود. همچنین کلاینت نباید برای ساختن شناسه‌های مرجع از wildcards استفاده نماید.
۸۵ | **الزامات پروتکل DTLS Client (۳)**
محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]]. **نکته کاربردی ۵۲:** اگر در الزام FTP_ITC پروتکل DTLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود. اگر در الزام FTP_ITT پروتکل DTLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود.
۸۶ | **الزامات پروتکل DTLS Client (۴)**
محصول باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب:secp256r1, secp384r1, secp521r1] و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد. **نکته کاربردی ۵۳:** اگر در الزام «الزامات پروتکل DTLS Client (۱)» مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام «الزامات پروتکل DTLS Client (۱)» هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب نگردد، عبارت "Supported Elliptic Curves Extension را ارائه نکند" باید انتخاب شود. این الزام مجموعه‌های رمز بیضوی مجاز برای احراز هویت و توافق کلید را به منحنی‌های NISTاز الزام‌های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌های که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.

۶,۲ الزامات پروتکل DTLS Clint /احراز هویت

شماره الزام	نام الزام
۸۷	**الزامات پروتکل DTLS Client/ احراز هویت ۱**
محصول باید [انتخاب: DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • [انتخاب: o TLS_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268	

- TLS_RSA_WITH_AES_192_CBC_SHAمطابق 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_192_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_192_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_192_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_192_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_192_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_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با5289 RFC
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289

- TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289
-].

نکته کاربردی ۵۴:

نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 6347، الزامی است.

در نسخه‌های آتی این پروفایل حفاظتی، DTLS v1.2 برای همه محصولات الزامی می‌گردد.

۸۸	**الزامات پروتکل DTLS Client/ احراز هویت ۲**

محصول باید مطابقت شناسه[۱] ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تائید نماید.

نکته کاربردی ۵۵:

قوانین مربوط به تائید شناسه در بخش ۶ از RFC 6125 توضیح داده شده‌اند. شناسه مرجع توسط سرپرست (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. کلاینت بر مبنای دامنه منبع و نوع سرویس برنامه کاربردی (مثلاً؛ HTTP، SIP، LDAP) مربوط به یک شناسه مرجع منحصربه‌فرد، همه شناسه‌های مرجع قابل‌قبول؛ نظیر یک Common Name برای قسمتName Subject از گواهی‌نامه و نام (حساس به بزرگ و کوچک بودن حروف) DNS، URI و سرویس برای قسمت Subject Alternative Name را منتشر می‌نماید. سپس کلاینت لیست همه شناسه‌های مرجع قابل‌قبول را با شناسه‌های ارائه‌شده در گواهی سرور DTLS مقایسه می‌کند.

روش ترجیحی برای تائید شناسه، Subject Alternative Name است که از نام‌های DNS، URI، یا سرویس‌ها استفاده می‌کند. تائید شناسه با استفاده از Common Name برای اهدافی مانند سازگاری پس‌زمینه[۲]، الزامی است. به علاوه، استفاده از آدرس‌های IP در

[۱] Identifier

[۲] Background

هرکدام از دو روش ذکر شده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود. همچنین کلاینت نباید برای ساختن شناسه‌های مرجع از wildcards استفاده نماید.	
الزامات پروتکل DTLS Client/ احراز هویت ۳	**۸۹**
محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]]. **نکته کاربردی ۵۶:** اگر در الزام FTP_ITC پروتکل DTLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود. اگر در الزام FTP_ITT پروتکل DTLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود.	
الزامات پروتکل DTLS Client/ احراز هویت ۴	**۹۰**
محصول باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب: secp256r1, secp384r1, secp521r1] و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد. **نکته کاربردی ۵۷:** اگر در الزام «الزامات پروتکل DTLS Client/ احراز هویت ۱» مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام «الزامات پروتکل DTLS Client/ احراز هویت ۱» هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب نگردد، عبارت "Supported Elliptic Curves Extension را ارائه نکند" باید انتخاب شود. این الزام مجموعه‌های رمز بیضوی مجاز برای احراز هویت و توافق کلید را به منحنی‌های NISTاز الزام‌های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌های که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.	
الزامات پروتکل DTLS Client/ احراز هویت ۵	**۹۱**
محصول باید احراز هویت دوطرفه را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید. **نکته کاربردی ۵۸:** استفاده از گواهی‌نامه‌های X509v3 برای پروتکل DTLS در الزام FIA_X509_EXT.2.1 ارائه شده است. در این الزام بیان می‌شود که کلاینت باید برای احراز هویت دوطرفه DTLS، قادر باشد یک گواهی‌نامه به سرور DTLS ارائه نماید.	
الزامات پروتکل DTLS Client/ احراز هویت ۶	**۹۲**
محصول باید هنگامی که یک پیام حاوی MAC غیرمعتبر دریافت می‌کند، [انتخاب: به نشست DTLS خاتمه دهد، بیصدا رکورد را دوربریزد].	

نکته کاربردی ۵۹:

کد احراز هویت پیام (MAC) در واقع یک تابع هش کلید است که در الزام FCS_COP.1/KeyedHash شرح داده شده است. این کد در طی فاز دست‌تکانی DTLS مخابره می‌شود و برای حفاظت از جامعیت پیام‌های است که از طرف فرستنده در مبادله داده DTLS، دریافت می‌شود. اگر تائید MAC شکست بخورد، نشست باید خاتمه یابد یا رکورد دریافت شده، بیصدا دور انداخته شود.

۹۳	**الزامات پروتکل DTLS Client/ احراز هویت ۷**

محصول باید پیام‌های تکرار/بازپخش[۱] شده برای موارد زیر را تشخیص و بیصدا دور بیاندازد:

- رکوردهای DTLS که قبلا دریافت شده است.
- رکوردهای DTLS که برای پنجره لغزنده، قدیمی محسوب می‌شود.

نکته کاربردی ۶۰:

تشخیص بازپخش در بخش 4.1.2.6 از DTLS v1.2 (RFC 6347) و بخش 4.1.2.5 از DTLS v1.0 (RFC 4347) تشریح شده است. برای هر رکورد دریافتی، دریافت کننده بررسی می‌کند که شماره توالی رکورد دریافتی در پنجره لغزنده دریافت تعریف شده باشد و قبلا توسط رکوردهای دریافت شده، استفاده نشده باشد. یعنی پیام تکرار نباشد.

۶,۳ الزامات پروتکل DTLS Server

شماره الزام	نام الزام
۹۴	**الزامات پروتکل DTLS Server (۱)**

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

- [انتخاب:
  - TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
  - TLS_RSA_WITH_AES_192_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_192_CBC_SHA مطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268

[۱] Replayed

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
- TLS_ECDHE_RSA_WITH_AES_192_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_192_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_192_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_192_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_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با5289 RFC
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289

•].
نکته کاربردی ۶۱: مجموعه‌های رمز که باید در پیکربندی ارزیابی‌شده آزمون شوند، توسط این الزام محدود شده‌اند. نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 6347، الزامی است. در نسخه‌های آتی این پروفایل حفاظتی، DTLS v1.2 برای همه محصولات الزامی می‌گردد.

۹۵	**الزامات پروتکل DTLS Server (۲)**
محصول باید برای کلاینت‌های دارای درخواست [هیچ موردی]، ارتباطات را ایجاد نکند.	
نکته کاربردی ۶۲: این پروفایل حفاظتی، محصول را ملزم به رد کردن درخواست DTLS v1.0 نمی‌کند. در نسخه آتی این پروفایل حفاظتی درخواست‌های DTLS v1.0 باید توسط تمامی محصولات، رد شود.	

۹۶	**الزامات پروتکل DTLS Server (۳)**
محصول نباید در صورت شکست خوردن اعتبارسنجی DTLS Client، تلاش دست‌تکانی ارتباط را پیش ببرد.	
نکته کاربردی ۶۳: فرآیند اعتبارسنجی کردن DTLS Client در بخش 4.2.1 از DTLS v1.2 (RFC 6347) و DTLS v1.0 (RFC 4347) تشریح شده است. محصول DTLS Client را قبل از ارسال پیام ServerHello توسط توابع امنیتی محصول و در طی برقراری ارتباط (دست‌تکانی)، اعتبارسنجی می‌نماید. سرور بعد از دریافت ClientHello، یک پیغام HelloVerifyRequest را از کوکی به کلاینت ارسال می‌کند. کوکی درواقع یک پیام امضاء شده با استفاده از توابع هش معرفی شده در الزام FCS_COP.1/KeyedHash است. کلاینت دوباره یک پیغام ClientHello را به همراه کوکی امضاء شده ارسال می‌کند، سرور در صورت تائید کردن کوکی ارسالی کلاینت، مطمئن می‌شود که کلاینت از آدرس IP جعلی استفاده نکرده است.	

۹۷	**الزامات پروتکل DTLS Server (۴)**
محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸بیت، ۳۰۷۲بیت، ۴۰۹۶بیت] اجرا نماید؛ پارامترهای EC-دیفی‌هلمن را به همراه منحنی‌های NIST[انتخاب:secp256r1, secp384r1, secp521r1] و هیچ منحنی دیگری، تولید نماید؛ پارامترهای دیفی‌هلمن را با اندازه [انتخاب: ۲۰۴۸بیت، ۳۰۷۲بیت] تولید کند].	

نکته کاربردی ۶۴: اگر سند هدف امنیتی در الزام «الزامات پروتکل DTLS Server (۱)» مجموعه‌های رمز DHE و ECDHE را ارائه کرده باشد، نویسنده سند هدف امنیتی باید امکان انتخاب دیفی‌هلمن یا منحنی‌های NIST را در الزام بگنجاند. الزام FMT_SMF.1 پیکربندی پارامترهای توافق کلید را برای برقراری یک ارتباط DTLS ملزم می‌کند که از لحاظ امنیتی قوی باشد.

۹۸	**الزامات پروتکل DTLS Server (۵)**
محصول باید هنگامی که یک پیام حاوی MAC غیرمعتبر دریافت می‌کند، [انتخاب: به نشست DTLS خاتمه دهد، بیصدا رکورد را دوربریزد].	
نکته کاربردی ۶۵: کد احراز هویت پیام (MAC) در واقع یک تابع هش کلید است که در الزام FCS_COP.1/KeyedHash شرح داده شده است. این کد در طی فاز دست‌تکانی DTLS مخابره می‌شود و برای حفاظت از جامعیت پیام‌های است که از طرف فرستنده در مبادله داده DTLS، دریافت می‌شود. اگر تائید MAC شکست بخورد، نشست باید خاتمه یابد یا رکورد دریافت شده، بیصدا دور انداخته شود.	

۹۹	**الزامات پروتکل DTLS Server (۶)**
محصول باید پیام‌های تکرار/بازپخش شده برای موارد زیر را تشخیص و بیصدا دور بیاندازد: • رکوردهای DTLS که قبلا دریافت شده است. • رکوردهای DTLS که برای پنجره لغزنده، قدیمی محسوب می‌شود. **نکته کاربردی ۶۶:** تشخیص بازپخش در بخش 4.1.2.6 از DTLS v1.2 (RFC 6347) و بخش 4.1.2.5 از DTLS v1.0 (RFC 4347) تشریح شده است. برای هر رکورد دریافتی، دریافت کننده بررسی می‌کند که شماره توالی رکورد دریافتی در پنجره لغزنده دریافت تعریف شده باشد و قبلا توسط رکوردهای دریافت شده، استفاده نشده باشد. یعنی پیام تکرار نباشد. عبارت "بیصدا دور بیاندازد" یعنی محصول بدون هیچ‌گونه پاسخی بسته را دور بیاندازد.	

۶,۴ الزامات پروتکل DTLS Server /احراز هویت دوطرفه

شماره الزام	نام الزام
۱۰۰	**الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۱**
محصول باید [انتخاب: DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • [انتخاب:	

- TLS_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
- TLS_RSA_WITH_AES_192_CBC_SHAمطابق 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_192_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_192_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_192_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_192_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_192_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_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با5289 RFC

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289

•].

نکته کاربردی ۶۷:

مجموعه‌های رمز که باید در پیکربندی ارزیابی‌شده آزمون شوند، توسط این الزام محدود شده‌اند.

نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 6347، الزامی است.

در نسخه‌های آتی این پروفایل حفاظتی، DTLS v1.2 برای همه محصولات الزامی می‌گردد.

۱۰۱	**الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۲**

محصول باید برای کلاینت‌های دارای درخواست [هیچ موردی]، ارتباطات را ایجاد نکند.

نکته کاربردی ۶۸:

این پروفایل حفاظتی، محصول را ملزم به رد کردن درخواست DTLS v1.0 نمی‌کند. در نسخه آتی این پروفایل حفاظتی درخواست‌های DTLS v1.0 باید توسط تمامی محصولات، رد شود.

۱۰۲	**الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۳**

محصول نباید در صورت شکست خوردن اعتبارسنجی DTLS Client، تلاش دست‌تکانی ارتباط را پیش ببرد.

نکته کاربردی ۶۹:

فرآیند اعتبارسنجی کردن DTLS Client در بخش 4.2.1 از (RFC 6347) DTLS v1.2 و (RFC 4347) DTLS v1.0 تشریح شده است. محصول DTLS Client را قبل از ارسال پیام ServerHello توسط توابع امنیتی محصول و در طی برقراری ارتباط (دست‌تکانی)، اعتبارسنجی می‌نماید. سرور بعد از دریافت ClientHello، یک پیغام HelloVerifyRequest را از کوکی به کلاینت ارسال می‌کند. کوکی درواقع یک پیام امضاء شده با استفاده از توابع هش معرفی شده در الزام FCS_COP.1/KeyedHash است. کلاینت دوباره یک پیغام

ClientHello را به همراه کوکی امضاء شده ارسال می‌کند، سرور در صورت تائید کردن کوکی ارسالی کلاینت، مطمئن می‌شود که کلاینت از آدرس IP جعلی استفاده نکرده است.
۱۰۳ **الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۴**
محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸بیت، ۳۰۷۲بیت، ۴۰۹۶بیت] اجرا نماید؛ پارامترهای EC-دیفی‌هلمن را به همراه منحنی‌های NIST[انتخاب:secp256r1, secp384r1, secp521r1] و هیچ منحنی دیگری، تولید نماید؛ پارامترهای دیفی‌هلمن را با اندازه [انتخاب: ۲۰۴۸بیت، ۳۰۷۲بیت] تولید کند]. **نکته کاربردی ۷۰:** اگر سند هدف امنیتی در الزام «الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۱» مجموعه‌های رمز DHE و ECDHE را ارائه کرده باشد، نویسنده سند هدف امنیتی باید امکان انتخاب دیفی‌هلمن یا منحنی‌های NIST را در الزام بگنجاند. الزام FMT_MOF.1 پیکربندی پارامترهای توافق کلید را برای برقراری یک ارتباط DTLS ملزم می‌کند که از لحاظ امنیتی قوی باشد.
۱۰۴ **الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۵**
محصول باید هنگامی که یک پیام حاوی MAC غیرمعتبر دریافت می‌کند، [انتخاب: به نشست DTLS خاتمه دهد، بیصدا رکورد را دوربریزد]. **نکته کاربردی ۷۱:** کد احراز هویت پیام (MAC) در واقع یک تابع هش کلید است که در الزام FCS_COP.1/KeyedHash شرح داده شده است. این کد در طی فاز دست‌تکانی DTLS مخابره می‌شود و برای حفاظت از جامعیت پیام‌های است که از طرف فرستنده در مبادله داده DTLS، دریافت می‌شود. اگر تائید MAC شکست بخورد، نشست باید خاتمه یابد یا رکورد دریافت شده، بیصدا دور انداخته شود.
۱۰۵ **الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۶**
محصول باید پیام‌های تکرار/بازپخش شده برای موارد زیر را تشخیص و بیصدا دور بیاندازد: • رکوردهای DTLS که قبلا دریافت شده است. • رکوردهای DTLS که برای پنجره لغزنده، قدیمی محسوب می‌شود. **نکته کاربردی ۷۲:** تشخیص بازپخش در بخش 4.1.2.6 از DTLS v1.2 (RFC 6347) و بخش 4.1.2.5 از DTLS v1.0 (RFC 4347) تشریح شده است. برای هر رکورد دریافتی، دریافت کننده بررسی می‌کند که شماره توالی رکورد دریافتی در پنجره لغزنده دریافت تعریف شده باشد و قبلا توسط رکوردهای دریافت شده، استفاده نشده باشد. یعنی پیام تکرار نباشد. عبارت "بیصدا دور بیاندازد" یعنی محصول بدون هیچ‌گونه پاسخی بسته را دور بیاندازد.

۱۰۶	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۷
محصول باید احراز هویت دوطرفه کلاینت‌های DTLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.	
۱۰۷	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۸
محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]]. **نکته کاربردی ۷۳:** استفاده از گواهی‌نامه‌های X509v3 برای پروتکل DTLS در الزام FIA_X509_EXT.2.1 ارائه شده است. در این الزام بیان می‌شود که گواهی‌نامه‌های سمت کلاینت باید برای احراز هویت دوطرفه DTLS پشتیبانی گردند. اگر در الزام FTP_ITC پروتکل DTLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود. اگر در الزام FTP_ITT پروتکل DTLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود.	
۱۰۸	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۹
محصول در صورت مطابقت نداشتن؛ نام متمایز[۱] یا نام دیگر فاعل[۲] موجود در گواهی‌نامه، با آنچه که از شناساننده[۳] کلاینت انتظار بوده است، نباید کانال امن را برقرار سازد. **نکته کاربردی ۷۴:** شناساننده کلاینت ممکن است در فیلد subject یا افزونه نام دیگر فاعل مربوط به یک گواهی‌نامه باشد. شناساننده مورد انتظار باید پیکربندی گردد. این شناساننده ممکن است با نام دامنه، آدرس IP، یا ادرس ایمیل که توسط نظیر استفاده می‌گردد، مقایسه گردد. همچنین ممکن است این شناساننده برای مقایسه، به یک دایرکتوری سرور داده شود.	

۶,۵ الزامات پروتکل HTTPS

شماره الزام	نام الزام
۱۰۹	**الزامات پروتکل HTTPS (۱)**
محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کنند.	

[۱] Distinquish Name (DN)
[۲] Subject Alternative Name (SAN)
[۳] Identifier

نکته کاربردی ۷۵:

نویسنده سند هدف امنیتی باید اطلاعات کافی را فراهم آورد و مشخص کند که پیاده‌سازی این پروتکل، مطابق استانداردهای تعریف‌شده است. برای انجام این کار می‌توان عناصری را به این مؤلفه افزود یا اطلاعاتی را به خلاصه مشخصات محصول اضافه کرد.

۱۱۰	**الزامات پروتکل HTTPS (۲)**

محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.

۱۱۱	**الزامات پروتکل HTTPS (۳)**

درصورتی‌که گواهی‌نامه همتا ارائه شده باشد و نامعتبر باشد، محصول مورد ارزیابی باید [انتخاب: اتصال را برقرار ننماید، برای برقراری اتصال درخواست مجوز نماید، هیچ اقدام دیگری انجام ندهد].

نکته کاربردی ۷۶:

اگر در الزام FTP_ITC.1 یا FTP_TRP.1/Admin پروتکل HTTPS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی‌نامه بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود.

اگر در الزام FTP_ITT.1 پروتکل HTTPS انتخاب گردد، آنگاه اعتبار گواهی‌نامه بر اساس الزام FIA_X509_EXT.1/ITT آزموده می شود.

۶,۶ 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 غیرقابل‌اعتماد 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
۱۱۲	**الزامات پروتکل IPSEC (۱)**
محصول مورد ارزیابی باید پروتکل IPsec را بر اساس آن چه در RFC 4301 مشخص شده است، پیاده‌سازی کند. **نکته کاربردی ۷۷:** بر اساس RFC 4301 برای پیاده سازی IPSEC جهت محافظت از ترافیک IP باید از یک پایگاه‌داده خط‌مشی امنیتی (SPD) استفاده کرد. با استفاده از SPD می‌توان تعیین کرد که بسته‌های IP چگونه باید مدیریت شوند: ۱- «PROTECT » از بسته‌ها (مثلاً رمزگذاری آن‌ها) ۲- «BYPASS » سرویس‌های IPSEC (مثلاً عدم رمزگذاری) ۳- «DISCARD » بسته (مثلاً دور ریختن بسته). پایگاه‌داده مذکور را می‌توان به روش‌های مختلفی پیاده‌سازی کرد که از آن جمله می‌توان به لیست‌های کنترل دسترسی به مسیریاب، مجموعه قوانین فایروال، استفاده از یک پایگاه داده SPD سنتی و مواردی از این دست اشاره کرد. صرف نظر از روشی که به کار گرفته می‌شود، مفهومی به نام "قانون[۱]" وجود دارد که بسته‌ها با آن "مطابقت" می‌کنند و در نتیجه یک اقدام انجام می‌گیرد. باید ابزارهایی برای مرتب کردن این قوانین وجود داشته باشد، ولی داشتن یک رویکرد عمومی در این زمینه الزام نشده است. 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.	
۱۱۳	**الزامات پروتکل IPSEC (۲)**
محصول مورد ارزیابی باید مقدار/قانون در پایگاه داده SPD، برای تمام موارد غیر منطبق داشته باشد و آن‌ها را طبق آن مقدار/قانون دور بریزد.	
۱۱۴	**الزامات پروتکل IPSEC (۳)**
محصول مورد ارزیابی باید [انتخاب: مد انتقال، مد تونل] را پیاده‌سازی کند. **نکته کاربردی ۷۸:** نویسنده سند هدف امنیتی باید مدهای عملیاتی پشتیبانی شده برای IPSec را مشخص نماید.	
۱۱۵	**الزامات پروتکل IPSEC (۴)**

[۱] rule

محصول مورد ارزیابی باید بر اساس آنچه در RFC 4303 گفته شده است فریمورک ESP از پروتکل IPSEC را با استفاده از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128، AES-CBC-128، AES-CBC-128 (تشریح شده در RFC 3602)، هیچ الگوریتم دیگری] به همراه یک HMAC مبتنی بر الگوریتم درهم‌سازی امن (SHA) [انتخاب: HMAC-SHA-1، HMAC-SHA-256، HMAC-SHA-384، HMAC-SHA-512، هیچ الگوریتم دیگری] و [انتخاب: AES-GCM-128، AES-GCM-192، AES-GCM-256 (تشریح شده در RFC 4106)، هیچ الگوریتم دیگری] پیاده‌سازی کند.

نکته کاربردی ۷۹:

وقتی که الگوریتم AES-CBC انتخاب گردد، حداقل یک HMAC مبتنی بر SHA نیز باید انتخاب شود. اگر یک AES-GCM انتخاب گردد، نیاز نیست که HMAC انتخاب شود زیرا AES-GCM محرمانگی و جامعیت را بوجود فراهم می‌نماید. در صورتی که برای IPSec با توجه به خروجی مورد انتظار، نوع خاصی از HMAC مبتنی بر SHA (مثلا، HMAC کوتاه شده[۱]) انتخاب گردد، در خلاصه مشخصات محصول باید مشخص شود.

۱۱۶	**الزامات پروتکل IPSEC (۵)**

محصول مورد ارزیابی باید یکی از این پروتکل‌ها را به کار گیرد: [انتخاب:

- IKEv1، با استفاده از مد اصلی[۲] برای انتقال در فاز اول، طبق آنچه که در RFC 4109, 2409, 2408, 2407 RFCs، [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] بیان شده است.

- IKEv2، مطابق با آنچه که در RFC 5996 و [انتخاب: بدون پشتیبانی از پیمایش NAT[۳]، 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] تشریح شده است.

].

نکته کاربردی ۸۰:

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 محصول از HMACs مبتنی بر SHA، کوتاه‌شده مطابق با RFC 4868 استفاده نماید، باید در خلاصه مشخصات محصول، مشخص گردد.

---

[۱] Truncated

[۲] Main Mode

[۳] NAT traversal

۱۱۷	الزامات پروتکل IPSEC (۶)
محصول مورد ارزیابی باید اطمینان حاصل کند که برای پی‌آیند[۱] رمزگذاری‌شده در پروتکل [انتخاب: IKEv1، IKEv2]، از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128، AES-CBC-192، AES-CBC-256 (تشریح شده در RFC 3602)، AES-GCM-128، AES-GCM-192، AES-GCM-256 (تشریح شده در RFC 5282) استفاده می‌شود.	

نکته کاربردی ۸۱:

از آنجایی که هیچ RFC وجود ندارد که AES-GCM را برای IKEv1 تعریف کرده باشد، AES-GCM-128، AES-GCM-192 و AES-GCM-256 تنها در صورتی انتخاب می‌شوند که IKEv2 نیز انتخاب شده باشد.

۱۱۸	الزامات پروتکل IPSEC (۷)

محصول مورد ارزیابی باید اطمینان حاصل کند که [انتخاب:

- سرپرست محصول می‌تواند طول عمر SA فاز اول IKEv1 را بر اساس [انتخاب:
  - تعداد بایت‌ها؛
  - مدت زمان که مقدار آن را می‌توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد؛] پیکربندی کند.
- سرپرست محصول 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 ۸۲:

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

۱۱۹	الزامات پروتکل IPSEC (۸)

محصول مورد ارزیابی باید اطمینان حاصل کند که [انتخاب:

- سرپرست محصول می‌تواند طول عمر SA فاز دوم IKEv1 را بر اساس [انتخاب:

[۱] Payload

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

نکته کاربردی ۸۳:

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

۱۲۰	**الزامات پروتکل IPSEC (۹)**

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

نکته کاربردی ۸۴:

در گروهای ۱۹ و ۲۰ دیفی‌هلمن، مقدار "x" ضریب نقطه‌ای برای g است.

از آنجایی که در پیاده‌سازی ممکن است گروه‌های مختلف Diffie-Hellman در مذاکره برای استفاده در SA مجاز باشند الزام «الزامات پروتکل IPSEC (۹)» می‌تواند مقادیر متعددی داشته باشند. نویسند سند هدف امنیتی برای هر گروه DH مورد پشتیبانی، از جدول ۲ در دفترچه NIST SP 800-57 «توصیه‌هایی برای مدیریت کلید – بخش اول: عمومی» برای تعیین قدرت امنیتی («تعداد بیت‌های امنیتی») مربوط به گروه DH راهنمایی بگیرد. سپس هر مقدار منحصربه‌فرد برای پر کردن قسمت اختصاص 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.

۱۲۱	**الزامات پروتکل IPSEC (۱۰)**

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

- [اختصاص: قدرت امنیتی مربوط به گروه Diffie-Hellman مذاکره‌شده]؛
- حداقل ۱۲۸ بیت اندازه و حداقل نصف اندازه خروجی تابع درهم‌سازی نیمه‌تصادفی[۱] مذاکره‌شده (PRF)] تولید کند.

نکته کاربردی ۸۵:

اگر IKEv2 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 برای استفاده از گروه‌های مختلف Diffie-Hellman در ساخت تضمین‌های امنیتی، مذاکره کردن مجاز باشد، اختصاص مربوط به «الزامات پروتکل IPSEC (۱۰)» می‌تواند مقادیر متعددی داشته باشد.

نویسنده سند هدف امنیتی برای هر گروه DH مورد پشتیبانی، از جدول ۲ در دفترچه NIST SP 800-57 «توصیه‌هایی برای مدیریت کلید – بخش اول: عمومی» برای تعیین قدرت امنیتی («تعداد بیت‌های امنیتی») مربوط به گروه DH راهنمایی بگیرد. سپس هر مقدار منحصربه‌فرد برای پر کردن قسمت اختصاص 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 گروه DH مذاکره شود، مبادله شوند، بنابراین توصیه می‌شود نانس به‌کاررفته به اندازه کافی بزرگ باشد که همه پیشنهادهای محصول انتخاب‌شده در تبادل را پشتیبانی نماید.

۱۲۲	**الزامات پروتکل IPSEC (۱۱)**

محصول باید اطمینان حاصل نماید که پروتکل‌های IKE، همه گروه(های) DH [انتخاب: ۱۴ (2048-bit MODP) و ۱۹ (256-bit Random ECP)، ۲۰ (384-bit Random ECP)، ۲۴ (2048-bit MODP به همراه 256-bit POS)] را پشتیبانی می‌کنند.

نکته کاربردی ۸۶:

قسمت "انتخاب" در این الزام جهت مشخص کردن این موضوع که گروه‌های DH اضافه پشتیبانی شده است، بکار می‌رود. این الزام برای هر دو IKEv1 و IKEv2 اعمال می گردد.

۱۲۳	**الزامات پروتکل IPSEC (۱۲)**

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

[۱] Pseudorandom Function hash

نکته کاربردی ۸۷:

نویسنده سند هدف امنیتی یکی یا هر دوی انتخاب‌های IKE را بر اساس اینکه کدام یک توسط محصول پیاده‌سازی می‌شود، انتخاب می‌کند. انتخاب نسخه(های) IKE نه فقط در این الزام بلکه در تمامی الزامات بخش IPSec، باید سازگار باشد.

۱۲۴	**الزامات پروتکل IPSEC (۱۳)**

محصول باید اطمینان حاصل نماید که همه پروتکل‌های IKE احراز هویت همتا را با استفاده از [انتخاب: RSA، ECDSA] که از گواهی‌های X.509v3 مطابق با RFC4945 و [انتخاب: کلیدهای پیش‌اشتراکی، هیچ روش دیگری] استفاده می‌کند، انجام می‌دهند.

نکته کاربردی ۸۸:

برای انطباق با این پروفایل حفاظتی، حداقل یک روش احراز هویت همتا مبتنی بر کلید عمومی لازم است؛ نویسنده سند هدف امنیتی باید اطمینان حاصل نماید که الزامات کلاس رمزنگاری متناسب که نشان دهنده الگوریتم‌های استفاده شده (و سازگاری کلیدهای تولید شده) برای پشتیبانی روش انتخابی است، ارائه شده باشد. خلاصه مشخصات محصول باید تشریح نماید که چگونه الگوریتم‌ها مورد استفاده قرار می‌گیرند (برای مثال؛ RFC 2409 سه روش احراز هویت با استفاده از کلید عمومی را مشخص می‌کند، هر کدام که استفاده می‌شود باید در خلاصه مشخصات محصول ذکر گردد).

۱۲۵	**الزامات پروتکل IPSEC (۱۴)**

محصول باید کانال امن را فقط در صورتی که شناساننده موجود در گواهی‌نامه دریافتی با شناساننده مرجع پیکربندی شده انطباق داشته باشد، برقرار نماید. شناساننده مرجع و ارائه شده از انواع زیر می‌باشند:

[انتخاب: آدرس IP، FQDN[۱]، FQDN کاربر، نام متمایز شده (DN[۲])] و[انتخاب: هیچ نوع شناساننده مرجع دیگری، [انتخاب: دیگر انواع شناساننده مرجع پشتیبانی شده]] .

نکته کاربردی ۸۹:

وقتی که از گواهی‌نامه‌های RSA یا ECDSA برای احراز هویت همتا استفاده می‌گردد، شناساننده مرجع و ارائه شده یکی از فرم‌های FQDN، DN، آدرس IP یا FQDN کاربر را پیدا می‌کند. لازم به ذکر است که شناساننده مرجع، در واقع همان شناساننده ای است که محصول انتظار دارد از IKE احراز هویت کاربر دریافت نماید. همچنین شناساننده ارائه شده، شناساننده ای است که در بدنه گواهی‌نامه ارائه می‌شود.

[۱] Fully Qualified Domain Name

[۲] Distinquished Name

روش ترجیحی برای تائید شناسه، Subject Alternative Name است که از نام‌های DNS، URI، یا سرویس‌ها استفاده می‌کند. تائید شناسه با استفاده از Common Name برای اهدافی مانند سازگاری پس‌زمینه[۱]، الزامی است. به علاوه، استفاده از آدرس‌های IP در هرکدام از دو روش ذکر شده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود.

۶,۷ الزامات پروتکل SSH Client

شماره الزام	نام الزام
۱۲۶	**الزامات پروتکل SSH Client (۱)**
محصول باید پروتکل SSH را مطابق با RFC های [انتخاب: 4251، 4252، 4253، 4254، 5647، 5656، 6187، 6668، هیچ RFC دیگری] پیاده‌سازی نماید. **نکته کاربردی ۹۰:** نویسنده سند هدف امنیتی انتخاب می‌کند که با کدام یک از RFC ها مطابقت وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً؛ الگوریتم‌های رمزنگاری معتبر). RFC 4253 الگوریتم‌های رمزنگاری مشخص را که "REQUIRED" (موردنیاز) هستند، تعیین می‌کند. در نتیجه، پشتیبانی از این الگورتیم‌ها باید پیاده‌سازی شود، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. مشخص کردن اینکه کدام یک از الگوریتم‌هایی که به صورت "REQUIRED" می‌باشند، لیست شده ولی پیاده‌سازی نشده است، در حوزه فعالیت ارزیابی این الزام قرار نمی‌گیرد.	
۱۲۷	**الزامات پروتکل SSH Client (۲)**
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، روش‌های احراز هویت زیر مطابق با آنچه که در RFC 4252 توضیح داده‌شده است، پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، [انتخاب: احراز هویت مبتنی بر گذرواژه، هیچ روش دیگری].	
۱۲۸	**الزامات پروتکل SSH Client (۳)**
همان طور که در RFC 4253 توضیح داده‌شده است، محصول باید اطمینان حاصل نماید که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک ارتباطات انتقال SSH، کنار گذاشته شوند. **نکته کاربردی ۹۱:**	

[۱] Background

RFC 4253 امکان پذیرش «بسته‌های بزرگ» را فراهم می‌کند، با این اخطار که بسته‌ها باید «طول معقولی» داشته باشند یا اینکه کنار گذاشته می‌شوند. توصیه می‌شود این اختصاص توسط نویسنده هدف امنیتی با درنظر گرفتن بیشترین اندازه بسته که قابل پذیرش است پر شود تا به این وسیله «طول معقول» برای محصول تعریف شود.
۱۲۹ | الزامات پروتکل SSH Client (۴)
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری [انتخاب: AES128-CBC، AES-256-CBC، AES128-CTR، AES256-CTR، AEAD_AES_128_GCM، AEAD_AES_256_GCM] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند. **نکته کاربردی ۹۲:** RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌نماید. چنانکه در این RFC مطرح شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌های برای MAC نیز انتخاب گردند.
۱۳۰ | الزامات پروتکل SSH Client (۵)
محصول باید اطمینان حاصل نماید که پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: ssh-rsa, ecdsa-sha2-nistp256] و [انتخاب: ecdsa-sha2-nistp384، ecdsa-sha2-nistp521، x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384، x509v3-ecdsa-sha2-nistp521، هیچ الگوریتم کلید عمومی دیگری] به عنوان الگوریتم(های) کلید عمومی خود استفاده کند و همه الگوریتم‌های دیگر را رد نماید. **نکته کاربردی ۹۳:** اگر x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384، x509v3-ecdsa-sha2-nistp521 انتخاب گردند، آنگاه لیستی از مراجع گواهی امن باید در الزام FCS_SSHC_EXT.1.9 انتخاب شود و الزامات FCS_X509_EXT قابل اعمال خواهند بود.
۱۳۱ | الزامات پروتکل SSH Client (۶)
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: hmac-sha1، hmac-sha1-96، hmac-sha2-256، hmac-sha2-512] و [انتخاب: AEAD_AES_128_GCM، AEAD_AES_256_GCM، هیچ الگوریتم MAC دیگری] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند. **نکته کاربردی ۹۴:** RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌نماید. چنانکه در این RFC مطرح شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌های برای MAC نیز انتخاب گردند. RFC 6668 استفاده از sha2 را در SSH مشخص می‌نماید.

۱۳۲	الزامات پروتکل SSH Client (۷)
محصول باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1, ecdh-sha2-nistp256] و [انتخاب: ecdh-sha2-nistp384، ecdh-sha2-nistp521، هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.	
۱۳۳	الزامات پروتکل SSH Client (۸)
محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه؛ طول نشست بیشتر از یک ساعت نباشد و حجم داده مخابره شده بیشتر از ۱ گیگابایت نباشد، استفاده می‌گردد. در صورت پر شدن حد آستانه هر کدام از موارد ذکر شده، مجددسازی کلید باید صورت بگیرد. **نکته کاربردی ۹۵:** این الزام حدآستانه‌هایی را برای، حداکثر زمانی که یک کلیدهای نشست می‌تواند استفاده گردد و حداکثر مقدار داده‌ای که می‌تواند با یک کلیدهای نشست، انتقال یابد. هر دو حد آستانه باید پیاده‌سازی گردد و یک مجددسازی کلید نیز وقتی هر کدام از دو مورد مذکور سر برسد، باید بکار گرفته شود. برای محاسبه حداکثر داده انتقالی، داده‌هایی که به محصول وارد و از محصول خارج می‌شوند باید محاسبه گردد. مجددسازی کلید باید روی تمام کلیدهای نشست (رمزنگاری، حفاظت از جامعیت) برای ترافیک ورودی و خروجی اعمال گردد. محصول همچنین می‌تواند مقادیری کمتر از مقادیر حد آستانه ذکر شده در این الزام را پیاده‌سازی نماید. سند راهنمای محصول، باید نحوه پیکربندی این مقادیر و نحوه سر رسیدن آن‌ها و همچنین چگونگی امکان تعریف مقادیر کمتر از حد آستانه را تشریح نماید.	
۱۳۴	الزامات پروتکل SSH Client (۹)
محصول باید اطمینان حاصل نماید که کلاینت SSH، سرور SSH را احراز هویت می‌کند. سرور SSH از یک پایگاه داده محلی که نام هر میزبان را با کلید عمومی متناظر آن یا [انتخاب: فهرستی از مراجع صدور گواهی مطمئن، هیچ روش دیگری] (تشریح شده در RFC 4251 بخش ۴,۱) همراه می‌کند، استفاده می‌نماید. **نکته کاربردی ۹۶:** تنها در صورتی می‌توان گزینه "فهرستی از مراجع صدور گواهی مطمئن" را انتخاب کرد که x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384 یا x509v3-ecdsa-sha2-nistp521در «الزامات پروتکل SSH Client (۵)» انتخاب‌شده باشد.	

۶,۸ الزامات پروتکل SSH Server

شماره الزام	نام الزام
۱۳۵	**الزامات پروتکل SSH Server (۱)**
محصول باید پروتکل SSH را مطابق با RFC های [انتخاب: 4251، 4252، 4253، 4254، 5647، 5656، 6187، 6668، هیچ RFC دیگری] پیاده‌سازی نماید.	
	نکته کاربردی ۹۷: نویسنده سند هدف امنیتی انتخاب می‌کند که با کدام یک از RFC ها مطابقت وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً؛ الگوریتم‌های رمزنگاری معتبر). RFC 4253 الگوریتم‌های رمزنگاری مشخص را که "REQUIRED" (موردنیاز) هستند، تعیین می‌کند. در نتیجه، پشتیبانی از این الگورتیم‌ها باید پیاده‌سازی شود، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. مشخص کردن اینکه کدام یک از الگوریتم‌هایی که به صورت "REQUIRED" می‌باشند، لیست شده ولی پیاده‌سازی نشده است، در حوزه فعالیت ارزیابی این الزام قرار نمی‌گیرد.
۱۳۶	**الزامات پروتکل SSH Server (۲)**
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، همان‌طور که در RFC 4252 توضیح داده‌شده است، روش‌های احراز هویت زیر پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، احراز هویت مبتنی بر گذرواژه.	
۱۳۷	**الزامات پروتکل SSH Server (۳)**
همان طور که در RFC 4253 توضیح داده‌شده است، محصول باید اطمینان حاصل نماید که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک ارتباطات انتقال SSH، کنار گذاشته شوند.	
	نکته کاربردی ۹۸: RFC 4253 امکان پذیرش «بسته‌های بزرگ» را فراهم می‌کند، با این اخطار که بسته‌ها باید «طول معقولی» داشته باشند یا اینکه کنار گذاشته می‌شوند. توصیه می‌شود این اختصاص توسط نویسنده هدف امنیتی با درنظر گرفتن بیشترین اندازه بسته که قابل پذیرش است پر شود تا به این وسیله «طول معقول» برای محصول تعریف شود.
۱۳۸	**الزامات پروتکل SSH Server (۴)**

محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، از الگوریتم‌های رمزنگاری [انتخاب: AES128-CBC، AES-256-CBC، AES128-CTR، AES256-CTR، AEAD_AES_128_GCM، AEAD_AES_256_GCM] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند. **نکته کاربردی ۹۹:** RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌نماید. چنانکه در این RFC مطرح شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌های برای MAC نیز انتخاب گردند.
۱۳۹ | **الزامات پروتکل SSH Server (۵)**
محصول باید اطمینان حاصل نماید که پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: ssh-rsa, ecdsa-sha2-nistp256] و [انتخاب: ecdsa-sha2-nistp384، ecdsa-sha2-nistp521، x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384، x509v3-ecdsa-sha2-nistp521، هیچ الگوریتم کلید عمومی دیگری] به عنوان الگوریتم(های) کلید عمومی خود استفاده کند و همه الگوریتم‌های دیگر را رد نماید. **نکته کاربردی ۱۰۰:** اگر x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384، x509v3-ecdsa-sha2-nistp521 انتخاب گردند، آنگاه الزامات FCS_X509_EXT قابل اعمال خواهند بود.
۱۴۰ | **الزامات پروتکل SSH Server (۶)**
محصول باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقال SSH، از [انتخاب: hmac-sha1، hmac-sha1-96، hmac-sha2-256، hmac-sha2-512] و [انتخاب: AEAD_AES_128_GCM، AEAD_AES_256_GCM، هیچ الگوریتم MAC دیگری] به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC صحت داده‌ها رد می‌شوند. **نکته کاربردی ۱۰۱:** RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌نماید. چنانکه در این RFC مطرح شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌های برای MAC نیز انتخاب گردند. RFC 6668 استفاده از sha2 را در SSH مشخص می‌نماید.
۱۴۱ | **الزامات پروتکل SSH Server (۷)**
محصول باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1, ecdh-sha2-nistp256] و [انتخاب: ecdh-sha2-nistp384، ecdh-sha2-nistp521، هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.
۱۴۲ | **الزامات پروتکل SSH Server (۸)**

محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه؛ طول نشست بیشتر از یک ساعت نباشد و حجم داده مخابره شده بیشتر از ۱ گیگابایت نباشد، استفاده می‌گردد. در صورت پر شدن حد آستانه هر کدام از موارد ذکر شده، مجددسازی کلید باید صورت بگیرد.

نکته کاربردی ۱۰۲:

این الزام حدآستانه‌هایی را برای، حداکثر زمانی که یک کلیدهای نشست می‌تواند استفاده گردد و حداکثر مقدار داده‌ای که می‌تواند با یک کلیدهای نشست، انتقال یابد. هر دو حد آستانه باید پیاده‌سازی گردد و یک مجددسازی کلید نیز وقتی هر کدام از دو مورد مذکور سر برسد، باید بکار گرفته شود. برای محاسبه حداکثر داده انتقالی، داده‌هایی که به محصول وارد و از محصول خارج می‌شوند باید محاسبه گردد. مجددسازی کلید باید روی تمام کلیدهای نشست (رمزنگاری، حفاظت از جامعیت) برای ترافیک ورودی و خروجی اعمال گردد.

محصول همچنین می‌تواند مقادیری کمتر از مقادیر حد آستانه ذکر شده در این الزام را پیاده‌سازی نماید.

سند راهنمای محصول، باید نحوه پیکربندی این مقادیر و نحوه سر رسیدن آن‌ها و همچنین چگونگی امکان تعریف مقادیر کمتر از حد آستانه را تشریح نماید.

۶,۹ الزامات پروتکل TLS Client

شماره الزام	نام الزام
۱۴۳	**الزامات پروتکل TLS Client (۱)**
محصول باید [انتخاب: TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد نماید. همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: [انتخاب: o TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 o TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268 o TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق 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_192_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_192_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_192_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_192_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_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با5289 RFC
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289

o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289 [.
نکته کاربردی ۱۰۳: مجموعه‌های رمز که باید در پیکربندی ارزیابی‌شده آزمون شوند، توسط این الزام محدود شده‌اند. نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 5246، الزامی است. در نسخه‌های آتی این پروفایل حفاظتی، TLS v1.2 برای همه محصولات الزامی می‌گردد.

۱۴۴	**الزامات پروتکل TLS Client (۲)**

محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تائید نماید.

نکته کاربردی ۱۰۴:

قوانین مربوط به تائید شناسه در بخش ۶ از RFC 6125 توضیح داده شده‌اند. شناسه مرجع توسط سرپرست (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. کلاینت بر مبنای دامنه منبع و نوع سرویس برنامه کاربردی (مثلاً؛ HTTP، SIP، LDAP) مربوط به یک شناسه مرجع منحصربه‌فرد، همه شناسه‌های مرجع قابل‌قبول؛ نظیر یک Common Name برای قسمتName Subject از گواهی‌نامه و نام (حساس به بزرگ و کوچک بودن حروف) DNS، URI و سرویس برای قسمت Subject Alternative Name را منتشر می‌نماید. سپس کلاینت لیست همه شناسه‌های مرجع قابل‌قبول را با شناسه‌های ارائه‌شده در گواهی سرور TLS مقایسه می‌کند.

روش ترجیحی برای تائید شناسه، Subject Alternative Name است که از نام‌های DNS، URI، یا سرویس‌ها استفاده می‌کند. تائید شناسه با استفاده از Common Name برای اهدافی مانند سازگاری پس‌زمینه، الزامی است. به علاوه، استفاده از آدرس‌های IP در هرکدام از دو روش ذکر شده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود. همچنین کلاینت نباید برای ساختن شناسه‌های مرجع از wildcards استفاده نماید.

۱۴۵	**الزامات پروتکل TLS Client (۳)**

محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]].

نکته کاربردی ۱۰۵:

اگر در الزام FTP_TRP.1/Admin یا FTP_ITC پروتکل TLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود. اگر در الزام FTP_ITT پروتکل TLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود.
۱۴۶ **الزامات پروتکل TLS Client (۴)**
محصول باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب: secp256r1, secp384r1, secp521r1] و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد. **نکته کاربردی ۱۰۶:** اگر در الزام «الزامات پروتکل TLS Client (۱)» مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام «الزامات پروتکل TLS Client (۱)» هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب نگردد، عبارت "Supported Elliptic Curves Extension را ارائه نکند" باید انتخاب شود. این الزام مجموعه‌های رمز بیضوی مجاز برای احراز هویت و توافق کلید را به منحنی‌های NISTاز الزام‌های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌های که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.

۶,۱۰ الزامات پروتکل TLS Client/ احراز هویت

شماره الزام	نام الزام
۱۴۷	**الزامات پروتکلTLS Client/ احراز هویت ۱**
محصول باید [انتخاب: TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد نماید. همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: [انتخاب: o TLS_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268 o TLS_RSA_WITH_AES_192_CBC_SHAمطابق با RFC 3268 o TLS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268	

- TLS_DHE_RSA_WITH_AES_192_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_192_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_192_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_192_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_192_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_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با5289 RFC
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289

○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289].
نکته کاربردی ۱۰۷: مجموعه‌های رمز که باید در پیکربندی ارزیابی‌شده آزمون شوند، توسط این الزام محدود شده‌اند. نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 5246، الزامی است. در نسخه‌های آتی این پروفایل حفاظتی، TLS v1.2 برای همه محصولات الزامی می‌گردد.
۱۴۸ | **الزامات پروتکلTLS Client/ احراز هویت ۲**
محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تائید نماید. **نکته کاربردی ۱۰۸:** قوانین مربوط به تائید شناسه در بخش ۶ از RFC 6125 توضیح داده شده‌اند. شناسه مرجع توسط سرپرست (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. کلاینت بر مبنای دامنه منبع و نوع سرویس برنامه کاربردی (مثلاً؛ HTTP، SIP، LDAP) مربوط به یک شناسه مرجع منحصربه‌فرد، همه شناسه‌های مرجع قابل‌قبول؛ نظیر یک Common Name برای قسمتName Subject از گواهی‌نامه و نام (حساس به بزرگ و کوچک بودن حروف) DNS، URI و سرویس برای قسمت Subject Alternative Name را منتشر می‌نماید. سپس کلاینت لیست همه شناسه‌های مرجع قابل‌قبول را با شناسه‌های ارائه‌شده در گواهی سرور TLS مقایسه می‌کند. روش ترجیحی برای تائید شناسه، Subject Alternative Name است که از نام‌های DNS، URI، یا سرویس‌ها استفاده می‌کند. تائید شناسه با استفاده از Common Name برای اهدافی مانند سازگاری پس‌زمینه، الزامی است. به علاوه، استفاده از آدرس‌های IP در هرکدام از دو روش ذکر شده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود. همچنین کلاینت نباید برای ساختن شناسه‌های مرجع از wildcards استفاده نماید.
۱۴۹ | **الزامات پروتکلTLS Client/ احراز هویت ۳**
محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]].

نکته کاربردی ۱۰۹:

اگر در الزام FTP_TRP.1/Admin یا FTP_ITC پروتکل TLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود.

اگر در الزام FTP_ITT پروتکل TLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود.

۱۵۰	**الزامات پروتکلTLS Client/ احراز هویت ۴**

محصول باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب:secp256r1, secp384r1, secp521r1] و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد.

نکته کاربردی ۱۱۰:

اگر در الزام «الزامات پروتکلTLS Client/ احراز هویت ۱» مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام «الزامات پروتکلTLS Client/ احراز هویت ۱» هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب نگردد، عبارت "Supported Elliptic Curves Extension را ارائه نکند" باید انتخاب شود. این الزام مجموعه‌های رمز بیضوی مجاز برای احراز هویت و توافق کلید را به منحنی‌های NISTاز الزام‌های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌های که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.

۱۵۱	**الزامات پروتکلTLS Client/ احراز هویت ۵**

محصول باید احراز هویت دوطرفه را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.

نکته کاربردی ۱۱۱:

استفاده از گواهی‌نامه‌های X509v3 برای پروتکل TLS در الزام FIA_X509_EXT.2.1 ارائه شده است. در این الزام بیان می‌شود که کلاینت باید برای احراز هویت دوطرفه TLS، قادر باشد یک گواهی‌نامه به سرور TLS ارائه نماید.

۶,۱۱ الزامات پروتکل TLS Server

شماره الزام	نام الزام
۱۵۲	**الزامات پروتکل TLS Server (۱)**

محصول باید [انتخاب: TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد نماید. همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید:

[انتخاب:

- TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
- TLS_RSA_WITH_AES_192_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_192_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_192_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_192_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_192_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_192_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_192_GCM_ SHA256 مطابق با RFC 5288
- TLS _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_192_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_SHA256مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق باRFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289].
نکته کاربردی ۱۱۲: مجموعه‌های رمز که باید در پیکربندی ارزیابی‌شده آزمون شوند، توسط این الزام محدود شده‌اند. نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 5246، الزامی است. در نسخه‌های آتی این پروفایل حفاظتی، TLS v1.2 برای همه محصولات الزامی می‌گردد.
۱۵۳ | **الزامات پروتکل TLS Server (۲)**
محصول باید برای کلاینت‌های دارای درخواست SSL 2.0، SSL 3.0، TLS 1.0 [انتخاب: TLS 1.1، TLS 1.2، هیچ موردی]، ارتباطات را ایجاد نکند. **نکته کاربردی ۱۱۳:** تمامی نسخه‌های SSL و TLS v1.0 رد می‌شوند. هر نسخه‌ای از TLS که در الزام «الزامات پروتکل TLS Server (۱)» انتخاب نگردد، باید در الزام آورده شود.
۱۵۴ | **الزامات پروتکل TLS Server (۳)**
محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸بیت، ۳۰۷۲بیت، ۴۰۹۶بیت] اجرا نماید؛ پارامترهای EC-دیفی‌هلمن را به همراه منحنی‌های NIST[انتخاب:secp256r1, secp384r1, secp521r1] و هیچ منحنی دیگری، تولید نماید؛ پارامترهای دیفی‌هلمن را با اندازه [انتخاب: ۲۰۴۸بیت، ۳۰۷۲بیت] تولید کند].

نکته کاربردی ۱۱۴:

اگر سند هدف امنیتی در الزام «الزامات پروتکل TLS Server (۱)» مجموعه‌های رمز DHE و ECDHE را ارائه کرده باشد، نویسنده سند هدف امنیتی باید امکان انتخاب دیفی‌هلمن یا منحنی‌های NIST را در الزام بگنجاند. الزام FMT_SMF.1 پیکربندی پارامترهای توافق کلید را برای برقراری یک ارتباط TLS ملزم می‌کند که از لحاظ امنیتی قوی باشد.

۶,۱۲ الزامات پروتکل TLS Server/ احراز هویت دو طرفه

شماره الزام	نام الزام
۱۵۵	**الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۱**

محصول باید [انتخاب: TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد نماید.
همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید:
[انتخاب:

- TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
- TLS_RSA_WITH_AES_192_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_192_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_192_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_192_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_192_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_192_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_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_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_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با5289 RFC
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289

].

نکته کاربردی ۱۱۵:

مجموعه‌های رمز که باید در پیکربندی ارزیابی‌شده آزمون شوند، توسط این الزام محدود شده‌اند.

نویسنده سند هدف امنیتی باید مجموعه‌های رمز پشتیبانی شده را انتخاب کند. محدود کردن مجموعه‌های رمز که می‌تواند در پیکربندی ارزیابی‌شده سرپرستی بر روی سرور در محیط آزمون، استفاده گردند، ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA در این پروفایل حفاظتی اجباری نیست ولی در صورت ادعای انطباق با RFC 5246، الزامی است.

در نسخه‌های آتی این پروفایل حفاظتی، TLS v1.2 برای همه محصولات الزامی می‌گردد.
۱۵۶ | **الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۲**
محصول باید برای کلاینت‌های دارای درخواست SSL 2.0، SSL 3.0، TLS 1.0 [انتخاب: TLS 1.1، TLS 1.2، هیچ موردی]، ارتباطات را ایجاد نکند. **نکته کاربردی ۱۱۶:** تمامی نسخه‌های SSL و TLS v1.0 رد می‌شوند. هر نسخه‌ای از TLS که در الزام «الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۱» انتخاب نگردد، باید در الزام آورده شود.
۱۵۷ | **الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۳**
محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸بیت، ۳۰۷۲بیت، ۴۰۹۶بیت] اجرا نماید؛ پارامترهای EC-دیفی‌هلمن را به همراه منحنی‌های NIST[انتخاب:secp256r1, secp384r1, secp521r1] و هیچ منحنی دیگری، تولید نماید؛ پارامترهای دیفی‌هلمن را با اندازه [انتخاب: ۲۰۴۸بیت، ۳۰۷۲بیت] تولید کند]. **نکته کاربردی ۱۱۷:** اگر سند هدف امنیتی در الزام «الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۱» مجموعه‌های رمز DHE و ECDHE را ارائه کرده باشد، نویسنده سند هدف امنیتی باید امکان انتخاب دیفی‌هلمن یا منحنی‌های NIST را در الزام بگنجاند. الزام FMT_SMF.1 پیکربندی پارامترهای توافق کلید را برای برقراری یک ارتباط TLS ملزم می‌کند که از لحاظ امنیتی قوی باشد.
۱۵۸ | **الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۴**
محصول باید احراز هویت دوطرفه کلاینت‌های TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.
۱۵۹ | **الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۵**
محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]]. **نکته کاربردی ۱۱۸:** استفاده از گواهی‌نامه‌های X509v3 برای پروتکل TLS در الزام FIA_X509_EXT.2.1 ارائه شده است. در این الزام بیان می‌شود که گواهی‌نامه‌های سمت کلاینت باید برای احراز هویت دوطرفه TLS پشتیبانی گردند. اگر در الزام FTP_TRP یا FTP_ITC پروتکل TLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود. اگر در الزام FTP_ITT پروتکل TLS انتخاب گردد، آنگاه اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/ITT آزموده می‌شود.

۱۶۰	الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۶
محصول در صورت مطابقت نداشتن؛ نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه که از شناساننده[۱] کلاینت انتظار بوده است، نباید کانال امن را برقرار سازد. **نکته کاربردی ۱۱۹:** شناساننده کلاینت ممکن است در فیلد subject یا افزونه نام دیگر فاعل مربوط به یک گواهی‌نامه باشد. شناساننده مورد انتظار باید پیکربندی گردد. این شناساننده ممکن است با نام دامنه، آدرس IP، یا ادرس ایمیل که توسط نظیر استفاده می‌گردد، مقایسه گردد. همچنین ممکن است این شناساننده برای مقایسه، به یک دایرکتوری سرور داده شود.	

۶,۱۳ الزامات شناسایی و احراز هویت

شماره الزام	نام الزام
۱۶۱	الزامات پروتکل X509 (۱)/ ابطال
محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تائید کند: • تائید گواهی‌نامه RFC 5280 و تائید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند. • مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد. • محصول 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 • محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC 6960، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۶,۳، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵، هیچ روش فسخ] تائید کند. • محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تائید کند: ○ گواهی‌نامه‌های مورداستفاده برای تائید 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	

[۱] Identifier

- 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-kp1 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.

۱۶۲	**الزامات پروتکل X509 (۲)/ ابطال**

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

نکته کاربردی ۱۲۰:

الزام «الزامات پروتکل X509 (۱)/ ابطال» قوانین برای تائید گواهی‌نامه‌ها را فهرست می‌کند. نوسینده سند هدف امنیتی باید مشخص نماید که تائید ابطال بر اساس OCSP یا CRLs انجام می‌گیرد. پروتکل‌های مسیر/کانال امن ممکن است استفاده از گواهی‌نامه‌ها را الزامی کنند؛ در این صورت، قوانین ExtendedKeyUsage باید بررسی و تائید شده باشند. اگر محصول قابلیت عملکردی که از انواع گواهی‌نامه‌های فهرست شده در قوانین ExtendedKeyUsage استفاده می‌کند را پشتیبانی نمی‌کند، این وضعیت باید در سند خلاصه مشخصات محصول شرح داده شود.

محصول باید از حداقل طول مسیر برای دو گواهی‌نامه پشتیبانی کند. بدین معنی که محصول باید از یک سلسله مراتب گواهی‌نامه که حداقل از گواهی‌نامه ریشه خود-امضاء و گواهی‌نامه هویت محصول تشکیل شده باشد، پشتیبانی نماید.

انتظار می‌رود که تائید گواهی‌ها تا یک گواهی‌نامه CA ریشه مورداعتماد در داخل یک منبع ریشه که به‌وسیله پلتفرم مدیریت می‌شود، انجام گیرد.

سند خلاصه مشخصات محصول باید مشخص نماید که چه مواقعی بررسی وضعیت فسخ انجام می‌گیرد. انتظار می‌رود که وقتی از گواهی‌نامه در احراز هویت استفاده می‌گردد، وضعیت فسخ نیز بررسی گردد. بررسی وضعیت یک گواهی‌نامه X509 فقط وقتی که روی دستگاه بارگذاری می‌شود، کافی نیست.

بررسی و تائید کردن وضعیت ابطال گواهی‌نامه‌های X509، حین روشن‌شدن و خودآزمایی‌ها ضروری نیست.

الزام «الزامات پروتکل X509 (۲)/ ابطال» 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.

نویسنده سند هدف امنیتی در تمامی موارد به جزء؛ وقتی فقط SSH در FTP_ITC.1 یا FPT_ITT.1 انتخاب گردد و احراز هویت به ssh-rsa، ssh-sha2-nistp256، ssh-sha2-nistp384 یا/و ssh-sha2-nistp521 محدود شده باشد، باید الزامات «الزامات پروتکل X509 (۱) و (۲)/ ابطال» را وارد نماید. به علاوه، وقتی که در FPT_TUD_EXT یا FPT_TST_EXT استفاده از گواهی X509 انتخاب گردد، الزامات «الزامات پروتکل X509 (۱) و (۲)/ ابطال» باید آورده شود.
۱۶۳ **الزامات پروتکل X509 (۳)**
محصول مورد ارزیابی باید جهت پشتیبانی احراز هویت برای [انتخاب: IPsec, DTLS, TLS, HTTPS, SSH] و [انتخاب: امضای کد برای به‌روزرسانی‌های نرم‌افزار سیستم، امضای کد برای تائید یکپارچگی، [اختصاص: سایر کاربردها]، هیچ کاربرد دیگر] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.
۱۶۴ **الزامات پروتکل X509 (۴)**
زمانی که محصول مورد ارزیابی نمی‌تواند اتصال مورد نیاز برای تائید اعتبار یک گواهی‌نامه را برقرار کند، باید [انتخاب: به سرپرست محصول اجازه دهد که در این مورد تصمیم‌گیری کند، گواهی‌نامه را بپذیرد، گواهی‌نامه را نپذیرد].

نکته کاربردی ۱۲۱:

در الزام «الزامات پروتکل X509 (۳)»، انتخاب نویسنده سند هدف امنیتی شامل IPsec، TLS، یا HTTPS می‌شود در صورتی که این پروتکل‌های در الزامات FTP_ITC.1.1 یا FPT_ITT.1 گنجانده شده باشند. اگر احرازهویتی غیر از ssh-rsa، ecdsa-sha2-nistp256، ecdsa-sha2-nistp384 و/یا ecdsa-sha2-nistp521، در الزام «الزامات پروتکل SSH Client (۵)» بیان شده باشد یا گواهی‌نامه‌های آن برای به‌روزرسانی‌های امن نرم‌افزار سیستم (FPT_TUD_EXT.2) و تائید جامعیت (FPT_TST_EXT.2) استفاده شده باشد، آنگاه الزام «الزامات پروتکل X509 (۳)» باید پروتکل SSH را نیز شامل گردد.

معمولاً برای بررسی وضعیت فسخ یک گواهی‌نامه باید اتصالی را برقرار نمود. این اتصال هم برای دانلود کردن یک CRL و هم برای جستجو با استفاده از OCSP لازم است. با استفاده از "انتخاب" در این الزام، می‌توان تعیین نمود که اگر برقراری این اتصال ممکن نباشد، باید چه اقدامی را انجام داد. اگر محصول مورد ارزیابی بر اساس تمام قوانین مورداشاره در الزامات «الزامات پروتکل X509 (۱) و (۲)» به این نتیجه برسد که گواهی‌نامه معتبر است، می‌تواند آن را بپذیرد. اگر هر یک از این قوانین نشان‌دهنده عدم تائید گواهی‌نامه باشند، محصول مورد ارزیابی نباید آن را بپذیرد. اگر نویسنده هدف امنیتی انتخاب اول را انجام دهد و به سرپرست محصول قدرت تصمیم‌گیری بدهد، باید تابع مربوطه از FMT_SMF.1 را نیز انتخاب نماید. این انتخاب باید با الزامات FCS_IPSEC_EXT.1.14، FCS_TLSC_EXT.1.3 و FCS_TLSC_EXT.2.3 سازگار باشد.

در صورتی که محصول توزیع‌شده باشد و الزام FIA_X509_EXT.1/ITT برای آن انتخاب شده باشد، بررسی وضعیت فسخ گواهی، اختیاری است.

۱۶۵	الزامات پروتکل X509 (۵)
محصول مورد ارزیابی باید مطابق با آنچه که در RFC 2986 تشریح شده است، یک Certificate Request Message تولید کند و بتواند اطلاعات؛ کلید عمومی و [انتخاب: اطلاعات مخصوص به دستگاه[۱]، Common Name، Orgsnization، Organization Unit، Country] را در درخواست فراهم کند. **نکته کاربردی ۱۲۲:** کلید عمومی در واقع بخش عمومی از جفت کلیدهای عمومی-خصوصی است که بر اساس آن چه در FCS_CKM.1 شرح داده‌شده است، توسط محصول مورد ارزیابی تولید می‌شود.	
۱۶۶	**الزامات پروتکل X509 (۶)**
محصول مورد ارزیابی باید زنجیره گواهی‌نامه‌ها از Root CA را بر اساس پاسخ گواهینامه‌های CA دریافت شده اعتبارسنجی کند.	

۶,۱۴ الزامات خودآزمایی محصول مورد ارزیابی

شماره الزام	نام الزام
۱۶۷	**خودآزمایی محصول مورد ارزیابی ۲**
اگر برای آزمون‌های خودآزمایی از یک گواهی‌نامه استفاده شود و آن گواهی‌نامه غیرمعتبر اعلام‌شده باشد، محصول باید در آزمون خودآزمایی ناموفق باشد. **نکته کاربردی ۱۲۳:** گواهی‌نامه‌ها را می‌توان به‌صورت اختیاری برای آزمون‌های خودآزمایی استفاده کرد (FPT_TST_EXT.1.1). اگر برای آزمون‌های خودآزمایی از گواهی‌نامه‌ها استفاده شود، سند هدف امنیتی باید شامل این مورد باشد. اگر در «الزامات پروتکل X509 (۳)» مقدار "امضای کد برای تائید یکپارچگی" انتخاب‌شده باشد، سند هدف امنیتی باید شامل «خودآزمایی محصول مورد ارزیابی۲» باشد. اعتبار به‌وسیله مسیر گواهی‌نامه، تاریخ انقضاء و وضعیت ابطال مطابق با FIA_X509_EXT.1/Rev تعیین می‌گردد.	
۱۶۸	**الزامات به‌روزرسانی امن ۴**

[۱] Device-specific information

محصول درصورتی‌که گواهی‌نامه امضای کد یک به‌روزرسانی غیرمعتبر باشد، نباید آن را نصب نماید.

۱۶۹	**الزامات به‌روزرسانی امن ۵**

هنگامی‌که گواهی‌نامه به علت انقضای آن، غیر معتبر اعلام‌شده است، محصول باید [انتخاب: اجازه بدهد که در این موارد سرپرست محصول در موردپذیرش گواهی تصمیم‌گیری نماید، گواهی را بپذیرد، گواهی را نپذیرد].

نکته کاربردی ۱۲۴:

گواهی‌نامه‌ها را می‌توان به‌صورت اختیاری برای امضای کدها در به‌روزرسانی‌های نرم‌افزار سیستم استفاده کرد (FPT_TUD_EXT.1.3). اگر در «الزامات پروتکل X509 (۳)» مقدار "امضای کد برای به‌روزرسانی‌های نرم‌افزار سیستم" انتخاب‌شده باشد، سند هدف امنیتی باید شامل «خودآزمایی محصول مورد ارزیابی۲» باشد. در صورتی که فقط از هش‌های انتشار یافته برای به‌روزرسانی‌های امن پشتیبانی گردد، گواهی X509 قابل اعمال نیست.

اعتبار به‌وسیله مسیر گواهی‌نامه، تاریخ انقضاء و وضعیت ابطال مطابق با تمامی FIA_X509_EXT.1/Rev تعیین می‌گردد. برای گواهی‌نامه‌های منقضی، نویسنده هدف امنیتی انتخاب می‌کند که گواهی‌نامه پذیرفته شود، رد شود یا تصمیم‌گیری در خصوص پذیرش یا رد گواهی‌نامه به سرپرست محصول واگذار شود.

۶,۱۵ الزامات به‌روزرسانی امن

شماره الزام	نام الزام
۱۷۰	**مدیریت کارکرد در محصول مورد ارزیابی ۱/ به‌روزرسانی خودکار**

محصول باید قابلیت [انتخاب: فعال کردن و غیرفعال کردن] توابع [انتخاب: جستجو برای به‌روزرسانی‌های خودکار، به‌روزرسانی خودکار] را به سرپرست امنیتی محصول محدود نماید.

نکته کاربردی ۱۲۵:

این الزام تنها زمانی قابل پیاده‌سازی است که محصول امکان پشتیبانی از جستجو برای به‌روزرسانی‌های خودکار و/یا به‌روزرسانی خودکار را فراهم کند و اجازه فعال و غیرفعال کردن این قابلیت‌ها را بدهد. فعال کردن و غیرفعال کردن جستجو برای به‌روزرسانی‌های خودکار

و/یا به‌روزرسانی خودکار به سرپرست‌های امنیتی محصول محدود شده است. گزینه "به‌روزرسانی خودکار" ممکن است فقط وقتی انتخاب شود که از امضاء دیجیتال برای تائید به‌روزرسانی امن استفاده گردد.
۱۷۱ | **مدیریت کارکرد در محصول مورد ارزیابی ۱/ توابع**
محصول باید قابلیت [انتخاب: تعیین رفتار[۱]، تغییر/اصلاح رفتار[۲]] مربوط به توابع [انتخاب: مخابره داده ممیزی به موجودیت IT خارجی، کنترل داده ممیزی، قابلیت عملکردی ممیزی درصورت پر بودن فضای محلی ذخیره‌سازی] را به سرپرست امنیتی محصول محدود نماید. **نکته کاربردی ۱۲۶:** این الزام در صورتی انتخاب می‌گردد که یک یا چند مورد از سناریوهای زیر اعمال شوند: • اگر پروتکل انتقال برای ارسال داده ممیزی به موجودیت IT خارجی که در الزام FAU_STG_EXT.1.1 تعریف شده است، قابل پیکربندی باشد و "ارسال داده ممیزی به موجودیت IT خارجی" انتخاب شده باشد. • اگر کنترل داده ممیزی قابل پیکربندی باشد، "کنترل داده ممیزی" باید انتخاب گردد. عبارت "کنترل داده ممیزی" به گزینه‌های مختلفی برای انتخاب و اختصاص در الزامات FAU_STG_EXT.1.2، FAU_STG_EXT.1.3 و FAU_STG_EXT.2/LocSpace اشاره دارد. • اگر رفتار قابلیت عملکردی ممیزی وقتی که فضای محلی ذخیره‌سازی ممیزی پر است، قابل پیکربندی باشد. عبارت "قابلیت عملکرد ممیزی درصورت پر بودن فضای محلی ذخیره‌سازی" باید انتخاب گردد.

۷ مراجع

- **Network Devices cPP V2.0 published by Network iTC**
- **Intrusion Detection System Protection Profile V 1.7 Published by U.S. Government Protection Profile**

[۱] Determine the behaviour

[۲] Modify the behaviour