به نام خدا

پروفایل حفاظتی سامانه مدیریت دسترسی خاص (PAM)

آذر ۹۶

نسخه ۱,۰

پیشگفتار

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی که در این سند برای برآورده کردن الزامات ارائه‌شده‌اند را در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد. مرکز مدیریت راهبردی افتا با همکاری سازمان فناوری اطلاعات ایران این سند را در راستای این هدف تهیه کرده است. این سند معرفی کننده‌ی الزامات کارکرد امنیتی برای محصولات «سامانهٔ مدیریت دسترسی خاص (PAM)[۱]» است؛ تا تولیدکنندگان این نوع محصولات بتوانند بر مبنای این سند، کارکردهای امنیتی را در محصول خود لحاظ نموده و همچنین سند هدف امنیتی آن را ارائه نمایند.

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

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

[۱] Privilege Access Management

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

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

فهرست

۱ اصطلاحات

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

متدلوژی ارزیابی معیار مشترک[۱] (CEM): متدلوژی ارزیابی معیار مشترک برای ارزیابی امنیت فناوری‌های اطلاعات.

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

پروفایل حفاظتی (PP[۲]): مجموعه‌ای از الزامات امنیتی برای دسته‌ای از محصولات؛ مجموعه‌ای که مستقل از پیاده‌سازی است.

هدف امنیتی (ST[۳]): مجموعه‌ای از الزامات امنیتی برای یک محصول خاص؛ مجموعه‌ای که وابسته به پیاده‌سازی است.

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

سطح تضمین ارزیابی (EAL[۴]): مجموعه‌ای از الزامات تضمین که از قسمت سوم از سندهای سه‌گانه «استاندارد ارزیابی معیار مشترک» برگرفته شده است و نشان‌دهنده سطح امنیتی محصول است. سطوح تضمین از سطح ۱ تا سطح ۷ می‌باشند، لازم به ذکر است که «سطح تضمین امنیتی» یک نوع «بسته» است.

خلاصه مشخصه محصول[۵] (TSS): شرحی از این‌که یک محصول چگونه الزامات کارکرد امنیتی را در یک هدف امنیتی برآورده می‌سازد.

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

---

[۱] Common Evaluation Methodology(CEM)

[۲] Protection Profile

[۳] Security Target

[۴] Evaluation Assurance Level

[۵] TOE Summary Specification (TSS)

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

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

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

مشخصه‌های امنیتی: می‌تواند شامل مشخصه‌های امنیتی موجودیت فعال (از قبیل شناسه کاربر، کلمه عبور، نقش‌های کاربر، جزئیات واسط کاربر، پیشینه احراز هویت) و یا مشخصه‌های امنیتی غیرفعال (از قبیل نوع، نام و اندازه مستند) باشد.

داده‌های محصول: می‌تواند شامل داده‌های ممیزی، کلیدها، مقادیر تنظیمات محصول و داده‌های احراز هویت و از این نوع داده‌ها باشد.

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

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

۲ شرح محصول

امروزه با رشد روزافزون فناوری اطلاعات و ارتباطات در سازمان‌ها، یکی از مسائل مهمی که در سازمان‌ها باید در نظر گرفته شود امنیت است. از طرفی، خطرات مختلفی از قبیل خطرات داخل و بیرونی، سازمان‌ها را تهدید می‌کنند؛ بنابراین استفاده از تجهیزات و سیاست‌ها و امکانات امنیتی می‌تواند نقش مهمی را در تأمین امنیت سازمان‌ها ایفا نماید. یکی از ابزارهای مهم در جلوگیری و کاهش تهدیدات، سامانه PAM است.

سامانه PAM به سامانه‌هایی اشاره دارد که به منظور مدیریت دسترسی مجموعه‌ای از «دارایی‌های فناوری اطلاعات» در یک سازمان مورد استفاده قرار می‌گیرد. این نوع سامانه‌ها از خط‌مشی‌هایی مانند زیر تعریف می‌شوند:

- **خط‌مشی کنترل دسترسی:** خط‌مشی‌هایی که اجرای عملیات، از سوی یک موجودیت فعال بر روی یک موجودیت غیرفعال را رد یا تائید می‌کند.
- **خط‌مشی شناسایی و اعتبارسنجی:** خط‌مشی‌هایی که پارامترهای لازم برای شناسایی، احراز هویت، اعتبارسنجی و پاسخگویی یک موجودیت فعال را تعریف و نگهداری می‌کنند.
- **خط‌مشی‌های ویژگی‌های موجودیت‌های غیرفعال:** خط‌مشی‌هایی که ویژگی‌های موجودیت‌های غیرفعال را تعریف و نگهداری می‌کنند.
- **خط‌مشی‌های پیکربندی امن**: خط‌مشی‌هایی که اصول اولیه پیکربندی برای دارایی‌های IT را تعریف می‌کنند.
- **خط‌مشی‌های ممیزی**: خط‌مشی‌هایی که چگونگی جمع‌آوری، یکپارچه‌سازی، گزارش دهی و نگهداری داده‌های ممیزی را تعریف می‌کنند.

سامانه PAM که خط‌مشی‌های مختلف را مدیریت و اعمال می‌کند، امنیت را به گونه‌های زیر پیاده‌سازی می‌کند:

- **پیشگیرانه**[۱]: در این روش با نقض یک خط‌مشی، اجرای عملیات به روی دارایی‌های IT ممنوع خواهد شد.

[۱] -Preventive

- **واکنش‌گرانه**[۱]: دارایی‌های IT با یک قوانین امن مرکزی تعریف‌شده در سازمان مقایسه می‌شوند و عملیات در صورتی انجام می‌شود که تفاوت‌ها شناسایی شود.

۲,۱ مروری بر پروفایل حفاظتی سامانه PAM

این پروفایل بر روی تصمیمات کنترل دسترسی و اعمال آن‌ها تمرکز دارد. محصولی که مطابق این پروفایل حفاظتی باشد، یک خط‌مشی کنترل دسترسی را تعریف و اعمال می‌کند که با این کار، امنیت پیشگیرانه‌ای را در سازمان بکار می‌گیرد. محصولی که مطابق با این پروفایل حفاظتی باشد، می‌بایست درخواست‌هایی که برای دسترسی به انواع منابع تعریف‌شده می‌شود را بررسی و تائید یا رد شدن درخواست را تعیین کند.

مؤلفه‌های کنترل دسترسی به عنوان بخشی از مؤلفه‌های سامانه PAM به حساب می‌آیند. یک مؤلفه کنترل دسترسی می‌بایست دارای قابلیت‌های زیر باشد:

- تعریف خط‌مشی متمرکز: یک قابلیت مدیریت خط‌مشی متمایز این است که مجموعه قوانینی را برای تصمیمات خط‌مشی محصول کنترل دسترسی تعریف نماید. این قوانین شامل عملیات-موجودیت‌های فعال و موجودیت‌های غیرفعال خواهد بود. موجودیت‌های فعال و غیرفعال توسط مشخص‌های تعیین‌شده سازمانی (از قبیل نام کاربری، موقعیت جغرافیایی، آدرس URL از یک منبع محافظت‌شده و زمان) تعریف‌شده هستند.
- تعریف موجودیت فعال مرکزی: یک قابلیت مدیریت شناسایی و احراز هویت باید یک تعریف واحد از کاربران داشته باشد.
- تعریف موجودیت غیرفعال: در بیشتر موارد انتظار می‌رود که مشخصه‌های موجودیت غیرفعال که توسط محصول کنترل دسترسی بررسی می‌شوند بخش ذاتی موجودیت غیرفعال در محیط عملیاتی خواهد بود. به عنوان مثال، مدیر بررسی وب ممکن است URL صفحه وب یا زمان دسترسی به آن را بررسی نماید.
- پشتیبانی از ممیزی متمرکز: یک سرور ممیزی جدا و متمایز داده‌های ممیزی را برای اهداف گزارش-گیری و مدیریت حوادث جمع‌آوری می‌نماید.

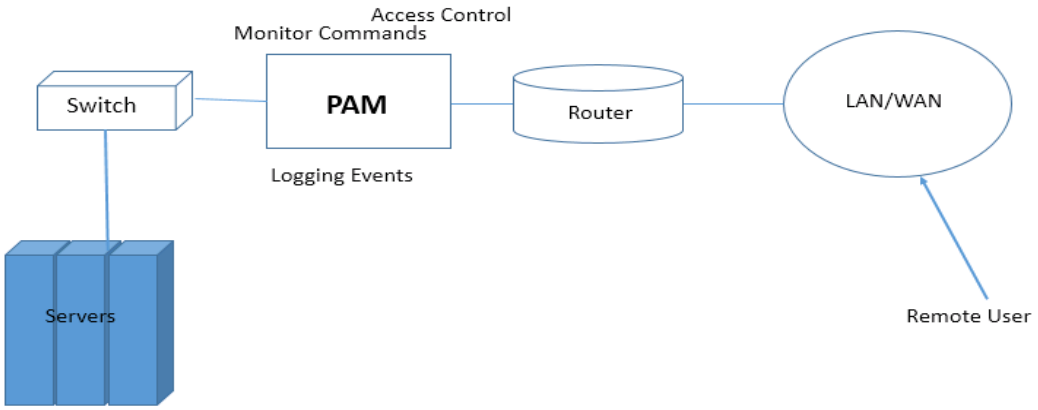
---

[۱] -Reactive

شکل ۱ معماری قرارگیری و نیز برخی از ماژول‌های سامانه PAM را نشان می‌دهد.

هنگام تهیه سند هدف امنیتی مطابق با این پروفایل حفاظتی، نویسنده باید به‌طور واضح انواع فنّاوری که در محصول بکار رفته است را شناسایی نماید. فنّاوری‌ها باید الزامات حفاظت از داده‌های کاربری را تحت پوشش قرار دهند.

بدون در نظر گرفتن نوع فنّاوری، ضروری است که محصول موجودیت‌های فعال و مشخصه‌های تعریف‌شده در سازمان‌ها را مطابق با این پروفایل حفاظتی مدیریت نماید. نویسنده هدف امنیتی باید داده‌های سازمانی را که در محصول استفاده خواهد شد را تعریف نماید. منابع امنی که داده‌ها را دریافت کرده و سازوکار تفسیر داده‌ها (از قبیل SAML یا گواهینامه X.509) باید ذکر شود.



شکل ۱- شمایی از سامانه مدیریت امنیت

۳ تعریف مسائل امنیتی

هر سامانه PAM باید مجموعه‌ای از حداقل کارکرد امنیتی مشترک[۱] که از آن‌ها انتظار می‌رود را ارائه نماید. حداقل کارکرد امنیتی مشترک برای مقابله با تهدیدات مشترک پیش روی این محصولات، مسئله امنیتی است که یک «سامانه PAM" مطابق با پروفایل حاضر باید به آن بپردازد. این تهدیدات در مقابل تهدیداتی قرار می‌گیرند که یک کارکرد خاص از یک نوع خاص از سامانه PAM را هدف قرار می‌دهند. مجموعه حداقل کارکرد امنیتی مشترک باید قابلیت‌های زیر را داشته باشند:

- برقراری ارتباط با دستگاه‌های مجاز و غیرمجاز شبکه

[۱] Common security functionality

- توانایی انجام به‌روزرسانی‌های معتبر و امن
- توانایی ممیزی فعالیت‌های دستگاه‌ها
- توانایی ذخیره‌سازی و استفاده امن از داده‌ها و اطلاعات محرمانه سرپرست و دستگاه
- توانایی انجام خودآزمایی برای ازکارافتادن مؤلفه‌های حیاتی دستگاه.

۳,۱ تهدیدات

در ادامه، تهدیدات پیش روی سامانه‌های PAM بر اساس عملکرد آن‌ها 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.

۳,۱,۱ ارتباط با دستگاه‌های شبکه

یک سامانه PAM با موجودیت‌های شبکه ارتباط برقرار می‌کند. مقصد این ارتباط ممکن است از لحاظ منطقی یا جغرافیایی یک دستگاه راه دور به شمار آید و مسیر ارتباط ممکن است از سامانه‌های متعدد دیگری بگذرد. این احتمال وجود دارد که سامانه‌های میانی مورد اعتماد نباشند و ارتباط غیرمجاز با دستگاه شبکه برقرار کنند یا ارتباطات مجاز را در معرض خطر قرار دهند. کارکرد امنیتی محصول 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 سامانه 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 حفاظت از این ارتباطات نیازمند استفاده از یک کانال امن است. کارکرد امنیتی سامانه PAM 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.

۳,۱,۱,۱ دسترسی سرپرستی غیرمجاز

ممکن است عامل تهدید تلاش کند تا با استفاده از ابزارهای بدخواهانه، به سامانه PAM دسترسی سرپرستی پیدا کند. به عنوان مثال، عامل تهدید خود را به عنوان سرپرست به سامانه معرفی می‌کند، 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 دسترسی پیدا کند. بدین ترتیب، عامل تهدید قادر خواهد بود تا اقدامات بدخواهانه‌ای را انجام دهد و کارکرد امنیتی دستگاه و شبکه را به خطر اندازد.

منطق الزام کارکرد امنیتی (SFR):

- نقش سرپرست در الزام FMT_SMR.2 تعریف‌شده است و توانایی‌های سرپرستی مربوطه نیز در الزامات FMT_SMF.1 و FMT_MTD.1/CoreData تعریف‌شده‌اند و همچنین توانایی‌های اضافه اختیاری نیز در الزامات FMT_MOF.1/Services و FMT_MOF.1/Functions تعریف‌شده 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 راه دور) و FTA_SSL_EXT.4 (برای تمامی نشست‌های تعاملی) تضمین می‌شود.
- کانال امن برای ارتباطات سرپرست راه دور 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.)

۳٫۱٫۱٫۲ *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.

۳,۱,۱,۳ کانال‌های ارتباطی غیرقابل‌اعتماد

ممکن است عامل تهدید آن دسته از سامانه‌های PAM 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 سامانه PAM را به خطر اندازند.

منطق الزام کارکرد امنیتی:

- استفاده عمومی پروتکل‌های امن برای کانال‌های ارتباطی تعریف‌شده، به صورت سطح بالا در الزامات FTP_ITC.1 و FTP_TRP.1/Admin مشخص شده است؛ برای محصولات توزیع‌شده، 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 تعریف‌شده‌اند.

۳,۱,۱,۴ 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 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 سامانه PAM 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 توزیع‌شده، 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.

۳,۱,۲ به‌روزرسانی‌های معتبر

برای حصول اطمینان از صحت کارکرد امنیتی سامانه PAM، 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 سامانه 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 به‌روز نشده نرم‌افزارها یا ثابت‌افزارها می‌توانند سامانه PAM را در معرض خطر عوامل تهدیدی قرار دهند که در پی سوءاستفاده از آسیب‌پذیری‌های شناخته‌شده آن‌ها هستند. به‌روزرسانی‌های تائید نشده یا به‌روزرسانی‌هایی که با استفاده از ابزارهای رمزنگاری ضعیف یا غیر امن تائید شده‌اند، نرم‌افزار یا ثابت‌افزار به‌روز شده را در معرض خطر عوامل تهدیدی قرار می‌دهند که به دنبال بهره‌گیری از نرم‌افزار یا ثابت‌افزار برای رسیدن به مقاصد خویش هستند.

۳,۱,۲,۱ به‌روزرسانی‌های مخرب

ممکن است عامل تهدید یک به‌روزرسانی معیوب و دستکاری‌شده‌ای را برای نرم‌افزار یا ثابت‌افزار سامانه PAM ارائه کند و کارکرد امنیتی دستگاه را در معرض خطر قرار دهد. به‌روزرسانی‌های تائید نشده یا به‌روزرسانی‌هایی که با استفاده از رمزنگاری ضعیف یا غیر امن تائید شده‌اند، نرم‌افزار یا ثابت‌افزار به‌روز شده 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.

۳,۱,۳ فعالیت ممیزی شده

سرپرستان می‌توانند با ممیزی فعالیت‌های سامانه PAM، وضعیت سامانه را به خوبی پایش نمایند. این فرایند امکان بررسی، گزارش دهی در خصوص کارکردهای امنیتی، بازسازی رویدادها و تحلیل مشکل امنیتی را برای سرپرست فراهم می‌آورد. پردازش‌هایی که در پاسخ به فعالیت‌های سامانه انجام می‌شوند، نشانه‌هایی از به خطر افتادن یا ازکارافتادن کارکردهای امنیتی را ارائه می‌کنند. در صورتی که فعالیت‌هایی انجام‌شده 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[۱] سامانه 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، دستگاه شبکه باید داده‌های ممیزی را تولید کند و قابلیت ارسال آن‌ها به یک موجودیت شبکه مورد اعتماد (مثال؛ سرور syslog) را داشته باشد.

۳,۱,۳,۱ فعالیت ردیابی نشده

ممکن است عامل تهدید تلاش کند تا بدون اطلاع سرپرست، به کارکرد امنیتی سامانه PAM دسترسی پیدا کند، آن را تغییر دهد و/یا دست‌کاری نماید. بدین ترتیب، ممکن است مهاجم راهی برای حمله به سامانه پیدا کند (مثال؛ از طریق پیکربندی‌های نامناسب، ایراد در محصول) و سرپرست نیز آگاه نشود که سامانه 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 تعریف‌شده است.
- الزامات برای مخابره امن رکوردهای ممیزی محلی به موجودیت IT خارجی از طریق کانال امن، در FAU_STG_EXT.1 تعریف‌شده است.

---

[۱] - Recovery

- الزامات اضافه اختیاری که با از دست دادن داده‌های ممیزی محلی ذخیره‌شده 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.

۳,۱,۴ داده‌ها و اطلاعات محرمانه دستگاه و سرپرست

سامانه PAM 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 سامانه 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 سامانه دسترسی پیدا کند و حتی امنیت شبکه را از طریق دست‌کاری ظاهراً مجاز پیکربندی یا ترتیب دادن حملات مردی در میان 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.

۳,۱,۴,۱ به خطر افتادن کارکرد امنیتی

ممکن است عامل تهدید داده‌های دستگاه و اطلاعات محرمانه را به خطر اندازد و بدین ترتیب، دسترسی غیرمجاز به سامانه PAM 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.)

۳,۱,۴,۲ هک شدن گذرواژه

ممکن است عامل تهدید از ضعیف بودن گذرواژه‌های سرپرستی بهره‌گیری کند و از سطح دسترسی ویژه‌ای به سامانه برخوردار گردد. دسترسی ویژه به سامانه، مهاجم را قادر می‌سازد تا به ترافیک شبکه نیز دسترسی پیدا کند و حتی از روابط مبتنی بر اعتماد سامانه 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.

۳,۱,۵ ازکارافتادن کارکردهای امنیتی دستگاه

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

۳,۱,۵,۱ ازکارافتادن کارکرد امنیتی

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

منطق الزام کارکرد امنیتی:

[۱] Roots of trust

- 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.)

۳,۲ فرضیات

در این بخش به فروض مربوط به شناسایی تهدیدات و الزامات امنیتی سامانه‌های PAM می‌پردازیم. انتظار نمی‌رود که سامانه PAM در هیچ‌یک از این موارد ضمانتی ارائه کند و در نتیجه، الزاماتی برای کاهش خسارات ناشی از مخاطرات نیز در نظر گرفته نشده‌اند.

۳,۲,۱ حفاظت فیزیکی

چنین فرض می‌شود که سامانه PAM 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 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.

۳,۲,۲ کارکرد محدود

چنین فرض می‌شود که سامانه PAM 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، سامانه نباید پلتفرم رایانشی را برای کاربردهای همه‌منظوره (کاربردهای غیر مرتبط با کارکرد شبکه) ارائه کند.

۳,۲,۳ سرپرست مورد اعتماد

چنین فرض می‌شود که سرپرستان امنیتی سامانه PAM مورد اعتماد هستند و در راستای منافع امنیتی سازمان فعالیت می‌کنند. آن‌ها آموزش مناسب دیده‌اند، از خط‌مشی‌ها پیروی می‌کنند و اسناد راهنما را رعایت می‌نمایند. چنین فرض می‌شود که سرپرستان امنیتی از اطلاعات محرمانه حساب کاربری و گذرواژه‌هایی با قدرت امنیتی و آنتروپی مناسب استفاده می‌کنند و در هنگام سرپرستی سامانه، اهداف بدخواهانه‌ای در سر

ندارند. از سامانه PAM انتظار نمی‌رود که در صورت انجام اقدامات بدخواهانه توسط سرپرست امنیتی، در مقابل اقدامات وی از خود محافظتی به عمل آورد.

۳,۲,۴ به‌روزرسانی منظم

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

۳,۲,۵ امنیت اطلاعات محرمانه سرپرست

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

۳,۲,۶ 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 پیش‌بینی‌نشده (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.

۳,۲,۷ اطلاعات باقیمانده

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

۳,۳ 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.

۳,۳,۱ 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.

۴ اهداف امنیتی

۴,۱ اهداف امنیتی مربوط به محیط عملیاتی

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

۴,۱,۱ امنیت فیزیکی

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

۴,۱,۲ عدم کارکرد عمومی

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

۴,۱,۳ محافظت از ترافیک

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

۴,۱,۴ 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.

۴,۱,۵ 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.

۴,۱,۶ 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.

۴,۱,۷ 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 پیش‌بینی‌نشده (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.

۴,۱,۸ اطلاعات باقیمانده

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

۵ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول ۵-۱ هستند و در ادامه هریک از الزامات شرح و بسط داده‌شده‌اند. همچنین الزامات مربوط به پیوست این سند نیز در ادامه جدول ۵-۱ 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 ۵-۱ الزامات کارکرد امنیتی

شماره الزام	نام الزام	عنصر متناظر با الزام
۱	تعریف خط‌مشی کنترل دسترسی ۱	ESM_ACD.1.1

شماره الزام	نام الزام	عنصر متناظر با الزام
۲	تعریف خط‌مشی کنترل دسترسی ۲	ESM_ACD.1.2
۳	تعریف خط‌مشی کنترل دسترسی ۳	ESM_ACD.1.3
۴	انتقال خط‌مشی کنترل دسترسی ۱	ESM_ACT.1.1
۵	تعریف مشخصات موجودیت غیرفعال ۱	ESM_ATD.1.1
۶	تعریف مشخصات موجودیت غیرفعال ۲	ESM_ATD.1.2
۷	تعریف مشخصات موجودیت فعال ۱	ESM_ATD.2.1
۸	تعریف مشخصات موجودیت فعال ۲	ESM_ATD.2.2
۹	اتکا به احراز هویت سازمانی ۱	ESM_EAU.2.1
۱۰	اتکا به احراز هویت سازمانی ۱	ESM_EAU.2.2
۱۱	تولید داده ممیزی ۱	FAU_GEN.1.1
۱۲	تولید داده ممیزی ۲	FAU_GEN.1.2
۱۳	محل ذخیره‌سازی داده ممیزی ۱	FAU_STG_EXT.1.1
۱۴	محل ذخیره‌سازی داده ممیزی ۲	FAU_STG_EXT.1.2
۱۵	محل ذخیره‌سازی داده ممیزی ۳	FAU_STG_EXT.1.3
۱۶	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1
۱۷	مدیریت کلید رمزنگاری ۴	FCS_CKM.4.1
۱۸	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1(1)
۱۹	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1(2)
۲۰	عملیات رمزنگاری ۱ (۳)	FCS_COP.1.1(3)
۲۱	عملیات رمزنگاری ۱ (۴)	FCS_COP.1.1(4)
۲۲	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۲۳	تولید بیت تصادفی ۲	FCS_RBG_EXT.1.2
۲۴	مدیریت کارکرد در محصول ۱	FMT_MOF.1.1
۲۵	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۲۶	نقش‌های امنیتی ۱	FMT_SMR.1.1
۲۷	نقش‌های امنیتی ۲	FMT_SMR.1.2

شماره الزام	نام الزام	عنصر متناظر با الزام
۲۸	حفاظت از گذرواژه سرپرست محصول ۱	FPT_APW_EXT.1.1
۲۹	حفاظت از گذرواژه سرپرست محصول ۲	FPT_APW_EXT.1.2
۳۰	محافظت از داده محصول (کلیدهای متقارن) ۱	FPT_SKP_EXT.1.1
۳۱	به‌روزرسانی امن ۱	FPT_TUD_EXT.1.1
۳۲	به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۳۳	به‌روزرسانی امن ۳	FPT_TUD_EXT.1.3
۳۴	مهرهای زمانی ۱	FPT_STM.1.1
۳۵	قفل‌کردن و خاتمه دادن به نشست‌ها ۷	FTA_SSL_EXT.1.1
۳۶	قفل‌کردن و خاتمه دادن به نشست‌ها ۵	FTA_SSL.3.1
۳۷	قفل‌کردن و خاتمه دادن به نشست‌ها ۶	FTA_SSL.4.1
۳۸	پیغام‌های هشدار در رابطه با استفاده محصول ۱	FTA_TAB.1.1
۳۹	کانال امن ۱	FTP_ITC.1.1
۴۰	کانال امن ۲	FTP_ITC.1.2
۴۱	کانال امن ۳	FTP_ITC.1.3
۴۲	مسیر امن ۱	FTP_TRP.1.1
۴۳	مسیر امن ۲	FTP_TRP.1.2
۴۴	مسیر امن ۳	FTP_TRP.1.3
الزامات مربوط به پیوست یک		
۴۵	ذخیره‌سازی رویدادهای ممیزی ۱	FAU_STG.1.1
۴۶	ذخیره‌سازی رویدادهای ممیزی ۲	FAU_STG.1.2
۴۷	محل ذخیره‌سازی داده ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی	FAU_STG_EXT.2.1/LocSpace
۴۸	ذخیره‌سازی رویدادهای ممیزی ۶/ فضای ذخیره‌سازی ممیزی محلی	FAU_STG.3.1/LocSpace

شماره الزام	نام الزام	عنصر متناظر با الزام
۴۹	مدیریت احراز هویت ناموفق ۱	FIA_AFL.1.1
۵۰	مدیریت احراز هویت ناموفق ۲	FIA_AFL.1.2
۵۱	مدیریت رمز عبور ۱	FIA_PMG_EXT.1.1
۵۲	الزامات پروتکل X509(۱)/ تبادل داده کاربردی داخل محصول	FIA_X509_EXT.1.1/ITT
۵۳	الزامات پروتکل X509 (۲)/ تبادل داده کاربردی داخل محصول	FIA_X509_EXT.1.2/ITT
۵۴	مدیریت کارکرد در محصول ۱ (۱)/ سرویس‌ها	FMT_MOF.1.1(1)/Services
۵۵	مدیریت داده محصول ۱	FMT_MTD.1.1
۵۶	مدیریت داده محصول ۱/ کلیدهای رمزنگاری	FMT_MTD.1.1/CryptoKeys
۵۷	انتقال داده امنیتی در داخل محصول ۱	FPT_ITT.1.1
۵۸	مسیر امن ۱/ پیوند زدن	FPT_TRP.1.1/Join
۵۹	مسیر امن ۲ / پیوند زدن	FPT_TRP.1.2/Join
۶۰	مسیر امن ۳ / پیوند زدن	FPT_TRP.1.3/Join
۶۱	تعریف کانال ثبت‌نام مؤلفه ۱	FCO_CPC_EXT.1.1
۶۲	تعریف کانال ثبت‌نام مؤلفه ۲	FCO_CPC_EXT.1.2
۶۳	تعریف کانال ثبت‌نام مؤلفه ۳	FCO_CPC_EXT.1.3
الزامات مربوط به پیوست دو		
۶۴	الزامات پروتکل DTLS Client (۱)	FCS_DTLSC_EXT.1.1
۶۵	الزامات پروتکل DTLS Client (۲)	FCS_DTLSC_EXT.1.2
۶۶	الزامات پروتکل DTLS Client (۳)	FCS_DTLSC_EXT.1.3
۶۷	الزامات پروتکل DTLS Client (۴)	FCS_DTLSC_EXT.1.4
۶۸	الزامات پروتکل DTLS Client/ احراز هویت ۱	FCS_DTLSC_EXT.2.1

شماره الزام	نام الزام	عنصر متناظر با الزام
۶۹	الزامات پروتکل DTLS Client/ احراز هویت ۲	FCS_DTLSC_EXT.2.2
۷۰	الزامات پروتکل DTLS Client/ احراز هویت ۳	FCS_DTLSC_EXT.2.3
۷۱	الزامات پروتکل DTLS Client/ احراز هویت ۴	FCS_DTLSC_EXT.2.4
۷۲	الزامات پروتکل DTLS Client/ احراز هویت ۵	FCS_DTLSC_EXT.2.5
۷۳	الزامات پروتکل DTLS Client/ احراز هویت ۶	FCS_DTLSC_EXT.2.6
۷۴	الزامات پروتکل DTLS Client/ احراز هویت ۷	FCS_DTLSC_EXT.2.7
۷۵	الزامات پروتکل DTLS Server (۱)	FCS_DTLSS_EXT.1.1
۷۶	الزامات پروتکل DTLS Server (۲)	FCS_DTLSS_EXT.1.2
۷۷	الزامات پروتکل DTLS Server (۳)	FCS_DTLSS_EXT.1.3
۷۸	الزامات پروتکل DTLS Server (۴)	FCS_DTLSS_EXT.1.4
۷۹	الزامات پروتکل DTLS Server (۵)	FCS_DTLSS_EXT.1.5
۸۰	الزامات پروتکل DTLS Server (۶)	FCS_DTLSS_EXT.1.6
۸۱	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۱	FCS_DTLSS_EXT.2.1
۸۲	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۲	FCS_DTLSS_EXT.2.2
۸۳	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۳	FCS_DTLSS_EXT.2.3
۸۴	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۴	FCS_DTLSS_EXT.2.4

شماره الزام	نام الزام	عنصر متناظر با الزام
۸۵	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۵	FCS_DTLSS_EXT.2.5
۸۶	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۶	FCS_DTLSS_EXT.2.6
۸۷	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۷	FCS_DTLSS_EXT.2.7
۸۸	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۸	FCS_DTLSS_EXT.2.8
۸۹	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۹	FCS_DTLSS_EXT.2.9
۹۰	الزامات پروتکل HTTPS (۱)	FCS HTTPS_EXT.1.1
۹۱	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2
۹۲	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۹۳	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1
۹۴	الزامات پروتکل IPSEC (۲)	FCS_IPSEC_EXT.1.2
۹۵	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
۹۶	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
۹۷	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.1.5
۹۸	الزامات پروتکل IPSEC (۶)	FCS_IPSEC_EXT.1.6
۹۹	الزامات پروتکل IPSEC (۷)	FCS_IPSEC_EXT.1.7
۱۰۰	الزامات پروتکل IPSEC (۸)	FCS_IPSEC_EXT.1.8
۱۰۱	الزامات پروتکل IPSEC (۹)	FCS_IPSEC_EXT.1.9
۱۰۲	الزامات پروتکل IPSEC (۱۰)	FCS_IPSEC_EXT.1.10
۱۰۳	الزامات پروتکل IPSEC (۱۱)	FCS_IPSEC_EXT.1.11
۱۰۴	الزامات پروتکل IPSEC (۱۲)	FCS_IPSEC_EXT.1.12
۱۰۵	الزامات پروتکل IPSEC (۱۳)	FCS_IPSEC_EXT.1.13

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۰۶	الزامات پروتکل IPSEC (۱۴)	FCS_IPSEC_EXT.1.14
۱۰۷	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.1.1
۱۰۸	الزامات پروتکل SSH Client (۲)	FCS_SSHC_EXT.1.2
۱۰۹	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.1.3
۱۱۰	الزامات پروتکل SSH Client (۴)	FCS_SSHC_EXT.1.4
۱۱۱	الزامات پروتکل SSH Client (۵)	FCS_SSHC_EXT.1.5
۱۱۲	الزامات پروتکل SSH Client (۶)	FCS_SSHC_EXT.1.6
۱۱۳	الزامات پروتکل SSH Client (۷)	FCS_SSHC_EXT.1.7
۱۱۴	الزامات پروتکل SSH Client (۸)	FCS_SSHC_EXT.1.8
۱۱۵	الزامات پروتکل SSH Client (۹)	FCS_SSHC_EXT.1.9
۱۱۶	الزامات پروتکل SSH Server (۱)	FCS_SSHS_EXT.1.1
۱۱۷	الزامات پروتکل SSH Server (۲)	FCS_SSHS_EXT.1.2
۱۱۸	الزامات پروتکل SSH Server (۳)	FCS_SSHS_EXT.1.3
۱۱۹	الزامات پروتکل SSH Server (۴)	FCS_SSHS_EXT.1.4
۱۲۰	الزامات پروتکل SSH Server (۵)	FCS_SSHS_EXT.1.5
۱۲۱	الزامات پروتکل SSH Server (۶)	FCS_SSHS_EXT.1.6
۱۲۲	الزامات پروتکل SSH Server (۷)	FCS_SSHS_EXT.1.7
۱۲۳	الزامات پروتکل SSH Server (۸)	FCS_SSHS_EXT.1.8
۱۲۴	الزامات پروتکل TLS Client (۱)	FCS_TLSC_EXT.1.1
۱۲۵	الزامات پروتکل TLS Client (۲)	FCS_TLSC_EXT.1.2
۱۲۶	الزامات پروتکل TLS Client (۳)	FCS_TLSC_EXT.1.3
۱۲۷	الزامات پروتکل TLS Client (۴)	FCS_TLSC_EXT.1.4
۱۲۸	الزامات پروتکل TLS Client/ احراز هویت ۱	FCS_TLSC_EXT.2.1
۱۲۹	الزامات پروتکل TLS Client/ احراز هویت ۲	FCS_TLSC_EXT.2.2
۱۳۰	الزامات پروتکل TLS Client/ احراز هویت ۳	FCS_TLSC_EXT.2.3
۱۳۱	الزامات پروتکل TLS Client/ احراز هویت ۴	FCS_TLSC_EXT.2.4

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۳۲	الزامات پروتکل TLS Client/ احراز هویت ۵	FCS_TLSC_EXT.2.5
۱۳۳	الزامات پروتکل TLS Server (۱)	FCS_TLSS_EXT.1.1
۱۳۴	الزامات پروتکل TLS Server (۲)	FCS_TLSS_EXT.1.2
۱۳۵	الزامات پروتکل TLS Server (۳)	FCS_TLSS_EXT.1.3
۱۳۶	الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۱	FCS_TLSS_EXT.2.1
۱۳۷	الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۲	FCS_TLSS_EXT.2.2
۱۳۸	الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۳	FCS_TLSS_EXT.2.3
۱۳۹	الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۴	FCS_TLSS_EXT.2.4
۱۴۰	الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۵	FCS_TLSS_EXT.2.5
۱۴۱	الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۶	FCS_TLSS_EXT.2.6
۱۴۲	الزامات پروتکل X509(۱)/ ابطال	FIA_X509_EXT.1.1/Rev
۱۴۳	الزامات پروتکل X509(۱)/ ابطال	FIA_X509_EXT.1.2/Rev
۱۴۴	الزامات پروتکل X509(۳)	FIA_X509_EXT.2.1
۱۴۵	الزامات پروتکل X509(۴)	FIA_X509_EXT.2.2
۱۴۶	الزامات پروتکل X509(۵)	FIA_X509_EXT.3.1
۱۴۷	الزامات پروتکل X509(۶)	FIA_X509_EXT.3.2
۱۴۸	الزامات به‌روزرسانی امن ۴	FPT_TUD_EXT.2.1
۱۴۹	الزامات به‌روزرسانی امن ۵	FPT_TUD_EXT.2.2
۱۵۰	مدیریت کارکرد در محصول ۱/ به‌روزرسانی خودکار	FMT_MOF.1.1/AutoUpdate

شماره الزام	نام الزام	عنصر متناظر با الزام
۱۵۱	مدیریت کارکرد در محصول ۱/ توابع	FMT_MOF.1.1/Functions

۵,۱ کلاس مدیریت امنیت سازمانی

الزامات کارکردی که در این کلاس مشخص می‌شوند از تعریف، استفاده و اجرای کنترل دسترسی مرکزی، احراز هویت، پیکربندی امن و ممیزی خط‌مشی‌ها پشتیبانی می‌نمایند. در این کلاس تضمین می‌گردد که امکان تعریف خط‌مشی‌های کنترل دسترسی مجاز برای استفاده در توسعه مدیریت امنیت سازمانی[۱] (ESM)، فراهم شده باشد. همچنین محصول باید امکان انتقال خط‌مشی‌های کنترل دسترسی به دیگر محصولات ESM را داشته باشد.

شماره الزام	نام الزام
۱	**تعریف خط‌مشی کنترل دسترسی ۱**
محصول باید توانایی تعریف خط‌مشی‌های کنترل دسترسی برای استفاده توسط یک یا چند محصول سازگار که کنترل دسترسی فراهم می‌نماید را مهیا کند. **نکته کاربردی ۱:** خط‌مشی‌های تعریف‌شده باید توسط دیگر محصولات کنترل دسترسی، قابل‌فهم و استفاده باشد. دیگر محصولات کنترل دسترسی، محصولاتی مانند دیواره‌آتش و ... هستند که ممکن است در سازمان برای اعمال کنترل دسترسی در لایه‌های مختلف، مورد استفاده قرار گیرند.	
۲	**تعریف خط‌مشی کنترل دسترسی ۲**
خط‌مشی‌های کنترل دسترسی تعریف‌شده توسط محصول باید قادر باشد موارد زیر شامل گردد: • **موجودیت فعال:** [اختصاص: فهرستی از موجودیت‌های فعال و منبعی که موجودیت‌ها از آن گرفته شده‌اند که می‌توانند برای تصمیم‌گیری کنترل دسترسی مورد استفاده قرار گیرند.] • **موجودیت غیرفعال:** [اختصاص: فهرستی از موجودیت‌های غیرفعال و منبعی که موجودیت‌ها از آن گرفته شده‌اند که می‌توانند برای تصمیم‌گیری کنترل دسترسی مورد استفاده قرار گیرند.] • **عملیات:** [اختصاص: فهرستی از عملیات و منبعی که عملیات از آن گرفته شده‌اند که می‌توانند برای تصمیم‌گیری	

[۱] Enterprise Security Management

کنترل دسترسی مورد استفاده قرار گیرند.]

- **مشخصه‌ها**: [اختصاص: فهرستی از مشخصه‌ها و منبعی که مشخصه‌ها از آن گرفته شده‌اند که می‌توانند برای تصمیم‌گیری کنترل دسترسی مورد استفاده قرار گیرند.]

نکته کاربردی ۲:

به‌عنوان نمونه برای هر کدام از موارد ذکرشده در این الزام، منبع می‌تواند به صورت زیر تعریف گردد:

- موجودیت فعال: یک محصول سازگار مدیریت اعتبارنامه و هویت
- موجودیت غیرفعال: سیستم‌عامل میزبانی که موجودیت غیرفعال روی آن استقرار دارد (موجودیت غیرفعال مبتنی بر میزبان)
- عملیات: عملیاتی که توسط سیستم‌عامل بر روی موجودیت غیرفعال صورت می‌گیرد
- مشخصه‌ها: یک محصول سازگار مدیریت اعتبارنامه و هویت یا خود محصول مورد ارزیابی

هدف اصلی در این الزام، این است که اگر محصول مورد ارزیابی با یک محصول کنترل دسترسی سازگار باشد، بتواند خط‌مشی‌هایی تولید نماید که همه ویژگی‌های محصول سازگار را پوشش دهد. به عنوان مثال، اگر محصول مورد ارزیابی با یک محصول کنترل دسترسی مبتنی بر میزبان، سازگار باشد و محصول مورد ارزیابی فقط خط‌مشی کنترل فایل را تولید کند، نمی‌تواند این محصول را به صورت مؤثر پوشش دهد.

۳	تعریف خط‌مشی کنترل دسترسی ۳

محصول باید به هر خط‌مشی، اطلاعات شناسایی منحصربه‌فردی را مرتبط سازد.

نکته کاربردی ۳:

این الزام برای نظارت بر خط‌مشی‌های پیاده‌سازی شده توسط محصولات سازگار و مورد استفاده قرار گرفتن خط‌مشی تولیدی محصول مورد ارزیابی است.

اقدامات ارزیابی:

ارزیاب باید برای آزمون الزامات تعریف خط‌مشی کنترل دسترسی (الزامات شماره ۱، ۲ و ۳) اقدامات زیر را انجام دهد:

۱- ارزیاب باید تائید نماید که سند خلاصه مشخصات محصول، یک یا چند مورد از محصولات سازگار کنترل دسترسی را معرفی کرده است.

۲- ارزیاب باید تائید نماید که سند خلاصه مشخصات محصول، حدود و اجزایی که خط‌مشی برای آن‌ها تعریف می‌شود (موجودیت‌های فعال و غیرفعال، عملیات و...) را توضیح داده است.

۳- ارزیاب باید سند هدف امنیتی را مرور کند و تائید نماید که محصولات کنترل دسترسی لیست شده توانایی استفاده از خط‌مشی‌های تولیدشده توسط محصول مورد ارزیابی را داشته باشند.

۴- ارزیاب باید اطمینان یابد که خط‌مشی‌های تولیدشده توانایی استفاده مؤثر از تمامی ویژگی محصولات کنترل دسترسی لیست شده در سند خلاصه مشخصات محصول را داشته باشند.

۴	انتقال خط‌مشی کنترل دسترسی ۱

محصول باید با توجه به شرایط زیر، خط‌مشی‌ها به محصولات سازگار و مجاز کنترل دسترسی انتقال دهد:
[انتخاب: بلافاصله بعد از ایجاد یا به‌روزرسانی خط‌مشی، به صورت دوره زمانی، با توجه به درخواست محصول سازگار مدیریت پیکربندی امن، [اختصاص: دیگر شرایط]]

نکته کاربردی ۴:

هدف از این الزام، اطمینان از وجود یک روش زمان‌بندی‌شده برای انتقال اطلاعات خط‌مشی کنترل دسترسی به یک محصول سازگار است. اگر گزینه «با توجه به درخواست محصول سازگار مدیریت پیکربندی امن» انتخاب شود، نویسنده سند هدف امنیتی باید محصولاتی که باید برای ارزیابی پیکربندی گردند را ذکر نماید.

اقدامات ارزیابی:

ارزیاب باید اقدامات زیر را انجام دهد:

۱- ارزیاب باید سند خلاصه مشخصات محصول را بررسی نماید و اطمینان یابد که توضیحاتی در خصوص زمان و نحوه انتقال داده خط‌مشی به محصولات ESM بیان گردیده است، این توضیحات لیست محصولات ESM نیز شامل می‌شود.

۲- ارزیاب باید سند راهنمای محصول را بررسی و تائید نماید که چگونگی ایجاد و به‌روزرسانی خط‌مشی‌ها و شرایطی که تحت آن خط‌مشی‌های جدید یا به‌روز شده به محصولات ESM انتقال می‌یابد، بیان گردیده است.

۳- ارزیاب باید یک یا چند محصول سازگار را پیکربندی نماید، سپس یک خط‌مشی ایجاد کند، (یک خط‌مشی موجود را به‌روزرسانی نماید، از یک خط‌مشی موجود استفاده کند) و آن را به محصول ارسال نماید، سپس اطمینان یابد که انتقال و اجرای آن در محصول به درستی صورت گرفته است.

۴- ارزیاب باید اقدام قبل را برای هر کدام از حالات ذکرشده در انتخاب این الزام، اجرا نماید و اطمینان یابد که به انتقال و اجرای خط‌مشی در محصول، درستی اجرا می‌شوند.

۵	تعریف مشخصات موجودیت غیرفعال ۱

محصول باید برای موجودیت‌های غیرفعال جداگانه، مشخصه‌های امنیتی [اختصاص: فهرستی از مشخصه‌های امنیتی موجودیت غیرفعال] را نگه‌داری کند.

نکته کاربردی ۵:

مشخصه‌های امنیتی موجودیت غیرفعال، به مشخصه‌هایی اشاره می‌کند که اگرچه ممکن است یک فاکتور برای تصمیم‌گیری کنترل دسترسی لحاظ گردد ولی این مشخصه‌ها به خط‌مشی کنترل دسترسی و کاربر مرتبط نیستند. یک محصول که

خط‌مشی‌های کنترل دسترسی را برای امنیت چند سطحی تعریف می‌کند، ممکن است نیاز باشد که برچسب‌های امنیتی برای موجودیت‌های غیرفعال تعریف نماید، این برچسب‌ها باعث می‌شوند که خط‌مشی برای موجودیت‌های غیرفعال قابل‌اعمال گردد.	
۶	**تعریف مشخصات موجودیت غیرفعال ۲**
محصول باید توانایی مرتبط ساختن مشخصه‌های امنیتی به موجودیت‌های غیرفعال جداگانه را داشته باشد.	
۷	**تعریف مشخصات موجودیت فعال ۱**
محصول باید برای موجودیت‌های فعال جداگانه، مشخصه‌های امنیتی [اختصاص: فهرستی از مشخصه‌های امنیتی موجودیت فعال] را نگه‌داری کند. **نکته کاربردی ۶:** مشخصه‌های امنیتی موجودیت فعال، به مشخصه‌هایی اشاره می‌کند که ممکن است به عنوان یک فاکتور برای تصمیم‌گیری کنترل دسترسی استفاده شوند و همچنین به موجودیت‌های فعال تحت خط‌مشی کنترل دسترسی نیز مرتبط هستند. یک محصول که خط‌مشی‌های کنترل دسترسی را برای امنیت چند سطحی تعریف می‌کند، ممکن است نیاز باشد که برچسب‌های امنیتی برای موجودیت‌های فعال/کاربران تعریف نماید، این برچسب‌ها باعث می‌شوند که خط‌مشی برای موجودیت‌های فعال/کاربران قابل‌اعمال گردد.	
۸	**تعریف مشخصات موجودیت فعال ۲**
محصول باید توانایی مرتبط ساختن مشخصه‌های امنیتی به موجودیت‌های فعال جداگانه را داشته باشد.	
۹	**اتکا به احراز هویت سازمانی ۱**
محصول باید برای احراز هویت موجودیت فعال به [انتخاب: [اختصاص: مؤلفه (های) شناسایی‌شده محصول که مسئول احراز هویت موجودیت فعال است]، [اختصاص: مؤلفه (های) شناسایی‌شده محیط عملیاتی که مسئول احراز هویت موجودیت فعال است]] اتکا نماید. **نکته کاربردی ۷:** اگر نحوه شناسایی به گونه‌ای است که بیان می‌گردد موجودیت‌های فعال، کاربران عادی یا سرپرستان هستند، آنگاه نیاز است که در اختصاص‌های این الزام، یک یا چند سرور احراز هویت ذکر گردد.	
۱۰	**اتکا به احراز هویت سازمانی ۲**
محصول باید هر موجودیت فعال را ملزم نماید که قبال از انجام هر اقدام میانی، به صورت موفق احراز هویت گردد. **نکته کاربردی ۸:** در صورتی که محصول از دو روش مختلف احراز هویت برای دو مجموعه متفاوت از موجودیت‌های فعال استفاده می‌نماید، نویسنده سند هدف امنیتی باید برای هرکدام از روش‌ها، الزامات این خانواده را ذکر نماید. همچنین الزامات «اتکا به احراز هویت	

سازمانی» برای کاربران و موجودیت‌های IT مجاز، مورد استفاده قرار می‌گیرد و اقدامات زیر نیز مربوط به هر دو الزام است.

اقدامات ارزیابی:

ارزیاب باید اقدامات زیر را انجام دهد:

۱- ارزیاب باید سند خلاصه مشخصات محصول را بررسی نماید اطمینان یابد که مکانیسم‌های احراز هویت برای هر کاربر و موجودیت‌های IT که بخواهند از محصول استفاده کنند، توضیح داده شده است.

۲- ارزیاب باید سند راهنمای محصول را بررسی نماید و اطمینان یابد که محصول چگونه کاربر یا موجودیت IT که درخواست دسترسی دارد را بررسی و از معتبر بودن داده‌های احراز هویت آن‌ها اطلاع پیدا می‌کند.

۳- ارزیاب باید با تنظیم مقادیر معتبر و غیر معتبر احراز هویت موجودیت‌ها را بررسی نماید.

۵,۲ 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 سامانه را در اختیاردارند، محصول باید این قابلیت را داشته باشد که داده‌های ممیزی موردنیاز برای تشخیص چنین فعالیت‌هایی را تولید نماید. ممیزی فعالیت‌های مدیریت سامانه سبب تولید اطلاعاتی می‌شود که در صورت نیاز به تغییر پیکربندی سامانه، 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 سامانه) 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
۱۱	**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 سامانه (درصورتی‌که مدیران سامانه 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 ۹:

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 ۱۰:

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

۱۲	**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 ۱۱:

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 «شناسایی و احراز هویت کاربر ۲» برای ثبت رکورد ممیزی علاوه بر اطلاعات بند الف این الزام باید آدرس IP منشأ احراز هویت را در رکورد ممیزی (به‌عنوان نمونه در قسمت توضیحات رکورد) ثبت نماید؛ بنابراین این اطلاعات توسط نویسنده سند هدف امنیتی در این قسمت قرار داده می‌شود.

- برای الزام «تعریف خط‌مشی کنترل دسترسی» اطلاعات ممیزی ایجاد یا اصلاح خط‌مشی ثبت می‌شود. این اطلاعات باید شامل شناسه منحصربه‌فرد خط‌مشی باشد.
- برای الزام «انتقال خط‌مشی کنترل دسترسی» اطلاعات انتقال خط‌مشی کنترل دسترسی به محصولات کنترل دسترسی ثبت می‌شود. این اطلاعات باید شامل مقصد خط‌مشی باشد.
- برای الزام «تعریف مشخصات موجودیت غیرفعال ۱» اطلاعات ممیزی تعریف مشخصه‌های امنیتی موجودیت غیرفعال ثبت می‌شود. این اطلاعات باید شامل شناسایی مشخصه تعریف‌شده باشد.
- برای الزام «تعریف مشخصات موجودیت غیرفعال ۲» اطلاعات ممیزی ارتباط مشخصه‌های امنیتی به موجودیت غیرفعال ثبت می‌شود. این اطلاعات باید شامل شناسایی مشخصه و موجودیت باشد.

[۱] Subject

- برای الزام «تعریف مشخصات موجودیت فعال ۱» اطلاعات ممیزی تعریف مشخصه‌های امنیتی موجودیت فعال ثبت می‌شود. این اطلاعات باید شامل شناسایی مشخصه تعریف‌شده باشد.
- برای الزام «تعریف مشخصات موجودیت فعال ۲» اطلاعات ممیزی تعریف مشخصه‌های امنیتی موجودیت فعال ثبت می‌شود.
- برای الزام «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 «سازوکار احراز هویت بر اساس رمز عبور» اطلاعات ممیزی تمام کاربردهای مکانیسم تعیین هویت و احراز هویت ثبت می‌شود. این اطلاعات باید شامل منشأ تلاش صورت گرفته (مانند آدرس IP) باشد.برای الزام «مدیریت کارکرد در محصول ۱ (۱)/ به‌روزرسانی امن» اطلاعات ممیزی مربوط به هرگونه تلاش برای آغاز یک به‌روزرسانی، دستی ثبت می‌شود.
- برای الزام «مدیریت داده‌های محصول» اطلاعات ممیزی تمام فعالیت‌های مدیریتی داده‌های محصول ثبت می‌شود.
- برای الزامات «به‌روزرسانی امن» اطلاعات ممیزی مربوط به آغاز به‌روزرسانی، نتیجه تلاش‌های به‌روزرسانی (موفقیت یا شکست) ثبت می‌شود.
- برای الزام «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 «قفل‌کردن و خاتمه دادن به نشست‌ها ۷» اگر «قفل‌کردن» 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 مکانیسم قفل‌کردن نشست ثبت می‌شود
- برای الزام «قفل‌کردن و خاتمه دادن به نشست‌ها ۵» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست راه دور از طریق یک مکانیسم قفل‌کردن نشست ثبت می‌شود.
- برای الزام «قفل‌کردن و خاتمه دادن به نشست‌ها ۶» اطلاعات ممیزی مربوط به خاتمه دادن یک نشست تعاملی ثبت می‌شود.
- برای الزامات «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 «مسیر امن» اطلاعات ممیزی مربوط به آغاز کردن مسیر امن / خاتمه دادن مسیر امن / شکست توابع مسیر امن ثبت می‌شود.

نکته کاربردی ۱۲:

[۱] Time stamps

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.
۱۳ | محل ذخیره‌سازی داده‌های ممیزی ۱
محصول باید قادر به ارسال داده ممیزی تولیدشده 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 IPsec،SSH،TLS،HTTPS به عنوان پروتکل‌های ارتباطی امن استفاده شود نیاز است از پیوست دو تمامی الزامات مربوط به آن پروتکل تکمیل و به سند هدف امنیتی اضافه گردد.** **نکته کاربردی ۱۳:** 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 حفاظت‌شده، به صورت مناسبی خارج نماید. حداقل یک مؤلفه باید توانایی خارج کردن رکوردهای ممیزی به سرور IT خارجی را داشته باشد.
۱۴ | محل ذخیره‌سازی داده‌های ممیزی ۲
محصول مورد ارزیابی باید بتواند داده‌های ممیزی تولیدشده را در خود ذخیره کند.
۱۵ | 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:

[۱] Overwrite

[اختصاص: قوانین بازنویسی سوابق ممیزی گذشته]، [اختصاص: اقدامات دیگر]].

نکته کاربردی ۱۴:

درصورتی‌که حافظه محلی پرشده باشد، سرور خارجی ثبت رویدادها[۱] 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 به‌طورکلی محصول باید توانایی ذخیره‌ی محلی داده‌های ممیزی را داشته باشد. هر مؤلفه حداقل باید توانایی ذخیره موقت اطلاعات ممیزی برای مواردی که ارتباط شبکه دچار مشکل می‌شود را داشته باشد. ذخیره موقت نیاز نیست که 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.

۵,۳ کلاس 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[۲]، نابودی کلید و انواع مختلف عملیات رمزنگاری برای رمزگذاری و رمزگشایی AES، تائید امضا، تولید درهم‌ساز و تولید درهم‌ساز کلید گذاری شده[۳] هستند. این الزامات کارکرد امنیتی، از پیاده‌سازی الزامات مبتنی بر انتخاب و پروتکل لیست شده در پیوست دو پشتیبانی می‌کنند.

شماره الزام	نام الزام
۱۶	**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.	

[۱] External log server

[۲] Key establishment

[۳] Keyed hash generation

شماره الزام	نام الزام
• 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 ۱۵:** 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 فهرست شده 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.	
۱۷	**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 غیر فرار، نابودی باید از طریق فراخوان[۲] یک واسط مهیا شده توسط محصول مورد ارزیابی که [انتخاب: ○ به‌صورت 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]	

[۱] Volatile Storage

[۲] Invocation

شماره الزام	نام الزام

انجام شود.]

نکته کاربردی ۱۶:

در قسمت مربوط به انتخاب در گزینه دوم از اولین اختصاص، جایی که 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 اشاره‌شده در الزام می‌تواند در محصولات مختلف، شکل متفاوتی داشته باشد. شاید مشهودترین شکل آن یک برنامه کاربردی روی یک سیستم‌عامل 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 به‌صورت 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 هیچ‌کدام از مقادیر تولیدشده توسط تولیدکننده بیت تصادفی موجود در الزام FCS_RBG_EXT یا مقادیر مشخص لیست شده در این الزام، مثلاً 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 حتماً بازنویسی داده با دقت انتخاب‌شده 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.

۱۸	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 تعریف‌شده است]] انجام دهد.

نکته کاربردی ۱۷:

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.

[۱] Cipher suite

شماره الزام	نام الزام
۱۹	**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،
- 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 ۱۸:

نویسنده هدف امنیتی الگوریتم(های) مورد استفاده برای اجرای امضای دیجیتال را انتخاب می‌کند. برای الگوریتم‌های انتخاب‌شده، نویسنده هدف امنیتی انتخاب‌ها و اختصاص‌های مناسب را انجام می‌دهد و پارامترهای الگوریتم‌ها را به شکل مناسب تعیین می‌نماید. نویسنده هدف امنیتی، با استفاده از انتخاب‌ها و اختصاص‌های این الزام، از شامل شدن تمامی مقادیر پارامترهای ضروری برای مجموعه رمز انتخاب‌شده به‌وسیله الزامات سند هدف امنیتی، اطمینان پیدا می‌نماید. نویسنده هدف امنیتی همچنین سازگار بودن انتخاب‌های انجام‌گرفته شده با دیگر الزامات رمزنگاری را بررسی می‌کند، خصوصاً زمانی که از منحنی‌های بیضوی پشتیبانی شود.

شماره الزام	نام الزام
۲۰	**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 ۱۹:

به تولیدکنندگان اکیداً توصیه می‌شود که از پروتکل‌های به‌روزرسانی شده‌ای که از خانواده SHA-2 پشتیبانی می‌نمایند، استفاده

شماره الزام	نام الزام
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 عملیات 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).	
۲۱	**عملیات رمزنگاری ۱ (۴)**
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 ۲۰:** اندازه کلید k در عبارت «اختصاص» بین L1 و L2 خواهد بود (که در ISO/IEC 10118 مربوط به توابع درهم‌ساز تعریف‌شده است). به عنوان مثال، در مورد SHA-256 داریم: L1=512, L2=256 که L2<=k<=L1.	
۲۲	**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.	
۲۳	**تولید بیت تصادفی ۲**
RBG قطعی باید دست‌کم توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی را از [انتخاب: [اختصاص: تعداد منابع مبتنی بر نرم‌افزار] منبع نویز مبتنی بر نرم‌افزار، [اختصاص: تعداد منابع مبتنی بر سخت‌افزار] منبع نویز مبتنی بر سخت‌افزار] گردآوری کند. این آنتروپی باید دست‌کم [انتخاب: ۱۲۸ بیت، ۱۹۲ بیت، ۲۵۶ بیت] و حداقل معادل بالاترین قدرت امنیتی کلیدها و CSPs که تولید می‌کند، مطابق با ISO/IEC 18031:2011، باشد. **نکته کاربردی ۲۱:** در مورد نخستین عبارت این الزام، نویسنده هدف امنیتی حداقل یکی از انواع منابع نویز را انتخاب می‌کند. اگر محصول مورد	

[1] Keyed-hash message authentication

شماره الزام	نام الزام
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 موردنیاز 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 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 آنتروپی تزریق‌شده به RBG را انتخاب می‌کند که این مقدار باید بزرگ‌تر یا مساوی طول هر کلید امنیتی باشد که توسط محصول تولید می‌شود.	

۵,۴ کلاس مدیریت امنیت

توابع مدیریتی موردنیاز در این بخش، شامل قابلیت‌های موردنیاز برای پشتیبانی از نقش سرپرست امنیتی محصول و همچنین مجموعه‌ای از توابع مدیریتی امنیت موردنیاز برای مدیریت بخش‌های قابل پیکربندی الزامات کارکرد امنیتی (FMT_SMF.1)، مدیریت کلی داده‌های توابع امنیتی محصول (FMT_MTD.1) 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 ذکرشده‌اند.

شماره الزام	نام الزام

شماره الزام	نام الزام
۲۴	**مدیریت کارکرد در محصول ۱**
محصول توانایی [انتخاب: تعیین کردن رفتار، فعال کردن، غیرفعال کردن، اصلاح کردن رفتار] توابع [اختصاص: فهرستی از توابع]را به [اختصاص: نقش‌های تعریف‌شده مجاز]محدود نماید. **نکته کاربردی ۲۲:** در نخستین اختصاص این الزام، توابع مطرح‌شده در الزام «کارکرد مدیریت محصول ۱» قرار می‌گیرند. در دومین اختصاص نیز نقش‌های تعریف‌شده در الزام «نقش‌های امنیتی ۱» قرار خواهند گرفت.	
۲۵	**کارکرد مدیریتی محصول ۱**
محصول مورد ارزیابی باید قابلیت انجام کارکردهای مدیریتی زیر را داشته باشد: [اختصاص: • اداره کردن محصول به‌صورت محلی و راه دور • پیکربندی بنر دسترسی • 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 ○ 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]	

شماره الزام	نام الزام

نکته کاربردی ۲۳:

محصول مورد ارزیابی باید به‌طورکلی، قابلیت کارکردی را برای سرپرستی محلی و راه دور فراهم آورد. این پروفایل حفاظتی کارکرد مدیریت امنیتی خاصی را برای واسط سرپرستی محلی یا راه دور، 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 غیرفعال 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 قابل پیکربندی توسط سرپرست باشد و در صورت ذکر شدن در سند هدف ارزیابی) 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 راه دور قرار داده باشد، آنگاه نویسنده هدف ارزیابی باید گزینه «فعال‌سازی 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 حد آستانه‌ها برای مکانیسم‌های 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 ذکرشده نباید انتخاب گردد.

شماره الزام	نام الزام
• 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 شناساننده‌هایی 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 (با توجه 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 راه دور» به «سرپرستی راه دور از طریق مؤلفه‌ی دیگر» می‌تواند به عنوان یک مثال برای پیکربندی تعاملات باشد.	
۲۶	**نقش‌های امنیتی ۱**
محصول باید نقش‌های [اختصاص: نقش‌های تعریف‌شده مجاز] را نگهداری کند.	
۲۷	**نقش‌های امنیتی ۲**
محصول مورد ارزیابی باید بتواند بین کاربران و نقش‌ها ارتباط برقرار نماید. **نکته کاربردی ۲۴:** یک محصول پیکربندی امن سازگار و مجاز ممکن است از طرف کاربر با نقش ارتباط داشته باشد.	

۵,۵ کلاس حفاظت از محصول مورد ارزیابی

در این بخش، الزامات مربوط به محصول مورد ارزیابی برای حفاظت از داده 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 قابل‌اعتمادی را برای پشتیبانی از ممیزی صحیح خانواده «تولید داده ممیزی» فراهم آورد.

شماره الزام	نام الزام
۲۸	**حفاظت از گذرواژه سرپرست محصول ۱**
محصول مورد ارزیابی نباید کلمه‌های عبور را به شکل متن ساده ذخیره کند.	

۲۹	حفاظت از گذرواژه سرپرست محصول ۲
محصول مورد ارزیابی باید از خوانده شدن گذرواژه‌هایی که به‌صورت متن ساده[۱] هستند، جلوگیری کند. **نکته کاربردی ۲۵:** 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 هنگام ورود در کنسول محلی، به صورت مبهم باشد.	
۳۰	**محافظت از داده 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 ۲۶:** 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، قابل‌دسترسی 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.	

۵,۵,۱ به‌روزرسانی امن

عدم موفقیت سرپرست محصول در تائید به‌روزرسانی‌های سامانه، ممکن است کل سامانه را در معرض خطر قرار دهد. برای اعتماد به منبع به‌روزرسانی‌ها، سامانه می‌تواند مجموعه‌ای از فرایندها و مکانیسم‌های رمزنگاری را مورداستفاده قرار دهد و با استفاده از آن‌ها، به‌روزرسانی‌ها را تهیه و تدارک ببیند، رمزنگاری به‌روزرسانی‌ها را از طریق مکانیسم امضای دیجیتال بررسی کند و به‌روزرسانی‌ها را روی سامانه 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.

[۱] Plaintext

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

شماره الزام	نام الزام
۳۱	**به‌روزرسانی امن ۱**

محصول مورد ارزیابی باید این امکان را به سرپرستان امنیتی محصول بدهد که به نسخه فعلی نرم‌افزار/میان‌افزار محصول و [انتخاب: جدیدترین نسخه نصب‌شده نرم‌افزار/میان‌افزار محصول، هیچ نسخه دیگری از نرم‌افزار/میان‌افزار محصول] دسترسی داشته باشد.

نکته کاربردی ۲۷:

اگر امکان نصب یک به‌روزرسانی مورد اعتماد که همان لحظه فعال نمی‌گردد یعنی فعال‌سازی آن دارای تأخیر است، در محصول وجود داشته باشد، آنگاه باید هر دو نسخه محصول: نسخه مورد استفاده و نسخه نصب‌شده (به صورت تصویری از غیرفعال بودن آن) فراهم گردد. در این‌گونه موارد، گزینه «جدیدترین نسخه نصب‌شده نرم‌افزار/میان‌افزار محصول» در انتخاب این الزام، باید منتخب گردد و همچنین در خلاصه مشخصات محصول باید مشخص گردد که چگونه و چه زمانی نسخه غیرفعال، فعال می‌گردد. اگر تمامی به‌روزرسانی‌ها هم‌زمان با نصب فعال می‌گردند، آنگاه فقط نسخه فعلی در حال اجرای محصول باید فراهم گردد و گزینه «هیچ نسخه دیگری از نرم‌افزار/میان‌افزار محصول» برای انتخاب این الزام برگزیده خواهد شد.

برای محصولات توزیع‌شده، نحوه تصمیم‌گیری در رابطه با نسخه‌های نصب‌شده روی هر مؤلفه در سند راهنمای عملیاتی توضیح داده شده است.

شماره الزام	نام الزام
۳۲	**به‌روزرسانی امن ۲**

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

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

نکته کاربردی ۲۸:

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

شماره الزام	نام الزام
دارد یا خیر و این امر را به سرپرست محصول اطلاع می‌دهد (مثلاً از طریق یک پیام یا یک پرچم)، اما نصب به‌روزرسانی نیازمند انجام اقداماتی توسط سرپرست محصول خواهد بود، اما «به‌روزرسانی خودکار» به یک محصول مورد ارزیابی اشاره دارد که به‌روزرسانی‌ها را جستجو می‌کند و در صورت وجود آن‌ها را نصب می‌نماید. خلاصه مشخصات محصول باید بیان کند که چه اقداماتی برای پشتیبانی محصول از گزینه‌های «از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند» یا «از به‌روزرسانی‌های خودکار پشتیبانی کند» در قسمت «انتخاب» این الزام، دخیل هستند. وقتی که برای حفاظت از مکانیسم به‌روزرسانی مورد اعتماد، مقادیر هش‌شده منتشرشده 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[1] از سرپرست امنیتی نصب کند، حتی برای مواردی که مقادیر محاسبه‌شده هش با مقادیر منتشرشده منطبق باشد. در این مورد نباید گزینه «از به‌روزرسانی‌های خودکار پشتیبانی کند» استفاده گردد (بررسی خودکار برای وجود به‌روزرسانی مانعی ندارد). در این‌گونه موارد باید همیشه یک مجوز فعال از سرپرست امنیتی وجود داشته باشد و گزینه «به‌روزرسانی دستی» باید انتخاب گردد، اگرچه ممکن است فایل (ها) به طور خودکار دانلود شده باشند. به‌روزرسانی‌های کاملاً خودکار فقط باید در حالتی که از مکانیسم امضاء دیجیتال استفاده شده باشد، انتخاب گردد.	
۳۳	**به‌روزرسانی امن ۳**
محصول مورد ارزیابی باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از [انتخاب: مکانیسم امضای دیجیتال، درهم‌ساز منتشرشده]، ابزاری را برای احراز هویت میان‌افزار آن‌ها در اختیار محصول مورد ارزیابی قرار دهد. **تذکر: در صورتی که از مکانیسم امضای دیجیتال استفاده شود نیاز است الزام‌های «الزامات به‌روزرسانی ۴» و «الزامات به‌روزرسانی ۵» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه کند.** **نکته کاربردی ۲۹:** مکانیسم امضاء دیجیتال که در این الزام به آن اشاره‌شده 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 تشریح شده در الزام «عملیات رمزنگاری ۱ (۳)» تولید می‌شود. نویسنده هدف امنیتی باید مکانیسم اجراشده توسط محصول مورد ارزیابی را تعیین نماید، هر دو مکانیسم نیز	

[1] active authorization

شماره الزام	نام الزام

می‌تواند مورد استفاده قرار گیرد.

وقتی که از مقادیر هش منتشرشده برای امن کردن مکانیسم به‌روزرسانی مورد اعتماد استفاده می‌شود، یک «مجوز فعال» برای فرآیند به‌روزرسانی، از طرف سرپرست امنیتی نیاز است. به علاوه، مخابره امن مقدار هش موثق[۱] از توسعه‌دهنده/تولیدکننده محصول به سرپرست امنیتی، یکی از فاکتورهای کلیدی برای حفاظت از مکانیسم به‌روزرسانی مورد اعتماد است و سند راهنما باید چگونگی انجام این انتقال/مخابره را توضیح دهد. برای تصدیق[۲] مقدار هش مورد اعتماد 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.

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

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

برای محصولات توزیع‌شده، 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 ۳۰:

اگر در مکانیسم تائید به‌روزرسانی از گواهی‌نامه‌ها استفاده شود، این گواهی‌ها باید از «الزامات پروتکل X509 (۳)» انتخاب‌شده و بر اساس «الزامات پروتکل X509» تائید گردند.

نکته کاربردی ۳۱:

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 سامانه بخواهد آن را به نسخه قدیمی‌تر برگرداند و این کار ایرادی ندارد (مثلاً هنگامی‌که شرکتی یک به‌روزرسانی معیوب را منتشر کند، یا هنگامی‌که سامانه مبتنی بر کارکرد یک ویژگی مستندسازی نشده، باشد که در به‌روزرسانی جدید وجود ندارد). همچنین، ممکن

[۱] Authentic hash value

[۲] Verification

شماره الزام	نام الزام
	است مالک سامانه بخواهد به‌روزرسانی را با تصویر NV انجام دهد تا معایب موجود را برطرف نماید. تمام مؤلفه‌های مجزای نرم‌افزار (مانند برنامه‌های کاربردی، درایورها، هسته و میان‌افزار[۱]) محصول مورد ارزیابی باید توسط تولیدکننده، امضای دیجیتال شوند و در نهایت توسط مکانیسم به‌روزرسانی تائید گردند. از آنجا که ممکن است مؤلفه‌ها توسط تولیدکننده‌های مختلف امضا شوند، لازم است که فرایند به‌روزرسانی هم تصویر NV و هم تصویر به‌روزرسانی تولیدشده توسط یک تولیدکننده واحد (مثلاً تائید از طریق مقایسه کلیدهای عمومی) یا امضاشده توسط کلیدهای امضای معتبر را تائید کند (مثلاً تائید گواهی‌نامه‌ها در صورت استفاده از گواهی‌نامه‌های X.509).
۳۴	**مهرهای زمانی ۱**
	محصول مورد ارزیابی باید قابلیت ارائه مهرهای زمانی قابل‌اطمینان[۲] برای استفاده خودش را داشته باشد. **نکته کاربردی ۳۲:** مهرهای زمانی قابل‌اطمینان جهت استفاده با دیگر توابع امنیتی محصول، موردنظر 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 برگزیده شود. استفاده از یک ساعت بلادرنگ محلی با قابلیت همگام‌سازی خودکار با یک منبع خارجی (مثلاً؛ 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 سامانه تغییر کند، نیاز به ممیزی نیست، این تغییرات دیگر در حوزه تغییرات ناپیوسته زمان، قرار نمی‌گیرند.

[۱] Firmware

[۲] Reliable time stamps

۵,۶ کلاس دسترسی به محصول

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

شماره الزام	نام الزام
۳۵	**قفل‌کردن و خاتمه دادن به نشست‌ها ۷**
در مورد نشست‌های تعاملی محلی[۱]، محصول مورد ارزیابی باید پس از اتمام زمان غیرفعال بودن که توسط سرپرست محصول تعیین‌شده است، [انتخاب: • نشست را قفل کند – تمام فعالیت‌های مربوط به دسترسی به داده‌های کاربری و نمایش این داده‌ها، به جز فعالیت‌های مربوط به قفل‌گشایی نشست را غیرفعال کند و از سرپرست محصول بخواهد که پیش از قفل‌گشایی نشست، مجدداً احراز هویت نماید؛ • نشست را خاتمه دهد].	
۳۶	**قفل‌کردن و خاتمه دادن به نشست‌ها ۵**
در مورد نشست‌های تعاملی راه دور[۲]، درصورتی که نشست تعاملی برای مدت معینی غیرفعال باشد، محصول مورد ارزیابی باید نشست تعاملی خاتمه دهد. مدت زمان مجاز برای غیرفعال بودن توسط سرپرست محصول تعیین می‌شود.	
۳۷	**قفل‌کردن و خاتمه دادن به نشست‌ها ۶**
محصول مورد ارزیابی باید به سرپرست محصول اجازه دهد که نشست تعاملی خود را خاتمه دهد.	
۳۸	**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 تأییدیه استفاده از محصول مورد ارزیابی را نشان دهد. **نکته کاربردی ۳۳:** این الزام در مورد نشست‌های تعاملی بین یک کاربر انسانی و یک محصول مورد ارزیابی اعمال می‌شود. موجودیت‌های IT که اتصالاتی مانند تماس‌های راه دور از طریق شبکه را برقرار می‌کنند، نیازی به رعایت این الزام نخواهند داشت.	

۵,۷ کلاس کانال‌ها/مسیرهای مورد اعتماد

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

شماره الزام	نام الزام
۳۹	**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.	
۴۰	**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.	
۴۱	**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 ۳۴:** هدف از الزام حاضر فراهم کردن روشی است که جهت حفاظت ارتباطات خارجی با موجودیت‌های معتبر IT، از پروتکل رمزنگاری استفاده گردد. منظور از موجودیت‌های معتبر IT، موجودیت‌هایی است که محصول مورد ارزیابی برای انجام کارکردهای خود با آن‌ها ارتباط برقرار می‌کند. محصول مورد ارزیابی دست‌کم از یکی از پروتکل‌های ذکرشده 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 ذکرشده حفاظت گردد. اگر سایر موجودیت‌های معتبر IT مورد حفاظت قرار گیرند، نویسنده هدف امنیتی باید انتخاب‌های مقتضی را انجام دهد و موارد مناسب را در عبارت اختصاص بگنجاند. نویسنده هدف امنیتی مکانیسم یا مکانیسم‌های پشتیبانی شده 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.	
۴۲	**مسیر امن ۱**
محصول، باید با استفاده از پروتکل [انتخاب: IPsec, SSH, TLS, DTLS, HTTPS] مسیر ارتباطی امنی را میان خود و	

شماره الزام	نام الزام
سرپرست‌های راه دور 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.**	
۴۳	**مسیر امن ۲**
محصول مورد ارزیابی باید به سرپرست‌های راه دور محصول اجازه دهد که ارتباطات را از طریق کانال امن آغاز کند.	
۴۴	**مسیر امن ۳**
محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه سرپرست محصول و تمام فعالیت‌های راه دور سرپرستی الزامی کند. **نکته کاربردی ۳۵:** این الزام اطمینان حاصل می‌نماید که سرپرست‌های راه دور 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 منتقل‌شده از طریق این مسیر، با استفاده از پروتکل انتخاب‌شده در عبارت «انتخاب»، رمزگذاری می‌شوند. نویسنده سند هدف امنیتی، مکانیسم یا مکانیسم‌های پشتیبانی شده 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.	

۶ الزامات تضمین امنیت

الزامات عملکرد تضمین توصیف‌کننده چگونگی ارزیابی محصول است. در این بخش الزامات EAL1 آورده می شود که لیست الزامات آن در جدول زیر آمده است.

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

Life cycle Support	ALC_CMC.1	برچسب‌گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

۶,۱ کلاس توسعه

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

۶,۱,۱ مشخصات کارکردی

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

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده‌سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. از آنجا

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح‌شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نیست.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1C)** **شرح مؤلفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجراکننده کارکرد امنیتی[۱] و پشتیبان کننده‌ی الزام کارکرد امنیتی[۲] توصیف نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2C)** **شرح مؤلفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجراکننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **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 ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.4C)**

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

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسطهای کارکرد امنیتی در سند مشخصات کارکردی باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **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 ابتدایی ۱ **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.

۶,۲ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل مدیریتی و نحوه بررسی محیط عملیاتی توسط مدیر (تا مشخص گردد که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می‌شود.

برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد. این راهنما شامل:

- دستورالعمل نصب موفقیت‌آمیز محصول در محیط
- دستورالعمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگ‌تر
- دستورالعمل‌هایی که ارائه‌دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو است.

۶,۲,۱ راهنمای کاربردی

مؤلفه‌های اقدامات توسعه‌دهنده	
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

مؤلفه‌های محتوایی	
نام خانواده	عنصر امنیتی
	شماره مؤلفه: (AGD_OPE.1.3C) **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های در دسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.5C)** **شرح مؤلفه:** سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آن‌ها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.6C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.7C)**

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: سند راهنمای کاربردی باید واضح و قابل‌فهم 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.

۶,۲,۲ راهنمای آماده‌سازی

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

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

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه‌دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکرشده 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.

۶,۳ کلاس آزمون

آزمون محصول برای بررسی بخش‌های کارکردی سامانه و همچنین بخش‌هایی که طراحی و پیاده‌سازی آن‌ها برای سامانه دارای آسیب‌های امنیتی است، در نظر گرفته می‌شود. آزمون بخش‌های کارکردی سامانه از طریق خانواده ATE_IND و آزمون بخش‌هایی که طراحی و پیاده‌سازی آسیب‌زایی دارند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) آزمون بر اساس کارکردی که برای محصول در نظر 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.

۶,۳,۱ 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 توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.

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

مؤلفه‌های اقدامات ارزیاب	
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده، مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آزمون مستقل ۱

مؤلفه‌های اقدامات ارزیاب	
	شماره مؤلفه: (ATE_IND.1.2E) **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.

۶,۴ کلاس آسیب‌پذیری

۶,۴,۱ تحلیل آسیب‌پذیری

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

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

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**

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 بر اساس آسیب‌پذیری‌های بالقوه شناسایی‌شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۶,۵ 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 قابل‌مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه‌دهنده نقش کمرنگی در قابل‌اعتماد بودن محصول دارد، بلکه در این سطح اطمینان (EAL1) تنها به این اطلاعات نیاز است.

۶,۵,۱ 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 از برچسب‌گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب‌گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصول که توسط مرکز گواهی تائید شده است را به آسانی تشخیص دهد.

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

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

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

۶,۵,۲ حوزه پیکربندی

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

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	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 موردنیاز 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.

۷ پیوست یک: الزامات اختیاری

چنان‌که در مقدمه این پروفایل حفاظتی نیز گفته شد، الزامات اولیه (الزاماتی که باید توسط محصول مورد ارزیابی رعایت شوند) در این پروفایل تشریح شده‌اند. علاوه بر این، دو نوع الزامات دیگر نیز وجود دارند که در پیوست‌های یک و دو به آن‌ها پرداخته شده است. نوع اول (پیوست حاضر) از الزاماتی تشکیل شده است که

می‌توان آن‌ها را در هدف امنیتی گنجاند، اما برای انطباق با این پروفایل حفاظتی ضروری نیستند. نوع دوم (پیوست دو) از الزاماتی تشکیل شده است که مبتنی بر عبارت‌های انتخاب سایر الزامات کارکرد امنیتی این پروفایل حفاظتی هستند. اگر انتخاب‌های خاصی انجام شده باشند، الزامات پیوست مربوطه نیز باید در متن هدف امنیتی گنجانده شوند (مثلاً پروتکل‌های رمزنگاری انتخاب‌شده در یک الزام کانال امن).

اگر محصول هر کدام از الزامات اختیاری را انجام دهد، توصیه شده است که فروشنده محصول قابلیت‌های عملکردی مرتبط را به سند هدف امنیتی اضافه نماید؛ بنابراین در نکات کاربردی مطرح‌شده در ادامه، عبارت «این گزینه باید انتخاب گردد...» تکرار شده است؛ اما این عبارت همچنین برای تأکید کردن روی این موضوع است که الزام وقتی انتخاب می‌گردد که قابلیت‌های عملکردی مرتبط توسط محصول فراهم شده باشد و نیاز نیست که جهت انطباق با این پروفایل حفاظتی، محصول حتماً قابلیت‌های عملکردی را پیاده‌سازی نماید. نویسندگان سند هدف امنیتی آزاد هستند که؛ هیچ، برخی یا تمامی الزامات مطرح‌شده 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.

۷,۱ 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 آنچه در «ذخیره‌سازی رویدادهای ممیزی» گفته شده است، از دست‌کاری غیرمجاز داده ممیزی جلوگیری به عمل آورد. فضای حافظه محلی دستگاه‌های شبکه برای ذخیره‌سازی داده ممیزی، محدود است. اگر این حافظه پر شود، امکان از دست رفتن داده ممیزی وجود خواهد داشت. ممکن است یک سرپرست محصول بخواهد اطلاعات مربوط به تعداد داده ممیزی ازدست‌رفته را داشته باشد. این تعداد می‌تواند نشان‌دهنده مشکلات سرور باشد؛ بنابراین، «محل ذخیره‌سازی داده 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 مطرح‌شده بود، در صورت نیاز باید به این جدول برای ثبت اطلاعات ممیزی مراجعه کرد.

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت‌شده
۱.	ذخیره‌سازی رویدادهای ممیزی ۱ و ۲		
۲.	محل ذخیره‌سازی داده 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 مورد اعتماد. شکست توابع کانال مورد اعتماد.	شناسایی آغازکننده و هدفی که تلاش در برقراری کانال‌های مورد اعتماد با آن/برای آن شکست خورده است
۸.	مسیر امن ۱، ۲ و ۳/ پیوند زدن	راه‌اندازی اولیه و خاتمه دادن به مسیر مورد اعتماد. شکست توابع مسیر مورد اعتماد.	
۹.		فعال‌سازی و غیر فعال‌سازی ارتباطات مابین یک جفت از مؤلفه‌ها.	هویت‌های جفت نقاط انتهایی[۱] فعال یا غیرفعال شده

نکته کاربردی ۳۶:

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 سلسله‌مراتبی مورد اعتماد
- خواندن و دسترسی به CRL یا دسترسی به سرور OCSP

[۱] Endpoints pairs

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
۴۵	**ذخیره‌سازی رویدادهای ممیزی ۱**
محصول مورد ارزیابی باید از پاک شدن غیرمجاز داده ممیزی جلوگیری نماید.	
۴۶	**ذخیره‌سازی رویدادهای ممیزی ۱**
محصول مورد ارزیابی باید از دست‌کاری غیرمجاز داده ممیزی جلوگیری نماید.	
۴۷	**محل ذخیره‌سازی داده ممیزی ۳/ فضای ذخیره‌سازی ممیزی محلی**
محصول مورد ارزیابی باید در صورت پر شدن حافظه محلی، اطلاعات مربوط به تعداد داده ممیزی [انتخاب: از بین رفته، بازنویسی شده را، [اختصاص: سایر اطلاعات]] ارائه کند. محصول مورد ارزیابی یکی از اقدامات تعیین‌شده در «محل ذخیره‌سازی داده ممیزی ۳» را انجام می‌دهد. **نکته کاربردی ۳۷:** 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 مکانیسمی 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.	
۴۸	**ذخیره‌سازی داده ممیزی ۶/ فضای ذخیره‌سازی ممیزی محلی**
در صورتی که حجم داده ممیزی از ظرفیت ذخیره‌سازی محلی داده ممیزی فراتر رود/سرریز کند، محصول مورد ارزیابی باید با تولید اخطار، سرپرست را آگاه نماید. **نکته کاربردی ۳۸:** 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 ذخیره‌شده باشند، این هشدار می‌تواند اهمیت بسیار زیادی داشته باشد.	

باید اطمینان حاصل نمود که هشدار مورد اشاره در «محل ذخیره‌سازی داده 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 نیست 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 غیرقابل‌مشاهده حذف می‌شود، ذکر نماید.

۷,۲ کلاس شناسایی و احراز هویت

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

شماره الزام	نام الزام
۴۹	**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 راه دور اتفاق میافتد را تشخیص دهد.	
۵۰	**مدیریت احراز هویت ناموفق ۲**
زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین‌شده برسد، محصول مورد ارزیابی باید [انتخاب: سرپرست راه دور تخطی‌کننده را از احراز هویت موفق جلوگیری نماید تا وقتی که یک [اختصاص: اقدام] توسط یک سرپرست	

محلی صورت گیرد، سرپرست راه دور تخطی‌کننده را از احراز هویت موفق جلوگیری نماید تا وقتی که یک دوره زمانی تعریف‌شده توسط سرپرست سپری شود.] انجام دهد.

نکته کاربردی ۳۹:

این الزام روی یک تعداد تلاش پی‌درپی احراز هویت ناموفق اعمال می‌شود و برای یک سرپرست در کنسول محلی اعمال نمی‌گردد، زیرا قفل‌کردن یک سرپرست محلی، مدنظر نیست. نیل به این مهم نیازمند وجود حساب‌های سرپرستی محلی و راه دور جداگانه یا داشتن مکانیسم احراز هویتی است که بتواند تلاش‌های ورود سرپرست محلی و راه دور را به‌صورت 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 رمز عبور[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 راه دور به دلیل شکست‌های احراز هویت، باعث به وجود آمدن عدم دسترس‌پذیری سرپرست نمی‌گردد (مثال: با تعریف کردن یک ورود محلی که مسدودسازی برای آن اعمال نمی‌شود). راهنمای محیط عملیاتی مشخص می‌سازد که چگونه همیشه یک دسترسی سرپرست نگه‌داری می‌شود حتی در صورتی که یک سرپرست راه دور در اثر موارد مطرح‌شده در این الزام، مسدود گردد.

۵۱	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 مطرح‌شده در این بخش ساخت: [انتخاب: "(", ")", "*", "&", "^", "%", "$", "#", "@", "!"، [اختصاص: سایر کاراکترها]]؛

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 ۴۰:

نویسنده هدف امنیتی کاراکترهای ویژه قابل‌استفاده 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 سامانه 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.

---

[۱] Administrator guidance

[۲] Password reset

[۳] Lockout reset

اختصاص مطرح‌شده در بند ب، باید به بزرگ‌ترین مقداری که می‌تواند برای کمینه طول رمز عبور توسط سرپرست پیکربندی شود، تنظیم گردد.

۵۲	**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 ۴۱:

این الزام باید انتخاب گردد، در صورتی که محصول توزیع‌شده باشد و پروتکل (های) انتخاب‌شده در الزام FPT_ITT.1 از گواهی نامه‌های 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 غیر فعال‌سازی 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 در صورت 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 سلسله‌مراتب گواهی‌نامه که حداقل از گواهی‌نامه ریشه خود-امضاء[۱] و گواهی‌نامه هویت محصول تشکیل شده باشد، پشتیبانی نماید.

[۱] Self-signed root certificate

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.

اگر محصول از هیچ‌کدام از موارد مطرح‌شده در قوانین extendedKeyUsage پشتیبانی نمی‌کند، این وضعیت باید در سند خلاصه مشخصات محصول شرح داده شود.

۵۳	**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 ۴۲:

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.

۷,۳ کلاس مدیریت امنیت

شماره الزام	نام الزام
۵۴	**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 ۴۳:

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 مطرح‌شده در الزام FAU_GEN.1.1 توضیح داده شده است.

۵۵	**مدیریت داده محصول ۱**

محصول مورد ارزیابی باید امکان «مدیریت» داده‌های توابع امنیتی محصول را به سرپرست‌های امنیتی محدود کند.

نکته کاربردی ۴۴:

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 گذرواژه کاربری به حالت پیش‌فرض توسط سرپرست محصول امنیتی است.

۵۶	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.	

۷,۴ کلاس حفاظت از محصول مورد ارزیابی

شماره الزام	نام الزام
۵۷	**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 قابل‌اعمال 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 مورد اعتماد عبور داده می‌شود، به‌وسیله پروتکل انتخاب‌شده 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.	
۵۸	**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.	
۵۹	**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.	
۶۰	**مسیر امن ۳/ پیوند زدن**

[۱] Joining

محصول مورد ارزیابی باید برای پیوند مؤلفه‌ها به توابع امنیتی تحت شرایط/قیدهای محیط عملیاتی تعریف‌شده 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.

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 تعریف‌شده» 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.

۷,۵ کلاس ارتباطات

شماره الزام	نام الزام
۶۱	**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.	
۶۲	**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.	
۶۳	**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، قابل‌اعمال 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 به دلیل امکان اقدامات پیکربندی قابل انجام توسط سرپرست محصول، نیاز به کانال ثبت‌نام نداشته باشد، آنگاه گزینه «هیچ کانالی» برای انتخاب الزام «تعریف کانال ثبت‌نام مؤلفه ۲» برگزیده می‌شود.
اگر نویسنده سند هدف امنیتی، کانال FPT_ITT.1/FTP_ITC.1 را برگزیند، آنگاه سند خلاصه مشخصات محصول باید تکرارهایی از الزام را که برای مشخص کردن استفاده محصول لازم است، تشریح نماید. درصورتی که FTP_TRP.1/Join انتخاب گردد، سند خلاصه مشخصات محصول (در صورت امکان با کمک سند راهنمای عملیاتی) باید جزییات کانال و مکانیسم‌هایی را که استفاده می‌کند تشریح نماید.
اگر نویسنده سند هدف امنیتی، کانال FPT_ITT.1/FTP_ITC.1 را برگزیند، آنگاه در سند هدف امنیتی باید کانال ثبت‌نام به عنوان یکی از تکرارهای الزام FPT_ITT.1 یا FTP_ITC.1 با یک نام مشخص (مثال؛ FPT_ITT.1/Join)، در قالب نکته کاربردی به الزام «تعریف کانال ثبت‌نام مؤلفه ۱» اضافه و اجرا گردد.

۸ پیوست دو: الزامات مبتنی بر انتخاب

چنان‌که 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 مطرح‌شده بود، در صورت نیاز باید به این جدول برای ثبت اطلاعات ممیزی مراجعه کرد.

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت‌شده
۱.	الزامات پروتکل DTLS Client	شکست در ایجاد یک نشست DTLS	دلایل شکست
۲.	الزامات پروتکل DTLS Client/ احراز هویت	شکست در ایجاد یک نشست DTLS	دلایل شکست
		تشخیص حملات تکرار	هویت منبع حمله تکرار (مثلاً؛ آدرس

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت‌شده
			IP)
۳.	الزامات پروتکل DTLS Server	شکست در ایجاد یک نشست DTLS	دلایل شکست
		تشخیص حملات تکرار	هویت منبع حمله تکرار (مثلاً؛ آدرس IP)
۴.	الزامات پروتکل DTLS Server/ احراز هویت دوطرفه	شکست در ایجاد یک نشست DTLS	دلایل شکست
		تشخیص حملات تکرار	هویت منبع حمله تکرار (مثلاً؛ آدرس IP)
۵.	الزامات پروتکل HTTPS	شکست در ایجاد 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 در ایجاد یک نشست SSH	دلایل شکست
		موفقیت در کلید دهی مجدد SSH	ارتباط با نقاط پایانی غیر محصول (آدرس IP)
۸.	الزامات پروتکلSSH Server	شکست در ایجاد 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 دوطرفه	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 دوطرفه	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)	-	-

ردیف	الزام	رویدادهای ممیزی	اطلاعات ممیزی ثبت‌شده
.۱۵	الزامات پروتکل X509(۵) و (۶)	-	-
.۱۶	الزامات به‌روزرسانی امن ۴ و ۵	شکست در به‌روزرسانی	دلایل شکست (شامل شناساننده گواهی‌نامه‌های غیر معتبر)
.۱۷	مدیریت کارکرد در محصول ۱/ به روزرسانی خودکار	فعال‌سازی و غیر فعال‌سازی جستجوی خودکار به‌روزرسانی‌ها یا به روزرسانی‌های خودکار	-
.۱۸	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 سلسله‌مراتبی مورد اعتماد
- خواندن و دسترسی به CRL یا دسترسی به سرور OCSP

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

۸,۱ الزامات پروتکل DTLS Client

شماره الزام	نام الزام
۶۴	**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_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 با RFC 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 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.

۶۵	**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 قسمت Name 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 ذکرشده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود. همچنین کلاینت نباید برای ساختن شناسه‌های مرجع از wildcards استفاده نماید.

۶۶	**الزامات پروتکل DTLS Client (۳)**

محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیر معتبر 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.

۶۷	**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 NIST از 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.

۸,۲ الزامات پروتکل DTLS Clint /احراز هویت

شماره الزام	نام الزام
۶۸	**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:
  - 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 با RFC 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 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.

۶۹	**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 قسمت Name 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 هرکدام از دو روش ذکرشده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود. همچنین کلاینت نباید برای ساختن شناسه‌های مرجع از wildcards استفاده نماید.

[۱] Identifier

[۲] Background

۷۰	الزامات پروتکل DTLS Client/ احراز هویت ۳

محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیر معتبر 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.

۷۱	الزامات پروتکل DTLS 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 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 NIST از 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.

۷۲	الزامات پروتکل DTLS Client/ احراز هویت ۵

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.

۷۳	الزامات پروتکل DTLS Client/ احراز هویت ۶

محصول باید هنگامی‌که یک پیام حاوی MAC غیر معتبر دریافت می‌کند، [انتخاب: به نشست DTLS خاتمه دهد، بی‌صدا رکورد را دور بریزد].

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.

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

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

- رکوردهای DTLS که قبلاً 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، دریافت‌کننده بررسی می‌کند که شماره توالی رکورد دریافتی در پنجره لغزنده دریافت تعریف‌شده باشد و قبلاً توسط رکوردهای دریافت شده، استفاده نشده باشد؛ یعنی پیام تکرار نباشد.

۸,۳ الزامات پروتکل DTLS Server

شماره الزام	نام الزام
۷۵	**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
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492
  - TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492

[۱] Replayed

- 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 با RFC 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 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.
۷۶ | **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.
۷۷ | **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 معرفی‌شده 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.
۷۸ | **الزامات پروتکل DTLS Server (۴)**
محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت] 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: ۲۰۴۸ بیت، ۳۰۷۲ بیت] 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.

۷۹	الزامات پروتکل DTLS Server (۵)
محصول باید هنگامی‌که یک پیام حاوی MAC غیر معتبر دریافت می‌کند، [انتخاب: به نشست DTLS خاتمه دهد، بی‌صدا رکورد را دور بریزد]. **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.	
۸۰	الزامات پروتکل DTLS Server (۶)
محصول باید پیام‌های تکرار/بازپخش شده برای موارد زیر را تشخیص و بی‌صدا دور بیندازد: • رکوردهای DTLS که قبلاً 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، دریافت‌کننده بررسی می‌کند که شماره توالی رکورد دریافتی در پنجره لغزنده دریافت تعریف‌شده باشد و قبلاً توسط رکوردهای دریافت شده، استفاده نشده باشد؛ یعنی پیام تکرار نباشد. عبارت «بی‌صدا دور بیندازد» یعنی محصول بدون هیچ‌گونه پاسخی بسته را دور بیندازد.	

۸,۴ الزامات پروتکل DTLS Server /احراز هویت دوطرفه

شماره الزام	نام الزام
۸۱	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: 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	

- 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_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_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_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.

۸۲	**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.

۸۳	**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 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 معرفی‌شده 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.

۸۴	**الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۴**

محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت] 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: ۲۰۴۸ بیت، ۳۰۷۲ بیت] 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.

۸۵	**الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۵**

محصول باید هنگامی‌که یک پیام حاوی MAC غیر معتبر دریافت می‌کند، [انتخاب: به نشست DTLS خاتمه دهد، بی‌صدا رکورد را دور بریزد].

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.

۸۶	**الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۶**

محصول باید پیام‌های تکرار/بازپخش شده برای موارد زیر را تشخیص و بی‌صدا دور بیندازد:

- رکوردهای DTLS که قبلاً 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، دریافت‌کننده بررسی می‌کند که شماره توالی رکورد دریافتی در پنجره لغزنده دریافت تعریف‌شده باشد و قبلاً توسط رکوردهای دریافت شده، استفاده نشده باشد؛ یعنی پیام تکرار نباشد.

عبارت «بی‌صدا دور بیندازد» یعنی محصول بدون هیچ‌گونه پاسخی بسته را دور بیندازد.

۸۷	**الزامات پروتکل DTLS Server/ احراز هویت دوطرفه ۷**

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

۸۸	**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 غیر معتبر 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.
۸۹ **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 آدرس ایمیل که توسط نظیر استفاده می‌گردد، مقایسه گردد. همچنین ممکن است این شناساننده برای مقایسه، به یک دایرکتوری سرور داده شود.

۸,۵ الزامات پروتکل HTTPS

شماره الزام	نام الزام
۹۰	**الزامات پروتکل HTTPS (۱)**
محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کنند. **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.	
۹۱	**الزامات پروتکل HTTPS (۲)**
محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	
۹۲	**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].	

[۱] Distinquish Name (DN)

[۲] Subject Alternative Name (SAN)

[۳] Identifier

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.

۸,۶ 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 سامانه 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
۹۳	**الزامات پروتکل IPSEC (۱)**
محصول مورد ارزیابی باید پروتکل IPsec را بر اساس آنچه در RFC 4301 مشخص شده است، پیاده‌سازی کند.	

نکته کاربردی ۷۷:

بر اساس RFC 4301 برای پیاده‌سازی IPSEC جهت محافظت از ترافیک IP باید از یک پایگاه داده خط‌مشی امنیتی (SPD) استفاده کرد. با استفاده از SPD می‌توان تعیین کرد که بسته‌های IP چگونه باید مدیریت شوند:

۱- «PROTECT» از بسته‌ها (مثلاً رمزگذاری آن‌ها)

۲- «BYPASS» سرویس‌های IPSEC (مثلاً عدم رمزگذاری)

۳- «DISCARD» بسته (مثلاً دور ریختن بسته). پایگاه داده مذکور را می‌توان به روش‌های مختلفی پیاده‌سازی کرد که از آن جمله می‌توان به فهرست‌های کنترل دسترسی به مسیریاب، مجموعه قوانین فایروال، استفاده از یک پایگاه داده SPD سنتی و مواردی از این دست اشاره کرد. صرف‌نظر از روشی که به کار گرفته می‌شود، 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.
۹۴ | 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.
۹۵ | 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.
۹۶ | الزامات پروتکل IPSEC (۴)
محصول مورد ارزیابی باید بر اساس آنچه در RFC 4303 گفته شده است چارچوب 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 به وجود فراهم می‌نماید. در صورتی که برای IPSec با توجه به خروجی مورد انتظار، نوع خاصی از HMAC مبتنی بر SHA (مثلاً، HMAC کوتاه شده[۲]) انتخاب گردد، در خلاصه مشخصات محصول باید مشخص شود.
۹۷ | الزامات پروتکل IPSEC (۵)

[۱] rule

[۲] Truncated

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

- IKEv1، با استفاده از مد اصلی[۱] 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[۲]، با پشتیبانی اجباری از پیمایش NAT چنان‌که 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.

۹۸	**الزامات پروتکل IPSEC (۶)**

محصول مورد ارزیابی باید اطمینان حاصل کند که برای پی‌آیند[۳] 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 انتخاب‌شده باشد.

۹۹	**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؛

[۱] Main Mode
[۲] NAT traversal
[۳] Payload

- 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 ذکرشده‌اند). به‌طورکلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SA را باید در سند شرح محصول در نظر گرفت.

۱۰۰	**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:
- 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 ذکرشده‌اند). به‌طورکلی، دستورالعمل‌های مربوط به تنظیم پارامترها شامل مدت زمان‌های SA را باید در سند شرح محصول در نظر گرفت.

۱۰۱	**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 مذاکره شده باشد] تولید نماید.

نکته کاربردی ۸۴:

در گروه‌های 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.

۱۰۲	**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 مذاکره شده]؛
- حداقل ۱۲۸ بیت اندازه و حداقل نصف اندازه خروجی تابع درهم‌سازی نیمه‌تصادفی[۱] مذاکره شده (PRF)] تولید کند.

نکته کاربردی ۸۵:

اگر IKEv2 انتخاب‌شده باشد (همان‌طور 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.

[۱] Pseudorandom Function hash

۱۰۳	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 می‌گردد.	
۱۰۴	**الزامات پروتکل IPSEC (۱۲)**
محصول باید به صورت پیش‌فرض بتواند اطمینان حاصل نماید که قدرت الگوریتم متقارن (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [انتخاب: فاز ۱ IKEv1، IKEv2 IKE_SA] مذاکره شده است، بیشتر یا مساوی قدرت الگوریتم متقارنی (از نظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [انتخاب: فاز ۲ IKEv1، IKEv2 CHILD_SA] مذاکره شده است، باشد.	
نکته کاربردی ۸۷: نویسنده سند هدف امنیتی یکی یا هردوی انتخاب‌های IKE را بر اساس اینکه کدام‌یک توسط محصول پیاده‌سازی می‌شود، انتخاب می‌کند. انتخاب نسخه(های) IKE نه فقط در این الزام بلکه در تمامی الزامات بخش IPSec، باید سازگار باشد.	
۱۰۵	**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 نشان‌دهنده الگوریتم‌های استفاده شده (و سازگاری کلیدهای تولیدشده) 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).	
۱۰۶	**الزامات پروتکل IPSEC (۱۴)**
محصول باید کانال امن را فقط در صورتی که شناساننده موجود در گواهی‌نامه دریافتی با شناساننده مرجع پیکربندی‌شده 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 شناساننده‌ای است که محصول انتظار دارد از IKE احراز هویت کاربر دریافت نماید. همچنین شناساننده ارائه شده، شناساننده‌ای است که در بدنه گواهی‌نامه ارائه می‌شود.

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[۳]، الزامی است. به علاوه، استفاده از آدرس‌های IP در هرکدام از دو روش ذکرشده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود.

۸,۷ الزامات پروتکل SSH Client

شماره الزام	نام الزام
۱۰۷	**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 کدام‌یک از RFC ها مطابقت وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح‌شده، مطابقت داشته باشند (مثلاً؛ الگوریتم‌های رمزنگاری معتبر). RFC 4253 الگوریتم‌های رمزنگاری مشخص را که "REQUIRED" (موردنیاز) هستند، تعیین می‌کند. در نتیجه، پشتیبانی از این الگوریتم‌ها باید پیاده‌سازی شود، نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. مشخص کردن اینکه کدام‌یک از الگوریتم‌هایی که به صورت "REQUIRED" می‌باشند، لیست شده ولی پیاده‌سازی نشده است، در حوزه فعالیت ارزیابی این الزام قرار نمی‌گیرد.

[۱] Fully Qualified Domain Name
[۲] Distinquished Name
[۳] Background

۱۰۸	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].	
۱۰۹	الزامات پروتکل SSH Client (۳)
همان‌طور 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:** 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 در نظر گرفتن بیشترین اندازه بسته که قابل‌پذیرش است پر شود تا به این وسیله «طول معقول» برای محصول تعریف شود.	
۱۱۰	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 مطرح‌شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌های برای MAC نیز انتخاب گردند.	
۱۱۱	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 فهرستی از مراجع گواهی امن باید در الزام FCS_SSHC_EXT.1.9 انتخاب شود و الزامات FCS_X509_EXT قابل‌اعمال خواهند	

بود.	
۱۱۲	**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 مطرح‌شده 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.	
۱۱۳	**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.	
۱۱۴	**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 ذکرشده، مجددسازی کلید باید صورت بگیرد. **نکته کاربردی ۹۵:** این الزام حد آستانه‌هایی 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 ذکرشده 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.	
۱۱۵	**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-nistp521 در «الزامات پروتکل SSH Client (۵)» انتخاب‌شده باشد.

۸,۸ الزامات پروتکل SSH Server

شماره الزام	نام الزام
۱۱۶	**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.	
۱۱۷	**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.	
۱۱۸	**الزامات پروتکل SSH Server (۳)**
همان‌طور 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 در نظر گرفتن بیشترین اندازه بسته که قابل‌پذیرش است پر شود تا به این وسیله «طول معقول» برای محصول تعریف شود.
۱۱۹ | **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 مطرح‌شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌های برای MAC نیز انتخاب گردند.
۱۲۰ | **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 قابل‌اعمال خواهند بود.
۱۲۱ | **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 مطرح‌شده 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.
۱۲۲ | **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.
۱۲۳ | **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 ذکرشده، مجددسازی کلید باید صورت بگیرد. **نکته کاربردی ۱۰۲:** این الزام حد آستانه‌هایی 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 ذکرشده 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.

۸,۹ الزامات پروتکل TLS Client

شماره الزام	نام الزام
۱۲۴	**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	

- 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_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_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_SHA256مطابق با RFC 5289
- 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.

۱۲۵	**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 قسمت Name 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 ذکرشده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود. همچنین کلاینت نباید برای ساختن شناسه‌های مرجع از wildcards استفاده نماید.

۱۲۶	**الزامات پروتکل TLS Client (۳)**

محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیر معتبر 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.

۱۲۷	**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 NIST از 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.

۸,۱۰ الزامات پروتکل TLS Client/ احراز هویت

شماره الزام	نام الزام
۱۲۸	**الزامات پروتکل TLS 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:

- 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_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_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_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.

۱۲۹	**الزامات پروتکل TLS 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 قسمت Name 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 ذکرشده، اگرچه می‌تواند پیاده‌سازی گردد ولی توصیه نمی‌شود. همچنین کلاینت نباید برای ساختن شناسه‌های مرجع از wildcards استفاده نماید.

۱۳۰	**الزامات پروتکل TLS Client/ احراز هویت ۳**

محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیر معتبر 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.
۱۳۱ **الزامات پروتکل TLS 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 پروتکل TLS 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 TLS 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 NIST از 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.
۱۳۲ **الزامات پروتکل TLS 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.

۸,۱۱ الزامات پروتکل TLS Server

شماره الزام	نام الزام
۱۳۳	**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_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289

- TLS_ECDHE_RSA_WITH_AES_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.

۱۳۴	**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.

۱۳۵	**الزامات پروتکل TLS Server (۳)**

محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت] 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: ۲۰۴۸ بیت، ۳۰۷۲ بیت] 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.

۸,۱۲ الزامات پروتکل TLS Server/ احراز هویت دوطرفه

شماره الزام	نام الزام
۱۳۶	**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: 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 o TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 o TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 o TLS_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246 o TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 o TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 مطابق با RFC 5246 o TLS_DHE_RSA_WITH_AES_192_CBC_ SHA256 مطابق با RFC 5246 o TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 مطابق 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 با RFC 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 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.

۱۳۷	**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.

۱۳۸	**الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۳**

محصول باید [انتخاب: استقرار کلید مبتنی بر RSA را با اندازه کلید [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت] 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: ۲۰۴۸ بیت، ۳۰۷۲ بیت] 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.

۱۳۹	**الزامات پروتکل TLS Server/ احراز هویت دوطرفه ۴**

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

۱۴۰	**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 غیر معتبر 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.

۱۴۱	**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:

[۱] Identifier

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 آدرس ایمیل که توسط نظیر استفاده می‌گردد، مقایسه گردد. همچنین ممکن است این شناساننده برای مقایسه، به یک دایرکتوری سرور داده شود.

۸,۱۳ الزامات شناسایی و احراز هویت

شماره الزام	نام الزام
۱۴۲	**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 ○ 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.	
۱۴۳	**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. نویسنده 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 سلسله‌مراتب 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 مورد اعتماد 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 روشن شدن 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.

۱۴۴	**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 سامانه، امضای کد برای تائید یکپارچگی، [اختصاص: سایر کاربردها]، هیچ کاربرد دیگر] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.	
۱۴۵	**الزامات پروتکل X509 (۴)**

زمانی که محصول مورد ارزیابی نمی‌تواند اتصال موردنیاز 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 احراز هویتی 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 سامانه (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 انتخاب‌شده باشد، بررسی وضعیت فسخ گواهی، اختیاری است.

۱۴۶	**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 آنچه در FCS_CKM.1 شرح داده‌شده است، توسط محصول مورد ارزیابی تولید می‌شود.

۱۴۷	**الزامات پروتکل X509 (۶)**

[۱] Device-specific information

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

۸,۱۴ الزامات به‌روزرسانی امن

شماره الزام	نام الزام
۱۴۸	**الزامات به‌روزرسانی امن ۴**
محصول درصورتی‌که گواهی‌نامه امضای کد یک به‌روزرسانی غیر معتبر باشد، نباید آن را نصب نماید.	
۱۴۹	**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 ۱۲۳: گواهی‌نامه‌ها را می‌توان به‌صورت اختیاری برای امضای کدها در به‌روزرسانی‌های نرم‌افزار سامانه استفاده کرد (FPT_TUD_EXT.1.3). اگر در «الزامات پروتکل X509 (۳)» مقدار «امضای کد برای به‌روزرسانی‌های نرم‌افزار سامانه» انتخاب‌شده باشد، سند هدف امنیتی باید شامل «خودآزمایی محصول مورد ارزیابی ۲» باشد. در صورتی که فقط از هش‌های انتشاریافته برای به‌روزرسانی‌های امن پشتیبانی گردد، گواهی X509 قابل‌اعمال 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.	
۱۵۰	**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 ۱۲۴:	

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.
۱۵۱ | **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 در صورت پر بودن فضای محلی ذخیره‌سازی] را به سرپرست امنیتی محصول محدود نماید. **نکته کاربردی ۱۲۵:** 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 تعریف‌شده است، قابل پیکربندی باشد و «ارسال داده ممیزی به موجودیت IT خارجی» انتخاب‌شده 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 در صورت پر بودن فضای محلی ذخیره‌سازی» باید انتخاب گردد.

۹ مراجع

- **Network Devices cPP V2.0 published by Network iTC**
- **Standard PP for Enterprise Secuirty Management – Policy Management V2.1**

[۱] Determine the behaviour

[۲] Modify the behaviour