

به نام خدا

پرو فایل حفاظتی تجهیز شبکه

آبان ۹۹
نسخه ۲,۲

پیشگفتار

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی را که در این سند برای برآورده کردن الزامات ارائه شده‌اند، در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک کنند. مرکز مدیریت راهبردی افتا با همکاری مرکز تحقیقات صنایع انفورماتیک و سازمان فناوری اطلاعات ایران این سند را در راستای این هدف تهیه کرده است. این سند معرفی کننده‌ی الزامات کارکرد امنیتی برای تجهیزات شبکه می‌باشد؛ تا تولیدکنندگان محصولات تجهیزات شبکه بتوانند بر مبنای این سند، کارکردهای امنیتی را در محصول خود لحاظ کرده، همچنین سند هدف امنیتی آن را ارائه نمایند.

در بخش اول به معرفی تجهیزات شبکه پرداخته شده 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 تشکیل شده است که هریک از این کلاس‌ها حوزه‌ی خاصی از امنیت را پوشش می‌دهد. کلاس‌هایی که برای تجهیزات شبکه در این سند مطرح شده است، عبارت‌اند از:

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

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

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

تذکر: این فایل از لحاظ الزامات مورد بروزرسانی قرار گرفته است. برخی نکات کاربردی نیز در فایل اصلی تغییر کرده یا بروز شده‌اند که این تغییرات در این پروفایل انجام نشده است و در نسخه‌های بعدی ارائه خواهند شد.

فهرست

- ۱- شرح محصول تجهیز شبکه ۶
- ۱-۱- موارد کاربرد محصول ۷
- ۲- تعریف مسائل امنیتی ۷
- ۱-۲- تهدیدات ۷
- ۱-۱-۲- ارتباط با دستگاه‌های شبکه ۸
- ۱-۱-۱-۲- دسترسی راهبری غیر مجاز ۸
- ۲-۱-۱-۲- رمزنگاری ضعیف ۹
- ۳-۱-۱-۲- کانال‌های ارتباطی غیر قابل اعتماد ۹
- ۴-۱-۱-۲- نقاط پایانی با احراز هویت ضعیف ۹
- ۲-۱-۲- به‌روزرسانی‌های معتبر ۹
- ۱-۲-۱-۲- به‌روزرسانی‌های مخرب ۱۰
- ۳-۱-۲- فعالیت‌های ممیزی‌شده ۱۰
- ۱-۳-۱-۲- فعالیت ردیابی‌نشده ۱۰
- ۴-۱-۲- داده‌ها و اطلاعات محرمانه دستگاه و راهبر ۱۰
- ۱-۴-۱-۲- به خطر افتادن کارکرد امنیتی ۱۱
- ۲-۴-۱-۲- هک شدن گذرواژه ۱۱
- ۵-۱-۲- از کار افتادن کارکردهای امنیتی دستگاه ۱۱
- ۱-۵-۱-۲- از کار افتادن کارکرد امنیتی ۱۱
- ۲-۲- فرضیات ۱۲
- ۱-۲-۲- حفاظت فیزیکی ۱۲
- ۲-۲-۲- کارکرد محدود ۱۲
- ۳-۲-۲- عدم محافظت از ترافیک ۱۲
- ۴-۲-۲- راهبر مورد اعتماد ۱۲
- ۵-۲-۲- به‌روزرسانی منظم ۱۳
- ۶-۲-۲- امنیت اطلاعات محرمانه راهبر ۱۳
- ۳-۲- خط‌مشی امنیتی سازمان ۱۳
- ۱-۳-۲- بذر دسترسی ۱۳
- ۳- اهداف امنیتی ۱۳
- ۱-۳- اهداف امنیتی مربوط به محیط عملیاتی ۱۳
- ۱-۱-۳- امنیت فیزیکی ۱۳

۱۳	۳-۱-۲- عدم کارکرد عمومی
۱۳	۳-۱-۳- محافظت از ترافیک
۱۴	۳-۱-۴- راهبر مورد اعتماد
۱۴	۳-۱-۵- به روزرسانی
۱۴	۳-۱-۶- امنیت حساب کاربری راهبر
۱۴	۴- الزامات کارکرد امنیتی
۲۱	۴-۱- کلاس ممیزی امنیت
۲۶	۴-۲- پشتیبانی رمزنگاری (FCS)
۳۳	۴-۳- کلاس شناسایی و احراز هویت
۳۷	۴-۴- کلاس مدیریت امنیت
۴۱	۴-۵- کلاس حفاظت از محصول مورد ارزیابی
۴۷	۴-۶- دسترسی به محصول
۴۸	۴-۷- کانال‌ها و مسیرهای مورد اعتماد
۵۱	۵- الزامات تضمین امنیت
۵۱	۵-۱- کلاس توسعه
۵۱	۵-۱-۱- مشخصات کارکردی
۵۳	۵-۲- کلاس راهنمای کاربر
۵۴	۵-۲-۱- راهنمای کاربردی
۵۶	۵-۲-۲- راهنمای آمادهدسازی
۵۷	۵-۳- کلاس تست
۵۷	۵-۳-۱- تست مستقل
۵۹	۵-۴- کلاس آسیب‌پذیری
۵۹	۵-۴-۱- تحلیل آسیب‌پذیری
۶۰	۵-۵- کلاس پشتیبانی از چرخه حیات
۶۰	۵-۵-۱- قابلیت‌های پیکربندی
۶۱	۵-۵-۲- حوزه پیکربندی
۶۳	۶- پیوست یک: الزامات اختیاری
۶۳	۶-۱- کلاس ممیزی امنیت
۶۶	۶-۲- کلاس شناسایی و تایید اعتبار
۶۸	۶-۳- کلاس حفاظت از محصول مورد ارزیابی
۷۰	۶-۴- کلاس ارتباطات



- ۷- پیوست دو: الزامات مبتنی بر انتخاب ۷۲
- ۷-۱- کلاس ممیزی امنیت ۷۴
- ۷-۱-۱- تولید داده های ممیزی امنیت ۷۴
- ۷-۲- کلاس پشتیبانی از رمزنگاری ۷۵
- ۷-۲-۱- الزامات پروتکل DTLS Client ۷۵
- ۷-۲-۲- الزامات پروتکل DTLS Client / احراز هویت ۷۸
- ۷-۲-۳- الزامات پروتکل DTLS Server ۷۸
- ۷-۲-۴- الزامات پروتکل DTLS Server / احراز هویت متقابل ۸۱
- ۷-۲-۵- الزامات پروتکل HTTPS ۸۲
- ۷-۲-۶- الزامات پروتکل IPSec ۸۲
- ۷-۲-۷- الزامات پروتکل NTP ۸۹
- ۷-۲-۸- الزامات پروتکل SSH Client ۸۹
- ۷-۲-۹- الزامات پروتکل SSH Server ۹۲
- ۷-۲-۱۰- الزامات پروتکل TLS Client ۹۴
- ۷-۲-۱۱- الزامات پروتکل TLS Client / احراز هویت ۹۷
- ۷-۲-۱۲- الزامات پروتکل TLS Server ۹۸
- ۷-۲-۱۳- الزامات پروتکل TLS Server همراه با احراز هویت دو طرفه ۱۰۰
- ۷-۳- کلاس شناسایی و احراز هویت ۱۰۰
- ۷-۳-۱- الزامات پروتکل X509 ۱۰۰
- ۷-۴- کلاس حفاظت از محصول ۱۰۳
- ۷-۴-۱- الزامات به روزرسانی امن ۱۰۳
- ۷-۵- کلاس مدیریت امنیت ۱۰۴

۱- شرح محصول تجهیز شبکه

سند حاضر، پروفایل حفاظتی برای ارزیابی محصولی است که به عنوان یک دستگاه شبکه شناخته می شود. منظور از یک دستگاه شبکه در این پروفایل حفاظتی، دستگاهی متشکل از سخت افزار و نرم افزار می باشد که به شبکه متصل است و یک نقش زیرساخت را در شبکه فراهم می آورد.

این پروفایل حفاظتی، مجموعه ای از حداقل الزامات امنیتی را ارائه می کند که دستگاه های شبکه باید به منظور کاهش تهدیدات، آن ها را رعایت نمایند. این الزامات اولیه برای هر نوع از تجهیز شبکه است و سایر الزامات آن از اسناد پروفایل حفاظتی اختصاصی آن محصول تکمیل خواهند شد تا مجموعه ای از روش های امنیتی را برای شبکه های سازمانی فراهم آورند. هدف سند حاضر این است که مجموعه ای از کارکردهای امنیتی معمول را ارائه کند که تمام شبکه ها، صرف نظر از کارکرد خاص هر تجهیز شبکه ای یا هر گونه ابزار امنیتی اضافه، باید آن ها را بکار گیرند. این مجموعه اولیه کارکردهای امنیتی، شامل مواردی از جمله حفاظت از تمام مسیرهای مدیریتی راه دور، ارائه خدمات شناسایی و احراز هویت برای ورودهای محلی و راه دور، ممیزی رویدادهای امنیتی، تأیید رمزنگاری امن تمام به روزرسانی ها و حفاظت در برابر حملات مرسوم به شبکه است. هدف این است که تمام دستگاه های شبکه که در حیطه شمول این پروفایل حفاظتی قرار می گیرند، به گونه مناسبی در شبکه «رفتار» کنند و آسیبی را به شبکه وارد ننمایند. بدین منظور، انتظار می رود که دستگاه شبکه از پروتکل های استاندارد مانند IPsec یا TLS یا SSH استفاده کند و بدین ترتیب از مسیرهای ارتباطی برقرار شده با موجودیت های خارجی محافظت نماید. همچنین لازم است که گواهی نامه های X.509 به منظور احراز هویت مورد استفاده قرار گیرند. استفاده از این گواهی نامه ها گزینه ای برای امضای دیجیتال و امضای کد می باشد.

محصولات توزیع شده در دامنه شمول این پروفایل حفاظتی قرار نمی گیرند، اما انتظار می رود که در پروفایل حفاظتی آینده به آن ها پرداخته شود. کارکردهای امنیتی اضافه ای که ممکن است نوع خاصی از دستگاه های شبکه بکار گیرند، نیز در دامنه شمول این پروفایل حفاظتی قرار نمی گیرد، بلکه در سایر پروفایل های حفاظتی مربوط به انواع مختلف دستگاه ها پوشش داده خواهند شد. علاوه بر این، اسکن ویروس ها و ایمیل ها، قابلیت های تشخیص و جلوگیری از نفوذ^۱، ترجمه آدرس شبکه^۲ (NAT) به عنوان یک کارکرد امنیتی و کارکردهای شبکه مجازی نیز در دامنه شمول این پروفایل حفاظتی قرار نمی گیرند. انتظار می رود که این پروفایل حفاظتی توسعه یابد و مواردی از جمله افزایش قابلیت انعطاف، کاربردهای مختلف و انطباق با فناوری های جدید را پوشش دهد. در حال حاضر تجهیزات شبکه باید به طور کامل از این پروفایل حفاظتی تبعیت نمایند.

^۱ Intrusion detection/prevention

^۲ Network Address Translation

۱-۱- موارد کاربرد محصول

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

۲- تعریف مسائل امنیتی

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

برقراری ارتباط با دستگاه‌های مجاز و غیر مجاز شبکه

توانایی انجام به‌روزرسانی‌های معتبر و امن

توانایی ممیزی فعالیت‌های دستگاه‌ها

توانایی ذخیره‌سازی و استفاده امن از داده‌ها و اطلاعات محرمانه راهبر و دستگاه

توانایی انجام خودآزمایی در صورت از کار افتادن مؤلفه‌های کلیدی.

۱-۲- تهدیدات

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

^۱Stateful Traffic Filter Firewall

۲-۱-۱- ارتباط با دستگاه‌های شبکه

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

۲-۱-۱-۱- دسترسی راهبری غیر مجاز

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

۲-۱-۱-۲- رمزنگاری ضعیف

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

۲-۱-۱-۳- کانال‌های ارتباطی غیر قابل اعتماد

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

۲-۱-۱-۴- 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 راهبر به دستگاه دیگری معرفی کند یا خود را در جریان شبکه قرار دهد و حملات مردی در میان را طراحی نماید. در نتیجه، ممکن است مهاجم به ترافیک حساس شبکه دسترسی پیدا کند، محرمانگی و یکپارچگی آن را به خطر اندازد و حتی دستگاه شبکه را در معرض خطر قرار دهد.

۲-۱-۲- به‌روزرسانی‌های معتبر

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

۲-۱-۲-۱- به روزرسانی های مخرب

ممکن است عامل تهدید یک به روزرسانی معیوب و دستکاری شده را برای نرم افزار یا ثابت افزار دستگاه شبکه ارائه کند و کارکرد امنیتی دستگاه را در معرض خطر قرار دهد. به روزرسانی های تأیید نشده یا به روزرسانی هایی که با استفاده از ابزارهای رمزنگاری ضعیف یا غیر امن تأیید شده اند، نرم افزار یا ثابت افزار به روز شده را در معرض خطر دستکاری غیر مجاز قرار می دهد.

۲-۱-۲-۳- فعالیت های ممیزی شده

راهبران می توانند با ممیزی فعالیت های دستگاه شبکه، وضعیت دستگاه را به خوبی پایش نمایند. این فرایند امکان بررسی، گزارش دهی در خصوص کارکردهای امنیتی، بازسازی رویدادها و تحلیل مشکل امنیتی را برای راهبر فراهم می آورد. پردازش هایی که در پاسخ به فعالیت های دستگاه انجام می شوند، نشانه هایی از به خطر افتادن یا از کار افتادن کارکردهای امنیتی را ارائه می کنند. در صورتی که فعالیت هایی انجام شده و بر کارکرد امنیتی تأثیر گذاشته باشند اما نشانه ای دال بر انجام شدن آن ها تولید و پایش نشده باشد، ممکن است که این فعالیت ها بدون آگاهی راهبر صورت گرفته باشند. علاوه بر این، در صورتی که سوابق تولید و نگهداری نشده باشند، امکان بازسازی شبکه و درک شدت و میزان آسیب های وارده تحت تأثیر قرار خواهد گرفت. داده های ممیزی ثبت شده در خصوص تغییر و حذف غیر مجاز، باید به دقت محافظت شوند. داده های مذکور ممکن است در درون محصول یا در هنگام انتقال به حافظه های خارجی مورد حمله قرار گیرند. توجه داشته باشید که بر اساس این پروفایل حفاظتی مشارکتی، دستگاه شبکه باید داده های ممیزی را تولید کند و قابلیت ارسال آن ها به یک موجودیت شبکه مورد اعتماد را داشته باشد.

۲-۱-۳-۱- فعالیت ردیابی نشده

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

۲-۱-۴- داده ها و اطلاعات محرمانه دستگاه و راهبر

دستگاه شبکه در بر دارنده داده ها و اطلاعات محرمانه ای است که باید به طور امن ذخیره سازی شوند و امکان دسترسی به آن ها تنها برای موجودیت های مجاز وجود داشته باشد. به عنوان مثال، می توان به اطلاعات محرمانه احراز هویت و پیکربندی نرم افزار و ثابت افزار و اطلاعات محرمانه راهبری اشاره کرد. کلیدهای راهبر و دستگاه، اطلاعات کلید و اطلاعات محرمانه احراز هویت را باید در برابر دستکاری و افشای غیر مجاز محافظت نمود. علاوه بر این، کارکرد امنیتی دستگاه باید کاربران را ملزم کند تا اطلاعات محرمانه احراز هویت پیش فرض را تغییر دهند (مثلاً راهبران ملزم باشند که اطلاعات محرمانه ورود پیش فرض را عوض کنند). عدم ذخیره سازی امن و مدیریت نامناسب داده ها و اطلاعات محرمانه (مانند رمزگذاری نکردن اطلاعات محرمانه درون فایل های پیکربندی یا

دسترسی به کلیدهای نشست کانال امن) به مهاجم امکان می‌دهد تا به دستگاه شبکه دسترسی پیدا کند و حتی امنیت شبکه را از طریق دستکاری ظاهراً مجاز پیکربندی یا ترتیب دادن حملات کسی در میانه در معرض خطر قرار دهد. این حملات به موجودیت غیر مجاز امکان می‌دهند تا با استفاده از اطلاعات محرمانه راهبر امنیتی، به کارکردهای راهبری دست پیدا کند و آن‌ها را اجرا نماید و همچنین به عنوان یک دستگاه پایانی مجاز، تمامی ترافیک را دریافت نماید. بدین ترتیب، شناسایی حملات امنیتی و بازسازی شبکه دشوار خواهد شد و حتی دسترسی غیر مجاز مهاجم به داده‌های دستگاه و راهبر ادامه خواهد یافت.

۲-۱-۴-۱- به خطر افتادن کارکرد امنیتی

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

۲-۱-۴-۲- هک شدن گذرواژه

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

۲-۱-۵- از کار افتادن کارکردهای امنیتی دستگاه

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

۲-۱-۵-۱- از کار افتادن کارکرد امنیتی

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

^۱ Roots of trust

۲-۲-۲- فرضیات

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

۲-۲-۱- حفاظت فیزیکی

چنین فرض می‌شود که دستگاه شبکه در محیط عملیاتی خود به صورت فیزیکی محافظت شده و در معرض حملات فیزیکی و خسارت‌های ناشی از آن‌ها قرار ندارد. چنین فرض می‌شود که این محافظت برای تأمین امنیت دستگاه و داده‌های آن کافی است. در نتیجه، این پروفایل حفاظتی مشارکتی شامل هیچ الزامی در زمینه حفاظت فیزیکی و ابزارهای لازم برای کاستن از خسارات ناشی از حملات فیزیکی نیست. این پروفایل از محصولات انتظار ندارد که از دسترسی فیزیکی به دستگاه (که به موجودیت‌های غیر مجاز امکان می‌دهد تا داده‌ها را استخراج کنند، سایر کنترل‌ها را دور بزنند یا به هر طریق دیگری دستگاه را دستکاری کنند) جلوگیری به عمل آورند.

۲-۲-۲- کارکرد محدود

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

۲-۲-۳- عدم محافظت از ترافیک

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

۲-۲-۴- راهبر مورد اعتماد

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

۲-۲-۵- به روزرسانی منظم

چنین فرض می شود که در صورت منتشر شدن به روزرسانی های جدید در پاسخ به آسیب پذیری های شناخته شده، راهبر نرم افزار و ثابت افزار دستگاه شبکه را به صورت منظم به روزرسانی می کند.

۲-۲-۶- امنیت اطلاعات محرمانه راهبر

اطلاعات محرمانه راهبر (کلید خصوصی) که برای دسترسی به دستگاه شبکه استفاده می شوند، توسط پلت فرمی که روی آن قرار دارند محافظت می گردند.

۲-۳- خط مشی امنیتی سازمان

خط مشی امنیتی سازمان مجموعه ای است از قوانین، اقدامات و رویه های سازمان برای برآورده ساختن نیازهای امنیتی آن. یک خط مشی امنیتی در بخش زیر ارائه شده است.

۲-۳-۱- بنر دسترسی

محصول باید یک بنر اولیه را نمایش دهد که محدودیت های کاربرد، موافقت نامه های قانونی و هرگونه اطلاعات مقتضی دیگر (که کاربران با دسترسی به محصول با آن ها موافقت کرده اند) را به نمایش می گذارد.

۳- اهداف امنیتی

۳-۱- اهداف امنیتی مربوط به محیط عملیاتی

بخش های زیر، اهداف امنیتی مربوط به محیط عملیاتی را تشریح می کنند.

۳-۱-۱- امنیت فیزیکی

امنیت فیزیکی، متناسب با ارزش محصول مورد ارزیابی و داده هایی که در آن قرار دارند، توسط محیط ارائه می شود.

۳-۱-۲- عدم کارکرد عمومی

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

۳-۱-۳- محافظت از ترافیک

محصول مورد ارزیابی از ترافیکی که از آن عبور می کند، محافظت نمی نماید. فرض بر این است که حفاظت از این ترافیک توسط سایر ابزارهای امنیتی و تضمینی موجود در محیط عملیاتی صورت می گیرد.

۳-۱-۴- راهبر مورد اعتماد

راهبران محصول مورد ارزیابی امن هستند و فرض بر این است که تمام موارد ذکر شده در اسناد راهنما را به طور صحیح انجام می دهند.

۳-۱-۵- به روز رسانی

نرم افزارها و میان افزارهای محصول مورد ارزیابی به طور منظم توسط سرپرست محصول به روز می شوند تا بتوانند خود را با به روز رسانی های محصولات همگام سازند و آسیب پذیری های شناخته شده را برطرف نمایند.

۳-۱-۶- امنیت حساب کاربری راهبر

اطلاعات حساب کاربری سرپرست محصول (کلید خصوصی) مورد استفاده برای دسترسی به محصول، باید در هر پلتفرمی که قرار دارند حفاظت شده باشند.

۴- الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند و در ادامه هریک از الزامات شرح و بسط داده شده اند. همچنین الزامات مربوط به پیوست این سند نیز در ادامه جدول زیر آمده اند. الزامات تشریح شده در این بخش الزامی هستند و تمامی محصولات باید آن ها را رعایت نمایند. بر اساس انتخاب هایی که در این الزامات صورت می گیرند، لازم خواهد بود که برخی الزامات مورد اشاره در پیوست دو نیز رعایت شوند. برخی الزامات اختیاری نیز ممکن است از پیوست یک برگزیده شوند. موارد ذکر شده در قالب فعالیت های ارزیابی، بیان می کنند که توسعه دهندگان محصول مورد ارزیابی باید چه مواردی را رعایت کنند.

به طور کلی، الزامات کارکرد امنیتی مورد اشاره در پیوست دو که در هدف امنیتی به عنوان موارد ضروری به آن ها اشاره شده است، در اثر انتخاب های صورت گرفته در سایر الزامات کارکرد امنیتی تعیین و تکمیل می شوند. به عنوان مثال، در هر یک از الزامات «کانال امن» و «مسیر امن» باید پروتکل هایی را برای انواع کانال های امن تشریح شده در الزامات کارکرد امنیتی انتخاب کرد. انتخاب این پروتکل ها تعیین می کند که کدام یک از الزامات کارکرد امنیتی مورد اشاره، در هدف امنیتی نیز لازم هستند. در صورتی که الزامات کارکرد امنیتی تشریح شده در پیوست یک توسط محصول مورد ارزیابی فراهم شده باشند، می توان آن ها را در هدف امنیتی گنجانند، اما این الزامات برای این که محصول مورد ارزیابی مطابق با این پروفایل حفاظتی باشد ضروری نیستند.



شماره الزام	نام الزام	عنصر متناظر با الزام
۱.	تولید داده ممیزی ۱	FAU_GEN.1.1
۲.	تولید داده ممیزی ۲	FAU_GEN.1.2
۳.	تولید داده ممیزی ۳	FAU_GEN.2.1
۴.	محل ذخیره سازی داده های ممیزی ۱	FAU_STG_EXT.1.1
۵.	محل ذخیره سازی داده های ممیزی ۲	FAU_STG_EXT.1.2
۶.	محل ذخیره سازی داده های ممیزی ۳	FAU_STG_EXT.1.3
۷.	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1
۸.	مدیریت کلید رمزنگاری ۲	FCS_CKM.2.1
۹.	نابودی کلید رمزنگاری ۴	FCS_CKM.4.1
۱۰.	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1/DataEncryption
۱۱.	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1/SigGen
۱۲.	عملیات رمزنگاری ۱ (۳)	FCS_COP.1.1/Hash
۱۳.	عملیات رمزنگاری ۱ (۴)	FCS_COP.1.1/KeyedHash
۱۴.	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۱۵.	تولید بیت تصادفی ۲	FCS_RBG_EXT.1.2
۱۶.	مدیریت احراز هویت ناموفق ۱	FIA_AFL.1.1
۱۷.	مدیریت احراز هویت ناموفق ۲	FIA_AFL.1.2
۱۸.	مدیریت رمز عبور ۱	FIA_PMG_EXT.1.1
۱۹.	شناسایی و احراز هویت کاربر ۱	FIA_UIA_EXT.1.1
۲۰.	شناسایی و احراز هویت کاربر ۲	FIA_UIA_EXT.1.2
۲۱.	سازوکار احراز هویت بر اساس رمز عبور ۲	FIA_UAU_EXT.2.1
۲۲.	احراز هویت کاربر ۱۰	FIA_UAU.7.1
۲۳.	مدیریت کارکرد در محصول ۱ (۱) / به روز رسانی دستی	FMT_MOF.1.1(1)/ManualUpdate
۲۴.	مدیریت داده های محصول ۱	FMT_MTD.1.1/CoreData
۲۵.	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۲۶.	نقش های امنیتی ۳	FMT_SMR.2.1
۲۷.	نقش های امنیتی ۴	FMT_SMR.2.2
۲۸.	نقش های امنیتی ۵	FMT_SMR.2.3
۲۹.	محافظت از داده های محصول (کلیدهای متقارن) ۱	FPT_SKP_EXT.1.1



شماره الزام	نام الزام	عنصر متناظر با الزام
۳۰.	حفاظت از کلمه عبور سرپرست محصول ۱	FPT_APW_EXT.1.1
۳۱.	حفاظت از کلمه عبور سرپرست محصول ۲	FPT_APW_EXT.1.2
۳۲.	خودآزمایی محصول ۱	FPT_TST_EXT.1.1
۳۳.	به روزرسانی امن ۱	FPT_TUD_EXT.1.1
۳۴.	به روزرسانی امن ۲	FPT_TUD_EXT.1.2
۳۵.	به روزرسانی امن ۳	FPT_TUD_EXT.1.3
۳۶.	مهرهای زمانی معتبر ۱	FPT_STM_EXT.1.1
۳۷.	مهرهای زمانی معتبر ۲	FPT_STM_EXT.1.2
۳۸.	قفل کردن و خاتمه دادن به نشست‌ها ۷	FTA_SSL_EXT.1.1
۳۹.	قفل کردن و خاتمه دادن به نشست‌ها ۵	FTA_SSL.3.1
۴۰.	قفل کردن و خاتمه دادن به نشست‌ها ۶	FTA_SSL.4.1
۴۱.	پیغام‌های هشدار در رابطه با استفاده محصول ۱	FTA_TAB.1.1
۴۲.	کانال امن ۱	FTP_ITC.1.1
۴۳.	کانال امن ۲	FTP_ITC.1.2
۴۴.	کانال امن ۳	FTP_ITC.1.3
۴۵.	مسیر امن ۱	FTP_TRP.1.1/Admin
۴۶.	مسیر امن ۲	FTP_TRP.1.2/Admin
۴۷.	مسیر امن ۳	FTP_TRP.1.3/Admin
الزامات مربوط به پیوست یک: الزامات اختیاری		
۴۸.	ذخیره سازی داده‌های ممیزی محافظت شده ۱	FAU_STG.1.1
۴۹.	ذخیره سازی داده‌های ممیزی محافظت شده ۲	FAU_STG.1.2
۵۰.	شمارش داده‌های ممیزی از دست رفته	FAU_STG_EXT.2.1/LocSpace
۵۱.	نمایش هشدار برای فضای ذخیره سازی محلی	FAU_STG.3.1/LocSpace
۵۲.	تایید گواهینامه X509 (۱)	FIA_X509_EXT.1.1/ITT
۵۳.	تایید گواهینامه X509 (۲)	FIA_X509_EXT.1.2/ITT
۵۴.	حفاظت از انتقال داخلی داده‌های اساسی محصول	FPT_ITT.1.1
۵۵.	مسیر امن ۱ / Join	FTP_TRP.1.1/Join
۵۶.	مسیر امن ۲ / Join	FTP_TRP.1.2/Join
۵۷.	مسیر امن ۳ / Join	FTP_TRP.1.3/Join



شماره الزام	نام الزام	عنصر متناظر با الزام
۵۸.	تعریف کانال ثبت مولفه ۱	FCO_CPC_EXT.1.1
۵۹.	تعریف کانال ثبت مولفه ۲	FCO_CPC_EXT.1.2
۶۰.	تعریف کانال ثبت مولفه ۳	FCO_CPC_EXT.1.3
الزامات مربوط به پیوست دو: الزامات مبتنی بر انتخاب		
۶۱.	تولید داده ممیزی ۱	FAU_GEN_EXT.1.1
۶۲.	محل ذخیره سازی داده های ممیزی حفاظت شده	FAU_STG_EXT.3.1
۶۳.	محل ذخیره سازی داده ممیزی ۴	FAU_STG_EXT.4.1
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
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 Server (۱)	FCS_DTLSS_EXT.1.1
۷۲.	الزامات پروتکل DTLS Server (۲)	FCS_DTLSS_EXT.1.2
۷۳.	الزامات پروتکل DTLS Server (۳)	FCS_DTLSS_EXT.1.3
۷۴.	الزامات پروتکل DTLS Server (۴)	FCS_DTLSS_EXT.1.4
۷۵.	الزامات پروتکل DTLS Server (۵)	FCS_DTLSS_EXT.1.5
۷۶.	الزامات پروتکل DTLS Server (۶)	FCS_DTLSS_EXT.1.6
۷۷.	الزامات پروتکل DTLS Server (۷)	FCS_DTLSS_EXT.1.7
۷۸.	الزامات پروتکل DTLS Server / احراز هویت متقابل (۱)	FCS_DTLSS_EXT.2.1
۷۹.	الزامات پروتکل DTLS Server / احراز هویت متقابل (۲)	FCS_DTLSS_EXT.2.2
۸۰.	الزامات پروتکل DTLS Server / احراز هویت متقابل (۳)	FCS_DTLSS_EXT.2.3
۸۱.	الزامات پروتکل HTTPS (۱)	FCS_HTTPS_EXT.1.1
۸۲.	الزامات پروتکل HTTPS (۲)	FCS_HTTPS_EXT.1.2
۸۳.	الزامات پروتکل HTTPS (۳)	FCS_HTTPS_EXT.1.3
۸۴.	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1



شماره الزام	نام الزام	عنصر متناظر با الزام
۸۵.	الزامات پروتکل IPSEC (۲)	FCS_IPSEC_EXT.1.2
۸۶.	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
۸۷.	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
۸۸.	الزامات پروتکل IPSEC (۵)	FCS_IPSEC_EXT.1.5
۸۹.	الزامات پروتکل IPSEC (۶)	FCS_IPSEC_EXT.1.6
۹۰.	الزامات پروتکل IPSEC (۷)	FCS_IPSEC_EXT.1.7
۹۱.	الزامات پروتکل IPSEC (۸)	FCS_IPSEC_EXT.1.8
۹۲.	الزامات پروتکل IPSEC (۹)	FCS_IPSEC_EXT.1.9
۹۳.	الزامات پروتکل IPSEC (۱۰)	FCS_IPSEC_EXT.1.10
۹۴.	الزامات پروتکل IPSEC (۱۱)	FCS_IPSEC_EXT.1.11
۹۵.	الزامات پروتکل IPSEC (۱۲)	FCS_IPSEC_EXT.1.12
۹۶.	الزامات پروتکل IPSEC (۱۳)	FCS_IPSEC_EXT.1.13
۹۷.	الزامات پروتکل IPSEC (۱۴)	FCS_IPSEC_EXT.1.14
۹۸.	الزامات پروتکل NTP (۱)	FCS_NTP_EXT.1.1
۹۹.	الزامات پروتکل NTP (۲)	FCS_NTP_EXT.1.2
۱۰۰.	الزامات پروتکل NTP (۳)	FCS_NTP_EXT.1.3
۱۰۱.	الزامات پروتکل NTP (۴)	FCS_NTP_EXT.1.4
۱۰۲.	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.1.1
۱۰۳.	الزامات پروتکل SSH Client (۲)	FCS_SSHC_EXT.1.2
۱۰۴.	الزامات پروتکل SSH Client (۳)	FCS_SSHC_EXT.1.3
۱۰۵.	الزامات پروتکل SSH Client (۴)	FCS_SSHC_EXT.1.4
۱۰۶.	الزامات پروتکل SSH Client (۵)	FCS_SSHC_EXT.1.5
۱۰۷.	الزامات پروتکل SSH Client (۶)	FCS_SSHC_EXT.1.6
۱۰۸.	الزامات پروتکل SSH Client (۷)	FCS_SSHC_EXT.1.7
۱۰۹.	الزامات پروتکل SSH Client (۸)	FCS_SSHC_EXT.1.8
۱۱۰.	الزامات پروتکل SSH Client (۹)	FCS_SSHC_EXT.1.9
۱۱۱.	الزامات پروتکل SSH Server (۱)	FCS_SSHS_EXT.1.1
۱۱۲.	الزامات پروتکل SSH Server (۲)	FCS_SSHS_EXT.1.2
۱۱۳.	الزامات پروتکل SSH Server (۳)	FCS_SSHS_EXT.1.3



شماره الزام	نام الزام	عنصر متناظر با الزام
۱۱۴.	الزامات پروتکل SSH Server (۴)	FCS_SSHS_EXT.1.4
۱۱۵.	الزامات پروتکل SSH Server (۵)	FCS_SSHS_EXT.1.5
۱۱۶.	الزامات پروتکل SSH Server (۶)	FCS_SSHS_EXT.1.6
۱۱۷.	الزامات پروتکل SSH Server (۷)	FCS_SSHS_EXT.1.7
۱۱۸.	الزامات پروتکل SSH Server (۸)	FCS_SSHS_EXT.1.8
۱۱۹.	الزامات پروتکل TLS Client ۱	FCS_TLSC_EXT.1.1
۱۲۰.	الزامات پروتکل TLS Client ۲	FCS_TLSC_EXT.1.2
۱۲۱.	الزامات پروتکل TLS Client ۳	FCS_TLSC_EXT.1.3
۱۲۲.	الزامات پروتکل TLS Client ۴	FCS_TLSC_EXT.1.4
۱۲۳.	الزامات پروتکل TLS Client / احراز هویت ۱	FCS_TLSC_EXT.2.1
۱۲۴.	الزامات پروتکل TLS Server ۱	FCS_TLSS_EXT.1.1
۱۲۵.	الزامات پروتکل TLS Server ۲	FCS_TLSS_EXT.1.2
۱۲۶.	الزامات پروتکل TLS Server ۳	FCS_TLSS_EXT.1.3
۱۲۷.	الزامات پروتکل TLS Server ۴	FCS_TLSS_EXT.1.4
۱۲۸.	الزامات پروتکل TLS Server / احراز هویت دو طرفه ۱	FCS_TLSS_EXT.2.1
۱۲۹.	الزامات پروتکل TLS Server / احراز هویت دو طرفه ۲	FCS_TLSS_EXT.2.2
۱۳۰.	الزامات پروتکل TLS Server / احراز هویت دو طرفه ۳	FCS_TLSS_EXT.2.3
۱۳۱.	اعتبارسنجی گواهینامه X509 (۱)	FIA_X509_EXT.1.1/Rev
۱۳۲.	اعتبارسنجی گواهینامه X509 (۲)	FIA_X509_EXT.1.2/Rev
۱۳۳.	احراز هویت گواهینامه X509 (۱)	FIA_X509_EXT.2.1
۱۳۴.	احراز هویت گواهینامه X509 (۲)	FIA_X509_EXT.2.2
۱۳۵.	درخواست‌های گواهینامه X509 (۱)	FIA_X509_EXT.3.1
۱۳۶.	درخواست‌های گواهینامه X509 (۲)	FIA_X509_EXT.3.2
۱۳۷.	الزامات به‌روزرسانی امن ۴	FPT_TUD_EXT.2.1
۱۳۸.	الزامات به‌روزرسانی امن ۵	FPT_TUD_EXT.2.2
۱۳۹.	الزامات به‌روزرسانی امن ۶	FPT_TUD_EXT.2.3
۱۴۰.	الزامات به‌روزرسانی امن ۷	FPT_TUD_EXT.2.4
۱۴۱.	مدیریت رفتار توابع امنیتی/به‌روزرسانی خودکار ۱	FMT_MOF.1.1/AutoUpdate
۱۴۲.	مدیریت رفتار توابع امنیتی/به‌روزرسانی خودکار ۲	FMT_MOF.1.1/Functions



شماره الزام	نام الزام	عنصر متناظر با الزام
۱۴۳.	مدیریت رفتار توابع امنیتی/خدمات ۱	FMT_MOF.1.1/Services
۱۴۴.	مدیریت رفتار توابع امنیتی/کلیدهای رمزنگاری ۱	FMT_MTD.1.1/CryptoKeys

۴-۱- کلاس ممیزی امنیت

برای حصول اطمینان از این که سرپرست محصول، اطلاعات لازم برای شناسایی مشکلات عمدی و غیرعمدی موجود در زمینه پیکربندی و/یا کارکرد سیستم را در اختیاردارند، محصول باید این قابلیت را داشته باشد که داده‌های ممیزی مورد نیاز برای تشخیص چنین فعالیت‌هایی را تولید نماید. ممیزی فعالیت‌های مدیریت سیستم سبب تولید اطلاعاتی می‌شود که در صورت نیاز به تغییر پیکربندی سیستم، می‌توان برای طراحی اقدامات اصلاحی از آن‌ها استفاده کرد. ممیزی رویدادهای گزینش شده نشان می‌دهد که آیا بخش‌هایی مهم محصول مورد ارزیابی در معرض شکست قرار دارند یا خیر (مثلاً این که فرایند رمزنگاری اجرا نشود) و همچنین به شناسایی فعالیت‌های غیرمعمول (مانند ایجاد یک نشست کاربری در زمان مشکوک، شکست مکرر نشست‌ها یا احراز هویت ناموفق به سیستم) یک مورد مشکوک، کمک می‌کند. در برخی موارد، ممکن است حجم اطلاعات ممیزی تولیدشده به اندازه‌ای زیاد شود که محصول مورد ارزیابی یا راهبران مسئول بازبینی این اطلاعات را دچار سردرگمی کند. محصول مورد ارزیابی باید بتواند اطلاعات ممیزی را به یک موجودیت مورداعتماد خارجی ارسال کند. این اطلاعات باید دارای مهرهای زمانی قابل اعتماد 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 می‌باشد.

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

شماره الزام	نام الزام
۱	تولید داده ممیزی ۱
توابع امنیتی هدف ارزیابی باید بتواند سوابق ممیزی را برای رویدادهای قابل ممیزی زیر تهیه کند: الف) آغاز و اتمام توابع ممیزی؛ ب) تمام اقدامات مدیریتی شامل موارد زیر: - ورود و خروج مدیریتی به سیستم (در صورتی که مدیران نیاز به حساب کاربری شخصی داشته باشند، نام حساب کاربری آن‌ها نیز باید ثبت شود) - تغییرات امنیتی در پیکربندی (علاوه بر اطلاعات حاکی از تغییرات رخ داده، باید ثبت شود که چه مواردی تغییر کرده‌اند)	

- تولید، وارد کردن، تغییر یا پاک کردن کلیدهای رمزنگاری (علاوه بر این کار، نام کلید اختصاصی یا یک مرجع کلید نیز باید ثبت شود)
 - تغییر کلمه عبور (نام حساب کاربری مربوطه نیز باید ثبت شود)
 - [انتخاب: هیچ اقدام دیگر، اختصاص: [لیست سایر کاربردهای ویژه]]؛
- ت) اختصاصا لیست رویدادهای قابل ممیزی تعریف شده در جدول زیر

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

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

FAU_GEN.1.2	تولید داده ممیزی ۲	۲
محصول مورد ارزیابی باید در هر یک از سوابق ممیزی، دست کم 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 مولفه های کارکردی ارائه شده در پروفایل حفاظتی یا هدف امنیتی، اطلاعات در ستون سوم از جدول الزام FAU_GEN.1.1 مشخص شده است.		
FAU_GEN.2.1	تولید داده ممیزی ۳	۳
در مورد آن دسته از رویدادهای ممیزی که حاصل اقدامات کاربران احراز هویت شده هستند، محصول مورد ارزیابی باید بتواند هر رویداد قابل ممیزی را با هویت کاربری که مسبب آن رویداد شده است، مرتبط سازد. نکته کاربردی:		

^۱ Subject

زمانی که یک رویداد ممیزی توسط مولفه دیگری triggered شده باشد، مولفه‌ای که رویدادها را ثبت می‌کند باید رویداد را با آن شناسه آغازگر مولفه که باعث رویداد شده است، مرتبط کند. (فقط برای اهداف ارزیابی توزیع شده اعمال می‌شود).		
۴	محل ذخیره‌سازی داده‌های ممیزی ۱	FAU_STG_EXT.1.1
توابع امنیتی هدف ارزیابی باید قادر به ارسال داده ممیزی تولید شده به یک موجودیت IT خارجی با استفاده از کانال مورد اعتماد مطابق با FTP_ITC.1 باشد. نکته کاربردی: برای انتخاب گزینه انتقال داده‌های ممیزی تولیدشده به یک موجودیت IT خارجی، ذخیره‌سازی و بازبینی سوابق ممیزی از یک سرور ممیزی به جز سرور محصول مورد ارزیابی متکی است. در این مورد ذخیره‌سازی، توسط محیط عملیاتی صورت می‌گیرد. تا زمانی که سرور ممیزی خارجی بخشی از هدف ارزیابی نباشد، به جز قابلیت‌های انتقال داده ممیزی FTP_ITC.1، هیچ الزامی برای آن وجود ندارد. هیچ الزامی برای قالب یا اساس پروتکل داده‌های ممیزی که منتقل می‌شوند وجود ندارد. هدف ارزیابی باید قادر به پیکربندی برای انتقال داده‌های ممیزی به موجودیت IT خارجی بدون مداخله مدیر باشد. انتقال دستی نیازمندی‌ها را برآورده نخواهد کرد. انتقال می‌تواند در زمان واقعی یا به صورت دوره‌ای انجام شود. اگر انتقال در زمان واقعی انجام نشود، TSS شرح می‌دهد که باید چه رویدادی برای انتقال ایجاد شود و چه محدوده‌ای از فرکانس‌های هدف ارزیابی برای ایجاد انتقال داده‌های ممیزی به سرور ممیزی پشتیبانی می‌شود. همچنین TSS فرکانس‌های قابل قبولی برای انتقال پیشنهاد می‌دهد. برای هدف‌های ارزیابی توزیع‌شده، هر مولفه باید به طور مناسبی قادر به استخراج داده ممیزی از طریق کانال محافظت شده خارجی (FTP_ITC.1) یا بین مولفه‌ای (FPT_ITT.1 یا FTP_ITC.1) باشد. حداقل یک مولفه از هدف ارزیابی باید قادر به استخراج سوابق ممیزی از طریق FTP_ITC.1 باشد تا تمامی سوابق ممیزی هدف ارزیابی را بتوان برای موجودیت IT خارجی استخراج کرد.		
۵	محل ذخیره‌سازی داده‌های ممیزی ۲	FAU_STG_EXT.1.2
محصول مورد ارزیابی باید بتواند داده‌های ممیزی تولیدشده را در خود ذخیره کند. [انتخاب: • هدف ارزیابی شامل تنها یک جزء مستقل است که داده‌های ممیزی را بصورت محلی ذخیره می‌کند. • هدف ارزیابی باید یک هدف ارزیابی توزیع شده باشد که داده‌های ممیزی را روی اجزاء هدف ارزیابی زیر ذخیره می‌کند: [اختصاص: شناسایی اجزاء هدف ارزیابی] • هدف ارزیابی یک هدف ارزیابی توزیع شده با ذخیره داده‌های ممیزی است که به صورت خارجی برای اجزای هدف ارزیابی زیر ارائه شده است. [اختصاص: لیستی از مؤلفه‌های هدف ارزیابی که داده‌های ممیزی را بصورت محلی ذخیره نمی‌کنند و سایر اجزای هدف ارزیابی که داده‌های ممیزی تولید شده خود را به آنها منتقل می‌کنند].		
۶	محل ذخیره‌سازی داده‌های ممیزی ۳	FAU_STG_EXT.1.3

در صورتی که فضای حافظه محلی داده ممیزی پر شده باشد محصول مورد ارزیابی باید [انتخاب: داده‌های ممیزی جدید را کنار بگذارد، سوابق ممیزی گذشته را بر اساس این قوانین بازنویسی^۱ کند: [اختصاص: قوانین بازنویسی سوابق ممیزی گذشته]، [اختصاص: اقدامات دیگر]].

نکته کاربردی:

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

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

^۱ Overwrite

^۲ External log server

۴-۲- پشتیبانی رمزنگاری (FCS)

در این بخش، الزامات رمزنگاری مربوط به سایر ویژگی‌های امنیتی محصول مورد ارزیابی تعریف می‌شوند. این الزامات شامل تولید کلید و تولید بیت تصادفی، روش‌های استقرار کلید^۱، نابودی کلید و انواع مختلف عملیات رمزنگاری برای رمزگذاری و رمزگشایی AES، تأیید امضا، تولید درهم‌ساز و تولید درهم‌ساز کلیدگذاری شده^۲ هستند. این الزامات کارکرد امنیتی، از پیاده‌سازی الزامات مبتنی بر انتخاب و پروتکل لیست شده در پیوست دو پشتیبانی می‌کنند.

شماره الزام	نام الزام
۷	مدیریت کلید رمزنگاری ۱
محصول مورد ارزیابی باید بر اساس الگوریتم‌های تولید کلید رمزنگاری مشخص شده، کلیدهای رمزنگاری نامتقارن را تولید کند: [انتخاب: • الگوهای RSA با استفاده از کلیدهای رمزنگاری با اندازه‌های ۲۰۴۸ بیت یا بزرگ‌تر که این الزامات را رعایت کنند: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.3؛ • الگوهای ECC با استفاده از «منحنی‌های NIST» [انتخاب: P-256, P-384, P-521] بر اساس این الزامات: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.4. • الگوهای FFC با استفاده از کلیدهای رمزنگاری با اندازه‌های ۲۰۴۸ بیت یا بزرگ‌تر که این الزامات را رعایت کنند: FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.1. رویه های FFC از Diffie-Hellman گروه ۱۴ استفاده می کند که موارد زیر را برآورده می کند: (RFC 3526، بخش ۳) نکته کاربردی: نویسنده هدف امنیتی، تمام الگوهای تولید کلید مورد استفاده برای استقرار کلید و احراز هویت دستگاه‌ها را انتخاب می‌کند. در صورتی که برای استقرار کلید از تولید کلید استفاده شود، الگوی در «مدیریت کلید رمزنگاری ۲» و پروتکل‌های رمزنگاری انتخاب شده باید مطابق با انتخاب باشند. در صورتی که برای احراز هویت دستگاه‌ها از تولید کلید استفاده شود، به غیر از ssh-rsa، ecdsa-sha2-nistp256، ecdsa-sha2-nistp384 و ecdsa-sha2-nistp521، انتظار می‌رود که کلید عمومی مرتبط با یک گواهی نامه X.509v3 باشد. اگر محصول مورد ارزیابی به عنوان یک دریافت کننده در الگوی استقرار کلید عمل کند و برای پشتیبانی از احراز هویت دوطرفه پیکربندی نشده باشد، نیازی نیست که هدف ارزیابی، تولید کلید را پیاده‌سازی نماید. در اهداف ارزیابی توزیع شده، اگر کامپوننت هدف ارزیابی به عنوان یک دریافت کننده در الگوی استقرار کلید عمل کند، نیازی نیست که هدف ارزیابی تولید کلید را پیاده‌سازی نماید.	
۸	مدیریت کلید رمزنگاری ۲
FCS_CKM.2.1	

^۱ Key establishment

^۲ Keyed hash generation

شماره الزام	نام الزام
محصول مورد ارزیابی باید استقرار کلید^۱ رمزنگاری را بر اساس یک روش خاص استقرار کلید رمزنگاری انجام دهد: [انتخاب: • الگوهای استقرار کلید RSA که این الزامات را رعایت کنند: شماره ویژه NIST 800-56B، مرور ۱ «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری فاکتورگیری عدد صحیح»^۲؛ • الگوهای استقرار کلید منحنی بیضوی^۳ که این الزامات را رعایت کنند: شماره ویژه NIST 800-56A، مرور ۲ «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته»^۴؛ • الگوهای استقرار کلید میدانی^۵ که این الزامات را رعایت کنند: شماره ویژه NIST 800-56A، مرور ۲ «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته». • الگوی استقرار کلید با استفاده از گروه ۱۴ Diffie-Hellman مطابق RFC 3526 بخش ۳. نکته کاربردی: این عنصر در واقع نسخه اصلاح شده الزام «مدیریت کلید رمزنگاری»^۶ در استاندارد ISO 15408 می‌باشد که به جای توزیع کلید، به استقرار کلید می‌پردازد. نویسنده هدف امنیتی، تمام الگوهای استقرار کلید مورد استفاده برای پروتکل‌های رمزنگاری منتخب را انتخاب می‌کند. برای گروه ۱۴ Diffie-Hellman، نویسنده هدف امنیتی باید به جای استفاده از انتخاب استقرار کلید میدانی محدود، از SFR به طور متناظر انتخاب کند. الگوهای استقرار کلید مبتنی بر RSA در بخش ۹ از نسخه ۱ NIST SP 800-56B تشریح شده‌اند؛ اما این بخش وابسته به پیاده‌سازی موارد مذکور در سایر بخش‌های نسخه ۱ SP 800-56B است. اگر محصول مورد ارزیابی در الگوی استقرار کلید RSA به عنوان گیرنده عمل کند، نیازی نخواهد بود که محصول، تولید کلید RSA را اجرا نماید. منحنی‌های بیضوی مورد استفاده در الگوهای استقرار کلید، با منحنی‌های مشخص شده در الزام شماره‌ی ۷ «مدیریت کلید رمزنگاری ۱» ارتباط دارند. پارامترهای دامنه مورد استفاده در الگوهای استقرار کلید میدانی، توسط تولید کلید مورد اشاره در «مدیریت کلید رمزنگاری ۱» مشخص شده‌اند.	
۹	نابودی کلید رمزنگاری ۴
FCS_CKM.4.1	
توابع امنیتی مورد ارزیابی باید کلیدهای رمزنگاری را بر اساس یک روش خاص برای نابودی کلیدهای رمزنگاری، از بین ببرد: [اختصاص:	

^۱ Key establishment

^۲ Integer factorization cryptography

^۳ Elliptic curve-based

^۴ Discrete logarithm cryptography

^۵ Finite field-based

^۶ FCS_CKM.2

شماره الزام	نام الزام
	- در مورد کلیدهای با متن ساده در ذخیره سازی فرار^۱، نابودی باید از طریق [انتخاب: یک باز نویسی ساده و مستقیم شامل [انتخاب: الگوی شبه تصادفی با استفاده از RBG محصول مورد ارزیابی، صفرها، یکها، مقدار جدیدی از کلید، [اختصاص: مقداری ایستا یا پویا که شامل هیچ CSP نباشد.]، از بین بردن ارجاع مستقیم به کلید پس از درخواست جمع آوری مقادیر باقی مانده] انجام شود - در مورد کلیدهای با متن ساده در ذخیره سازی غیر فرار، نابودی باید از طریق فراخوانی یک رابط ارائه شده توسط بخشی از توابع امنیتی هدف امنیتی که [انتخاب: - به طور منطقی محل ذخیره سازی کلید را تعیین کرده و [انتخاب: تنها، [اختصاص: تعداد انجام]-بار] باز نویسی شامل [انتخاب: یک الگوی شبه تصادفی با استفاده از RBG توابع امنیتی هدف ارزیابی، صفرها، یکها، مقدار جدیدی از کلید، [اختصاص: یک مقدار استاتیک یا پویا که شامل هیچ CSP نباشد]] انجام دهد. - آموزش بخشی از توابع امنیتی هدف ارزیابی برای تخریب انتزاعی که نشان دهنده کلید است. [باشد.
	نکته کاربردی: در بخش هایی از انتخاب ها که کلیدهای تخریب شده توسط "بخشی از TSF" شناسایی شده اند؛ TSS بخش مربوطه و رابط درگیر را تشخیص می دهد. رابطی که در این الزام مورد ارجاع قرار می گیرد، می تواند اشکال مختلفی برای اهداف ارزیابی داشته باشد، که بیشتر مانند رابط برنامه نویسی برنامه کاربردی برای هسته سیستم عامل است. ممکن است سطوح مختلفی از abstraction مشاهده شود. برای مثال، در یک پیاده سازی داده شده، برنامه ممکن است به جزئیات فایل سیستم دسترسی داشته باشد و ممکن است بتواند به به طور منطقی محل حافظه خاصی را آدرس دهی نماید. در پیاده سازی دیگری، برنامه ممکن است مدیریت ساده ای روی منبعی داشته باشد و فقط بتواند از بخش دیگری از توابع امنیتی هدف ارزیابی مانند مترجم^۲ یا سیستم عامل درخواست حذف منبع کند. در صورتی که برای کلیدهای مختلف و/یا وضعیت های تخریب مختلف، از روش های مختلف تخریب کلید استفاده شود، وضعیت های متفاوت و کلیدها/روش های اعمال آنها در TSS شرح داده می شود. (و ممکن است سند هدف امنیتی برای کمک به وضوح بیشتر از تکرارهای مجزایی از SFR ها استفاده کند. TSS تمامی کلیدهای مرتبط مورد استفاده در پیاده سازی SFR ها، از جمله مواردی که کلیدها در فرم غیر متنی ذخیره می شوند را شرح می دهد. در مورد ذخیره سازی غیر متنی، روش رمزنگاری و کلید مرتبط-کلید رمزنگاری در TSS شناسایی می شوند. برخی انتخاب ها اجازه اختصاص "مقداری که شامل هیچ CSP نیست" می دهند. به این معنی است که، هدف ارزیابی از برخی داده های مشخصی استفاده می کند که توسط RBG برای برآورده کردن نیازمندی های FCS_RBG_EXT در نظر گرفته نشده است، و هیچ کدام از مقادیر خاص ذکر شده در گزینه های دیگر انتخاب نیست. عبارت "شامل هیچ CSP" برای اطمینان از انتخاب

^۱ Volatile memory

^۲ interpreter

شماره الزام	نام الزام	
		با دقت داده‌ها است و از منبعی عمومی که ممکن است شامل داده‌های حاضر یا قبلی که خود نیازمند حفظ محرمانگی هستند، گرفته نشده است. برای اجتناب از تردید: "کلیدهای رمزنگاری" در این SFR شامل کلیدهای نشست است. تخریب کلید بر روی مولفه‌های عمومی جفت کلید نامتقارن اعمال نمی‌شود.
۱۰	عملیات رمزنگاری ۱(۱)	FCS_COP.1.1/DataEncryption
		توابع امنیتی مورد ارزیابی باید رمزگذاری و رمزگشایی را بر اساس الگوریتم‌های رمزنگاری خاص AES که در حالت [انتخاب: GCM, CTR, CBC] استفاده می‌شوند و در اندازه‌های کلید رمزنگاری [اختصاص: ۱۲۸ بیتی، ۱۹۲ بیتی، ۲۵۶ بیتی] و با توجه به استاندارد AES که در ISO 18033-3 تعریف شده است، [انتخاب: CBC همانطور که در ISO 10116 مشخص شده است، CTR مشخص شده در ISO 10116، GCM همانطور که در ISO 19772 مشخص شده است]. انجام دهد. نکته کاربردی: در مورد نخستین انتخاب عملیات رمزنگاری ۱(۱)/رمزنگاری داده، نویسنده هدف امنیتی باید حالت یا حالت‌های کارکردی AES را انتخاب کند. در مورد دومین انتخاب، نویسنده هدف امنیتی باید اندازه کلیدهای پشتیبانی شده توسط این کارکرد را انتخاب کند. حالت‌ها و اندازه کلیدهای انتخاب‌شده در این مرحله، متناظر با انتخاب مجموعه رمز ^۱ در الزامات کانال امن هستند.
۱۱	عملیات رمزنگاری ۲(۲)	FCS_COP.1.1/SigGen
		توابع امنیتی مورد ارزیابی باید خدمات امضای رمزنگاری (تولید و تأیید) را بر اساس الگوریتم‌های رمزنگاری خاص ارائه کند: [انتخاب: - الگوریتم امضای دیجیتال RSA و اندازه کلیدهای رمزنگاری (ماژول‌ها) [اختصاص: ۲۰۴۸ بیتی یا بزرگ‌تر] - الگوریتم امضای دیجیتال منحنی بیضوی و اندازه کلیدهای رمزنگاری [اختصاص: ۲۵۶ بیتی یا بزرگ‌تر]] با رعایت موارد زیر: [انتخاب: - در مورد الگوهای RSA: FIPS PUB 186-4: RSA، «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: ECDSA، «استاندارد امضای دیجیتال (DSS)»، بخش ۶ و پیوست D، با اجرای منحنی‌های NIST [انتخاب: P-384، P-256، P-521، هیچ منحنی دیگر]؛ ISO/IEC 14888-3، بخش ۶،۴]

^۱ Cipher suite

شماره الزام	نام الزام	
	نکته کاربردی: نویسنده هدف امنیتی باید الگوریتم پیاده سازی شده برای اجرای امضای دیجیتال را انتخاب کند. نویسنده هدف امنیتی باید اختصاص‌های مناسبی به منظور مشخص نمودن پارامترهایی که برای الگوریتم پیاده‌سازی می‌شوند، ایجاد کند. نویسنده هدف امنیتی باید اطمینان حاصل نماید که اختصاص‌ها و انتخاب‌های این SFR شامل تمامی مقادیر پارامترهای ضروری برای مجموعه رمزهای منتخب در سند هدف امنیتی برای پروتکل SFRها می‌باشد. (پیوست B.2.1 را ببینید) نویسنده سند هدف امنیتی انطباق انتخاب‌ها با سایر الزامات SFR، مخصوصاً زمانی که از منحنی‌های بیضوی پشتیبانی می‌شود بررسی می‌کند.	
۱۲	عملیات رمزنگاری ۱ (۳)	FCS_COP.1.1/Hash
	توابع امنیتی مورد ارزیابی باید خدمات درهم‌سازی رمزنگاری را بر اساس یک الگوریتم رمزنگاری مشخص [انتخاب: SHA-1, SHA-256, SHA-384, SHA-512] و اندازه پیام هشدار [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیت با رعایت استاندارد ISO/IEC 10118-3:2004. ارائه نماید نکته کاربردی: به تولیدکنندگان اکیداً توصیه می‌شود که از پروتکل‌های به‌روزرسانی شده‌ای که از خانواده SHA-2 پشتیبانی می‌نمایند، پیاده‌سازی کنند. تا زمانی که پروتکل‌های به‌روز شده پشتیبانی شوند، این پروفایل حفاظتی اجازه پشتیبانی از پیاده‌سازی‌های SHA-1 را بر اساس SP 800-131A فراهم می‌کند. در نسخه بعدی این پروفایل حفاظتی، SHA-256 حداقل نیازمندی برای تمامی اهداف امنیتی خواهد بود. انتخاب درهم‌ساز باید بر اساس قدرت کلی الگوریتم مورد استفاده برای الزام شماره ۱۰ «عملیات رمزنگاری ۱ (۱)» و الزام شماره ۱۱ «عملیات رمزنگاری ۱ (۲)» انجام شود (مثلاً SHA 256 برای کلیدهای ۱۲۸ بیتی).	
۱۳	عملیات رمزنگاری ۱ (۴)	FCS_COP.1.1/KeyedHash



شماره الزام	نام الزام
محصول مورد ارزیابی باید احراز هویت پیام مبتنی بر کلید درهم‌سازی شده^۱ را بر اساس الگوریتم رمزنگاری خاص [انتخاب: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] و اندازه کلید رمزنگاری [اختصاص: اندازه کلید مورد استفاده در HMAC (بر حسب بیت)] و اندازه خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیت و با توجه به موارد مطرح شده در [اختصاص: بخش هفتم ISO/IEC 9797-2:2011 با نام «الگوریتم ۲ MAC»] انجام دهد. نکته کاربردی ۱۵: اندازه کلید k در عبارت «اختصاص» بین L1 و L2 خواهد بود (که در ISO/IEC 10118 مربوط به توابع درهم‌ساز تعریف شده است). به عنوان مثال، در مورد SHA-256 داریم: L1=512, L2=256 که $L2 \leq k \leq L1$.	
۱۴	تولید بیت تصادفی ۱
محصول مورد ارزیابی باید تمامی خدمات تولید بیت تصادفی قطعی را بر اساس ISO/IEC 18031:2011 و با استفاده از [انتخاب: Hash_DRBG (هر)، HMAC_DRBG (هر)، CTR_DRBG (AES)] ارائه دهد.	
۱۵	تولید بیت تصادفی ۲
FCS_RBG_EXT.1.1	
FCS_RBG_EXT.1.2	

^۱ Keyed-hash message authentication

شماره الزام	نام الزام
	RBG قطعی باید دست کم توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی را از [انتخاب: اختصاص: تعداد منابع مبتنی بر نرم افزار] منبع نويز مبتنی بر نرم افزار، [اختصاص: تعداد منابع مبتنی بر سخت افزار] منبع نويز مبتنی بر سخت افزار] گردآوری کند. این آنتروپی باید دست کم [انتخاب: ۱۲۸ بیت، ۱۹۲ بیت، ۲۵۶ بیت] و حداقل معادل بالاترین قدرت امنیتی کلیدها و درهم سازهای تولید شده مورد اشاره در ISO/IEC 18031:2011 از کلیدها و CSP هایی که تولید خواهد کرد، باشد. نکته کاربردی ۱۶: در مورد نخستین عبارت انتخاب در «تولید بیت تصادفی ۲»، هدف امنیتی باید حداقل به یکی از انواع منابع نويز اشاره کند. اگر محصول مورد ارزیابی شامل چندین منابع نويز از یک نوع باشد، نویسنده هدف امنیتی عبارت اختصاص را با تعداد مناسبی برای هر یک از انواع منابع پر می کند (مثلاً دو منبع نويز مبتنی بر نرم افزار و یک منبع نويز مبتنی بر سخت افزار). مستندات و آزمون های مورد اشاره در فعالیت های ارزیابی برای این عنصر، باید تکرار شود تا تمام منابع مورد اشاره در هدف امنیتی را پوشش می دهند. سند ISO/IEC 18031:2011 شامل سه روش مختلف تولید اعداد تصادفی است که هر یک از آن ها، به نوبه خود، به عناصر اولیه رمزنگاری اساسی (توابع درهم ساز و رمزها) بستگی دارد. نویسنده هدف امنیتی، تابع مورد استفاده را انتخاب خواهد کرد و شامل عناصر اولیه رمزنگاری اساسی خاص مورد استفاده در الزام است با اینکه هریک از توابع درهم ساز تعیین شده (SHA-1, , SHA-256, SHA-384, SHA-512) را می توان در Hash_DRBG یا HMAC_DRBG مورد استفاده قرار داد، تنها اجازه پیاده سازی های مبتنی بر AES در CTR_DRBG وجود دارد. اگر اندازه کلید برای پیاده سازی AES متفاوت از اندازه کلید مورد استفاده برای رمزگذاری داده های کاربری باشد، ممکن است نیاز به تنظیم یا تکرار «عملیات رمزنگاری» باشد تا اندازه کلید مختلف در آن لحاظ گردد. برای انتخاب در «تولید بیت تصادفی ۲»، نویسنده هدف امنیتی حداقل تعداد بیت های آنتروپی تزریق شده به RBG را تعیین می کند. که باید برابر با، یا بیشتر از قدرت امنیتی هر کلید تولید شده توسط هدف ارزیابی باشد.

۴-۳- کلاس شناسایی و احراز هویت

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

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

مورد نیاز است را ارائه می‌دهد، حتی اگر مدیر راه دور در نتیجه FIA_AFL.1 به دلیل مسدود شدن حساب‌ها، به طور دائمی یا موقت در دسترس نباشد.		
FIA_PMG_EXT.1.1	مدیریت رمز عبور ۱	۱۸
توابع امنیتی مورد ارزیابی باید قابلیت‌های مدیریت کلمه عبور زیر را برای کلمه عبور سرپرست محصول فراهم آورد: الف) کلمه عبور را باید بتوان با هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای ویژه مطرح شده در این بخش ساخت: [انتخاب: ("(", ")", "*", "&", "%", "\$", "#", "@", "!",", اختصاص: سایر کاراکترها]]؛ ب) حداقل طول کلمه عبور باید بین [اختصاص: حداقل تعداد کاراکترهای پشتیبانی شده توسط هدف ارزیابی] و [اختصاص: تعداد کاراکترهای بزرگتر یا مساوی ۱۵] قابل پیکربندی باشد. نکته کاربردی: نویسنده هدف امنیتی کاراکترهای ویژه که توسط هدف ارزیابی پشتیبانی می‌شوند را تعیین می‌کند. وی می‌تواند با استفاده از عبارت اختصاص، کاراکترهای ویژه دیگری را به لیست اختیاری بیفزاید. منظور از «کلمه‌های عبور سرپرستی»، کلمه‌های عبوری هستند که توسط مدیران سیستم در کنسول محلی مورد استفاده قرار می‌گیرند. این کلمه‌های عبور روی پروتکل‌هایی استفاده می‌شوند که از آن‌ها پشتیبانی کنند. به عنوان مثال، می‌توان از SSH و HTTPS نام برد. این کلمه‌های عبور گاهی نیز برای ارائه آن دسته از داده‌های پیکربندی مورد استفاده قرار می‌گیرند که از دیگر الزامات کارکرد امنیتی در هدف امنیتی پشتیبانی می‌کنند. اختصاص دوم باید با حداقل طول بزرگترین کلمه عبور توسط مدیر امنیتی پیکربندی شود.		
FIA_UIA_EXT.1.1	شناسایی و احراز هویت کاربر ۱	۱۹
توابع امنیتی مورد ارزیابی پیش از آن که از دیگر موجودیت‌های خارج از محصول بخواهد که فرایند تعیین و احراز هویت را انجام دهد، باید اجازه انجام فعالیت‌های زیر را بدهد: • نمایش بنر هشدار مطابق با FTA_TAB.1 • [انتخاب: هیچ اقدامات دیگری، تولید خودکار کلیدهای رمزنگاری [اختصاص: لیست خدمات، اقدامات انجام‌شده توسط محصول مورد ارزیابی در پاسخ به درخواست‌های غیر از هدف ارزیابی]]		
FIA_UIA_EXT.1.2	شناسایی و احراز هویت کاربر ۲	۲۰
پیش از آن که توابع امنیتی مورد ارزیابی امکان انجام هر اقدامات میانی دیگری از طرف کاربر مدیریتی سیستم را فراهم آورد، باید مدیر سیستم را با موفقیت شناسایی و احراز هویت نماید. نکته کاربردی: این الزام برای کاربران خدماتی که به طور مستقیم توسط محصول مورد ارزیابی در دسترس قرار می‌گیرند (چه مدیران سیستم و چه موجودیت‌های IT خارجی) اعمال می‌شود و در مورد خدماتی که از طریق ارتباطات محصول مورد ارزیابی در دسترس قرار می‌گیرند، اعمال نمی‌شود. از آنجا که موجودیت‌های خارجی پیش از تعیین و احراز هویت تنها باید به چند خدمت محدود (و یا هیچ خدمتی) دسترسی داشته باشند، این خدمات باید در عبارت اختصاص ذکر شوند. در غیر این صورت، باید «هیچ اقدام دیگر» را انتخاب کرد.		

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

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

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

FIA_UAU_EXT.2.1	سازوکار احراز هویت بر اساس رمز عبور ۲	۲۱
-----------------	---------------------------------------	----

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

نکته کاربردی:

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

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

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

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

نکته کاربردی:

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

^۱ Obscured feedback

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

۴-۴- کلاس مدیریت امنیت

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

شماره الزام	نام الزام	
۲۳	مدیریت کارکرد در محصول ۱ (۱)/ به روزرسانی دستی	FMT_MOF.1.1/ManualUpdate
توابع امنیتی مورد ارزیابی باید توانایی فعال کردن توابع به‌منظور به‌روزرسانی دستی را به سرپرست امنیتی محدود نماید. نکته کاربردی: این الزام امکان آغاز به‌روزرسانی دستی را به سرپرستان امنیتی محدود می‌کند.		
۲۴	مدیریت داده‌های محصول ۱	FMT_MTD.1.1/CoreData
توابع امنیتی مورد ارزیابی باید امکان «مدیریت» داده‌های محصول را به سرپرست‌های امنیتی محدود کند. نکته کاربردی: منظور از «مدیریت» می‌تواند هر یک از این اقدامات و موارد دیگری از این دست باشد: تولید، آغاز، بازدید، تغییر پیش فرض، تغییر، حذف، پاک کردن و اضافه نمودن. الزام کارکرد امنیتی حاضر همچنین شامل بازگرداندن کلمه عبور کاربری به حالت پیش فرض توسط سرپرست امنیتی است. در اینجا شناسه "CoreData" برای تفکیک الزام FMT_MTD.1 از الزام اختیاری FMT_MTD.1 تعریف شده در پیوست A.4.2.1 (FMT_MTD.1/CryptoKeys) می‌باشد.		
۲۵	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
توابع امنیتی مورد ارزیابی باید قابلیت انجام کارکردهای مدیریتی زیر را داشته باشد: [اختصاص: • توانایی مدیریت محصول به‌صورت محلی و از راه دور • توانایی پیکربندی بئر دسترسی • توانایی پیکربندی زمان غیرفعال بودن نشست پیش از قفل کردن یا خاتمه دادن آن • توانایی به‌روزرسانی محصول مورد ارزیابی و تأیید به‌روزرسانی‌ها با استفاده از قابلیت [انتخاب: امضای دیجیتال، مقایسه درهم‌سازی] پیش از نصب شدن این به‌روزرسانی‌ها		

شماره الزام	نام الزام
•	توانایی پیکربندی پارامترهای احراز هویت ناموفق برای FIA_AFL.1
•	انتخاب:
•	توانایی شروع و متوقف کردن سرویس ها .
○	توانایی پیکربندی رفتار ممیزی
○	توانایی تغییر رفتار انتقال داده ممیزی به یک موجودیت فناوری اطلاعات خارجی، بررسی داده های ممیزی، عملکرد ممیزی وقتی که فضای ذخیره سازی محلی پر است.
○	توانایی پیکربندی لیست خدمات ارائه شده در دسترس توسط محصول مورد ارزیابی پیش از شناسایی و احراز هویت یک موجودیت، چنان که در «شناسایی و احراز هویت کاربر ^۱ » تشریح شده است.
○	توانایی مدیریت کلیدهای رمزنگاری
○	توانایی پیکربندی کارکرد رمزنگاری
○	توانایی پیکربندی آستانه ^۲ برای تجدید کلید SSH
○	توانایی پیکربندی مدت زمان برای SA در IPsec
○	توانایی پیکربندی اثر متقابل بین اجزای هدف ارزیابی
○	توانایی فعال یا غیرفعال کردن بررسی خودکار برای به روزرسانی ها یا به روزرسانی های خودکار
○	توانایی فعالسازی مجدد حساب کاربری مدیر
○	توانایی تنظیم زمانی که برای مهرهای زمانی استفاده می شود.
○	توانایی پیکربندی NTP
○	توانایی پیکربندی مرجع شناسایی همتا
○	توانایی مدیریت انبار اطمینان هدف ارزیابی و تعیین گواهی های X509.v3 به عنوان لنگر اطمینان
○	توانایی وارد کردن گواهی X509.v3 به انبار اطمینان هدف ارزیابی
○	هیچ قابلیت دیگری]
[	
نکته کاربردی:	
محصول مورد ارزیابی باید کارکردهای لازم برای مدیریت سیستم به صورت محلی و مدیریت از راه دور را فراهم آورد.	
به طور کلی، این پرو فایل حفاظتی، تابع مدیریت امنیتی خاصی که از طریق رابط مدیر محلی یا رابط مدیر از راه دور یا هر دو قابل دسترسی باشد را الزام نمی کند. TSS باید با جزئیات مشخص کند که کدام توابع مدیریت امنیتی از طریق کدام رابطها قابل دسترسی هستند. هدف ارزیابی باید قابلیت پیکربندی بئر دسترسی را برای FTA_TAB.1 و قابلیت پیکربندی زمان غیرفعال بودن نشست را برای FTA_SSL_EXT.1 و FTA_SSL.3 ارائه دهد. آیت "توانایی بروزرسانی هدف ارزیابی و تایید بروزرسانی هایی که از قابلیت	

^۱ FIA_UIA_EXT.1

^۲ Threshold

شماره الزام	نام الزام
	امضای دیجیتالی استفاده می کنند قبل از نصب این بروزرسانی ها " شامل توابع مدیریتی مربوطه از FMT_MOF.1/ManualUpdate ، FMT_MOF.1/AutoUpdate (اگر در ST باشد) و FIA_X509_EXT.2.2 و FPT_TUD_EXT.1.2 و FPT_TUD_EXT.2.2 (اگر در ST باشند و اگر شامل اقدام قابل پیکربندی توسط مدیر باشند) می باشند به طور مشابه، انتخاب "توانایی پیکربندی رفتار ممیزی" شامل توابع امنیتی مربوطه از FMT_MOF.1/Services و FMT_MOF.1/Functions (برای تمام این SFRهایی که در سند ST هستند) می باشند. اگر هدف ارزیابی توانایی غیرفعال کردن حساب کاربری مدیر از راه دور را از طریق FIA_AFL.1 ارائه کند، نویسنده سند هدف امنیتی باید گزینه "توانایی فعالسازی مجدد حساب مدیر" را برای مجوز فعالسازی مجدد حساب توسط مدیر محلی، انتخاب کند. اگر هدف ارزیابی برای مدیر توانایی پیکربندی رفتار ممیزی، قبل از شناسایی یا احراز هویت ارائه کند، یا اگر هر کدام از عملکردهای رمزنگاری در هدف ارزیابی قابل پیکربندی باشد، یا اگر ST هدف ارزیابی توزیع شده ای را شرح دهد، نویسنده هدف امنیتی باید انتخاب مناسبی انجام دهد یا در انتخاب دوم، گزینه در غیر این صورت "هیچ قابلیت دیگری" را انتخاب کند. (انتخاب دوم ممکن است متناوبا در ST خالی بماند) اگر هدف ارزیابی از پیکربندی آستانه برای مکانیسم های مورد استفاده برای FCS_SSHC_EXT.1.8 یا FCS_SSHS_EXT.1.8 (لازم است برای این تنظیمات FMT_MOF.1/Functions در ST باشد). پشتیبانی می کند، گزینه "توانایی پیکربندی آستانه برای تجدید کلید SSH" باید در سند هدف امنیتی انتخاب شده باشد. اگر هدف ارزیابی محدودیتی برای مقادیر قابل قبول آستانه قرار داده است، باید در TSS بیان شود. اگر هدف ارزیابی از ارتباط امن از طریق IPsec پشتیبانی کند و الزامات FCS_IPSEC_EXT.1 در سند هدف امنیتی باشد، باید در سند هدف امنیتی گزینه "توانایی تنظیم طول عمر IPsec SAs" انتخاب شود. تنظیمات طول عمر برای IPsec SAs لازم است از طریق انتخاب در FCS_IPSEC_EXT.1.7 باشد. (لازم است برای این تنظیمات FMT_MOF.1/Functions در ST باشد). اگر هدف ارزیابی به مدیر اجازه تنظیم زمان دستگاهی که در مهرهای زمانی استفاده می شود داده باشد، گزینه "توانایی تنظیم زمانی که برای مهرهای زمانی استفاده می شود" باید در ST انتخاب شود. اگر هدف ارزیابی اجازه تنظیمات دستی زمان را نداده و فقط متکی به هماهنگی با منابع خارجی زمان مانند سرورهای NTP می باشد، این گزینه نباید انتخاب شود. اگر هدف ارزیابی از ارتباطات امن از طریق پروتکل IPsec پشتیبانی می کند و الزامات FCS_IPSEC_EXT.1 در ST باشد، گزینه "توانایی پیکربندی مرجع شناسایی همتا" باید در ST انتخاب شود. ممکن است پیکربندی مرجع شناسایی برای اهداف امنیتی که فقط از آدرس IP و انواع شناسه FQDN پشتیبانی می کنند، همانند پیکربندی نام های همتا برای اهداف ارتباط باشد. برای اهداف ارزیابی توزیع شده، تعامل بین مولفه های هدف امنیتی قابل تنظیم خواهد بود (FCO_CPC_EXT.1 را ببینید). بنابراین، نویسنده هدف امنیتی گزینه "توانایی پیکربندی اثر متقابل بین اجزای هدف ارزیابی" را برای اهداف ارزیابی توزیع شده انتخاب می کند. یک مثال ساده، "تغییر پروتکل ارتباطی مطابق FPT_ITT.1" است. مثال دیگر، "تغییر مدیریت مولفه هدف ارزیابی از مدیریت مستقیم از راه دور، به مدیریت از راه دور از طریق یک مولفه دیگری از هدف ارزیابی"، می باشد. یک مورد استفاده پیچیده تر، "اگر تحقق یک SFR از طریق دو مولفه یا بیشتر از هدف ارزیابی بدست آید و مسئولیت ها بین دو مولفه یا بیشتر قابل تغییر باشد"، است.

شماره الزام	نام الزام	
		برای اهداف ارزیابی که کانال registration را پیاده سازی کرده اند (همانطور که در FCO_CPC_EXT.1.2 شرح داده شده است)، نویسندگان هدف امنیتی از گزینه "توانایی پیکربندی کارکرد رمزنگاری" در این SFR استفاده می کنند، و به طور متناظر در TSS برای تشریح پیکربندی هر منظر رمزنگاری کانال registration که برای بهبود امنیتی کانال، توسط محیط عملیاتی قابل تغییر است نگاشت می شود. (cf. توصیف محتوای رویه های آمادگی در [SD, 3.6.1.2])
۲۶	نقش های امنیتی ۳	FMT_SMR.2.1
		توابع امنیتی هدف ارزیابی باید نقش های زیر را نگهداری کند. سرپرست امنیتی
۲۷	نقش های امنیتی ۴	FMT_SMR.2.2
		توابع امنیتی مورد ارزیابی باید بتواند بین کاربران و نقش ها ارتباط برقرار نماید.
۲۸	نقش های امنیتی ۵	FMT_SMR.2.3
		توابع امنیتی مورد ارزیابی باید از برقرار بودن شرایط زیر اطمینان حاصل کند: - نقش سرپرست امنیتی باید بتواند محصول مورد ارزیابی را به صورت محلی مدیریت کند. - نقش سرپرست امنیتی باید بتواند محصول مورد ارزیابی را از راه دور مدیریت کند. نکته کاربردی: بر اساس این الزام سرپرست امنیتی باید بتواند محصول مورد ارزیابی را از طریق یک کنسول محلی و یک مکانیسم راه دور مدیریت کند. نویسندگان هدف امنیتی باید برای نشان دادن نحوه دستیابی به ارتباط امن FTP_ITC.1، FPT_ITT.1 و/یا FTP_TRP.1/Admin را انتخاب کند. در این SFR، پیاده سازی مدیریت کاربر خود، برای تمامی مولفه های هدف ارزیابی، در اهداف ارزیابی توزیع شده، الزامی نیست. حداقل یک مولفه باید از احراز هویت و شناسایی مدیران امنیتی مطابق با FIA_UA_EXT.1 و FIA_UAU_EXT.2 پشتیبانی کند. احراز هویت سایر مولفه های هدف ارزیابی به عنوان مدیر امنیتی، می تواند از طریق کانال امن (یا مطابق با FTP_ITC.1 یا FPT_ITT.1) با استفاده از مولفه ای که احراز هویت مدیران را مطابق با FIA_UA_EXT.1 و FIA_UAU_EXT.2 پشتیبانی می کند محقق شود. شناسایی کاربران مطابق با FIA_UA_EXT.1.2 و وابستگی کاربران با قوانین مطابق FMT_SMR.2.2، از طریق مولفه هایی که احراز هویت مدیران امنیتی را مطابق با FIA_UA_EXT.1 و FIA_UAU_EXT.2 پشتیبانی می کنند انجام می شود. پشتیبانی از مدیریت^۱ محلی مولفه های تعریف شده در FMT_SMR.2.3، توسط مولفه های هدف ارزیابی که مدیران امنیتی را از طریق استفاده از کانال امن احراز هویت می کنند الزامی نیست.

^۱ administration

۴-۵- کلاس حفاظت از محصول مورد ارزیابی

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

شماره الزام	نام الزام
۲۹	محافظت از داده‌های محصول (برای خواندن تمامی کلیدهای از پیش به اشتراک گذاشته شده، متقارن و خصوصی) ۱
توابع امنیتی مورد ارزیابی باید از خواندن تمام کلیدهایی که از پیش به اشتراک گذاشته شده‌اند، کلیدهای متقارن و کلیدهای خصوصی جلوگیری به عمل آورد. نکته کاربردی: هدف از الزام حاضر این است که دستگاه بتواند مانع از افشای غیر مجاز به کلیدها، اطلاعات کلیدها و اعتبارنامه احراز هویت شود. این داده‌ها باید تنها برای هدف کارکردهای امنیتی مربوطه، قابل دسترسی باشند و نیازی به دسترسی و نمایش آن‌ها در هر زمان دیگر نخواهد بود. این الزام مانع از مشخص شدن وجود این اطلاعات، در حال استفاده بودن آن‌ها، یا معتبر بودن آن‌ها نیست. با این حال، الزام حاضر امکان خواندن این اطلاعات را کاملاً محدود می‌کند.	
۳۰	حفاظت از کلمه عبور سرپرست محصول ۱
توابع امنیتی مورد ارزیابی نباید کلمه‌های عبور را به شکل متن ساده ذخیره کند.	
۳۱	حفاظت از کلمه عبور سرپرست محصول ۲
FPT_SKP_EXT.1.1	
FPT_APW_EXT.1.1	
FPT_APW_EXT.1.2	

توابع امنیتی مورد ارزیابی باید از خوانده شدن کلمه‌های عبوری که به صورت متن ساده^۱ هستند، جلوگیری کند.

نکته کاربردی:

هدف از الزام حاضر این است که داده‌های خام مربوط به احراز هویت از طریق گذرواژه، به شکل واضح ذخیره نشوند و هیچ کاربر و سرپرست محصول نتواند کلمه عبور متن ساده را از طریق واسط «عادی» بخواند. البته سرپرست محصولی که تمام دسترسی‌ها را داشته باشد می‌تواند بطور مستقیم حافظه را به منظور ضبط کلمه عبور بخواند؛ اما به وی اعتماد می‌شود و فرض می‌گردد که وی این کار را نخواهد کرد. باید کلمه‌های عبور در هنگام ورود به کنسول محلی، مطابق با FIA_UAU.7 مبهم باشند.

FPT_TST_EXT.1.1	خودآزمایی محصول ۱	۳۲
-----------------	-------------------	----

توابع امنیتی مورد ارزیابی باید مجموعه‌ای از این خودآزمایی‌ها را [انتخاب: در مرحله راه‌اندازی اولیه (روشن شدن دستگاه)، به طور دوره‌ای در حین کارکرد عادی، در صورت درخواست کاربر مجاز، در شرایط [اختصاص: شرایطی که باید در آن‌ها خودآزمایی‌ها را انجام داد]] برای نشان دادن کارکرد صحیح توابع امنیتی مورد ارزیابی انجام دهد: [اختصاص: لیست خودآزمایی‌هایی که باید توسط محصول مورد ارزیابی انجام شوند].

تذکر: در صورتی که برای خودآزمایی‌ها از مکانیسم امضای دیجیتال استفاده شود نیاز است الزام FPT_TST_EXT.2 از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه گردد.

نکته کاربردی:

انتظار می‌رود که خودآزمایی‌ها در مرحله راه‌اندازی اولیه (روشن شدن دستگاه) انجام شوند. سایر گزینه‌ها در صورتی در نظر گرفته می‌شوند که توسعه دهنده دستگاه توجیه کند که چرا خودآزمایی در مرحله راه‌اندازی اولیه (روشن شدن دستگاه) انجام نمی‌شود. انتظار می‌رود که دست کم خودآزمایی‌های لازم برای حصول اطمینان از صحت و یکپارچگی نرم‌افزار و میان‌افزار و کارکرد صحیح توابع رمزنگاری به منظور برآورده کردن الزامات کارکرد امنیتی انجام شوند. اگر تمام خودآزمایی‌ها در مرحله راه‌اندازی اولیه (روشن شدن دستگاه) انجام نشوند، الزام کارکرد امنیتی حاضر چند بار و هر بار با انتخاب‌های مناسب اجرا می‌شود. در نسخه‌های آینده از این CPP مجموعه‌ای از خودآزمایی مورد نیاز خواهد بود که شامل حداقل مکانیسم‌ها برای اندازه‌گیری boot است از جمله خودآزمایی مولفه‌ها که اندازه‌گیری را انجام می‌دهند.

ممکن است اهداف ارزیابی توزیع نشده از چندین مولفه که به اجرای SFRها کمک می‌کنند تشکیل شده باشد. خودآزمایی باید تمامی نرم‌افزارهایی که به اجرای SFRها در تمامی مولفه‌ها کمک می‌کنند را پوشش دهد. برای تمامی اهداف ارزیابی توزیع نشده، تمامی مولفه‌ها باید خودآزمایی را اجرا کنند. الزاما به این معنی نیست که هر مولفه هدف ارزیابی باید خودآزمایی‌های یکسانی انجام دهد: ST کاربرد انتخاب (برای مثال زمانی که خودآزمایی اجرا می‌شود) و اختصاص نهایی (برای مثال کدام خودآزمایی‌ها باید اجرا شوند) هر مولفه هدف ارزیابی را شرح می‌دهد.

^۱ Plaintext

نکته کاربردی:

اگر در خودآزمایی‌ها از گواهی‌نامه‌ها استفاده شود (مثلاً برای تأیید امضا جهت تأیید صحت و یکپارچگی)، گواهی‌نامه‌ها باید از « FIA_X509_EXT.1/Rev » انتخاب شوند و بر اساس الزام FIA_X509_EXT.1 و الزام FIA_X509_EXT.2.1 تأیید گردند. علاوه بر این، الزام FPT_TST_EXT.2 باید در سند هدف امنیتی در نظر گرفته شوند.

FPT_TUD_EXT.1.1

به روز رسانی امن ۱

۳۳

توابع امنیتی مورد ارزیابی باید این امکان را به سرپرستان امنیتی بدهد که هم به نسخه فعلی در حال اجرا نرم‌افزار/میان‌افزار هدف ارزیابی و [انتخاب: هم به جدیدترین نسخه نصب‌شده نرم‌افزار/میان‌افزار هدف ارزیابی، به هیچ نسخه نرم‌افزار/میان‌افزار دیگر] دسترسی داشته باشد.

نکته کاربردی:

اگر بتوان بروزرسانی امن را بر روی هدف ارزیابی نصب کرده و با تاخیر فعال شود، هر دو ورژن نسخه در حال اجرا و نسخه غیرفعال نصب شده باید ارائه شود. در این مورد، گزینه "نسخه اخیراً نصب شده نرم‌افزار/میان‌افزار هدف ارزیابی" لازم است از گزینه‌های FPT_TUD_EXT.1.1 انتخاب شود و لازم است TSS نحوه و زمان فعال شدن نسخه غیرفعال را شرح دهد. اگر تمامی بروزرسانی‌های امن به عنوان بخشی از فرآیند نصب فعال شوند، فقط نسخه در حال اجرا لازم به ارائه است. در این مورد، گزینه "هیچ نسخه نرم‌افزار/میان‌افزار دیگری" باید از گزینه‌های FPT_TUD_EXT.1.1 انتخاب شود. برای اهداف ارزیابی توزیع شده، روش تعیین نسخه‌های نصب شده بر روی هر مولفه از هدف ارزیابی باید در راهنمای عملکردی شرح داده شود.

FPT_TUD_EXT.1.2

به روز رسانی امن ۲

۳۴

توابع امنیتی مورد ارزیابی باید این امکان را برای سرپرستان امنیتی فراهم کنند که به‌روزرسانی نرم‌افزار/میان‌افزار محصول مورد ارزیابی را به صورت دستی انجام دهد و [انتخاب: از بررسی 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 مورد ارزیابی ۱ (۲)» به‌روزرسانی امن» از پیوست دو را تکمیل کرده و به سند هدف امنیتی اضافه نماید.

نکته کاربردی:

عبارت «انتخاب» در این الزام، بین پشتیبانی از «بررسی خودکار به‌روزرسانی‌ها» و «به‌روزرسانی خودکار» تمایز قائل می‌شود. بررسی خودکار به‌روزرسانی‌ها به یک محصول مورد ارزیابی اشاره دارد که بررسی می‌کند تا بیند به‌روزرسانی جدیدی وجود دارد یا خیر و این امر را به سرپرست محصول اطلاع می‌دهد (مثلاً از طریق یک پیام در طول نشست سرپرست یا فایل‌های log)، اما نصب

به روزرسانی نیازمند انجام اقداماتی توسط سرپرست محصول خواهد بود، اما به روزرسانی خودکار به یک محصول مورد ارزیابی اشاره دارد که به روزرسانی‌ها را بررسی می‌کند و در صورت وجود آن‌ها را نصب می‌نماید.

TSS اقداماتی که در پشتیبانی هدف ارزیابی هنگام استفاده از گزینه‌های "پشتیبانی از بررسی خودکار به روزرسانی‌ها" یا "پشتیبانی از به روزرسانی‌های خودکار" درگیر می‌شوند را شرح می‌دهد.

زمانی که مقادیر درهم‌سازی منتشر شده (FPT_TUD_EXT.1.3 را ببینید) برای محافظت از مکانیسم به روزرسانی امن استفاده می‌شوند، هدف ارزیابی نباید به طور خودکار فایل‌های به روزرسانی را با مقادیر درهم‌سازی (یا ادغام شده در فایل‌های به روزرسانی یا به طور جداگانه) دانلود کند و نباید به روزرسانی را به طور خودکار و بدون هیچ احراز هویت فعالی از مدیر امنیتی نصب نماید؛ حتی در زمانی که مقدار درهم‌سازی محاسبه شده با مقدار درهم‌سازی منتشر شده مطابقت داشته باشد.

هنگامی که از مقادیر درهم‌سازی منتشر شده برای محافظت از مکانیسم به روزرسانی امن استفاده می‌شود، نباید گزینه "پشتیبانی از به روزرسانی خودکار" استفاده شود (هرچند، بررسی خودکار به روزرسانی‌ها مجاز است). هدف ارزیابی ممکن است به طور خودکار برای خودش فایل‌های به روزرسانی را دانلود کند ولی نه مقدار درهم‌سازی. برای رویکرد درهم‌سازی منتشر شده، همواره درخواست مدیر امنیتی برای دریافت احراز هویت فعال جهت نصب به روزرسانی (مطابق جزئیات بیشتر شرح داده شده در FPT_TUD_EXT.1.3) مدنظر است. بنابراین نوع مکانیسم به روزرسانی به عنوان "آغاز به روزرسانی دستی" در نظر گرفته شده است، حتی اگر ممکن باشد فایل‌های به روزرسانی به طور خودکار دانلود شوند. رویکرد کاملاً خودکار (بدون دخالت مدیر امنیتی) فقط زمانی که "مکانیسم امضای دیجیتال" در FPT_TUD_EXT.1.3 انتخاب شده باشد می‌تواند مورد استفاده قرار گیرد.

FPT_TUD_EXT.1.3	به روز رسانی امن ۳	۳۵
-----------------	--------------------	----

توابع امنیتی مورد ارزیابی باید پیش از نصب به روزرسانی‌های نرم‌افزاری/میان‌افزاری، با استفاده از [انتخاب: مکانیسم امضای دیجیتال، درهم‌ساز منتشر شده]، ابزاری را برای احراز هویت میان‌افزار/نرم‌افزار در اختیار محصول مورد ارزیابی قرار دهد.

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

نکته کاربردی:

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

زمانی که برای حفاظت از مکانیسم به روزرسانی امن از مقادیر درهم‌سازی منتشر شده استفاده می‌شود، احراز هویت فعال از فرآیند به روزرسانی توسط مدیر امنیتی، همواره مورد نیاز است. انتقال امن مقدار درهم‌سازی معتبر از توسعه دهنده به مدیر امنیتی، یکی از

فاکتورهای کلیدی برای حفاظت از مکانیسم بروزرسانی امن هنگام استفاده از درهمسازیهای منتشر شده است و لازم است سند راهنما نحوه اجرای انتقال را شرح دهد. برای تایید مقدار درهمسازی امن توسط مدیر امنیتی، موارد استفاده مختلفی ممکن است. مدیر امنیتی می تواند مقدار درهمسازی منتشر شده را مانند فایل های بروزرسانی بدست آورد و تا زمانی که درهمسازی فایل های بروزرسانی توسط هدف ارزیابی یا به روش دیگری در حال انجام است، خارج از هدف ارزیابی تایید را انجام دهد. احراز هویت مدیر امنیتی و آغاز بروزرسانی امن در این مورد با عنوان "احراز هویت فعال" از بروزرسانی امن است. متناوباً، مدیر می تواند هدف ارزیابی را با مقدار درهمسازی منتشر شده و همچنین با فایل های بروزرسانی و درهمسازی و مقایسه های درهمسازی انجام شده توسط هدف ارزیابی باهم ارائه دهد. در مورد تایید درهمسازی موفق، هدف ارزیابی می تواند بروزرسانی را بدون هیچ مرحله اضافی توسط مدیر امنیتی انجام دهد. احراز هویت به عنوان مدیر امنیتی و ارسال مقدار درهمسازی به هدف ارزیابی برای "احراز هویت فعال" از بروزرسانی امن (در مورد تایید درهمسازی موفق) در نظر گرفته شده است، زیرا از مدیر انتظار می رود که مقدار درهمسازی را فقط برای هدف ارزیابی در زمانی که قصد انجام بروزرسانی داشته باشد، بارگذاری کند. تا زمانی که انتقال مقدار درهمسازی به هدف ارزیابی توسط مدیر امنیتی انجام شود، بارگذاری فایل های بروزرسانی توسط مدیر امنیتی قابل انجام است یا به طور خودکار می تواند توسط هدف ارزیابی از منبع دانلود شود.

اگر مکانیسم امضای دیجیتال انتخاب شده باشد، تایید امضا باید توسط خود هدف ارزیابی انجام شود. برای گزینه درهمسازی منتشر شده، خود هدف ارزیابی می تواند همانند مدیر امنیتی تایید نماید. در مورد بعدی استفاده از قابلیت هدف ارزیابی، اختیار تایید ندارد، بنابراین تایید می تواند با استفاده از قابلیت غیر هدف ارزیابی، از دستگاه شامل هدف ارزیابی یا با دستگاهی که شامل هدف ارزیابی نباشد، انجام شود.

برای اهداف ارزیابی توزیع شده، باید تمامی مولفه ها از بروزرسانی امن پشتیبانی نمایند. تایید امضا یا درهمسازی در بروزرسانی باید توسط هر مولفه هدف ارزیابی (تایید امضا) یا برای هر مولفه هدف ارزیابی (تایید درهمسازی) انجام شود. ممکن است بروزرسانی هدف ارزیابی توزیع شده منجر به وضعیتی شود که مولفه های مختلف هدف ارزیابی، نسخه های مختلف نرم افزاری را اجرا کنند. مطابق تفاوت های بین نسخه های مختلف نرم افزار، ممکن است با اثر ترکیبی از نسخه های مختلف نرم افزار در مشکلی در هیچ جا وجود نداشته باشد و یا برای عملکرد هدف ارزیابی بحرانی باشد. TSS باید مکانیسم هایی را که از عملکرد متوالی مناسب هدف ارزیابی در طول بروزرسانی امن اهداف امنیتی توزیع شده پشتیبانی می کنند، با جزئیات مشخص نماید.

نکته کاربردی:

در نسخه های بعدی این پروفایل حفاظتی، لازم خواهد شد که برای به روزرسانی های امن، از یک مکانیسم امضای دیجیتال استفاده شود.

نکته کاربردی:

اگر در مکانیسم تأیید به روزرسانی از گواهی نامه ها استفاده شود، این گواهی ها باید از FIA_X509_EXT.2.1 انتخاب شده و بر اساس FIA_X509_EXT.1 تأیید گردند. علاوه بر این، FPT_TUD_EXT.2 باید در سند هدف امنیتی در نظر گرفته شود.

نکته کاربردی:

در این الزام کارکرد امنیتی، منظور از «به روزرسانی»، فرایند جایگزین کردن یک مؤلفه نرم افزاری غیر فرار (non-volatile) با یک مؤلفه دیگر است. به مؤلفه اول، تصویر غیر فرار یا تصویر NV و به مؤلفه دوم، تصویر به روزرسانی گفته می شود. هر چند که تصویر به روزرسانی معمولاً جدیدتر از تصویر NV است، اما الزامی در این زمینه وجود ندارد. در مواردی ممکن است مالک سیستم بخواهد مؤلفه را به نسخه قدیمی تر برگرداند (مثلاً هنگامی که تولید کننده مؤلفه یک به روزرسانی معیوب را منتشر کند، یا هنگامی که سیستم مبتنی بر یک ویژگی مستندسازی نشده باشد که در به روزرسانی جدید وجود ندارد). همچنین، ممکن است مالک سیستم بخواهد به روزرسانی را با تصویر NV انجام دهد تا معایب موجود را برطرف نماید.

تمام مؤلفه های مجزای میان افزار و نرم افزار (مانند برنامه های کاربردی، درایورها، هسته) محصول مورد ارزیابی لازم است محافظت شوند برای مثال، یا توسط تولید کننده متناظر امضای دیجیتال شوند و در نهایت توسط مکانیسم به روزرسانی تأیید گردند، و یا باید یک درهم سازی برای آنها منتشر شود که نیازمند تأیید قبل از به روزرسانی می باشد.

FPT_STM_EXT.1.1	مهرهای زمانی معتبر ۱	۳۶
-----------------	----------------------	----

توابع امنیتی مورد ارزیابی باید قابلیت ارائه مهرهای زمانی معتبر را برای استفاده خود داشته باشد.

FPT_STM_EXT.1.2	مهرهای زمانی معتبر ۲	۳۷
-----------------	----------------------	----

توابع امنیتی هدف ارزیابی باید [انتخاب: به مدیر امنیتی اجازه تنظیم زمان بدهد، زمان را با یک سرور NTP هماهنگ کند]

نکته کاربردی:

انتظار می رود مهرهای زمانی معتبر با سایر توابع امنیتی هدف ارزیابی مورد استفاده قرار گیرد، مثال: برای تولید داده ممیزی، مجوز بررسی ترتیب رویدادها برای رسیدگی به حوادث و اجازه تعیین زمان واقعی محلی هنگامی که رویدادی رخ داده باشد، به مدیر امنیتی می دهد. تصمیم گیری در مورد میزان دقت مورد نیاز اطلاعات بر عهده سرپرست است. هدف ارزیابی به اطلاعات زمان و تاریخ خارجی بستگی دارد یا به صورت دستی توسط مدیر امنیتی ارائه می شود یا از یک یا بیشتر منبع زمانی خارجی مانند سرورهای NTP استفاده می کند. در این الزام، باید از انتخاب گزینه های متناظر برگزیده شوند. توصیه می شود از ساعت محلی در زمان واقعی استفاده شده و به طور خودکار با یک منبع زمانی خارجی (مانند سرور NTP) هماهنگ شود. توجه داشته باشید که برای ارتباط با منبع زمانی خارجی مانند سرور NTP، استفاده از FTP_ITC.1 اختیاری است. نویسنده سند هدف امنیتی باید در TSS نحوه دریافت اطلاعات زمان و تاریخ خارجی توسط هدف ارزیابی و نحوه نگهداری این اطلاعات را شرح دهد.

The TOE depends on time and date information, either provided by a local real-time clock that is manually managed by the Security Administrator or through the use of one or more external NTP servers. The corresponding option(s) shall be chosen from the selection in FPT_STM_EXT.1.2. The use the automatic synchronisation with an external NTP server is recommended but not mandated. Note that for the communication with an external NTP server, collaborative Protection Profile for Network Devices v2.1, 24-September-2018 Page 70 of 192 FCS_NTP_EXT.1 shall be claimed.

عبارت «مهر زمانی معتبر» به استفاده محدود از اطلاعات زمانی و تاریخی (که توسط موجودیت‌های خارجی ارائه شده‌اند) و تمام تغییرات ثبت‌شده در تنظیمات زمانی (شامل اطلاعات مربوط به زمان قدیم و جدید) اشاره دارد. با استفاده از این اطلاعات، می‌توان زمان واقعی تمام داده‌های ممیزی را محاسبه کرد. توجه داشته باشید باید تمام تغییرات ناپیوسته زمان انجام شده توسط مدیر یا از طریق یک فرآیند خودکار، ممیزی شوند. هنگامی که زمان توسط هسته یا امکانات سیستم تغییر می‌کند، نیازی به ممیزی نیست. مانند روز- که در زمان ناپیوستگی ایجاد نمی‌کند.

برای اهداف امنیتی توزیع شده، انتظار می‌رود مدیر امنیتی از هماهنگی تنظیمات زمانی بین مولفه‌های مختلف هدف ارزیابی اطمینان حاصل نماید. باید تمامی مولفه‌های هدف ارزیابی هماهنگ باشند و یا باید Offset برای هر جفت مولفه هدف ارزیابی برای مدیر شناخته شود (به عنوان مثال از طریق هماهنگی بین مولفه‌های هدف ارزیابی یا از طریق هماهنگی مولفه‌های مختلف هدف ارزیابی با سرورهای NTP خارجی). این مورد شامل مولفه‌های هدف ارزیابی هماهنگ با مناطق مختلف زمانی می‌باشد.

۴-۶- 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 غیر فعال بودن شناسایی شوند و قفل شدن یا خاتمه یافتن آن‌ها نیز در صورت رسیدن به آستانه زمانی بررسی می‌شود. راهبران باید قادر باشند نشست‌های تعاملی خود را خاتمه دهند. در ابتدای هر نشست باید یک اطلاعیه مشاوره‌ای برای آن‌ها نمایش داده شود.

شماره الزام	نام الزام
۳۸	قفل کردن و خاتمه دادن به نشست‌ها ۷
در مورد نشست‌های تعاملی محلی^۱، توابع امنیتی مورد ارزیابی باید پس از اتمام زمان غیرفعال بودن که توسط سرپرست محصول تعیین شده است، انتخاب: - نشست را قفل کند - تمام فعالیت‌های مربوط به دستگاه‌های دسترسی به داده‌های کاربری و نمایش این داده‌ها، به جز فعالیت‌های مربوط به قفل‌گشایی نشست را غیر فعال کند و از سرپرست محصول بخواهد که پیش از قفل‌گشایی نشست، مجدداً احراز هویت نماید؛ - نشست را خاتمه دهد^۱.	
۳۹	قفل کردن و خاتمه دادن به نشست‌ها ۵
FTA_SSL_EXT.1.1	
FTA_SSL.3.1	

^۱ Local

شماره الزام	نام الزام	
در مورد نشست‌های تعاملی راه دور ^۱ ، در صورتی که نشست تعاملی برای مدت معینی غیرفعال باشد، توابع امنیتی مورد ارزیابی باید نشست تعاملی خاتمه دهد. مدت زمان مجاز برای غیرفعال بودن نشست توسط سرپرست امنیتی تعیین می‌شود.		
۴۰	قفل کردن و خاتمه دادن به نشست‌ها ۶	FTA_SSL.4.1
توابع امنیتی مورد ارزیابی باید به سرپرست آغاز کننده اجازه دهد که نشست مدیریتی تعاملی خود را خاتمه دهد.		
۴۱	پیغام‌های هشدار در رابطه با استفاده محصول ۱	FTA_TAB.1.1
قبل از ایجاد نشست برای کاربر سرپرست، توابع امنیتی مورد ارزیابی باید توصیه‌های امنیتی مدیریتی و همچنین پیام هشدار اطلاعیه و توافق‌نامه استفاده از محصول مورد ارزیابی را به سرپرست محصول نشان دهد. نکته کاربردی: این الزام در مورد نشست‌های تعاملی بین یک کاربر انسانی و یک محصول مورد ارزیابی اعمال می‌شود. موجودیت‌های IT که اتصالاتی یا اتصالات برنامه‌ریزی شده‌ای مانند تماس‌های راه دور از طریق شبکه را برقرار می‌کنند، نیازی نیست توسط این الزام پوشش داده شود.		

۴-۷- کانال‌ها و 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: HTTPS, TLS, DTLS, IPsec و SSH. این پروتکل‌ها توسط RFC هایی تعیین می‌شوند که گزینه‌های پیاده‌سازی مختلفی را در اختیار کاربران قرار می‌دهند. در مورد برخی از این گزینه‌ها الزاماتی نیز جود دارد (مخصوصاً گزینه‌های مربوط به مقادیر اولیه رمزنگاری). هدف این است که قابلیت همکاری و مقاومت در برابر حملات رمزنگاری افزایش یابد. این پروتکل‌ها علاوه بر حفاظت در برابر افشای اطلاعات (و شناسایی تغییرات ایجادشده)، امکان احراز هویت دوطرفه را نیز برای هر یک از نقاط پایانی فراهم می‌آورند و این کار را به صورت امن و با استفاده از روش‌های رمزنگاری انجام می‌دهند. بدین معنی که حتی اگر یک مهاجم بدخواه نیز در بین دو نقطه پایانی حضور داشته باشد، هرگونه تلاش وی برای اینکه خود را به عنوان یکی از طرفین ارتباط معرفی کند، شناسایی خواهد شد.

^۱ Remote

FTP_ITC.1.1	کانال امن ۱	۴۲
توابع امنیتی هدف ارزیابی، باید کانال ارتباطی امنی را با استفاده از [انتخاب: SSH، IPsec، DTLS، TLS، HTTPS] میان خود و دیگر موجودیت‌های IT معتبر همچون سرور ممیزی، [انتخاب: سرور احراز هویت، اختصاص: [دیگر قابلیت‌ها]، هیچ قابلیت دیگری] که به طور منطقی از کانال‌های ارتباطی دیگر متمایز است فراهم نماید تا تعیین هویت مطمئنی از نقاط انتهایی ارائه دهد و از داده‌های کانال در برابر تغییر و افشاء محافظت نموده و تغییرات داده‌های کانال را تشخیص دهد. تذکر: در صورتی که هر یک از پروتکل‌های HTTPS، TLS، SSH، IPsec به عنوان پروتکل‌های ارتباطی امن استفاده شود نیاز است از پیوست دو تمامی الزامات مربوط به آن پروتکل تکمیل و به سند هدف امنیتی اضافه گردد.		
FTP_ITC.1.2	کانال امن ۲	۴۳
توابع امنیتی مورد ارزیابی باید به خود یا به موجودیت‌های معتبر IT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.		
FTP_ITC.1.3	کانال امن ۳	۴۴
توابع امنیتی مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای [اختصاص: لیست خدماتی که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباطات را آغاز کند] راه‌اندازی نماید. نکته کاربردی: هدف از الزام حاضر این است که ابزاری را برای استفاده از پروتکل رمزنگاری جهت حفاظت از ارتباطات خارجی با موجودیت‌های معتبر IT کارکرد فراهم آورد. منظور از موجودیت‌های معتبر IT موجودیت‌هایی است که محصول مورد ارزیابی برای انجام کارکردهای خود با آن‌ها ارتباط برقرار می‌کند. محصول مورد ارزیابی دست کم از یکی از پروتکل‌های لیست شده استفاده می‌کند تا با سرور جمع‌آوری اطلاعات ممیزی ارتباط برقرار کند. اگر ارتباط با یک سرور احراز هویت (مانند RADIUS) برقرار شود، نویسنده هدف امنیتی باید عبارت «سرور احراز هویت» را در الزام FTP_ITC.1.1 انتخاب کند. این اتصال باید توسط یکی از پروتکل‌های لیست شده حفاظت گردد. اگر سایر موجودیت‌های معتبر IT (مانند سرور NTP) مورد حفاظت قرار گیرند، نویسنده هدف امنیتی باید انتخاب‌های مقتضی (برای پروتکل‌هایی که به منظور محافظت اتصالات مورد استفاده قرار می‌گیرند) را انجام دهد و موارد مناسب (برای آن موجودیت‌ها) را در عبارت اختصاص بگنجاند. نویسنده هدف امنیتی 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. تا زمانی که هیچ الزامی برای بخش آغازین ارتباطات وجود ندارد، نویسنده سند هدف امنیتی باید در اختصاص موجود در این الزام، لیست سرویس‌هایی از هدف ارزیابی را که می‌تواند ارتباط را با موجودیت IT احراز هویت شده آغاز نمایند، را ارائه دهد. 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 بخشی از راه‌اندازی هدف ارزیابی نیاز به تنظیم دستی کانال‌هایی برای حفاظت		

از سایر ارتباطات وجود داشته باشد. در صورتی که پس از یک قطعی، محصول مورد ارزیابی تلاش کند تا ارتباطات را به صورت خودکار و با دخالت عامل انسانی (در صورت لزوم) 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.

در جایی که گواهینامه‌های کلید عمومی برای پشتیبانی از کانال FTP_ITC.1 استفاده شود، FIA_X509_EXT.1/Rev نیز باید استفاده شود (این الزامات فسخ گواهینامه را بررسی می‌کنند) و FIA_X509_EXT.1/ITT که فقط برای استفاده بین مولفه‌ای کانال‌های هدف ارزیابی توزیع شده می‌باشد، تکرار نشود.

۴۵	مسیر امن ۱	FTP_TRP.1.1/Admin
توابع امنیتی هدف ارزیابی، باید قادر باشد مسیر ارتباطی بین خود و مدیران از راه دور مجاز که به طور منطقی از مسیرهای ارتباطی دیگر متمایز است را با استفاده از [انتخاب: IPsec, SSH, DTLS, TLS, HTTPS] فراهم نماید و نقاط پایانی را به صورت مطمئن شناسایی کرده و از داده‌های ارتباطی در برابر افشاء محافظت نموده و تغییرات داده‌های کانال را تشخیص دهد. تذکر: در صورتی که هر یک از پروتکل‌های 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.		
۴۶	مسیر امن ۲	FTP_TRP.1.2/Admin
توابع امنیتی مورد ارزیابی باید به سرپرست راه‌دور اجازه دهد که ارتباطات را از طریق مسیر امن آغاز کند.		
۴۷	مسیر امن ۳	FTP_TRP.1.3/Admin
توابع امنیتی مورد ارزیابی باید استفاده از مسیر امن را برای احراز هویت اولیه سرپرست و تمام فعالیت‌های راه دور سرپرستی الزامی کند. نکته کاربردی: این الزام اطمینان حاصل می‌نماید که مدیران راه‌دور معتبر، تمام ارتباطات را با محصول مورد ارزیابی، از طریق یک مسیر امن آغاز می‌کنند و در طی تمام ارتباطات با محصول مورد ارزیابی توسط سرپرستان دوردست، همچنان از مسیر امن استفاده می‌نمایند. داده‌های منتقل شده از طریق این کانال ارتباطی امن، با استفاده از پروتکل انتخاب‌شده در عبارت انتخاب، رمزگذاری می‌شوند. نویسنده هدف امنیتی، مکانیسم یا مکانیسم‌های پشتیبانی‌شده توسط محصول مورد ارزیابی را انتخاب می‌کند و اطمینان حاصل می‌نماید که الزامات پروتکل پیوست دو متناظر با انتخاب وی، در هدف امنیتی گنجانده شده‌اند.		

۵- الزامات تضمین امنیت

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی محصول است. در این بخش الزامات EAL1 آورده 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 آماده سازی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب پذیری
Life cycle Support	ALC_CMC.1	برچسب گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

۵-۱- کلاس توسعه

اطلاعات محصول، از طریق «مستندات راهنمای کاربر» و بخش «مشخصات امنیتی محصول» از سند هدف امنیتی در اختیار کاربر نهایی قرار می گیرد. الزامی بر وجود بخش «مشخصات امنیتی محصول» در سند هدف امنیتی نمی باشد، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تأیید توسعه دهندگان محصول باشد.

۵-۱-۱- مشخصات کارکردی

مشخصات کارکردی، واسطه های کارکرد امنیتی محصول را توصیف می نماید اما نیازی به شرح مفصل و کاملی از این واسطه ها نمی باشد. فعالیت های این خانواده باید بر روی شناخت واسطه های معرفی شده در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و «مستندات راهنما» متمرکز گردد.

مولفه های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
مشخصات کارکردی (ADV_FSP)	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مولفه: (ADV_FSP.1.1D) شرح مولفه: توسعه دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱

مولفه‌های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
	شماره مولفه: (ADV_FSP.1.2D) شرح مولفه: توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. نکته کاربردی: مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده‌سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی‌باشد.

مولفه‌های محتوایی	
نام خانواده	عنصر امنیتی
مشخصات کارکردی (ADV_FSP)	نام عنصر: مشخصات کارکرد ابتدایی^۱ شماره مولفه: (ADV_FSP.1.1C) شرح مولفه: مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی^۱ و پشتیبان کننده الزام کارکرد امنیتی^۲ توصیف نماید.
	نام عنصر: مشخصات کارکرد ابتدایی^۱ شماره مولفه: (ADV_FSP.1.2C) شرح مولفه: مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی^۱ شماره مولفه: (ADV_FSP.1.3C)

^۱-SFR-enforcing TSFI

^۲-SFR-supporting TSFI

مولفه‌های محتوایی	
نام خانواده	عنصر امنیتی
	شرح مولفه: مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مولفه: (ADV_FSP.1.4C) شرح مولفه: ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌های کارکرد امنیتی در سند مشخصات کارکردی باشد.

مولفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
مشخصات کارکردی (ADV_FSP)	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مولفه: (ADV_FSP.1.1E) شرح مولفه: ارزیاب باید تأیید نماید که اطلاعات ارائه شده تمام الزامات مولفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ شماره مولفه: (ADV_FSP.1.2E) شرح مولفه: ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.

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

۵-۲- 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 می تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می شود.

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

دستورالعمل نصب موفقیت آمیز محصول در محیط

دستورالعمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگتر

دستورالعمل هایی که ارائه دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت های محصول، محیط عملیاتی یا هر دو می باشد.

۵-۲-۱- راهنمای کاربردی

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

مولفه های محتوایی	
نام خانواده	عنصر امنیتی
راهنمای کاربردی (AGD_OPE)	نام عنصر: راهنمای کاربردی ۱ شماره مولفه: (AGD_OPE.1.1C) شرح مولفه: سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.
	نام عنصر: راهنمای کاربردی ۱ شماره مولفه: (AGD_OPE.1.2C) شرح مولفه: سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسطه های در دسترس ارائه شده توسط محصول به صورت امن استفاده می گردد.

مولفه های محتوایی	
نام خانواده	عنصر امنیتی
	نام عنصر: راهنمای کاربردی ۱ شماره مولفه: (AGD_OPE.1.3C) شرح مولفه: سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسطه های 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 مولفه: (AGD_OPE.1.4C) شرح مولفه: 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 موجودیت های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ شماره مولفه: (AGD_OPE.1.5C) شرح مولفه: سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آنها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر: راهنمای کاربردی ۱ شماره مولفه: (AGD_OPE.1.6C) شرح مولفه: سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ شماره مولفه: (AGD_OPE.1.7C) شرح مولفه:



مولفه های محتوایی	
نام خانواده	عنصر امنیتی
	سند راهنمای کاربردی باید واضح و قابل فهم باشد.

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

۵-۲-۲- راهنمای آماده سازی

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

مولفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
راهنمای آماده سازی (AGD_PRE)	نام عنصر: راهنمای آماده سازی ۱ شماره مولفه: (AGD_PRE.1.1C) شرح مولفه: مستندات آماده سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه های تحویل توسعه دهنده شرح دهند.
	نام عنصر: راهنمای آماده سازی ۱

مولفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
	شماره مولفه: (AGD_PRE.1.2C) شرح مولفه: مستندات آماده سازی باید تمام مراحل لازم برای نصب امن محصول و آماده سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

مولفه های اقدامات ارزیاب	
راهنمای آماده سازی (AGD_PRE)	نام عنصر: راهنمای آماده سازی ۱ شماره مولفه: (AGD_PRE.1.1E) شرح مولفه: ارزیاب باید تأیید نماید که اطلاعات ارائه شده تمام مولفه های محتوایی را برآورده می نماید.
	نام عنصر: راهنمای آماده سازی ۱ شماره مولفه: (AGD_PRE.1.2E) شرح مولفه: ارزیاب باید رویه های آماده سازی شرح داده شده در سند را بکار ببرد تا تأیید نماید، محصول می تواند به صورت امن برای عمل نمودن آماده شود.

۵-۳- کلاس تست

تست محصول برای بررسی بخش های کارکردی سیستم و همچنین بخش هایی که طراحی و پیاده سازی آنها برای سیستم دارای آسیب های امنیتی است، در نظر گرفته می شود. تست بخش های کارکردی سیستم از طریق خانواده ATE_IND و تست بخش هایی که طراحی و پیاده سازی آسیب زایی دارند از طریق خانواده AVA_VAN صورت می گیرد. در این سطح از ارزیابی (سطح EAL1) تست براساس کارکردی که برای محصول در نظر گرفته شده و واسطه هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می گیرد، انجام می گردد. نتایج تست و تحلیل آسیب پذیری باید در گزارش تست لحاظ شوند این مسئله در الزامات زیر در نظر گرفته شده است.

۵-۳-۱- تست مستقل

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

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

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

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



۵-۴- کلاس آسیب پذیری

۵-۴-۱- تحلیل آسیب پذیری

مولفه های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
آسیب پذیری (AVA_VAN)	نام عنصر: آسیب پذیری ۱
	شماره مولفه: (AVA_VAN.1.1D) شرح مولفه: توسعه دهنده باید برای آزمودن، محصول را ارائه نماید.

مولفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
آسیب پذیری (AVA_VAN)	نام عنصر: آسیب پذیری ۱
	شماره مولفه: (AVA_VAN.1.1C) شرح مولفه: محصول باید مناسب آزمودن باشد.

مولفه های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
آسیب پذیری (AVA_VAN)	نام عنصر: آسیب پذیری ۱
	شماره مولفه: (AVA_VAN.1.1E) شرح مولفه: ارزیاب باید تأیید نماید که اطلاعات ارائه شده، تمام مولفه های محتوایی را برآورده می نماید.
	نام عنصر: آسیب پذیری ۱
آسیب پذیری (AVA_VAN)	شماره مولفه: (AVA_VAN.1.2E) شرح مولفه: ارزیاب باید برای شناسایی آسیب پذیری های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب پذیری ۱

مولفه‌های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
	شماره مولفه: (AVA_VAN.1.3E) شرح مولفه: ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۵-۵- کلاس پشتیبانی از چرخه حیات

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

۵-۵-۱- قابلیت‌های پیکربندی

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

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

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

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

۵-۵-۲- حوزه پیکربندی

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

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



مولفه‌های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
	نام عنصر: پوشش پیکربندی محصول ۱ شماره مولفه: (ALC_CMS.1.1C) شرح مولفه: لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

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

۶- پیوست یک: الزامات اختیاری

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

۶-۱- کلاس ممیزی امنیت

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

جدول ۲. الزامات انتخابی هدف ارزیابی و رویدادهای قابل ممیزی

ردیف	الزام	رویدادهای ممیزی	لیست سوابق ممیزی اضافی
۱.	FAU_STG.1	هیچ	هیچ
۲.	FAU_STG_EXT.2/LocSpace	هیچ	هیچ
۳.	FAU_STG.3/LocSpace	کمبود فضای ذخیره‌سازی برای رویدادهای ممیزی	هیچ
۴.	FIA_X509_EXT.1/ITT	تلاش ناموفق برای تایید یک گواهینامه	دلیل شکست
۵.	FMT_MOF.1/Services	آغاز و پایان سرویس‌ها	هیچ
۶.	FMT_MTD.1/CryptoKeys	مدیریت کلیدهای رمزنگاری	هیچ

شناسایی آغاز کننده و هدف تلاش ناموفق برای برقراری کانال های امن	آغاز یک کانال امن خاتمه یک کانال امن شکست عملکرد کانال امن	FPT_ITT.1	۷.
هیچ	آغاز یک مسیر امن خاتمه یک مسیر امن شکست عملکرد مسیر امن	FTP_TRP.1/Join	۸.
هویت جفت نقاط پایانی فعال یا غیرفعال شده	فعالسازی ارتباط بین یک جفت مولفه غیرفعالسازی ارتباط بین یک جفت مولفه	FCO_CPC_EXT.1	۹.

نکته کاربردی:

رویدادهای ممیزی FIA_X509_EXT.1/ITT بر اساس هدف ارزیابی است که با اطمینان از موارد زیر، قادر به تکمیل اعتبار گواهینامه نمی باشد:

- وجود افزونه basicConstraints و پرچم CA که برای تمامی گواهینامه های CA به حالت «True» تنظیم شده باشد.
 - تایید امضای دیجیتالی CA سلسله مراتبی معتبر
 - خواندن/دسترسی به CRL یا دسترسی به سرور OCSP (مطابق انتخاب در سند هدف امنیتی)
- اگر هر کدام از این موارد رد شوند، باید یک رویداد ممیزی عدم موفقیت، در لاگ ممیزی نوشته شود.



نام الزام		شماره الزام
FAU_STG.1.1	ذخیره سازی داده های ممیزی محافظت شده ۱	۴۸
توابع امنیتی مورد ارزیابی باید از پاک شدن غیر مجاز داده های ممیزی ذخیره شده در دنباله ممیزی محافظت نماید.		
FAU_STG.1.2	ذخیره سازی داده های ممیزی محافظت شده ۲	۴۹
توابع امنیتی مورد ارزیابی باید قادر باشد از تغییرات غیر مجاز داده های ممیزی ذخیره شده در دنباله ممیزی جلوگیری نماید.		
FAU_STG_EXT.2.1/LocSpace	شمارش داده های ممیزی از دست رفته	۵۰
توابع امنیتی هدف ارزیابی باید در صورت پر شدن حافظه محلی، اطلاعات مربوط به تعداد داده های ممیزی [انتخاب: از بین رفته، بازنویسی شده، [اختصاص: سایر اطلاعات]] را ارائه کند. توابع امنیتی هدف ارزیابی یکی از اقدامات تعیین شده در «محل ذخیره سازی داده های ممیزی ۱۳» را انجام می دهد. نکته کاربردی ۴۲: این گزینه در صورتی باید انتخاب شود که هدف مورد ارزیابی از این کارکرد پشتیبانی کند. در صورتی که حافظه محلی داده های ممیزی توسط سرپرست محصول خالی شود، شمارنده های مربوط به انتخاب انجام شده باید به مقادیر اولیه خود برگردند (این مقدار در اکثر موارد صفر است). اسناد راهنما باید به سرپرست محصول هشدار دهند که خالی کردن حافظه ممکن است سبب از دست رفتن داده ها شود. برای اهداف ارزیابی توزیع شده، هر کامپوننتی که شمارش داده های ممیزی از دست رفته را پیاده سازی کرده است، باید مکانیسم دسترسی و مدیریت این اطلاعات برای مدیر را فراهم نماید. اگر این الزام به سند هدف امنیتی اضافه شود، سند هدف امنیتی باید هر وضعیتی که داده ممیزی از دست رفته شمارش نمی شود را مشخص نماید.		

^۱ FAU_STG_EXT.1.3



FAU_STG.3.1/LocSpace	نمایش هشدار برای فضای ذخیره سازی محلی	۵۱
توابع امنیتی هدف ارزیابی باید در صورتی که دنباله ممیزی بیش از ظرفیت ذخیره سازی دنباله ممیزی باشد، برای اطلاع رسانی به مدیر هشدار ایجاد نماید. نکته کاربردی: در صورتی که هدف ارزیابی امکان تولید پیام مربوطه را داشته باشد این گزینه انتخاب می شود. در صورتی که داده های مربوط به رویدادهای قابل ممیزی تنها در حافظه محلی ذخیره شده باشند، این هشدار می تواند اهمیت بسیار زیادی داشته باشد. باید اطمینان حاصل نمود که هشدار مورد اشاره در «محل ذخیره سازی داده های ممیزی ۳» را می توان به اطلاع مدیر رساند. ارتباط باید از طریق سوابق ممیزی صورت گیرد، زیرا ممکن است در هنگام رخ دادن اتفاق، نشست فعالی برای مدیریت این کار وجود نداشته باشد. پیام هشدار باید هنگامی که فضای محلی برای ذخیره داده ممیزی در حال پر شدن بود و/یا ممکن باشد هدف ارزیابی به علت فضای محلی ناکافی داده های ممیزی را از دست بدهد، مدیر را مطلع نماید. برای اهداف ارزیابی توزیع شده ای که در زمان پر شدن فضای حافظه محلی داده ممیزی هشدار می دهند، باید مشخص شود که کدام مولفه های هدف ارزیابی از این ویژگی پشتیبانی می کنند (اگر به عنوان هدف ارزیابی کلی انتخاب شده باشد، پشتیبانی تمامی مولفه های هدف ارزیابی از این ویژگی الزامی نیست). هر مولفه ای که از این ویژگی پشتیبانی می کند باید هشدار را خودش یا از طریق مولفه دیگری تولید کند. اگر FAU_STG.3/LocSpace به سند هدف امنیتی اضافه شده باشد، سند هدف امنیتی باید هر حالتی که ممکن است سوابق ممیزی "به طور مخفی از دست روند" را مشخص نماید.		

۶-۲- کلاس شناسایی و تایید اعتبار

شماره الزام	نام الزام	
۵۲	تایید گواهینامه X509 (۱)	FIA_X509_EXT.1.1/ITT

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

- تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه با پشتیبانی از حداقل طول مسیر دو گواهی‌نامه
- مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد
- توابع امنیتی مورد ارزیابی باید برای تأیید یک مسیر گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم شده است.
- توابع امنیتی مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنالین (OCSP) چنان که در RFC 6960 تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در RFC 5759 بخش ۵ تعریف شده است، لیست فسخ گواهی‌نامه (CRL) چنان که در RFC 5280 بخش ۶،۳ تعریف شده است، هیچ روش فسخی] تأیید کند
- توابع امنیتی مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید کند:
 - گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف "Server Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.
 - گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف "Client Authentication" (id-kp2 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.
 - گواهی‌نامه‌های OCSP ارائه شده برای پاسخ‌های OCSP باید هدف «OCSP Signing» (id-kp9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.

نکته کاربردی:

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

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

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

در صورتی که هدف ارزیابی از عملکردهایی پشتیبانی کند که از هیچکدام از انواع گواهی‌نامه‌های لیست شده در قوانین extendedKeyUsage در FIA_X509_EXT.1.1 پشتیبانی نکند، باید در TSS تعیین شود و بخش مربوط به SFR به طور کلی عملکردهای مورد پذیرش را در نظر می‌گیرد. هر چند، اگر هدف ارزیابی از عملکردهایی پشتیبانی کند که از هرکدام از انواع این گواهی‌نامه‌ها استفاده می‌کند، باید قوانین متناظر همانند SFR رعایت شوند.

FIA_X509_EXT.1.2/ITT	تایید گواهینامه X509 (۲)	۵۳
توابع امنیتی مورد ارزیابی تنها در صورتی که افزونه مربوط به basicConstraints از پیش تنظیم شده باشد و پرچم CA به حالت «TRUE» تنظیم شده باشد، یک گواهی نامه را به عنوان گواهی نامه CA می پذیرد. نکته کاربردی: این الزام در مورد گواهی نامه هایی اعمال می شود که توسط محصول مورد ارزیابی بکار رفته و پردازش شده باشند. این الزام همچنین اضافه شدن گواهی نامه ها به لیست گواهی نامه های معتبر CA را محدود می کند.		

۳-۶- کلاس حفاظت از محصول مورد ارزیابی

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

FTP_TRP.1.3/Join	مسیر امن ۳ / Join	۵۷
توابع امنیتی هدف ارزیابی باید برای اتصال مولفه‌ها به توابع امنیتی هدف ارزیابی تحت محدودیت‌های محیطی مشخص شده در مرجع راهنمای عملیاتی، از مسیر امن استفاده کند. نکته کاربردی ۴۹: این الزام یکی از انواع شناسایی کانال در انتخاب اصلی الزام FCO_CPC_EXT.1.2 را برقرار می‌کند. در FTP_TRP.1.1/Join، "مولفه joining"، موجودیت IT است که برای پیوستن به هدف ارزیابی توزیع شده توسط فرآیند ثبت تلاش می‌کند. این الزام نیازمند توانایی مولفه‌ها برای برقراری ارتباط امن در طول ایجاد توابع امنیتی هدف ارزیابی توزیع شده (یا زمانی که مولفه‌ای به توابع امنیتی هدف ارزیابی توزیع شده موجود اضافه می‌شود) می‌باشد. در این الزام، زمانی که توابع امنیتی هدف ارزیابی از جفت مولفه‌های اولیه ایجاد می‌شوند، ممکن است هر کدام از این مولفه‌ها به عنوان توابع امنیتی هدف ارزیابی شناسایی شوند. انتخاب موجود در انتهای FTP_TRP.1.1/Join تشخیص می‌دهد که در برخی موارد ممکن است محرمانگی توسط کانال ارائه نشود (به عنوان مثال، حفاظت از افشای داده‌ها). در این مورد، نویسنده هدف امنیتی باید در TSS، هدف ارزیابی مربوط به محیط برای ارائه محرمانگی را (به عنوان بخشی از محدودیت‌های اشاره شده در FTP_TRP.1.3/Join) مشخص نماید یا تعیین کند که ثبت داده تبادل شده نیازمند محرمانگی نمی‌باشد (در کدام مورد این ادعا صدق می‌کند). اگر "هیچ" انتخاب شود، ممکن است در سند هدف امنیتی برای بهبود خوانایی این عبارت حذف شود. اختصاص موجود در FTP_TRP.1.3/Join، اطمینان حاصل می‌کند که سند هدف امنیتی هر جزئیات خاص مورد نیاز برای محافظت از محیط ثبت را مشخص کرده است. توجه داشته باشید زمانی که سند هدف امنیتی از FTP_TRP.1/Join برای کانال ثبت استفاده می‌کند، این کانال نمی‌تواند مجدداً به عنوان کانال ارتباطی طبیعی بین مولفه‌ای استفاده شود (کانال بعدی باید FTP_ITC.1 یا FPT_ITT.1 را رعایت کند). الزامات خاص برای فرآیندهای مقدماتی مربوط به FTP_TRP.1/Join در فعالیتهای ارزیابی در [SD] تعریف شده‌اند.		



۴-۶- کلاس ارتباطات

شماره الزام	نام الزام	
۵۸	تعریف کانال ثبت مولفه ۱	FCO_CPC_EXT.1.1
توابع امنیتی هدف ارزیابی باید از مدیر امنیتی درخواست فعالسازی ارتباطات بین هر جفت مولفه‌های هدف ارزیابی کند، قبل از این که چنین ارتباطی قابل انجام باشد.		
۵۹	تعریف کانال ثبت مولفه ۲	FCO_CPC_EXT.1.2
توابع امنیتی هدف ارزیابی باید فرآیند ثبتي که در آن مولفه‌ها ایجاد می‌شوند را پیاده‌سازی کند و برای حداقل داده‌های توابع امنیتی هدف ارزیابی از کانال ارتباطی استفاده کند که: [انتخاب: ○ کانالی که الزامات کانال امن را در [انتخاب: FTP_ITC.1, FPT_ITT.1] برآورده می‌کند. ○ کانالی که الزامات کانال ثبت را در FTP_TRP.1/Join برآورده می‌کند. ○ هیچ کانالی]		
۶۰	تعریف کانال ثبت مولفه ۳	FCO_CPC_EXT.1.3
توابع امنیتی هدف ارزیابی باید یک مدیر امنیتی را قادر به غیرفعالسازی ارتباطات بین هر جفت مولفه هدف ارزیابی نماید. نکته کاربردی ۵۰: این الزام فقط وقتی هدف ارزیابی توزیع شده باشد و دارای مولفه‌های متعددی که نیازمند برقراری ارتباط از طریق کانال داخلی توابع امنیتی هدف ارزیابی هستند باشد، مناسب است. زمانی که توابع امنیتی هدف ارزیابی از جفت مولفه‌های اولیه ایجاد می‌شوند، ممکن است هرکدام از این مولفه‌ها به عنوان توابع امنیتی هدف ارزیابی شناسایی شوند. هدف این الزام اطمینان از وجود فرآیند ثبتي است که، قبل از این که مولفه‌های متصل به توابع امنیتی هدف ارزیابی توزیع شده بتوانند با سایر مولفه‌های هدف ارزیابی ارتباط برقرار کنند، و قبل از اینکه مولفه جدید بتواند به عنوان بخشی از توابع امنیتی هدف ارزیابی عمل کند؛ شامل یک مرحله مثبت قابل فعالسازی توسط مدیر باشد. ممکن است خود فرآیند ثبت شامل ارتباط با مولفه متصل باشد: برخی تجهیزات شبکه از فرآیندی سفارشی برای این مورد استفاده می‌کنند، و الزامات امنیتی برای "ارتباطات ثبت" در FCO_CPC_EXT.1.2 تعریف شده‌اند. استفاده از این کانال "ارتباطات ثبت"، متناقض با الزامات FCO_CPC_EXT.1.1 تلقی نمی‌شود. (به عنوان مثال، کانال ثبت می‌تواند قبل از مرحله قابل فعالسازی و فقط برای تکمیل فرآیند ثبت، استفاده شود)		

انتخاب کانال (برای کانال ثبت) در FCO_CPC_EXT.1.2 اساساً یک انتخاب بین استفاده از کانال امن معمولی که معادل یک کانال استفاده شده برای ارتباط با موجودیت‌های IT خارجی (FTP_ITC.1) می‌باشد، یا مولفه‌های هدف ارزیابی موجود (FPT_ITT.1)، یا نوع مجزای دیگری از کانال که برای ثبت مشخص شده است (FTP_TRP.1/Join)، می‌باشد. اگر هدف ارزیابی نیازی به کانال ارتباطی برای ثبت نداشته باشد (به عنوان مثال، ثبت توسط مدیر از طریق اقدامات پیکربندی به طور کامل برای هر مولفه انجام شده باشد)، انتخاب اصلی در FCO_CPC_EXT.1.2 با گزینه "هیچ کانالی" تکمیل شود.

اگر نویسنده هدف امنیتی نوع کانال FTP_ITC.1/FPT_ITT.1 را در انتخاب اصلی از FCO_CPC_EXT.1.2 برگزیده باشد، TSS باید مربوطه‌ای که کانال مورد استفاده را مشخص می‌کند تعیین کند. اگر نویسنده هدف امنیتی نوع کانال FTP_TRP.1/Join را انتخاب کند، خلاصه مشخصات هدف ارزیابی (احتمالاً با پشتیبانی از راهنمای عملیاتی)، جزئیات کانال و مکانیسم‌هایی که استفاده می‌کند را شرح می‌دهد (و شرح دهد که فرآیند ثبت چگونه اطمینان می‌یابد که کانال فقط توسط joiner و gatekeeper قابل استفاده است). توجه داشته باشید که نوع کانال FTP_TRP.1/Join ممکن است در محیط عملیاتی، از اقدامات امنیتی درخواست پشتیبانی نماید. (برای جزئیات تعریف FTP_TRP.1/Join را ببینید)

اگر نویسنده هدف امنیتی نوع کانال FTP_ITC.1/FPT_ITT.1 را از انتخاب اصلی FTP_ITC.1/FPT_ITT.1 برگزیده باشد، سند هدف امنیتی باید کانال ثبت را به عنوان تکرار جداگانه‌ای از FTP_ITC.1 یا FPT_ITT.1 تعریف کند و شناسه تکرار را برای FCO_CPC_EXT.1 در نکته کاربردی سند هدف امنیتی ارائه دهد.

توجه داشته باشید که کانال راه‌اندازی و استفاده شده برای ثبت، در صورتی که مطابق با الزامات FTP_ITC.1 یا FPT_ITT.1 باشد، ممکن است به عنوان یک کانال ارتباطی داخلی مداوم در نظر گرفته شده باشد. به عبارت دیگر کانال ثبت بعد از استفاده بسته می‌شود و کانال جداگانه‌ای برای ارتباطات داخلی استفاده می‌شود.

الزامات خاص برای رویه‌های مقدماتی مربوط به FCO_CPC_EXT.1 در فعالیت‌های ارزیابی در SD تعریف شده است.

۷- پیوست دو: الزامات مبتنی بر انتخاب

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

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

جدول ۳. الزامات مبتنی بر انتخاب و رویدادهای قابل ممیزی

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

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

نکته کاربردی:

رویدادهای ممیزی FIA_X509_EXT.1/Rev بر اساس هدف ارزیابی است که با اطمینان از موارد زیر، قادر به تکمیل اعتبار گواهینامه نمی‌باشد:

- وجود افزونه basicConstraints و پرچم CA که برای تمامی گواهینامه‌های CA به حالت «True» تنظیم شده باشد.
 - تایید امضای دیجیتالی CA سلسله مراتبی معتبر
 - خواندن/دسترسی به CRL یا دسترسی به سرور OCSP (مطابق انتخاب در سند هدف امنیتی)
- اگر هرکدام از این موارد رد شوند، باید یک رویداد ممیزی عدم موفقیت، در لاگ ممیزی نوشته شود.



۷-۱- کلاس ممیزی امنیت

۷-۱-۱- تولید داده های ممیزی امنیت

شماره الزام	نام الزام
۶۱	تولید داده ممیزی ۱
توابع امنیت هدف ارزیابی قادر به تولید سوابق حسابرسی برای هر مؤلفه هدف ارزیابی است. سوابق حسابرسی ایجاد شده توسط توابع امنیت هدف ارزیابی از هر مؤلفه محصول مورد ارزیابی شامل زیر مجموعه رویدادهای مربوط به ممیزی امنیت است که می توانند روی مؤلفه هدف ارزیابی اتفاق بیفتند.	
۶۲	محل ذخیره سازی داده های ممیزی حفاظت شده
توابع امنیتی هدف ارزیابی باید قبل از اینکه ممیزی از ظرفیت ذخیره سازی ردیابی ممیزی محلی بیشتر شود، اخطار لازم را به مدیر ارائه دهد.	
۶۳	محل ذخیره سازی داده ممیزی ۴
هر مؤلفه هدف ارزیابی که داده های ممیزی امنیتی را به صورت محلی ذخیره نمی کند ، می تواند داده های ممیزی امنیتی را بصورت محلی بافر کند تا زمانی که به یک مؤلفه دیگر هدف ارزیابی که آن را ذخیره یا انتقال می دهد ، انتقال داده شود. [انتخاب: FPT_ITC.1 ، FPT_ITT.1]	

۷-۲- کلاس پشتیبانی از رمزنگاری

۷-۲-۱- الزامات پروتکل DTLS Client

شماره الزام	نام الزام
۶۴	الزامات پروتکل DTLS Client (۱)
FCS_DTLSC_EXT.1.1	

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

[انتخاب:

- TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289

[نکته کاربردی:

توسط این الزام مجموعه رمزهای مورد آزمایش در تنظیمات ارزیابی محدود می‌شوند. نویسنده سند هدف امنیتی باید مجموعه رمزهایی که پشتیبانی می‌شوند را انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با نسخه دوم ND cPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 6347 وجود داشته باشد، الزامی است. به علت اینکه نسخه‌های جدید DTLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند. در نسخه آینده این cPP، نسخه ۱،۲ DTLS برای تمامی اهداف ارزیابی الزامی خواهد بود.

۶۵	الزامات پروتکل DTLS Client (۲)	FCS_DTLSC_EXT.1.2
----	--------------------------------	-------------------

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

[نکته کاربردی:

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

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

۶۶	الزامات پروتکل DTLS Client (۳)	FCS_DTLSC_EXT.1.3
----	--------------------------------	-------------------

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

۶۷	الزامات پروتکل DTLS Client (۴)	FCS_DTLSC_EXT.1.4
----	--------------------------------	-------------------

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

نکته کاربردی:

اگر مجموعه رمزهای با منحنی elliptic در FCS_DTLSC_EXT.1.1 انتخاب شده باشد، انتخاب یک یا چند منحنی الزامی است. اگر هیچ مجموعه رمزی با منحنی elliptic در FCS_DTLSC_EXT.1.1 انتخاب نشده باشد، باید گزینه "Supported Elliptic Curves Extension" را ارائه ندهد. این الزام منحنی‌های elliptic مجاز را برای احراز هویت و پذیرش کلید منحنی‌های NIST از FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌کند. این تعمیم برای کلاینت‌هایی که از Elliptic Curve ciphersuites پشتیبانی می‌کنند، می‌باشد.

^۱ backwards compatibility

۷-۲-۲- الزامات پروتکل DTLS Client / احراز هویت

FCS_DTLSC_EXT.2.1	الزامات پروتکل DTLS Client / احراز هویت (۱)	۶۸
توابع امنیتی هدف ارزیابی باید احراز هویت متقابل را با استفاده از گواهینامه X.509 نسخه ۳، پشتیبانی کند.		
FCS_DTLSC_EXT.2.2	الزامات پروتکل DTLS Client / احراز هویت (۲)	۶۹
توابع امنیتی هدف ارزیابی باید در صورت دریافت پیامی حاوی invalid MAC [انتخاب: نشست DTLS را خاتمه دهد، رکورد را بی سر و صدا دور بیاندازد.]		
FCS_DTLSC_EXT.2.3	الزامات پروتکل DTLS Client / احراز هویت (۳)	۷۰
توابع امنیتی هدف ارزیابی باید پیام‌های replayed را برای موارد زیر شناسایی کرده و بدون پاسخ دور بریزد:		
• سوابق DTLS قبلاً دریافت شده • سوابق DTLS انقدر قدیمی باشند که متناسب پنجره لغزان نباشند.		
شناسایی کرده و بی‌صدا از بین ببرد.		

۷-۲-۳- الزامات پروتکل DTLS Server

FCS_DTLSS_EXT.1.1	الزامات پروتکل DTLS Server (۱)	۷۱
توابع امنیتی هدف ارزیابی باید [انتخاب: DTLS 1.0 (RFC 4347), DTLS 1.2 (RFC 6347)] را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید:		
[انتخاب:		
○ TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 ○ TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492		

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289

[

نکته کاربردی:

مجموعه رمزهای آزمایش شده در تنظیمات ارزیابی توسط این الزام محدود می‌شوند. نویسنده هدف امنیتی باید مجموعه رمزهایی که پشتیبانی می‌شوند را انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با نسخه دوم ND cPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 6347 و RFC 5246 وجود داشته باشد، الزامی است. به علت اینکه نسخه‌های جدید DTLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند. در نسخه آینده این cPP، نسخه ۱،۲ DTLS برای تمامی اهداف ارزیابی الزامی خواهد بود.

FCS_DTLSS_EXT.1.2	الزامات پروتکل DTLS Server (۲)	۷۲
-------------------	--------------------------------	----

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

نکته کاربردی:

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

۷۳	الزامات پروتکل DTLS Server (۳)	FCS_DTLSS_EXT.1.3
----	--------------------------------	-------------------

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

نکته کاربردی:

فرآیند تایید کلاینت DTLS، در بخش ۴،۲،۱ از DTLS 1.2 RFC 6347 و DTLS 1.0 RFC 4347 شرح داده شده است. هدف ارزیابی کلاینت DTLS را طی برقراری ارتباط (Handshaking) و قبل از اینکه توابع امنیتی هدف ارزیابی پیام Server Hello ارسال نماید، تایید کند. پس از دریافت ClientHello، سرور DTLS، به همراه کوکی^۱ HelloVerifyRequest ارسال می‌کند. کوکی، پیام امضا شده‌ای است که از توابع درهم‌سازی کلید شده مشخص شده در FCS_COP.1/KeyedHash استفاده می‌کند. سپس کلاینت DTLS یک ClientHello دیگری به پیوست کوکی ارسال می‌کند. اگر سرور DTLS با موفقیت کوکی امضا شده را تایید کند، کلاینت از آدرس IP جعلی استفاده نمی‌کند.

۷۴	الزامات پروتکل DTLS Server (۴)	FCS_DTLSS_EXT.1.4
----	--------------------------------	-------------------

توابع امنیتی هدف ارزیابی باید برای TLS از [انتخاب: کلید RSA را با اندازه [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت]، پارامترهای Diffie-Hellman با اندازه [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲ بیت، ۴۰۹۶ بیت، ۶۱۴۴ بیت، ۸۱۹۲ بیت] گروه‌های Diffie-Hellman [انتخاب: ffdhe2048، ffdhe3072، ffdhe4096، ffdhe6144، ffdhe8192، هیچ گروه دیگری]، منحنی‌های ECDHE [انتخاب: secp256r1، secp384r1، secp521r1] و هیچ منحنی دیگری] استفاده کند.

۷۵	الزامات پروتکل DTLS Server (۵)	FCS_DTLSS_EXT.1.5
----	--------------------------------	-------------------

در صورت دریافت پیامی شامل MAC نامعتبر، توابع امنیتی هدف ارزیابی باید [انتخاب: نشست DTLS را خاتمه دهد، سوابق را بدون پاسخ دور بریزد^۲].

نکته کاربردی:

Message Authentication Code (MAC) تابع درهم‌ساز کلید شده مشخص شده در FCS_COP.1/KeyedHash می‌باشد. MAC، در مرحله DTLS handshake تبادل می‌شود و برای حفظ صحت پیام‌های دریافت شده از فرستنده در طول تبادل داده DTLS استفاده می‌شود. در صورتی که MAC تایید نشود، باید نشست خاتمه یابد یا باید سوابق بدون پاسخ رها شوند.

^۱ cookie

^۲ Silently discard the record

FCS_DTLSS_EXT.1.6	الزامات پروتکل DTLS Server (۶)	۷۶
توابع امنیتی هدف ارزیابی باید پیام‌های replayed را برای موارد زیر شناسایی کرده و بدون پاسخ دور بریزد: ○ سوابق DTLS قبلاً دریافت شده ○ سوابق DTLS انقدر قدیمی باشند که متناسب پنجره لغزان نباشند. نکته کاربردی: شناسایی Replay در بخش ۴,۱,۲,۶ از DTLS 1.2 (RFC 6347) و بخش ۴,۱,۲,۵ از DTLS 1.0 (RFC 4347) شرح داده شده است. برای هر سوابق دریافت شده، دریافت کننده سوابق حاوی دنباله شماره‌ای که در پنجره دریافت لغزان قرار دارد را تایید می‌کند و دنباله شماره هر سوابق دریافت شده دیگر را در طول نشست تکرار نمی‌کند. "Silently Discard" به این معنی است که هدف ارزیابی بسته‌ها را بدون پاسخ دور بریزد.		
FCS_DTLSS_EXT.1.7	الزامات پروتکل DTLS Server (۷)	۷۷
توابع امنیتی هدف ارزیابی باید از [انتخاب: هیچ از سرگیری جلسه یا بلیط های جلسه، از سرگیری نشست بر مبنای session ID بر اساس RFC 4346(TLS1.1) یا RFC5246(TLS1.2)، از سرگیری نشست بر مبنای بلیط های نشست با توجه به RFC 5077] پشتیبانی کند.		

۷-۲-۴- الزامات پروتکل DTLS Server / احراز هویت متقابل

FCS_DTLSS_EXT.2.1	الزامات پروتکل DTLS Server / احراز هویت متقابل (۱)	۷۸
توابع امنیتی هدف ارزیابی باید احراز هویت متقابل DTLS Client را با استفاده از گواهینامه X.509 نسخه ۳، پشتیبانی کند.		
FCS_DTLSS_EXT.2.2	الزامات پروتکل DTLS Server / احراز هویت متقابل (۲)	۷۹
زمانی که کانال مورد اعتماد ایجاد می‌شود، اگر گواهینامه کلاینت معتبر نباشد به صورت پیشفرض توابع امنیتی هدف ارزیابی نباید یک کانال مورد اعتماد را ایجاد کند. همچنین توابع امنیتی هدف ارزیابی باید: [انتخاب: - هیچ مکانیزم لغو سرپرستی را اجرا نکند. - در صورت عدم موفقیت توابع امنیتی هدف ارزیابی در [انتخاب: تطابق با شناسه مرجع، تائید مسیر گواهینامه، تایید تاریخ انقضاء، تعیین وضعیت ابطال] گواهینامه مشتري ارائه شده، به مجوز سرپرست برای برقراری ارتباط نیاز دارد.]		
FCS_DTLSS_EXT.2.3	الزامات پروتکل DTLS Server / احراز هویت متقابل (۳)	۸۰

در صورتی که نام مشخص شده^۱ (DN) یا نام مستعار موجودیت فعال^۲ (SAN) در یک گواهی نامه با شناسه مورد انتظار برای همتا مطابقت نداشته باشد، محصول نباید کانال امن را برای کلاینت برقرار سازد.

۷-۲-۵- الزامات پروتکل HTTPS

شماره الزام	نام الزام
۸۱	الزامات پروتکل HTTPS (۱)
توابع امنیتی هدف ارزیابی باید پروتکل HTTPS مطابق با RFC 2818 را اجرا کنند. نکته کاربردی: نویسنده سند هدف امنیتی باید اطلاعات کافی را فراهم آورد و مشخص کند که پیاده سازی این پروتکل، مطابق استانداردهای تعریف شده است. برای انجام این کار می توان جزئیات بیشتری را به TSS اضافه کرد.	
۸۲	الزامات پروتکل HTTPS (۲)
توابع امنیتی هدف ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	
۸۳	الزامات پروتکل HTTPS (۳)
در صورتی که گواهی نامه همتا ^۳ ارائه شده باشد، توابع امنیتی هدف ارزیابی باید [انتخاب: نیاز به احراز هویت کلاینت نداشته باشد، اتصال را برقرار ننماید، برای برقراری اتصال درخواست احراز هویت ننماید، [اختصاص: اقدام دیگر]].	

۷-۲-۶- الزامات پروتکل IPSec

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

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

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

^۱Distinguished name

^۲Subject Alternative Name

^۳Peer certificate

شماره الزام	نام الزام	
۸۴	الزامات پروتکل IPSEC (۱)	FCS_IPSEC_EXT.1.1
در توابع امنیتی هدف ارزیابی باید معماری IPsec را بر اساس آن چه در RFC 4301 مشخص شده است، پیاده‌سازی شود. نکته کاربردی: بر اساس RFC 4301 برای پیاده‌سازی IPSEC جهت محافظت از ترافیک IP باید از یک پایگاه‌داده خط‌مشی امنیتی (SPD) استفاده کرد. با استفاده از SPD می‌توان تعیین کرد که بسته‌های IP چگونه باید مدیریت شوند: ۱- «PROTECT» از بسته‌ها (مثلاً رمزگذاری آن‌ها) ۲- «BYPASS» از سرویس IPSEC (مثلاً عدم رمزگذاری) ۳- «DISCARD» بسته (مثلاً دور ریختن بسته). پایگاه‌داده مذکور را می‌توان به روش‌های مختلفی پیاده‌سازی کرد که از آن جمله می‌توان به لیست‌های کنترل دسترسی به مسیر، مجموعه قوانین فایروال، استفاده از یک پایگاه داده SPD سنتی و مواردی از این دست اشاره کرد. صرف نظر از روشی که به کار گرفته می‌شود، قوانینی وجود دارند که بسته‌ها باید از آن‌ها پیروی کنند و اقدامات باید بر اساس آن‌ها انجام شوند. باید ازارهایی برای تنظیم این قوانین وجود داشته باشند، اما رویکردی عمومی و کلی در این زمینه وجود ندارد. قاعده کلی این است که SPD باید بتواند بسته‌های IP را از یکدیگر تمایز دهد و قوانین مربوطه را در مورد آن‌ها اعمال نماید. ممکن است چند SPD وجود داشته باشند (یک پایگاه داده برای هر واسط شبکه)، اما الزامی در این زمینه وجود ندارد.		
۸۵	الزامات پروتکل IPSEC (۲)	FCS_IPSEC_EXT.1.2
توابع امنیتی هدف ارزیابی باید اسمی داشته باشد خط‌مشی پایانی موجود در SPD با هر چیز مطابقت داشته باشد. در غیر این صورت غیرمنطبق است، و دور انداخته می‌شود.		
۸۶	الزامات پروتکل IPSEC (۳)	FCS_IPSEC_EXT.1.3
توابع امنیتی هدف ارزیابی باید [انتخاب: مد انتقال، مد تونل] پیاده‌سازی کند. نکته کاربردی: نویسنده هدف امنیتی باید حالت‌های پشتیبانی شده برای عملکرد IPsec را انتخاب نماید.		
۸۷	الزامات پروتکل IPSEC (۴)	FCS_IPSEC_EXT.1.4
توابع امنیتی هدف ارزیابی باید بر اساس آنچه در RFC 4303 گفته شده است، پروتکل ESP مربوط به IPSEC را با استفاده از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128 (RFC 3602), AES-CBC-192 (RFC 3602), AES-CBC-256 (RFC 3602), AES-GCM-128 (RFC 4106), AES-GCM-192 (RFC 4106), AES-GCM-256 (RFC 4106)] به همراه الگوریتم درهم‌سازی امن HMAC مبتنی بر SHA، [انتخاب: HMAC-SHA-1، HMAC-SHA-256، HMAC-SHA-384، HMAC-SHA-512، هیچ الگوریتم دیگری] پیاده‌سازی کند. نکته کاربردی: زمانی که یک الگوریتم AES-CBC انتخاب شود، باید حداقل یک HMAC مبتنی بر SHA نیز انتخاب شود. اگر فقط یک الگوریتم AES-GCM انتخاب شده باشد، HMAC مبتنی بر SHA، تا زمانی که AES-GCM هر دو عملکرد محرمانگی و یکپارچگی را		

برآورده می‌کند، الزامی نیست. ممکن است Isec از یک نسخه کوتاه توابع HMAC مبتنی بر SHA موجود در انتخاب‌ها، استفاده کند. در صورت استفاده از خروجی کوتاه، باید در TSS مشخص شود.		
FCS_IPSEC_EXT.1.5	الزامات پروتکل IPSEC (۵)	۸۸
توابع امنیتی هدف ارزیابی باید یکی از این پروتکل‌ها را پیاده‌سازی کند: [انتخاب: • IKEv1، با استفاده از مد اصلی برای تبادلات^۱ در فاز اول، طبق آنچه که در RFCs 2407,2408,2409, RFC 4109، [انتخاب: هیچ RFC دیگر برای اعداد متوالی بسط‌یافته، RFC4304 برای اعداد متوالی بسط‌یافته] و [انتخاب: هیچ RFC دیگر برای توابع درهم‌ساز، RFC 4868 برای توابع درهم‌ساز] • IKEv2، مطابق با آنچه که در RFC 5996 تشریح شده است و [انتخاب: بدون پشتیبانی از پیمایش NAT^۲، با پشتیبانی اجباری از پیمایش NAT چنان که در بخش ۲،۲۳ از RFC 5996 تشریح شده است] و [انتخاب: هیچ RFC دیگر برای توابع درهم‌ساز، RFC 4868 برای توابع درهم‌ساز]]. نکته کاربردی: اگر محصول مورد ارزیابی برای دو پروتکل IKEv1 یا IKEv2 از الگوریتم درهم‌ساز SHA-2 استفاده کند، نویسنده سند هدف امنیتی باید RFC 4868 را انتخاب نماید. اگر هدف ارزیابی از HMAC های کوتاه شده مبتنی بر SHA، همانطور که در RFC 4868 شرح داده شده است، استفاده کند، باید در TSS مشخص شود.		
FCS_IPSEC_EXT.1.6	الزامات پروتکل IPSEC (۶)	۸۹
توابع امنیتی هدف ارزیابی باید اطمینان حاصل کند که برای رمزگذاری پی‌آیند^۳ در پروتکل [انتخاب: IKEv2, IKEv1]، از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128، AES-CBC-192، AES-CBC-256، AES-GCM-128، AES-GCM-192، AES-GCM-256] استفاده شده است. الگوریتم‌های رمزنگاری AES-CBC-128، AES-CBC-192 و AES-CBC-256 در RFC 3602 تشریح شده‌اند. همچنین AES-GCM-128، AES-GCM-192 و AES-GCM-256 در RFC5282 تشریح شده‌اند. نکته کاربردی: AES-GCM-128، AES-GCM-192 و AES-GCM-256 تنها در صورتی انتخاب می‌شوند که IKEv2 نیز انتخاب شده باشد، همچنین هیچ RFC ای وجود ندارد که AES-GCM را برای IKEv1 تعریف کرده باشد.		
FCS_IPSEC_EXT.1.7	الزامات پروتکل IPSEC (۷)	۹۰

^۱ exchanges

^۲ NAT traversal

^۳ Payload

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

- سرپرست امنیتی می تواند طول عمر SA فاز اول IKEv1 را بر اساس [انتخاب:
- تعداد بایت ها،

- مدت زمان که مقدار آن را می توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد.
- [

پیکر بندی کند.

- سرپرست امنیتی می تواند طول عمر IKEv2 SA را بر اساس [انتخاب:
- تعداد بایت ها،

- مدت زمان که مقدار آن را می توان در بازه [اختصاص: اعداد صحیح شامل ۲۴] ساعت قرار داد.
- [

پیکر بندی کند.

نکته کاربردی:

نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در FCS_IPSEC_EXT.1.5 صورت گرفته است) را انتخاب می کند. نویسنده سند هدف امنیتی همچنین طول عمر را بر اساس مقادیر یا بر اساس زمان (ترکیبی از این دو) انتخاب می کند. برای رعایت این الزام، لازم است که مدت زمان توسط سرپرست محصول قابل پیکربندی باشد (بر اساس دستورالعمل هایی که در سند شرح محصول ذکر شده اند). محدودیت های Hardcoded این الزام را برآورده نمی کند. به طور کلی، دستورالعمل های مربوط به تنظیم پارامترها شامل مدت زمان های SA را باید در سند شرح محصول در نظر گرفت.

FCS_IPSEC_EXT.1.8

الزامات پروتکل IPSEC (۸)

۹۱

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

- سرپرست امنیتی می تواند طول عمر SA فاز دوم IKEv1 را بر اساس [انتخاب:
- تعداد بایت ها،

- مدت زمان که مقدار آن را می توان در بازه [اختصاص: اعداد صحیح شامل ۸] ساعت قرار داد.
- [

پیکربندی کند.

- سرپرست امنیتی می تواند طول عمر IKEv2 Child SA را بر اساس [انتخاب:
- تعداد بایت ها،

- مدت زمان که مقدار آن را می توان در بازه [اختصاص: اعداد صحیح شامل ۸] ساعت قرار داد.
- [

پیکربندی کند.

نکته کاربردی:

نویسنده سند هدف امنیتی الزامات IKEv1 یا الزامات IKEv2 (و یا هر دو، بسته به انتخابی که در FCS_IPSEC_EXT.1.5 صورت گرفته است) را انتخاب می کند. نویسنده سند هدف امنیتی همچنین طول عمر را بر اساس مقادیر یا بر اساس زمان (ترکیبی از این دو) انتخاب می کند. برای رعایت این الزام، لازم است که مدت زمان توسط سرپرست محصول قابل پیکربندی باشد (بر اساس دستورالعمل هایی که در سند شرح محصول ذکر شده اند). محدودیت های Hardcoded این الزام را برآورده نمی کند. به طور کلی، دستورالعمل های مربوط به تنظیم پارامترها شامل مدت زمان های SA را باید در سند شرح محصول در نظر گرفت.

FCS_IPSEC_EXT.1.9	الزامات پروتکل IPSEC (۹)	۹۲
-------------------	--------------------------	----

توابع امنیتی هدف ارزیابی باید مقدار x را که در تبادل کلید IKE DiffieHellman (x در $g^x \bmod p$) به کار می رود، با استفاده از تولیدکننده بیت تصادفی که در الزام FCS_RBGT_EXT.1 مشخص شده است و دست کم طول آن [اختصاص: تعداد بیت های (یک یا بیش از یک) باشد که حداقل دو برابر قدرت امنیتی گروه Diffie-Hellman مذاکره شده باشد] تولید نماید.

نکته کاربردی:

از آنجایی که در پیاده سازی ممکن است گروه های مختلف Diffie-Hellman در مذاکره برای استفاده در SA مجاز باشند الزام FCS_IPSEC_EXT.1.9 می تواند مقادیر متعددی داشته باشند. نویسند سند هدف امنیتی برای هر گروه DH مورد پشتیبانی، از جدول ۲ در دفترچه NIST SP 800-57 «توصیه هایی برای مدیریت کلید - بخش اول: عمومی» برای تعیین قدرت امنیتی («تعداد بیت های امنیتی») مربوط به گروه DH راهنمایی بگیرد. سپس هر ارزش منحصر به فرد برای پر کردن قسمت اختصاص هر مورد به کار می رود. برای مثال، اگر فرض کنیم در پیاده سازی گروه DH ۱۴ (2048-bit MODP) و گروه ۲۰ (ECDH) با استفاده Curve P-384 در NIST پشتیبانی می شود، با توجه به جدول ۲، تعداد بیت های امنیتی برای گروه ۱۴، ۱۱۲ و برای گروه ۲۰، ۱۹۲ است.

FCS_IPSEC_EXT.1.10	الزامات پروتکل IPSEC (۱۰)	۹۳
--------------------	---------------------------	----

توابع امنیتی هدف ارزیابی باید نانس‌های مورد استفاده در تبادلات [انتخاب: IKEv1، IKEv2] با طول [انتخاب:

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

نکته کاربردی:

اگر IKEv2 نیز انتخاب شده باشد (همان طور که در RFC5996 اجباری شده است)، نویسنده سند هدف امنیتی باید دومین گزینه را برای طول نانس انتخاب کند. نویسنده سند هدف امنیتی مجاز است هر یک از گزینه‌ها را برای IKEv1 انتخاب نماید. در اولین گزینه برای طول نانس، از آنجایی که در پیاده‌سازی ممکن است مذاکره کردن برای استفاده از گروه‌های مختلف Diffie-Hellman در ساخت تضمین‌های امنیتی مجاز باشد، اختصاص FCS_IPSEC_EXT.1.10 می‌تواند مقادیر متعددی داشته باشد. نویسنده سند هدف امنیتی برای هر گروه DH مورد پشتیبانی، از جدول ۲ در دفترچه NIST SP 800-57 «توصیه‌هایی برای مدیریت کلید - بخش اول: عمومی» برای تعیین قدرت امنیتی («تعداد بیت‌های امنیتی») مربوط به گروه DH راهنمایی بگیرد. سپس هر ارزش منحصر به فرد برای پر کردن قسمت اختصاص هر مورد به کار می‌رود. برای مثال، اگر فرض کنیم در پیاده‌سازی گروه DH ۱۴ (2048-bit MODP) و گروه ۲۰ (ECDH با استفاده Curve P-384 در NIST) پشتیبانی می‌شود، با توجه به جدول ۲، تعداد بیت‌های امنیتی برای گروه ۱۴، ۱۱۲ و برای گروه ۲۰، ۱۹۲ است. به این دلیل که نانس‌ها ممکن است پیش از اینکه در مورد گروه DH مذاکره شود، مبادله شوند، توصیه می‌شود نانس به کاررفته به اندازه کافی بزرگ باشد که همه پیشنهادها محصول انتخاب شده در تبادلات را پشتیبانی نماید.

FCS_IPSEC_EXT.1.11	الزامات پروتکل IPSEC (۱۱)	۹۴
--------------------	----------------------------------	-----------

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که همه پروتکل‌های IKE، گروه‌های DH [انتخاب: ۱۴ (2048-bit MODP)، ۱۵ (3072-bit MODP)، ۱۶ (4096-bit MODP)، ۱۷ (6144-bit MODP)، ۱۸ (8192-bit MODP)] با توجه به RFC 3526 - [انتخاب: ۱۹ (2048-bit Random ECP)، ۲۰ (384-bit Random ECP)، ۲۱ (521-bit Random ECP)، ۲۴ (2048-bit MODP به همراه 256-bit POS)] با توجه به RFC 5114 [را پشتیبانی می‌کنند.

FCS_IPSEC_EXT.1.12	الزامات پروتکل IPSEC (۱۲)	۹۵
--------------------	----------------------------------	-----------

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

نکته کاربردی:

نویسنده سند هدف امنیتی یکی یا هر دوی انتخاب‌های IKE را بر اساس اینکه کدام یک توسط محصول پیاده‌سازی می‌شود، انتخاب می‌کند.

FCS_IPSEC_EXT.1.13	الزامات پروتکل IPSEC (۱۳)	۹۶
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که همه پروتکل های IKE احراز هویت همتا را با استفاده از [انتخاب: RSA, ECDSA] که از گواهی های X.509v3 مطابق با RFC4945 و [انتخاب: کلیدهای پیش اشتراکی، هیچ روش دیگری] استفاده می کند، انجام می دهند. نکته کاربردی: حداقل یک روش احراز هویت همتا مبتنی بر کلید عمومی مطابق با این پرو فایل حفاظتی مورد نیاز است؛ یک یا چند طرح کلید عمومی توسط نویسنده هدف امنیتی انتخاب می شود تا مشخص شود چه چیزی پیاده سازی شده است. نویسنده هدف امنیتی همچنین اطمینان حاصل می کند که الزامات FCS الگوریتم های مورد استفاده به منظور پشتیبانی از آن روش ها را لیست کرده است (قابلیت های تولید کلید، اگر فراهم شده است). قابل ذکر است TSS شرح خواهد داد کدام یک از این الگوریتم ها استفاده شده است (برای مثال، RFC2409 سه روش احراز هویت با استفاده از کلیدهای عمومی؛ هر یک از پشتیبانی شده ها در TSS شرح داده خواهد شد).		
FCS_IPSEC_EXT.1.14	الزامات پروتکل IPSEC (۱۴)	۹۷
توابع امنیتی هدف ارزیابی باید کانال امن را فقط در صورتی که شناسه ارائه شده در گواهینامه دریافت شده با شناسه پیکربندی شده مرجع تطابق داشته، و شناسه ارائه شده و مرجع یکی از انواع [انتخاب: SAN: آدرس IP، SAN: نام کامل واجد شرایط دامنه (FQDN)^۱، SAN: کاربر FQDN، CN: آدرس IP، CN: نام کامل واجد شرایط دامنه (FQDN) نام مشخص شده^۲ (DN) و [انتخاب: هیچ نوع شناسه مرجع دیگری، [اختصاص: سایر انواع شناسه مرجع پشتیبانی شده]] باشد، برقرار سازد. نکته کاربردی: زمانی که از گواهینامه های RSA یا ECDSA برای احراز هویت همتا استفاده شود، شناسه و گواهینامه های ارائه شده به شکل DN، آدرس IP، FQDN یا FQDN کاربر می باشند. شناسه مرجع، شناسه ای است که هدف ارزیابی انتظار دارد در طول احراز هویت IKE از همتا دریافت شود. شناسه ارائه شده، شناسه ای است که در گواهینامه همتا قرار دارد. نویسنده هدف امنیتی باید انواع شناسه ارائه شده و مرجع پشتیبانی شده را انتخاب کند و ممکن است به صورت اختیاری انواع پشتیبانی شده بیشتری را نیز در انتخاب دوم اختصاص دهد. به جز نوع شناسه DN، ممکن است هدف ارزیابی شناسه را در نام عمومی یا Subject Alternative Name (SAN) یا هردو، پشتیبانی کند. Subject Alternative Name با استفاده از نام های DNS، نام های URI یا نام های Service، روش ترجیحی برای تایید است. تایید با استفاده از نام عمومی برای هدف پس سازگاری^۳ مورد نیاز است. علاوه بر این، ممکن است استفاده از آدرس IP در Subject Name یا Subject Alternative Name پشتیبانی شود ولی برای بهترین روش، ممنوع است. الگوریتم های گواهینامه همتای پشتیبانی شده همانند FCS_IPSEC_EXT.1.13 هستند.		

^۱ Fully Qualified Domain Name

^۲ Distinguished name

^۳ backwards compatibility



۷-۲-۷- الزامات پروتکل NTP

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

۷-۲-۸- الزامات پروتکل SSH Client

شماره الزام	نام الزام	
۱۰۲	الزامات پروتکل SSH Client (۱)	FCS_SSHC_EXT.1.1

توابع امنیتی هدف ارزیابی باید پروتکل SSH را مطابق با RFC های [انتخاب: 4251, 4252, 4253, 4254, 5647, 5656, 6187, 8332, 6668] پیاده سازی نماید.

نکته کاربردی:

نویسنده سند هدف امنیتی انتخاب می کند که مطابقت با کدام یک از RFC های وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً، الگوریتم های رمزنگاری معتبر). RFC4253 مشخص می کند که الگوریتم های رمزنگاری خاصی "REQUIRED" (مورد نیاز) هستند. در نتیجه، پشتیبانی از این الگوریتم ها باید پیاده سازی شوند، نه اینکه صرفاً امکان استفاده از آن ها وجود داشته باشد. اطمینان حاصل نمایید الگوریتم های اجرا شده ای که با عنوان "REQUIRED" مشخص شده اند ولی در عناصر بعد از این بخش لیست نشده اند، خارج از محدوده فعالیت ارزیابی برای این الزام باشند.

RFC 5647 only applies to the RFC compliant implementation of GCM; a TOE that only implements the "@openssh.com" variant of GCM should not select 5647. aes*- gcm@openssh.com is specified in Section 1.6 of the OpenSSH Protocol Specification (<https://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/PROTOCOL?rev=1.31>).

FCS_SSHC_EXT.1.2	الزامات پروتکل SSH Client (۲)	۱۰۳
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده سازی پروتکل SSH، روش های احراز هویت زیر مطابق با آنچه که در RFC4252 توضیح داده شده است، پشتیبانی می شوند: احراز هویت مبتنی بر کلید عمومی، [انتخاب: احراز هویت مبتنی بر کلمه عبور، هیچ روش دیگری].		

FCS_SSHC_EXT.1.3	الزامات پروتکل SSH Client (۳)	۱۰۴
همان طور که در RFC4253 توضیح داده شده است، توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که بسته های دارای بایت های بیشتر از [اختصاص: تعداد بایت ها] در یک ارتباطات انتقال SSH کنار گذاشته شوند.		
نکته کاربردی:		
RFC4253 امکان پذیرش «بسته های بزرگ» را فراهم می کند، با این اخطار که بسته ها باید «طول مناسبی» داشته باشند یا اینکه کنار گذاشته می شوند. توصیه می شود این اختصاص توسط نویسنده هدف امنیتی با در نظر گرفتن بیشترین اندازه بسته که قابل پذیرش است پر شود تا به این وسیله «طول مناسب» برای محصول تعریف شود.		

FCS_SSHC_EXT.1.4	الزامات پروتکل SSH Client (۴)	۱۰۵
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده سازی انتقال SSH، از الگوریتم های رمزنگاری [انتخاب: aes128-cbc, aes128-ctr, aes256-cbc, aes128-ctr, aes256-ctr, AEAD_AES_128_GCM, AEAD_AES_256_GCM, aes128-gcm@openssh.com, aes256-gcm@openssh.com] استفاده می شود و سایر الگوریتم های رمزنگاری رد می شوند.		

نکته کاربردی:

RFC 5647 استفاده از الگوریتم های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می کند. همانطور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم MAC استفاده شده باشد،

الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM فقط به عنوان الگوریتم‌های رمزنگاری قابل انتخاب هستند. در سند هدف امنیتی، ورودی‌های متناظر FCS_COP برای الگوریتم‌های انتخاب شده در اینجا هستند.		
FCS_SSHC_EXT.1.5	الزامات پروتکل SSH Client (۵)	۱۰۶
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که پیاده‌سازی احراز هویت مبتنی بر کلید عمومی SSH، از انتخاب [x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-, ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256 x509v3-, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256 nistp521 rsa2048-sha256] به عنوان الگوریتم‌های کلید عمومی خودش استفاده می‌کند و سایر الگوریتم‌های کلید عمومی رد می‌شوند. نکته کاربردی: اگر x509v3-ssh-rsa, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384 یا x509v3-rsa2048-sha256 انتخاب شده باشند، باید لیستی از گواهینامه‌های معتبر مجاز از FCS_SSHC_EXT.1.9 انتخاب شوند و SFR های FIA_X509_EXT در پیوست B، کاربردی هستند. It is recommended to configure the TOE to reject presented RSA keys with a key length below 2048 bit. RFC 8332 specifies the use of rsa-sha2-256 or rsa-sha2-512 in SSH.		
FCS_SSHC_EXT.1.6	الزامات پروتکل SSH Client (۶)	۱۰۷
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل انتقال SSH، از انتخاب: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512, AEAD_AES_128_GCM, AEAD_AES_256_GCM, MAC به عنوان الگوریتم‌های MAC صحت داده‌ها استفاده می‌شود و سایر الگوریتم‌های MAC رد می‌شوند. نکته کاربردی ۹۹: RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌کند. همانطور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم‌های رمزنگاری استفاده شده باشد، الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM فقط به عنوان الگوریتم MAC قابل انتخاب هستند. در سند هدف امنیتی، ورودی‌های متناظر FCS_COP برای الگوریتم‌های انتخاب شده در اینجا هستند. RFC 6668 استفاده از الگوریتم‌های sha2 در SSH را مشخص می‌کند.		
FCS_SSHC_EXT.1.7	الزامات پروتکل SSH Client (۷)	۱۰۸
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdh-sha2-nistp256] و [انتخاب: group15-sha512, ecdh-sha2-nistp256, diffie-hellman-group17-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp384, ecdh-sha2-nistp521, هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.		
FCS_SSHC_EXT.1.8	الزامات پروتکل SSH Client (۸)	۱۰۹

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در اتصالات SSH کلیدهای یکسان برای آستانه بیشتر از یک ساعت و بیشتر از یک گیگابایت تبادل داده، استفاده نشود. لازم است پس از رسیدن به هر یک از آستانه‌ها، تجدید کلید انجام شود.

نکته کاربردی:

این الزام، دو آستانه تعریف می‌کند. یکی برای حداکثر فاصله زمانی که کلیدهای همان نشست می‌توانند استفاده شوند، و دیگری برای حداکثر مقدار داده‌ای که می‌توان با کلیدهای همان نشست انتقال داد. هر دو آستانه باید اجرا شوند و تجدید کلید باید روی هر کدام از آستانه‌ها که زودتر رسید، انجام شود. برای آستانه حداکثر داده منتقل شده، باید مجموع داده‌های ورودی و خروجی محاسبه شود. تجدید کلید بر روی تمامی کلیدها (رمزنگاری، حفظ صحت) برای ترافیک ورودی و خروجی اعمال می‌شود.

برای هدف ارزیابی، اجرای آستانه‌های کمتر از حداکثر مقادیر تعریف شده در الزام قابل قبول است. برای هر آستانه قابل تنظیم مربوط به این الزام، باید سند راهنما نحوه تنظیم آستانه را مشخص کند. مقادیر مجاز باید هم در سند راهنما مشخص شوند و هم باید کمتر یا برابر آستانه‌های مشخص شده در این الزام باشند، یا هدف ارزیابی نباید مقادیر خارج از آستانه‌های تعریف شده در این الزام را بپذیرد.

۱۱۰	الزامات پروتکل SSH Client (۹)	FCS_SSHC_EXT.1.9
-----	-------------------------------	------------------

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که کاربر SSH، سرور SSH را با استفاده از یک پایگاه داده محلی احراز هویت می‌کند و نام هر میزبان را با کلید عمومی متناظر آن یا [انتخاب: فهرستی از مراجع صدور گواهی مطمئن، هیچ روش دیگری] همان‌طور که در RFC 4251 بخش ۴،۱ تشریح شده است مطابقت می‌دهد.

نکته کاربردی:

تنها در صورتی می‌توان گزینه «لیست مراجع صدور گواهی مطمئن» را انتخاب کرد که x509v3-ecdsa-sha2-nistp256 یا x509v3-ecdsa-sha2-nistp521 در FCS_SSHC_EXT.1.5 انتخاب شده باشد.

۷-۲-۹- الزامات پروتکل SSH Server

شماره الزام	نام الزام	
۱۱۱	الزامات پروتکل SSH Server (۱)	FCS_SSHS_EXT.1.1
توابع امنیتی هدف ارزیابی باید پروتکل SSH مطابق با RFC های ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، [انتخاب: ۴۲۵۶، ۴۳۴۴، ۵۶۴۷، ۵۶۵۶، ۶۱۸۷، ۶۶۶۸، ۸۳۰۸، ۸۲۶۸، ۸۳۳۲] پیاده‌سازی نماید.		
نکته کاربردی:		
نویسنده سند هدف امنیتی انتخاب می‌کند که مطابقت با کدام یک از RFC های وجود دارد. توجه کنید که این موضوع باید با انتخاب سایر الزامات مطرح شده، مطابقت داشته باشند (مثلاً، الگوریتم‌های رمزنگاری معتبر). RFC4253 مشخص می‌کند که الگوریتم‌های رمزنگاری خاصی "REQUIRED" (موردنیاز) هستند. در نتیجه، پشتیبانی از این الگوریتم‌ها باید پیاده‌سازی شوند،		

نه اینکه صرفاً امکان استفاده از آن‌ها وجود داشته باشد. اطمینان حاصل نمایید الگوریتم‌های اجرا شده‌ای که با عنوان "REQUIRED" مشخص شده‌اند ولی در عناصر بعد از این بخش لیست نشده‌اند، خارج از محدوده فعالیت ارزیابی برای این الزام باشند.

۱۱۲	الزامات پروتکل SSH Server (۲)	FCS_SSHS_EXT.1.2
-----	-------------------------------	------------------

توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده‌سازی پروتکل SSH، همان‌طور که در RFC4252 توضیح داده شده است، روش‌های احراز هویت زیر پشتیبانی می‌شوند: مبتنی بر کلید عمومی، مبتنی بر کلمه عبور.

۱۱۳	الزامات پروتکل SSH Server (۳)	FCS_SSHS_EXT.1.3
-----	-------------------------------	------------------

همان‌طور که در RFC4253 توضیح داده شده است، محصول باید اطمینان حاصل نماید که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک اتصال انتقال SSH کنار گذاشته شوند.

نکته کاربردی:

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

۱۱۴	الزامات پروتکل SSH Server (۴)	FCS_SSHS_EXT.1.4
-----	-------------------------------	------------------

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

نکته کاربردی:

RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌کند. همان‌طور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم MAC استفاده شده باشد، الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM فقط به عنوان الگوریتم‌های رمزنگاری قابل انتخاب هستند. در سند هدف امنیتی، ورودی‌های متناظر FCS_COP برای الگوریتم‌های انتخاب شده در اینجا هستند.

۱۱۵	الزامات پروتکل SSH Server (۵)	FCS_SSHS_EXT.1.5
-----	-------------------------------	------------------

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

نکته کاربردی:

اگر x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384 یا x509v3-ecdsa-sha2-nistp521 انتخاب شده باشند، SFRهای FIA_X509_EXT در پیوست B، کاربردی هستند.

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

FCS_SSHS_EXT.1.6	الزامات پروتکل SSH Server (۶)	۱۱۶
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که در پیاده سازی پروتکل انتقال SSH، از [انتخاب: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256] به عنوان الگوریتم های MAC صحت داده ها استفاده می شود و سایر الگوریتم های MAC صحت داده ها رد می شوند. نکته کاربردی: RFC 5647 استفاده از الگوریتم های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می کند. همانطور که در RFC 5647 شرح داده شده است، زمانی که الگوریتم مشابهی به عنوان الگوریتم های رمزنگاری استفاده شده باشد، الگوریتم های AEAD_AES_128_GCM و AEAD_AES_256_GCM فقط به عنوان الگوریتم MAC قابل انتخاب هستند. در سند هدف امنیتی، ورودی های متناظر FCS_COP برای الگوریتم های انتخاب شده در اینجا هستند. RFC 6668 استفاده از الگوریتم های sha2 در SSH را مشخص می کند.		
FCS_SSHS_EXT.1.7	الزامات پروتکل SSH Server (۷)	۱۱۷
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که [انتخاب: diffie-hellman-group14-sha1, diffie-hellman-group15-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group17-sha512, diffie-hellmangroup18-sha512, group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group17-sha512, diffie-hellmangroup18-sha512] هیچ روش دیگری [تنها روش های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می روند].		
FCS_SSHS_EXT.1.8	الزامات پروتکل SSH Server (۸)	۱۱۸
توابع امنیتی هدف ارزیابی باید اطمینان حاصل نماید که اتصالات SSH کلیدهای یکسان برای آستانه بیشتر از یک ساعت و بیشتر از یک گیگابایت تبادل داده، استفاده نشود. لازم است پس از رسیدن به هر یک از آستانه ها، تجدید کلید انجام شود. نکته کاربردی: این الزام، دو آستانه تعریف می کند. یکی برای حداکثر فاصله زمانی که کلیدهای همان نشست می توانند استفاده شوند، و دیگری برای حداکثر مقدار داده ای که می توان با کلیدهای همان نشست انتقال داد. هر دو آستانه باید اجرا شوند و تجدید کلید باید روی هر کدام از آستانه ها که زودتر رسید، انجام شود. برای آستانه حداکثر داده منتقل شده، باید مجموع داده های ورودی و خروجی محاسبه شود. تجدید کلید بر روی تمامی کلیدها (رمزنگاری، حفظ صحت) برای ترافیک ورودی و خروجی اعمال می شود. برای هدف ارزیابی، اجرای آستانه های کمتر از حداکثر مقادیر تعریف شده در الزام قابل قبول است. برای هر آستانه قابل تنظیم مربوط به این الزام، باید سند راهنما نحوه تنظیم آستانه را مشخص کند. مقادیر مجاز باید هم در سند راهنما مشخص شوند و هم باید کمتر یا برابر آستانه های مشخص شده در این الزام باشند، یا هدف ارزیابی نباید مقادیر خارج از آستانه های تعریف شده در این الزام را بپذیرد.		

۷-۲-۱۰- الزامات پروتکل TLS Client



نام الزام		شماره الزام
FCS_TLSC_EXT.1.1	الزامات پروتکل TLS Client	۱۱۹
توابع امنیتی هدف ارزیابی باید [انتخاب: TLS 1.2 (RFC5246), TLS 1.1 (RFC 4346)] را پیاده‌سازی کرده و تمامی نسخه‌های TLS و SSL را رد نماید. پیاده‌سازی توابع امنیتی هدف ارزیابی باید با پشتیبانی از مجموعه‌های رمز زیر باشد: ○ [انتخاب: ○ TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268] ○ TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 ○ TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 ○ TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288 ○ TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 ○ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288 ○ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 ○ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288 ○ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		

○ RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با

[[.

نکته کاربردی:

مجموعه رمزهای آزمایش شده در تنظیمات ارزیابی توسط این الزام محدود می‌شوند. نویسنده هدف امنیتی باید مجموعه رمزهایی که پشتیبانی می‌شوند را انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با نسخه دوم ND CPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 5246 وجود داشته باشد، الزامی است. به علت اینکه نسخه‌های جدید TLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند. در نسخه آینده این CPP، نسخه ۱٫۲ TLS برای تمامی اهداف ارزیابی الزامی خواهد بود.

FCS_TLSC_EXT.1.2

الزامات پروتکل TLS Client

۱۲۰

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

نکته کاربردی:

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

روش مورد ترجیح برای تأیید این است که Subject Alternative Name از نام DNS، نام URL، یا نام سرویس استفاده کند. برای هدف پس‌سازگاری^۱ تأیید با استفاده از نام عمومی مورد نیاز است. علاوه بر این، ممکن است استفاده از آدرس IP در Subject Name یا Subject Alternative Name پشتیبانی شود ولی برای بهترین روش، ممنوع است. در نهایت، کلاینت باید

^۱ backwards compatibility

از ایجاد شناسه‌های مرجع با استفاده از wildcards اجتناب نماید. هرچند، اگر شناسه‌های ارائه شده حاوی wildcards باشند، کلاینت باید از بهترین روش منطبق پیروی کند؛ این بهترین شیوه‌ها در فعالیت ارزیابی بدست می‌آیند.

۱۲۱	الزامات پروتکل TLS Client	FCS_TLSC_EXT.1.3
توابع امنیتی هدف ارزیابی باید فقط در صورتی که گواهینامه سرور معتبر باشد کانال امن را برقرار سازد. همچنین توابع امنیتی هدف ارزیابی باید [انتخاب]: - هیچ مکانیزم لغو سرپرستی پیاده سازی نشود. - در صورت شکست توابع امنیتی هدف ارزیابی، به مجوز مدیریت برای ایجاد ارتباط به [انتخاب]: مطابقت با شناسه مرجع، تأیید مسیر گواهی، تأیید تاریخ انقضاء، تعیین وضعیت لغو] از گواهی سرور ارائه شده نیاز دارید.]		

نکته کاربردی:

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

۱۲۲	الزامات پروتکل TLS Client	FCS_TLSC_EXT.1.4
توابع امنیتی هدف ارزیابی باید در Client Hello، [انتخاب: Supported Elliptic Curves Extension] را ارائه ندهد، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب: ffdhe8192, ffdhe6144, ffdhe4096, ffdhe3072, ffdhe2048, secp521r1, secp384r1, secp256r1] ارائه دهد و هیچ منحنی دیگری]		

نکته کاربردی:

اگر در FCS_TLSC_EXT.1.1 مجموعه‌های رمز بیضوی انتخاب شده باشند، انتخاب یک یا چند مورد از منحنی‌ها الزامی است. اگر در FCS_TLSC_EXT.1.1 هیچ کدام از مجموعه‌های رمز بیضوی انتخاب نشده باشند، سپس "عدم نمایش افزونه پشتیبانی منحنی های بیضوی" باید انتخاب شود.

این الزام مجموعه رمزهای بیضوی مجاز برای احراز هویت و توافق کلید را به NIST curve های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازند. این افزونه برای کاربرانی که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.

۷-۲-۱۱- الزامات پروتکل TLS Client / احراز هویت

شماره الزام	نام الزام
۱۲۳	الزامات پروتکل TLS Client / احراز هویت ۱
	FCS_TLSC_EXT.2.1



توابع امنیتی هدف ارزیابی باید با استفاده از گواهینامه X.509v3، از احراز هویت دوطرفه پشتیبانی نماید.

۷-۲-۱۲- الزامات پروتکل TLS Server

شماره الزام	نام الزام
۱۲۴	الزامات پروتکل TLS Server ۱
FCS_TLSS_EXT.1.1	
توابع امنیتی هدف ارزیابی باید [انتخاب: TLS 1.2 (RFC5246), TLS1.1 (RFC4346)] را پیاده‌سازی نماید و تمامی نسخه‌های TLS و SSL دیگر را رد نماید. پیاده‌سازی توابع امنیتی هدف ارزیابی باید از مجموعه‌های رمز زیر پشتیبانی نماید: انتخاب: ○ TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 ○ TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 ○ TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246 ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246 ○ TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288 ○ TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 ○ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288 ○ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 ○ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289	

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289

].

نکته کاربردی:

مجموعه‌های رمز که باید در پیکربندی ارزیابی تست شوند، توسط این الزام محدود شده‌اند. نویسنده هدف امنیتی باید مجموعه رمزهایی که پشتیبانی می‌شوند را انتخاب نماید. در محیط آزمایش، محدود کردن مجموعه رمزهایی که می‌توانند در تنظیمات ارزیابی مدیریتی بر روی سرور استفاده شوند ضروری است. TLS_RSA_WITH_AES_128_CBC_SHA برای انطباق با نسخه دوم ND CPP اجباری نیست؛ هرچند، اگر ادعای انطباق با RFC 5246 وجود داشته باشد، الزامی است. به علت اینکه نسخه‌های جدید TLS توسط IETF استاندارد شده‌اند، این الزامات مجدداً مورد بررسی قرار می‌گیرند. در نسخه آینده این CPP، نسخه ۱,۲ TLS برای تمامی اهداف ارزیابی الزامی خواهد بود.

۱۲۵	الزامات پروتکل TLS Server ۲	FCS_TLSS_EXT.1.2
توابع امنیتی هدف ارزیابی باید اتصال‌های کاربرانی را که درخواست SSL2.0، SSL3.0، TLS1.0 و [انتخاب: TLS1.1، TLS1.2، هیچ‌کدام] دارند، رد نماید. نکته کاربردی: تمام نسخه‌های SSL و نسخه TLS 1.0 رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در FCS_TLSS_EXT.1.1 انتخاب نشده است، در اینجا انتخاب شود. در صورتی که گزینه هیچ‌کدام انتخاب شود، عبارت هیچ‌کدام توسط نویسنده سند هدف امنیتی قابل حذف است.		
۱۲۶	الزامات پروتکل TLS Server ۳	FCS_TLSS_EXT.1.3
توابع امنیتی هدف ارزیابی باید [انتخاب: کلید RSA با اندازه کلید [انتخاب: ۲۰۴۸ بیت و ۳۰۷۲ بیت، ۴۰۹۶ بیت] پیاده‌سازی کند، پارامترهای EC Diffie-Hellman را بر روی منحنی‌های NIST [انتخاب: secp256r1، secp384r1، secp521r1] و هیچ منحنی دیگری تولید کند، پارامترهای Diffie-Hellman را با اندازه [انتخاب: ۳۰۷۲ بیت، ۲۰۴۸ بیت، ۴۰۹۶ بیت، ۶۱۴۴ بیت، ۸۱۹۲ بیت] همچنین گروه‌های Diffie-Hellman را با [انتخاب: fdhe2048، ffdhe3072، ffdhe4096، ffdhe6144، ffdhe8192] ایجاد نماید]. نکته کاربردی: اگر در بخش FCS_TLSS_EXT.1.1 سند هدف امنیتی مجموعه رمزهای DHE یا ECDHE لیست شده باشند، سند هدف امنیتی باید شامل Diffie-Hellman یا منحنی‌های NIST لیست شده در این الزام باشد. FMT_SMF.1 تنظیمات پارامترهای پذیرش کلید برای برقراری قدرت امنیتی ارتباط TLS، الزامی می‌کند.		
۱۲۷	الزامات پروتکل TLS Server ۴	FCS_TLSS_EXT.1.4
توابع امنیتی هدف ارزیابی باید از [انتخاب: بدون از سرگیری نشست یا بلیط نشست، از سرگیری نشست براساس شناسه‌های نشست با توجه به RFC4346(TLS1.1) یا RFC		



از سرگیری نشست مبتنی بر بلیط های با توجه به RFC 5077 [پشتیبانی کنند. TLS1.2) 5246،

۷-۲-۱۳- الزامات پروتکل TLS Server همراه با احراز هویت دو طرفه

شماره الزام	نام الزام
۱۲۸	الزامات پروتکل TLS Server / احراز هویت دوطرفه ۱
توابع امنیتی هدف ارزیابی باید در ارتباط TLS با احراز هویت دوطرفه TLS کلاینتها، از گواهینامه های X509v3 استفاده کند.	
۱۲۹	الزامات پروتکل TLS Server / احراز هویت دوطرفه ۲
زمانی که کانال مورد اعتماد ایجاد می شود، اگر گواهینامه کلاینت معتبر نباشد به صورت پیش فرض توابع امنیتی هدف ارزیابی نباید یک کانال مورد اعتماد را ایجاد کند. همچنین توابع امنیتی هدف ارزیابی باید: [انتخاب: - هیچ مکانیزم لغو سرپرستی را اجرا نکند. - در صورت عدم موفقیت توابع امنیتی هدف ارزیابی در [انتخاب: تطابق با شناسه مرجع، تأیید مسیر گواهینامه، تأیید تاریخ انقضا، تعیین وضعیت ابطال] گواهینامه مشتری ارائه شده، به مجوز سرپرست برای برقراری ارتباط نیاز دارد.]	
۱۳۰	الزامات پروتکل TLS Server / احراز هویت دوطرفه ۳
اگر شناسه مندرج در یک گواهینامه با شناسه مورد انتظار کلاینت مطابقت نداشته باشد، توابع امنیتی هدف ارزیابی نباید یک کانال قابل اعتماد ایجاد کند. اگر شناسه یک FQDN باشد آنگاه توابع امنیتی هدف ارزیابی باید شناسه ها را با توجه به RFC 6125 با هم انطباق دهد، در غیر این صورت توابع امنیتی هدف ارزیابی باید شناسه را از گواهینامه parse کرده آن را با شناسه مورد انتظار کلاینت که در شرح خلاصه محصول، توصیف شده است، انطباق دهد.	

۷-۳-۳- کلاس شناسایی و احراز هویت

۷-۳-۱- الزامات پروتکل X509

شماره الزام	نام الزام
۱۳۱	اعتبارسنجی گواهینامه X509 (۱)
توابع امنیتی مورد ارزیابی باید گواهی نامه ها را بر اساس قوانین زیر تأیید کند:	

- تأیید گواهی نامه RFC 5280 و تأیید مسیر گواهی نامه با پشتیبانی از حداقل طول مسیر از سه گواهی نامه
- مسیر گواهی نامه باید با یک گواهی نامه CA امن پایان یابد.
- توابع امنیتی مورد ارزیابی باید برای تأیید یک مسیر گواهی نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی نامه های CA به حالت «True» تنظیم شده است.
- توابع امنیتی مورد ارزیابی باید وضعیت فسخ گواهی نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی نامه آنلاین (OCSP) چنان که در RFC 6960 تعریف شده است، لیست فسخ گواهی نامه (CRL) چنان که در بخش ۵ از RFC 5759 تعریف شده است، لیست فسخ گواهی نامه (CRL) چنان که در بخش ۶،۳ از RFC 5280 تعریف شده است] را تأیید کند
- توابع امنیتی مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تأیید کند:
 - گواهی نامه های مورد استفاده برای به روز رسانی های امن و اعتبار سنجی 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
 - گواهی نامه های سرور ارائه شده برای TLS باید هدف "Server Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.
 - گواهی نامه های کلاینت ارائه شده برای TLS باید هدف "Client Authentication" (id-kp2 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.
 - گواهی نامه های OCSP مورد استفاده برای پاسخ های 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.

FIA_X509_EXT.1.2	اعتبار سنجی گواهی نامه X509 (۲)	۱۳۲
توابع امنیتی مورد ارزیابی تنها در صورتی که افزونه مربوط به basicConstraints ارائه شده باشد و پرچم CA به حالت «TRUE» تنظیم شده باشد، یک گواهی نامه را به عنوان گواهی نامه CA می پذیرد. نکته کاربردی: الزام FIA_X509_EXT.1.1/Rev قوانین تایید گواهی نامه ها را لیست کرده است. نویسنده سند هدف امنیتی وضعیت لغوی که با استفاده از OCSP یا CRL ها تایید می شود، را انتخاب می کند. ممکن است پروتکل های کانال/مسیر امن استفاده از آن گواهی نامه ها را الزام کند. این استفاده مستلزم آن است که قوانین extendedKeyUsage تایید شده باشد. اگر هدف ارزیابی عملکردی را که از هر نوع گواهی نامه لیست شده در قوانین extendedKeyUsage از FIA_X509_EXT.1.1 استفاده می کند، پشتیبانی نکند؛ باید در TSS مشخص شده باشد و بخش مربوط به SFR به طور کلی عملکردهای مورد پذیرش را در نظر می گیرد. هر چند، اگر هدف ارزیابی از عملکردهایی پشتیبانی کند که از هر کدام از انواع این گواهی نامه ها استفاده می کند، باید قوانین متناظر همانند SFR رعایت شوند. هدف ارزیابی باید قادر به پشتیبانی از حداقل طول مسیر سه گواهی نامه باشد. به این معنی که، باید از سلسله مراتبی حاوی حداقل یک گواهی نامه اصلی self-signed، گواهی نامه CA فرعی و گواهی نامه هویت هدف ارزیابی باشد، پشتیبانی کند.		

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

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

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

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

FIA_X509_EXT.2.1	احراز هویت گواهینامه X509 (۱)	۱۳۳
------------------	-------------------------------	-----

توابع امنیتی مورد ارزیابی باید برای پشتیبانی از احراز هویت در [انتخاب: IPsec، TLS، HTTPS، SSH، DTLS] و همچنین برای [انتخاب: امضای کد برای به‌روزرسانی نرم‌افزار سیستم، امضای کد برای تأیید اعتبارسنجی، [اختصاص: سایر کاربردها]، هیچ کاربرد اضافی دیگر] از گواهی‌نامه‌های X.509v3 تعریف شده در RFC 5280 استفاده کند.

FIA_X509_EXT.2.2	احراز هویت گواهینامه X509 (۲)	۱۳۴
------------------	-------------------------------	-----

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

نکته کاربردی:

انتخاب نویسنده هدف امنیتی در FIA_X509_EXT.2.1 شامل IPsec، TLS، HTTPS می‌باشد؛ اگر این پروتکل‌ها در FTP_ITC.1 یا FPT_ITT.1 باشند. اگر احراز هویتی غیر از ssh-rsa، ecdsa-sha2-nistp256، ecdsa-sha2-nistp384 و/یا ecdsa-sha2-nistp521 در FCS_SSHC_EXT.1.5 یا FCS_SSHS_EXT.1.5 انتخاب شده باشد، باید ST حاوی SSH باشد. ممکن است گواهینامه‌ها به صورت اختیاری برای بروزرسانی‌های امن نرم‌افزار سیستم (FPT_TUD_EXT.2) و برای تایید صحت (FPT_TST_EXT.2) استفاده شوند.

معمولاً باید برای بررسی وضعیت لغو یک گواهینامه، دانلود یک CRL یا جستجو با استفاده از OCSP ارتباطی برقرار شود. انتخاب موجود در FIA_X509_EXT.2.2 برای شرح رفتار رویدادی در حالتی است که چنین ارتباطی برقرار نشده باشد (برای مثال، به علت خطای شبکه). اگر هدف ارزیابی، گواهینامه معتبری مطابق تمام قوانین دیگر موجود در FIA_X509_EXT.1 تعیین کرده باشد، رفتار مربوط به انتخاب، اعتبار را تعیین می‌کند. هدف ارزیابی باید گواهینامه را در صورتی که هر قانون



اعتبارسنجی دیگری را در FIA_X509_EXT.1 نفی می‌کند، نپذیرد. اگر گزینه‌های تنظیمات مدیر توسط نویسنده هدف امنیتی انتخاب شده باشد، باید عملکردهای متناظر در FMT_SMF.1 را نیز انتخاب کند. انتخاب باید شامل الزامات اعتبارسنجی FCS_IPSEC_EXT.1.14، FCS_TLSC_EXT.1.3 و FCS_TLSC_EXT.2.3 باشد.

اگر هدف ارزیابی توزیع شده باشد و FIA_X509_EXT.1/ITT انتخاب شده باشد، گواهینامه بررسی لغو اختیاری است. این مورد ناشی از اقدامات احراز هویت اضافی برای فعالسازی و غیرفعالسازی کانال امن داخلی هدف ارزیابی است؛ همانطور که در FCO_CPC_EXT.1 تعریف شده است. در این مورد، ارتباطی برای تایید اعتبار گواهینامه مورد نیاز نیست و این الزام به طور قطعی رعایت می‌شود.

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

FIA_X509_EXT.3.1	درخواست‌های گواهینامه X509 (۱)	۱۳۵
------------------	--------------------------------	-----

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

نکته کاربردی:

کلید عمومی در واقع بخش کلید عمومی از جفت کلیدهای عمومی-خصوصی است که بر اساس آن چه در FCS_CKM.1 شرح داده شده است، توسط هدف ارزیابی تولید می‌شود.

FIA_X509_EXT.3.2	درخواست‌های گواهینامه X509 (۲)	۱۳۶
------------------	--------------------------------	-----

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

۴-۷- کلاس حفاظت از محصول

۷-۴-۱- الزامات به‌روزرسانی امن

FPT_TUD_EXT.2.1	الزامات به‌روزرسانی امن ۴	۱۳۷
توابع امنیتی مورد ارزیابی قبل از نصب هر به‌روزرسانی، اعتبار گواهی امضای کد را بررسی کند.		
FPT_TUD_EXT.2.2	الزامات به‌روزرسانی امن ۵	۱۳۸

^۱ Public Key

^۲ Device-specific information

اگر اطلاعات لغو برای گواهی در زنجیره اعتماد موجود نباشد، گواهینامه معتبری نیست تا به عنوان مهار مطمئن تعیین شده باشد، توابع امنیتی هدف ارزیابی باید [انتخاب: update] را نصب نکند، اجازه بدهد که در این موارد سرپرست محصول در مورد پذیرش update تصمیم بگیرد.		
FPT_TUD_EXT.2.3	الزامات به روزرسانی امن ۶	۱۳۹
هنگامی که گواهینامه به علت انقضای آن، غیر معتبر اعلام شده است، توابع امنیتی هدف ارزیابی باید [انتخاب: اجازه بدهد که در این موارد سرپرست محصول در مورد پذیرش گواهی تصمیم گیری نماید، گواهی را بپذیرد، گواهی را نپذیرد].		
FPT_TUD_EXT.2.4	الزامات به روزرسانی امن ۷	۱۴۰
هنگامی که گواهینامه به علتی غیر از انقضای آن، غیر معتبر اعلام شده است، یا اطلاعات ابطال آن در دست نباشد توابع امنیتی هدف ارزیابی نباید اجازه update دهند.		

۷-۵- کلاس مدیریت امنیت

FMT_MOF.1.1/AutoUpdate	مدیریت رفتار توابع امنیتی/به روزرسانی خودکار ۱	۱۴۱
توابع امنیتی هدف ارزیابی باید قابلیت [انتخاب: فعال سازی، غیرفعال سازی] کارکردهای [انتخاب: جستجو برای به روزرسانی خودکار، به روزرسانی خودکار] را برای سرپرست امنیتی فراهم آورد. نکته کاربردی: این الزام تنها زمانی قابل پیاده سازی است که محصول امکان پشتیبانی از بررسی به روزرسانی خودکار و به روزرسانی خودکار را فراهم کند و اجازه فعال و غیرفعال سازی این قابلیت را بدهد. فعال سازی و غیرفعال سازی قابلیت بررسی به روزرسانی خودکار و/یا به روزرسانی خودکار به سرپرست امنیتی محدود می شود. گزینه "به روزرسانی خودکار" فقط زمانی ممکن است انتخاب شود که از امضاهای دیجیتالی برای اعتبار به روزرسانی امن استفاده شده باشد.		
FMT_MOF.1.1/Functions	مدیریت رفتار توابع امنیتی/به روزرسانی خودکار ۲	۱۴۲
توابع امنیتی هدف ارزیابی باید توانایی [انتخاب: تعیین رفتار، تغییر رفتار] توابع [انتخاب: انتقال داده های ممیزی به موجودیت IT خارجی، مدیریت داده های ممیزی، عملکرد ممیزی زمانی که فضای حافظه محلی ممیزی پر شده باشد] را به سرپرست امنیتی محدود کند. نکته کاربردی: این الزام تنها در صورتی باید انتخاب شود که یک یا چند مورد از سناریوهای زیر اعمال شده باشد: - اگر پروتکل انتقال برای انتقال داده های ممیزی به یک موجودیت IT خارجی، مطابق آنچه که در FAU_STG_EXT.1.1 تعریف شده است قابل تنظیم باشد، گزینه "انتقال داده ممیزی به موجودیت IT خارجی" باید انتخاب شود. - اگر مدیریت داده های ممیزی قابل تنظیم باشد، "مدیریت داده ممیزی" باید انتخاب شود. اصطلاح "مدیریت داده ممیزی" به گزینه های مختلف برای انتخاب و اختصاص در الزامات FAU_STG_EXT.1.2، FAU_STG_EXT.1.3 و FAU_STG_EXT.2/LocSpace اشاره می کند.		

- اگر رفتار عملکرد ممیزی زمان پر شدن فضای ذخیره‌سازی ممیزی محلی قابل تنظیم باشد، گزینه "عملکرد ممیزی زمانی که فضای ذخیره‌سازی ممیزی محلی پر شده باشد" باید انتخاب شود.
- انتخاب اول برای "تعیین رفتار" و "تغییر رفتار" باید به صورت مناسب انتخاب شود. ممکن است بر اساس انتخاب دوم، لازم به انتخاب‌های مختلفی برای انتخاب اول باشد (برای مثال، "مدیریت داده ممیزی" ممکن است "تعیین رفتار" و "تغییر رفتار" را برای انتخاب اول الزام کند و از طرف دیگر "توابع امنیتی هدف ارزیابی" ممکن است فقط "تغییر رفتار" را الزام کند). در آن صورت، FMT_MOF.1/Functions باید با افزایش شماره پیوست تکرار شود. (به عنوان مثال، FMT_MOF.1/Functions1، FMT_MOF.1/Functions2، غیره).

FMT_MOF.1.1/Services	مدیریت رفتار توابع امنیتی/خدمات ۱	۱۴۳
توابع امنیتی هدف ارزیابی باید قابلیت شروع و متوقف کردن توابع سرویس‌ها را به سرپرست امنیتی محدود سازد.		
FMT_MTD.1.1/CryptoKeys	مدیریت رفتار توابع امنیتی/کلیدهای رمزنگاری ۱	۱۴۴
توابع امنیتی هدف ارزیابی باید توانایی مدیریت کلید های رمزنگاری را به سرپرست امنیتی محدود کند.		