به نام خدا

پروفایل حفاظتی
برنامه‌های کاربردی تحت شبکه

اسفند ۹۶

نسخه ۱,۱

فهرست

۱ مقدمه ۵
۲ اصطلاحات ۵
۳ شرح محصول ۶
۳,۱ مولفه‌های محیط عملیاتی ۸
۳,۲ انواع کاربران ۱۰
۳,۳ ویژگی‌های امنیتی محصول ۱۱
۴ مسائل امنیتی ۱۳
۴,۱ تهدیدات ۱۳
۴,۲ خطمشی امنیتی ۱۵
۴,۳ فرضیات ۱۶
۵ اهداف امنیتی ۱۷
۵,۱ اهداف امنیتی برای محصول ۱۷
۵,۲ اهداف امنیتی برای محیط عملیاتی ۲۰
۶ الزامات کارکرد امنیتی ۲۱
۶,۱ کلاس ممیزی امنیت ۲۶
۶,۲ کلاس پشتیبانی از رمزنگاری ۳۷
۶,۳ کلاس حفاظت از داده کاربری ۳۸

۶,۴ کلاس شناسایی و احرازهویت ۴۶
۶,۵ کلاس مدیریت امنیت ۵۵
۶,۶ کلاس حفاظت از توابع امنیتی محصول ۶۱
۶,۷ کلاس تخصیص منابع ۶۵
۶,۸ کلاس دسترسی به محصول ۶۵
۶,۹ کلاس کانال‌های/مسیرهای مورد اعتماد ۶۹
۷ الزامات تضمین امنیت ۷۰
۷,۱ کلاس توسعه ۷۲
۷,۲ کلاس راهنمای کاربر ۷۵
۷,۲,۱ راهنمای کاربردی ۷۵
۷,۲,۲ راهنمای آمادهسازی ۷۸
۷,۳ کلاس پشتیبانی از چرخه حیات ۸۰
۷,۳,۱ قابلیتهای پیکربندی ۸۰
۷,۳,۲ حوزه پیکربندی ۸۲
۷,۴ کلاس هدف امنیتی ۸۳
۷,۴,۱ ادعاهای انطباق ۸۳
۷,۴,۲ تعریف مؤلفه‌های توسعه‌یافته ۸۶
۷,۴,۳ معرفی هدف امنیتی ۸۸

۷,۴,۴ اهداف امنیتی ۹۱
۷,۴,۵ الزامات امنیتی معین ۹۲
۷,۴,۶ خلاصه مشخصات هدف ارزیابی ۹۵
۷,۵ کلاس آزمون ۹۷
۷,۵,۱ آزمون مستقل ۹۷
۷,۶ کلاس آسیب‌پذیری ۹۸
۷,۶,۱ تحلیل آسیب‌پذیری ۹۹
۸ پیوست یک: الزامات اختیاری ۱۰۰
۸,۱ الزامات کلاس پشتیبانی از رمزنگاری ۱۰۰
۹ پیوست دو: الزامات مبتنی بر انتخاب ۱۰۳
۹,۱ الزامات پروتکل HTTPS ۱۰۳
۹,۲ الزامات پروتکل TLS Client ۱۰۴
۹,۳ الزامات پروتکل TLS Server ۱۰۷
۹,۴ الزامات پروتکل TLS مشترک کلاینت و سرور ۱۰۹
۹,۵ الزامات شناسایی و احرازهویت ۱۱۰

۱ مقدمه

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 سازند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد. مرکز افتا با مشارکت سازمان فناوری اطلاعات این سند را بر اساس سند نظام ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 در راستای این هدف تهیه کرده است. این پروفایل حفاظتی، به بیان الزامات برنامه کاربردی تحت شبکه می‌پردازد.

۲ اصطلاحات

مستند: به هر سندی که حاوی اطلاعات برای اجرا و پشتیبانی عملیات و فعالیت‌های سازمانی مورد استفاده قرار می‌گیرند، مستند گفته می‌شود.

رکورد: مستندی که اطلاعات فعالیت‌ها، رویدادها و نتایج حاصله را نگهداری می‌کند؛ به عبارت دیگر یک رکورد مستندی است که مدرک انجام یک فعالیتی مشخص است. یک رکورد می‌تواند شامل دو یا چند مستند باشد.

رکورد ممیزی: رکوردی که حاوی اطلاعات رویدادهایی است که برای ممیزی برنامه کاربردی تحت شبکه مورد نیاز است و در محل ذخیره‌سازی ممیزی، ذخیره می‌شود.

داده‌های کاربری ذخیره شده: فایل‌های داده و اطلاعاتی هستند که توسط کاربر ایجاد و ذخیره می‌شوند. این داده‌ها می‌تواند شامل مستندات تولید شده با استفاده از برنامه کاربردی Microsoft Office، نامه‌های ارجاع کار و پاسخ الکترونیکی و اسکن تصاویر باشد.

موجودیت فعال: موجودیتی در محصول که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون مدیر، کاربر نهایی و غیره.

موجودیت غیرفعال: موجودیتی در محصول، که حاوی اطلاعات است و یا اطلاعات را دریافت می‌کند و توسط موجودیت‌های فعال، عملیاتی بر روی آن انجام می‌گیرد. همانند لیست کردن رکوردها توسط مدیر سیستم، حذف فایل‌ها توسط مهاجم. (رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.)

مشخصه‌های موجودیت فعال: مشخصه‌های هر موجودیت فعال می‌تواند از قبیل نام کاربری، کلمه عبور، آدرس IP کاربر باشد.

مشخصه‌های موجودیت غیرفعال: مشخصه‌های هر موجودیت غیرفعال می‌تواند از قبیل نوع، نام و اندازه مستند باشد.

۳ شرح محصول

محصول مورد ارزیابی، برنامه کاربردی مبتنی بر شبکه است که برای مدیریت رکوردها و مستندات مورد استفاده قرار می‌گیرد. از جمله وظایف این برنامه‌های کاربردی می‌توان به جمع‌آوری، ذخیره و توزیع مستندات، پیام‌ها و فرم‌های ارتباطات اداری بین افراد اشاره نمود.

به‌طور کلی برنامه کاربردی تحت شبکه برای رکوردها و مستندات الکترونیکی از فعالیت‌های زیر استفاده می‌کند:

- ثبت رکوردهای الکترونیکی
- مدیریت گردش کار رکوردهای الکترونیکی
- ایجاد و مدیریت فرآیندهای آرشیو
- انجام امور جستجو و گزارش دهی
- قابلیت مدیریت کاربران
- پشتیبانی از سازوکارهای امن‌سازی ارتباطات
- سازوکارهای احراز هویت و کنترل دسترسی

محصول اعمال فوق را با کمک مؤلفه‌های نشان داده شده در شکل ۱ انجام می‌دهد.

شکل ۱: مؤلفه‌های برنامه کاربردی تحت شبکه

۳,۱ مؤلفه‌های محیط عملیاتی

یک برنامه کاربردی تحت شبکه، یک برنامه اجرایی بر روی بستر شبکه است و با مؤلفه‌های شبکه در تعامل است که بر روی سیستم‌عامل اجرایی در محیط شبکه اجرا می‌گردد. محصول با واحد/واحدهای ذخیره‌سازی به منظور نگهداری رکوردها و با مؤلفه‌های ممیزی به منظور نگهداری رکوردهای ممیزی در تعامل است؛ در ادامه، این مؤلفه‌ها با جزئیات شرح داده می‌شوند.

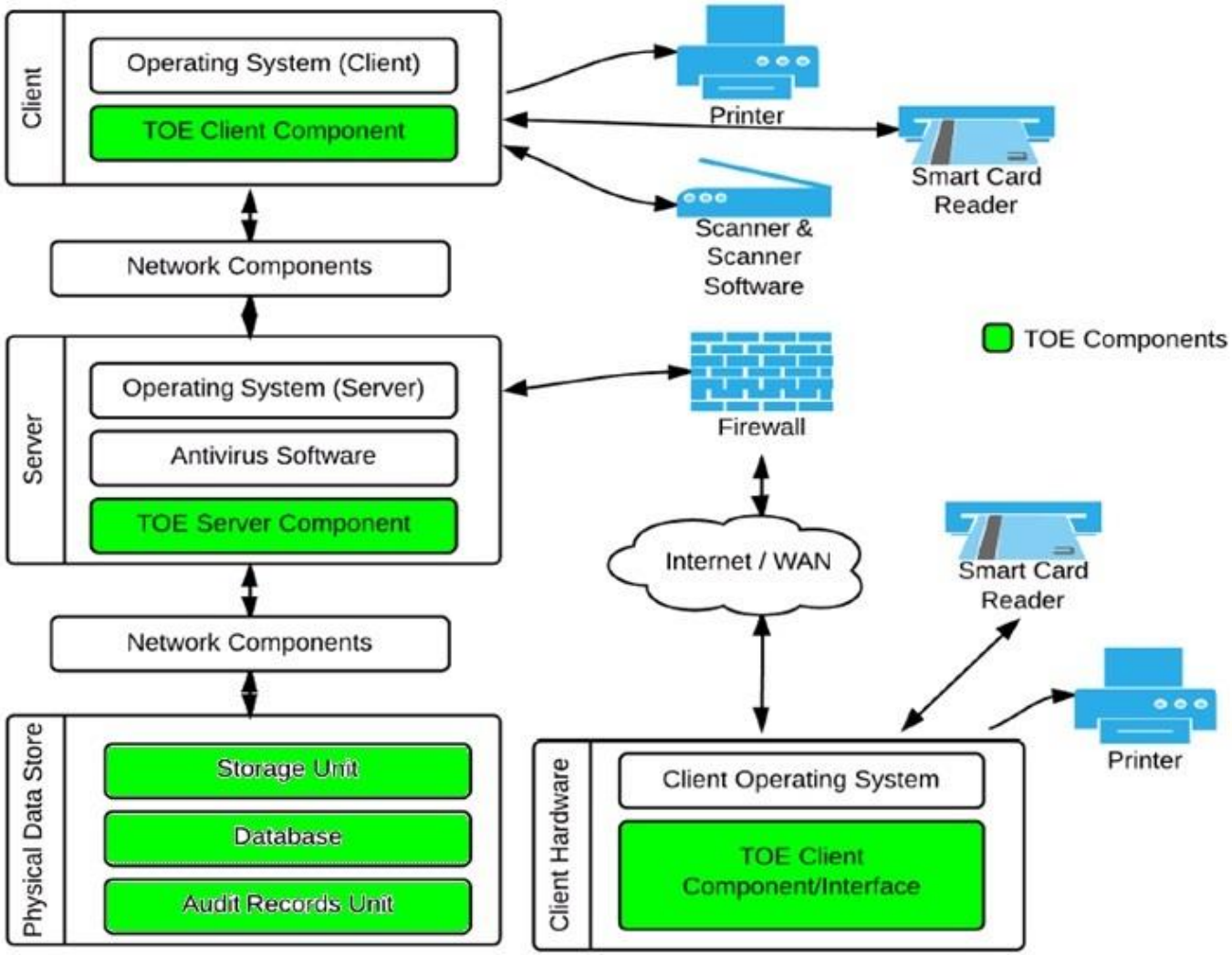
محیط عملیاتی محصول شامل مؤلفه‌های نرم‌افزاری و سخت‌افزاری و همچنین ویژگی‌های کارکردی و امنیتی اصلی است که در این سند پوشش داده شده‌اند. شکل ۲ بیانگر سخت‌افزار و نرم‌افزارهایی است که محصول با آن‌ها در تعامل است، این شکل چگونگی تعاملات محصول با محیط عملیاتی را نمایش می‌دهد:

سرور: سرور مؤلفه سخت‌افزاری است که مؤلفه سروری محصول بر روی آن اجرا می‌گردد. سرور می‌تواند به صورت فیزیکی یا مجازی باشد، در هر دو حالت امنیت سرور به امنیت محصول بستگی دارد. پیکربندی و قابلیت‌های سرور می‌تواند با توجه به تعداد کاربران، تعداد اتصالات و غیره متفاوت باشد.

سیستم کاربر: سخت‌افزار و سیستم‌عاملی است که به کاربران اجازه دسترسی به محصول را می‌دهد. این مؤلفه معمولاً یک کامپیوتر بوده ولی می‌تواند یک تبلت یا گوشی هوشمند نیز باشد، در این پروفایل حفاظتی فرض شده که کلاینت یک کامپیوتر است. دو نوع کلاینت وجود دارد. یکی برای کاربر پایانی و نوع دیگر برای کاربرانی که رکوردها و مستندات را به داخل محصول وارد می‌نمایند. اتصالات بین کلاینت‌ها و مؤلفه‌های مرکزی محصول می‌تواند به صورت اینترنت، اینترانت یا VPN باشد.

سیستم‌عامل: محصول بر روی یک سیستم‌عامل اجرا می‌شود و ارتباطات بین محصول و واحد ذخیره‌سازی، واحد رکوردهای ممیزی، مؤلفه‌های شبکه و سرور توسط سیستم‌عامل ارائه می‌شود.

مؤلفه‌های شبکه: محصول به واسطه سیستم‌عامل و سرور با مؤلفه‌های شبکه در تعامل است. لازم است اتصالات شبکه بین کلاینت‌ها و سرور محصول به صورت امن باشد. کلاینت محصول قادر به انجام اقداماتی همانند چاپ، اسکن و غیره است. اتصالات بین این مؤلفه‌ها و سرور معمولاً به صورت یک شبکه محلی است.



شکل ۲: محیط عملیاتی محصول

فایروال: دسترسی اینترانت به‌وسیله‌ی این مؤلفه امن می‌گردد.

نرم‌افزار آنتی‌ویروس: نرم‌افزار آنتی‌ویروس جهت بررسی مستندات و رکوردهای ورودی مورد استفاده قرار می‌گیرد.

پایگاه داده: محصول با یک پایگاه داده برای حفظ و نگهداری داده‌های خود در تعامل نزدیک است. رکوردها و مستندات می‌توانند در پایگاه داده یا به صورت مجزا حفظ و نگهداری شوند. در زمان نیاز به یک مجموعه داده خاص، یک درخواست به پایگاه داده ارسال و نتایج آن گرفته می‌شود.

واحد ذخیره‌سازی مستندات و رکوردها: رکوردها و مستندات می‌توانند به صورت مجزا در سمت سروری که محصول بر روی آن اجرا می‌گردد باقی‌مانده تا محصول به آسانی تحت تأثیر آسیب‌پذیری امنیتی بالقوه در واحد ذخیره‌سازی قرار نگیرد.

واحد ذخیره رکوردهای ممیزی: همانند واحدهای ذخیره‌سازی، واحد رکوردهای ممیزی در سمت سروری قرار می‌گیرد که محصول بر روی آن اجرا می‌گردد. این واحد می‌تواند به صورت مؤلفه مجزا و یا بخشی از واحد ذخیره‌سازی باشد.

کارت‌خوان هوشمند: کارت‌خوان یک مؤلفه سخت‌افزاری است که دارای گواهی مورد اعتماد است و برای امضاء اسناد الکترونیکی مورد استفاده قرار می‌گیرد. در حال حاضر رایج‌ترین نوع کارت‌خوان توکن USB است. از آنجائی که این مؤلفه مبتنی بر سخت‌افزار بوده و به شبکه متصل نیست، سطح بالایی از امنیت را فراهم می‌کند. از این‌رو می‌تواند برای احراز هویت مورد استفاده قرار گیرد.

اسکنر و درایور آن: کاربرانی که برای اسکن نمودن مجاز هستند، رکوردها و مستنداتی که به شکل کاغذی دریافت می‌کنند را اسکن می‌کند.

پرینتر: مؤلفه‌ای است که به کاربران محصول مطابق با مجوز کاربر، اجازه چاپ هر رکورد یا مستندی را می‌دهند.

۳,۲ انواع کاربران

حداقل دو دسته کاربر برای محصول وجود دارد:

- کاربر عادی

- مدیر سیستم

علاوه بر نقش‌های لیست شده در بالا، محصول ممکن است دارای نقش‌های دیگری نیز باشد. در صورت وجود نقش‌های دیگر لازم است در سند هدف امنیتی ذکر گردد.

کاربر عادی: کاربر عادی از محصول به صورت یک جعبه سیاه استفاده می‌کند و نیز قادر به مدیریت داده‌های تحت مالکیتش است. کاربر عادی در صورت داشتن مجوز می‌تواند رکوردها و مستندات را جستجو، لیست و مشاهده کند. علاوه بر آن کاربر عادی می‌تواند سند یا رکورد جدیدی ایجاد کند یا سند و رکوردی که مالک آن است را حذف کند. این نوع کاربر می‌تواند مستندات را بایگانی کند و باید قادر به دسترسی اسناد بایگانی شده خود باشد.

مدیر سیستم: مدیر، دارای مجوز خاص برای مدیریت محصول است. مدیر سیستم می‌تواند یک نفر باشد یا برای بخش‌های مختلف محصول مدیران مختلفی وجود داشته باشد، همانند مدیر پایگاه داده، مدیر شبکه، مدیر برنامه کاربردی و غیره. همچنین مدیر دارای سطح دسترسی کامل برای دسترسی به برنامه کاربردی، پایگاه داده، فایل سیستم و دیگر موجودیت‌ها است.

۳,۳ ویژگی‌های امنیتی محصول

احرازهویت و مجوزدهی: عملیات احراز هویت و مجوزدهی باید به طور مؤثری انجام شود. احرازهویت به طور کلی با بررسی و تائید نام کاربری و کلمه عبور صورت می‌گیرد. لازم به ذکر است برای مدیریت کلمه عبورهای مورد استفاده باید روال‌های امن وجود داشته باشد. در صورتی که محصول به سطح بالایی از امنیت نیاز داشته باشد، از یک سازوکار احرازهویت دیگر یا ترکیبی از دو یا بیشتر از دو سازوکار استفاده می‌شود. از جمله سازوکارهای احراز هویت می‌توان به وارسی نام کاربری و کلمه عبور، وارسی SMS، احراز هویت از طریق یک برنامه موبایل، گواهی دیجیتال، وارسی بیومتریک و توکن سخت‌افزاری اشاره نمود.

کنترل دسترسی: محصول، قابلیت‌های لازم برای محدود کردن دسترسی را دارد، به طوری که تنها موجودیت‌های مجاز، دارای دسترسی به داده و کارکردهای محصول هستند. برای کاربران مجاز، کنترل دسترسی معمولاً با استفاده از داده احراز هویت انجام می‌گیرد. محصول ممکن است همچنین آدرس‌های IP اتصالات فعال را کنترل کند و تنها به آدرس‌های IP از پیش تعریف شده در یک بازه زمانی خاص برای عملیات حساس اجازه اتصال دهد.

ممیزی: محصول به صورت خودکار، رکوردهای ممیزی را به منظور ردیابی و کنترل فعالیت‌های کاربر بر روی دارایی‌ها، تغییرات کنترل دسترسی و پیکربندی جمع‌آوری می‌کند. محتوای رکوردهای ممیزی، روش‌های حفظ رکورد و فواصل نگهداری را می‌توان توسط رابط گرافیکی محصول پیکربندی نمود. هیچ فردی جز افرادی که محصول، مجاز نموده همچون مدیر، امکان تغییر یا حذف محتویات رکوردهای ممیزی را ندارند.

مدیریت: محصول، برای مدیریت کاربران و دسترسی‌ها واسط‌های مدیریتی لازم را فراهم می‌کند. سرعت و دقت این واسط‌ها در تصمیم‌گیری در طول یک رخداد امنیتی بسیار مهم است.

صحت رکوردها و بررسی منابع: حذف یا تغییر هر رکورد توسط محصول مجاز نیست؛ بنابراین، دسترسی و تغییر سند و/یا فراداده[۱] آن باید محدود گردد. صحت رکوردهای ذخیره شده، توسط روشی مانند امضای دیجیتال مهیا می‌گردد.

پشتیبان‌گیری: عملیات پشتیبان‌گیری بر روی داده، مستندات و رکوردهای ممیزی که محصول از آن‌ها محافظت می‌کند، می‌تواند توسط خود محصول و یا یک ابزار خارجی که بدین منظور استفاده می‌گردد، صورت گیرد. عملیات پشتیبان نسبت به عدم از دست رفتن داده اطمینان می‌دهد.

کنترل گردش مستندات و اطلاعات: حداکثر اندازه فایل می‌تواند به صورت پویا برای هر نوع سند تعریف شود. محصول، فضای خالی ذخیره‌سازی را در نظر می‌گیرد و در برابر سرریز ذخیره‌سازی اقدامات احتیاطی لازم را اتخاذ می‌کند. همچنین تنها کاربران مجاز، مجوز صدور و ارسال هر رکورد یا سندی را دارند.

درهم‌سازی/رمز نمودن داده حساس: مثالی از داده حساس کلمه‌های عبور یا رکوردهای محرمانه است. داده حساس بر روی محصول به صورت واضح ذخیره نمی‌شوند و با سازوکاری از آن‌ها حفاظت می‌شود. همچنین باید رکوردهای محرمانه به صورت رمز شده نگهداری شود. ارتباط بین کاربر و سرور باید با استفاده از رمزنگاری امن شود تا از افشای محتوی رکوردها جلوگیری گردد. روش درهم‌سازی و رمزنگاری انتخاب شده باید به اندازه کافی قوی باشد طوری که توسط فناوری‌های امروزی در یک بازه‌ی منطقی قابل شکسته شدن نباشد.

---

[۱] MetaData

۴ مسائل امنیتی

۴,۱ تهدیدات

تهدیدات	توضیحات
دسترسی غیرمجاز	مهاجم می‌تواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا کند. این دسترسی می‌تواند با استفاده هویت سرقتی، آدرس IP جعلی و غیره صورت گیرد. مهاجم می‌تواند با سود بردن از نقض‌های امنیتی همچون تغییر ندادن کلمه عبور و نام کاربری، استفاده از کلمه عبور ساده، غیرفعال نکردن حساب کاربری آزمون بر روی سیستم واقعی به محصول دسترسی پیدا کند. همچنین مهاجم می‌تواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد. این داده‌های می‌توانند داده‌های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم می‌تواند با دسترسی به داده‌ها و خود محصول سبب آسیب شود.
تغییر غیرمجاز	رکوردهای، مستندات و داده‌های حفاظت شده توسط محصول می‌تواند بدون مجوز تغییر یابند. مهاجم می‌تواند با گمراه نمودن مدیر سیستم، واردکننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می‌تواند از طرق غیرقانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده‌های حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ می‌دهد که صحت رکوردها و مستندات تضمین شده نیست. مهاجم ممکن است درصدد تغییر داده ممیزی یا کد منبع برآید. بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا کند.
انکار	یک اقدام یا یک تراکنش صورت گرفته بر روی محصول می‌تواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول است تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم می‌تواند از

تهدیدات	توضیحات
	رکوردهای ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم می‌تواند با اضافه کردن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه کند.
افشای اطلاعات	داده‌های محرمانه که توسط محصول محافظت می‌شوند می‌تواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی می‌تواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی می‌تواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور واردکننده داده می‌تواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.
انکار سرویس	مهاجم می‌تواند سبب گردد محصول در یک بازه زمانی غیرقابل‌دسترسی یا بلااستفاده گردد. این امر معمولاً با ارسال درخواست‌های بسیار در یک بازه زمانی کوتاه صورت می‌گیرد طوری که محصول قادر به پاسخ نخواهد بود. نوع ساده‌ای از حمله شامل ارسال درخواست‌های بسیار از یک رنج IP مشخص است که به نام حمله DoS شناخته می‌شود. نوع دیگر پیشرفته‌تر حمله DDoS است که از BOTNET استفاده می‌کند و محدودیتی بر روی آدرس IP ورودی ندارد.
داده‌های ورودی مخرب	مهاجم می‌تواند یک رکورد، سند یا داده مضر را در داخل محصول وارد کند. با استفاده از این تهدید، مهاجم می‌تواند به داده کاربر خاص دسترسی پیدا کند، حساب کاربری یک کاربر را به دست گیرد یا به بخشی از کارکردها یا تمام کارکردهای محصول دسترسی یابد.
سطح دسترسی بالاتر	مهاجم می‌تواند با سود بردن از دسترسی غیرمجاز، ورود داده‌های مخرب و تغییر داده‌ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاتر کند.
شنود شبکه	در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر می‌شود تا انتقال داده‌های حساس بین محصول و مقصد موردنظر را مورد نظارت قرار دهد. این حمله شامل نظارت بر داده‌های ردوبدل شده بین محصول و یک یا چند کاربر

تهدیدات	توضیحات
	از راه دور و یا محلی است. به عنوان مثال می‌توان به موردی اشاره کرد که در آن یک کاربر تلاش می‌کند تا جهت احراز هویت و ورود به برنامه، اطلاعات محرمانه خود را وارد می‌کند.

۴,۲ خط‌مشی امنیتی

خط‌مشی‌ها	توضیحات
ممیزی کامل	تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردها محافظت شده هستند و معمولاً به منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار می‌گیرند.
پیکربندی مناسب	پیکربندی پیش‌فرض محصول و مؤلفه‌های تعاملی تحت کنترل محصول باید تغییر یابند. طوری که مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویس‌هایی که مورد استفاده نیستند، باید غیرفعال گردند. پارامترهای پیکربندی همچون دایرکتوری root پیش‌فرض، خطاهای پیش‌فرض و صفحات 404، مقادیر احراز هویت پیش‌فرض، نام کاربری پیش‌فرض، پورت‌های پیش‌فرض، صفحات پیش‌فرض که اطلاعات داخلی همچون شماره نسخه را آشکار می‌نمایند. این خط‌مشی سازمانی بسیار مهم است به خصوص زمانی که محصول یا هر مؤلفه تعاملی به طور گسترده مورد استفاده قرار می‌گیرد؛ بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی می‌توان از حمله‌ی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.
امضای دیجیتال	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تائید موجود باشد.

۴,۳ فرضیات

فرضیات	توضیحات
کاربران آموزش‌دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده‌اند و قوانین را دنبال می‌نمایند.
توسعه‌دهندگان آموزش‌دیده	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه‌نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال می‌نمایند.
توسعه‌دهندگان مجرب	فرض شده است تمام کارمندان توسعه‌دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب‌پذیری‌های شناخته شده را اتخاذ می‌نمایند.
محیط امن	فرض شده است که تمام پیش‌بینی‌های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری محصول به طور مناسب محدود شده و رکوردهای دسترسی برای یک بازه زمانی منطقی حفظ شده است. فرض شده است که سازوکاری وجود دارد تا رکوردها و مستندات که غیرقانونی از محصول به دست آمده را تشخیص دهد. همچنین فرض شده است که در قبال حملات DoS اقدامات مناسبی صورت می‌گیرد.
پشتیبان گیری مناسب	فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره‌سازی و دیگر مؤلفه‌های سخت‌افزاری دارای پشتیبان مناسبی هستند و بنا بر وجود نسخه پشتیبان هیچ داده‌ای از دست نمی‌رود همچنین به علت شکست در سیستم، قطع سرویسی رخ نمی‌دهد.
ارتباطات	فرض شده است که تمام ارتباطات و کانال‌های ارتباطی مورد استفاده توابع امنیتی محصول جهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به طور مناسبی در قبال حملاتی چون DoS و شنود شبکه و غیره حفاظت می‌شوند.

فرضیات	توضیحات
تحویل امن	فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت می‌گیرد.
انکار سرویس توزیع شده	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می‌شود.

۵ اهداف امنیتی

۵,۱ اهداف امنیتی برای محصول

هدف امنیتی	توضیحات
ممیزی	محصول باید هر رخدادی که در زمینه امنیتی دارای ارزش است را در حوزه مالکیتش رکورد کند. محصول باید از این رکوردها در قبال تغییرات و حذف محافظت کند. محصول باید به کاربران مجاز امکان بررسی آسان و سریع رکوردها را بدهد و مدیر سیستم را به موقع از رخداد امنیتی بحرانی آگاه کند.

هدف امنیتی	توضیحات
احراز هویت	محصول باید هر کاربری را تعریف نموده و آن‌ها را به طور امن احراز هویت کند و مطابق با نقش و مجوزهایشان مجاز کند. محصول باید برای احراز هویت کاربر، قوانینی تعریف کند طوری که کاربران را ملزم به استفاده از کلمه‌های عبور قدرتمند کند. محصول باید اجازه طبقه‌بندی رکوردها و مستندات را دهد و با توجه به طبقه‌بندی آن‌ها قوانینی را تعریف کند. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم می‌کند. محصول باید برای کاربران به صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها فراهم کند. مهاجم در تلاش است تا از تهدیدی چون رسیدن به سطح دسترسی بالاتر نهایت سود را ببرد. برای جلوگیری از این تهدید، محصول باید با استفاده از سازوکارهای قوی‌تری مدیر سیستم را احرازهویت کند. از جمله سازوکارها می‌توان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احرازهویت بر اساس توکن، احرازهویت چند فاکتوری و ترکیبی از این روش‌ها اشاره نمود.
کنترل جریان داده	محصول باید گردش داده‌های غیرمجاز را کنترل و مدیریت کند. داده‌های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواست‌ها از یک رنج IP تعریف شده می‌تواند بیانگر حمله DoS باشد. محصول باید برای مدیر سیستم واسطی را فراهم کند که به وی اجازه حفظ ترافیک شبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده کند.
صحت داده	محصول باید نسبت به صحت داده ممیزی و داده‌ی رکورد با تشخیص هرگونه تغییر بر روی این داده‌ها اطمینان حاصل کند و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.

هدف امنیتی	توضیحات
مدیریت	محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارآمد سیستم فراهم کند. محصول باید سازوکارهای کنترل دسترسی مناسبی جهت حفاظت از واسط‌های مدیریتی در نظر گیرد. محصول باید برای مدیر سیستم امکان تغییر مجوزها و نقش‌های کاربران را فراهم آورد و مدیر بتواند برای یک کاربر خاص و/یا گروهی از کاربران نقش‌ها و مجوزهایی تنظیم کند.
مدیریت خطا	محصول باید صورت امن و کارآمد سازوکار مدیریت خطا فراهم کند. خطاهای رخ داده در طول عملیات محصول باید به کاربر به صورت امن و معنادار نشان داده شود. برای مثال، محصول باید اطلاعات کلی مربوط به احراز هویت ناموفق را برگرداند، همچنین برای کاربر عادی نباید اطلاعات جزئی چون شماره خط خطا برگردانده شود. از سوی دیگر مدیر سیستم باید سریعاً از شکست بحرانی که رخ داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صورت رخ دادن خطا باید وضعیت امنی را حفظ کند.
مدیریت داده‌های باقیمانده	محصول باید اطمینان دهد که هر داده‌ی باقیمانده از محصول زمانی که دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل‌دسترس می‌گردد.
ارتباطات امن مبتنی برTLS	تمام کانال‌های ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.

۵,۲ اهداف امنیتی برای محیط عملیاتی

اهداف امنیتی محیطی	توضیحات
محیط امن	محیط عملیاتی محصول باید نسبت به امنیت محیطی و فیزیکی محصول اطمینان دهد. دسترسی غیرمجاز باید محدود گردیده و تمام مؤلفه‌ها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مؤلفه‌های حساس را داشته باشند. محیط عملیاتی محصول باید اطمینان دهد محصول به طور مناسب در قبال هر حمله DoS یا DDoS محافظت شده است. از جمله سازوکارهای حفاظتی می‌توان به غیرفعال نمودن سرویس‌ها، پورت‌ها و دیگر موارد استفاده شده اشاره نمود.
ارتباطات	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه‌های ارتباطی امن باید فراهم گردد.
کاربران آموزش‌دیده	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده‌کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه‌دهندگان آموزش‌دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه‌دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه‌دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه‌دهنده‌ی محصول در زمینه امنیت تجربه داشته و آن‌ها اقدامات مقابله‌ای لازم برای تمام آسیب‌پذیری‌های امنیتی شناخته شده را در نظر می‌گیرد.
ممیزی کامل	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مؤلفه‌های غیر از محصول نیز مورد ممیزی قرار می‌گیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول است. رکوردهای ممیزی محصول در صورت ترکیب با باقی رکوردهای ممیزی بسیار معنادار خواهند بود.
تحویل امن	تحویل و نصب محصول باید بدون به خطر افتادن هرگونه محدودیت امنیتی انجام شود. علاوه بر این، کارکردها و/یا پارامترهای استفاده شده به منظور آزمون باید پاک یا غیرقابل‌دسترس گردند.

اهداف امنیتی محیطی	توضیحات
پشتیبان‌گیری مناسب	نسخه پشتیبان باید ایجاد گردیده و برای یک بازه زمانی منطقی تمام داده‌های باقیمانده در محیط عملیاتی محصول را حفظ کند. برای این منظور ممکن است از روال‌های از پیش تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره‌سازی و دیگر مؤلفه‌های سخت‌افزاری نیز نسخه پشتیبان تهیه گردد.

۶ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند. در ادامه هر یک از الزامات شرح و بسط داده شده‌اند.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**تولید داده ممیزی ۱**	FAU_GEN.1.1
۲	**تولید داده ممیزی ۲**	FAU_GEN.1.2
۳	**مرتبط نمودن هویت کاربر به رویداد ۱**	FAU_GEN.2.1
۴	**بازبینی داده ممیزی ۱**	FAU_SAR.1.1
۵	**بازبینی داده ممیزی ۲**	FAU_SAR.1.2
۶	**بازبینی داده ممیزی محدود ۱**	FAU_SAR.2.1
۷	**بازبینی داده ممیزی قابل انتخاب ۱**	FAU_SAR.3.1
۸	**انتخاب داده ممیزی ۱**	FAU_SEL.1.1
۹	**ذخیره‌سازی رویدادهای ممیزی ۱**	FAU_STG.1.1
۱۰	**ذخیره‌سازی رویدادهای ممیزی ۲**	FAU_STG.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۱	اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	FAU_STG.3.1
۱۲	پیشگیری از اتلاف و از بین رفتن داده ممیزی ۱	FAU_STG.4.1
۱۳	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1(1)
۱۴	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1(2)
۱۵	خط‌مشی کنترل دسترسی ۱	FDP_ACC.1.1
۱۶	عملیات کنترل دسترسی ۱	FDP_ACF.1.1
۱۷	عملیات کنترل دسترسی ۲	FDP_ACF.1.2
۱۸	عملیات کنترل دسترسی ۳	FDP_ACF.1.3
۱۹	عملیات کنترل دسترسی ۴	FDP_ACF.1.4
۲۰	حفاظت کامل از اطلاعات باقیمانده در منابع ۱	FDP_RIP.2.1
۲۱	ورود داده کاربری به محصول با مشخصه امنیتی ۱	FDP_ITC.2.1
۲۲	ورود داده کاربری به محصول با مشخصه امنیتی ۲	FDP_ITC.2.2
۲۳	ورود داده کاربری به محصول با مشخصه امنیتی ۳	FDP_ITC.2.3
۲۴	خروج داده کاربری از محصول با مشخصه امنیتی ۱	FDP_ETC.2.1
۲۵	خروج داده کاربری از محصول با مشخصه امنیتی ۲	FDP_ETC.2.2
۲۶	خروج داده کاربری از محصول با مشخصه امنیتی ۴	FDP_ETC.2.4
۲۷	صحت داده کاربری ذخیره شده ۲	FDP_SDI.2.1
۲۸	صحت داده کاربری ذخیره شده ۳	FDP_SDI.2.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۲۹	**مدیریت احرازهویت ناموفق ۱**	FIA_AFL.1.1
۳۰	**مدیریت احرازهویت ناموفق ۲**	FIA_AFL.1.2
۳۱	**تعریف مشخصات کاربر ۱**	FIA_ATD.1.1
۳۲	**مدیریت کلمه عبور**	FIA_PMG_EXT.1.1
۳۳	**احرازهویت کاربر ۱**	FIA_UAU.1.1
۳۴	**احرازهویت کاربر ۲**	FIA_UAU.1.2
۳۵	**سازوکار احرازهویت چندگانه ۱**	FIA_UAU.5.1
۳۶	**سازوکار احرازهویت چندگانه ۲**	FIA_UAU.5.2
۳۷	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱**	FIA_USB.1.1
۳۸	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲**	FIA_USB.1.2
۳۹	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳**	FIA_USB.1.3
۴۰	**مدیریت کارکرد در محصول ۱**	FMT_MOF.1.1
۴۱	**مدیریت مشخصه‌های امنیتی ۱**	FMT_MSA.1.1
۴۲	**مدیریت داده محصول ۱**	FMT_MTD.1.1
۴۳	**کارکردهای مدیریتی محصول ۱**	FMT_SMF.1.1
۴۴	**نقش‌های امنیتی ۱**	FMT_SMR.1.1
۴۵	**نقش‌های امنیتی ۲**	FMT_SMR.1.2
۴۶	**حفظ وضعیت امن در زمان شکست ۱**	FPT_FLS.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۴۷	**انتقال داده امنیتی در داخل محصول ۱**	FPT_ITT.1.1
۴۸	**سازگاری داده امنیتی بین محصول و موجودیت امن ۱**	FPT_TDC.1.1
۴۹	**مهرهای زمانی ۱**	FPT_STM.1.1
۵۰	**به‌روزرسانی امن ۲**	FPT_TUD_EXT.1.2
۵۱	**به‌روزرسانی امن ۳**	FPT_TUD_EXT.1.3
۵۲	**تحمل خطا ۱**	FRU_FLT.1.1
۵۳	**محدودیت بر روی چندین نشست هم‌زمان ۱**	FTA_MCS.1.1
۵۴	**خاتمه دادن به نشست‌ها توسط محصول ۱**	FTA_SSL.3.1
۵۵	**خاتمه دادن به نشست‌ها توسط کاربر ۱**	FTA_SSL.4.1
۵۶	**سوابق دسترسی به محصول ۱**	FTA_TAH.1.1
۵۷	**سوابق دسترسی به محصول ۲**	FTA_TAH.1.2
۵۸	**سوابق دسترسی به محصول ۳**	FTA_TAH.1.3
۵۹	**برقراری نشست ۱**	FTA_TSE.1.1
۶۰	**مسیر امن ۱**	FTP_TRP.1.1
۶۱	**مسیر امن ۲**	FTP_TRP.1.2
۶۲	**مسیر امن ۳**	FTP_TRP.1.3
الزامات پیوست یک		
۶۳	**تولید کلید رمزنگاری ۱**	FCS_CKM.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۶۴	**تخریب کلید رمزنگاری ۱**	FCS_CKM.4.1
۶۵	**عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱ (۳)**	FCS_COP.1.1(3)
۶۶	**عملیات رمزنگاری ۱ (۴)**	FCS_COP.1.1(4)
	الزامات پیوست دو	
۶۷	**الزامات پروتکل HTTPS (۱)**	FCS_HTTPS_EXT.1.1
۶۸	**الزامات پروتکل HTTPS (۲)**	FCS_HTTPS_EXT.1.2
۶۹	**الزامات پروتکل HTTPS (۳)**	FCS_HTTPS_EXT.1.3
۷۰	**الزامات پروتکل TLS Client (۱)**	FCS_TLSC_EXT.1.1
۷۱	**الزامات پروتکل TLS Client (۲)**	FCS_TLSC_EXT.1.2
۷۲	**الزامات پروتکل TLS Client (۳)**	FCS_TLSC_EXT.1.3
۷۳	**الزامات پروتکل TLS Client (۴)**	FCS_TLSC_EXT.1.4
۷۴	**الزامات پروتکل TLS Server (۱)**	FCS_TLSS_EXT.1.1
۷۵	**الزامات پروتکل TLS Server (۲)**	FCS_TLSS_EXT.1.2
۷۶	**الزامات پروتکل TLS Server (۳)**	FCS_TLSS_EXT.1.3
۷۷	**الزامات پروتکل TLS Server/ احرازهویت (۴)**	FCS_TLSS_EXT.2.4
۷۸	**الزامات پروتکل TLS Server/ احرازهویت (۵)**	FCS_TLSS_EXT.2.5
۷۹	**الزامات پروتکل TLS Server/ احرازهویت (۶)**	FCS_TLSS_EXT.2.6
۸۰	**الزامات پروتکل X509(۱)/ ابطال**	FIA_X509_EXT.1.1/Rev

شماره الزام	نام الزام	تطابق الزام با استاندارد
۸۱	**الزامات پروتکل X509(۱) / ابطال**	FIA_X509_EXT.1.2/Rev
۸۲	**الزامات پروتکل X509(۳)**	FIA_X509_EXT.2.1

۶,۱ کلاس ممیزی امنیت

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

محصول باید بر اساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید کند:

- آغاز و اتمام توابع ممیزی؛
- تمامی رویدادهای قابل ممیزی (برای نوع داده حساس و داده‌هایی که بار حقوقی دارند) که در جدول ۱ آمده است.

جدول ۱- لیست رویدادهای قابل ممیزی

مؤلفه	رویداد قابل ممیزی	جزئیات
مرتبط نمودن هویت کاربر به رویداد ۱	تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی (پایه)	
بازبینی داده ممیزی ۱	خواندن اطلاعات از رکوردهای ممیزی (پایه)	
انتخاب داده ممیزی ۱	ثبت تمام تغییراتی که در پیکربندی ممیزی اتفاق می‌افتد در حالی که توابع ممیزی در حال انجام عملیات باشند. (حداقل)	

اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	عملیات انجام شده به دلیل پر شدن حافظه ممیزی بیش از حد آستانه (پایه)	
پیشگیری از اتلاف و از بین رفتن داده‌های ممیزی ۱	عملیات انجام شده به دلیل شکست ذخیره‌سازی ممیزی (پایه)	
صحت داده‌های کاربری ذخیره شده ۲	تلاش‌های موفقیت‌آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (حداقل) تمامی تلاش‌ها برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (پایه)	
احراز هویت کاربر	ثبت کاربرد ناموفق از سازوکار احرازهویت (حداقل) ثبت تمام کاربردهای سازوکار احراز هویت (پایه)	
سازوکار احرازهویت چندگانه	ثبت نتایج احرازهویت (حداقل) ثبت هر سازوکار احرازهویت فعال همراه با نتیجه نهائی (پایه)	
شناسایی کاربر	تمامی کاربردهای سازوکارها برای شناسایی کاربر (موفق و ناموفق)	شناسه کاربر شامل آدرس مبدأ، شناسایی نقطه پایانی اتصال
مدیریت کلمه عبور	ثبت رد هر کلمه عبور آزمون شده توسط محصول (حداقل) ثبت تلاش موفق و ناموفق هر کلمه عبور آزمون شده توسط محصول (پایه)	برای مثال، رد و یا قبول کلمه عبور کاربر
انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر	ثبت شکست انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، ایجاد موجودیت فعال) (حداقل) شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، شکست و موفقیت ایجاد موجودیت فعال) (پایه)	
مدیریت مشخصه‌های امنیتی	تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی (پایه)	

مدیریت داده‌های محصول ۱-مدیر سیستم	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
مدیریت داده‌های محصول ۱-کاربر عادی، واردکننده داده	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	به خصوص تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
عملیات رمزنگاری ۱(۱)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیرفعال (پایه)	
عملیات رمزنگاری ۱ (۲)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیرفعال (پایه)	
عملیات کنترل دسترسی ۱	درخواست‌های موفقیت‌آمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول (حداقل) تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول (پایه)	شناسایی داده‌های موجودیت غیرفعال
ورود داده‌های کاربری به محصول با مشخصه امنیتی	ورود داده کاربری موفقیت‌آمیز، شامل هرگونه مشخصه‌های امنیتی (حداقل) تمامی تلاش‌ها برای وارد کردن داده‌های کاربری، شامل هرگونه مشخصه‌های امنیتی (پایه)	
خروج داده‌های کاربری از محصول با مشخصه امنیتی	خروج اطلاعات به‌طور موفقیت‌آمیز (حداقل) همه تلاش‌ها برای خارج کردن اطلاعات از محصول (پایه)	
مدیریت کارکرد در محصول	تمامی تغییرات در رفتارهای کارکردی محصول	
کارکردهای مدیریتی محصول	ثبت استفاده از کارکردهای مدیریتی (حداقل)	
نقش‌های امنیتی	ثبت تغییرات در گروه‌های کاربری که بخشی از یک نقش است (حداقل)	

سازگاری داده‌های امنیتی بین محصول و موجودیت امن	ثبت استفاده موفق از سازوکار سازگاری داده‌های محصول (حداقل) ثبت استفاده از سازوکار سازگاری داده‌های محصول (پایه)	
حفظ وضعیت امن در زمان شکست	ثبت شکست در محصول (پایه)	
تحمل خطا	ثبت هر شکست شناسایی شده توسط محصول (حداقل) ثبت تمامی قابلیت‌های در حال قطع شدن محصول که به دلیل شکست است (پایه)	
برقراری نشست ۱	ثبت منع آغاز نشست به دلیل سازوکار آغاز نشست (حداقل) ثبت تمامی تلاش‌ها در آغاز نشست کاربر (پایه)	
محدودیت بر روی چندین نشست هم‌زمان	ثبت رد یک نشست مبتنی بر محدودیت نشست‌های هم‌زمان (حداقل)	
خاتمه دادن به نشست‌ها	ثبت خاتمه دادن به یک نشست بیکار توسط سازوکار قفل نشست (حداقل) ثبت خاتمه به نشست بیکار توسط مدیر سیستم (حداقل)	

اقدامات ارزیابی:

- **بخش خلاصه مشخصات محصول[۱]**

توسعه‌گر محصول باید قالب و نحوه ذخیره‌سازی رکوردهای ممیزی را در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی بیان کند و چگونگی استخراج رکوردهای ممیزی توسط مدیر سیستم و یا ارزیاب به منظور تحلیل داده‌ها، توضیح داده شود.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند تا نسبت به ارائه لیستی از رویدادهای قابل ممیزی در محل ذخیره‌سازی به شکل مناسب و قابل‌درک اطمینان حاصل کند.

[۱] TOE Summory Specification (TSS)

• **آزمون‌ها** ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید نشستی را با سرور ایجاد و درخواستی به آن ارسال کند. سپس باید تولید لاگ در سرور برای درخواست ارسال شده را بررسی کند. آزمون دوم: ارزیاب باید عملیاتی را انجام دهد که منجر به ثبت هر کدام از رویدادهای قابل ممیزی می‌شود. سپس ثبت و یا عدم ثبت آن‌ها را بررسی نماید. آزمون سوم: ارزیاب باید با انجام یک عمل غیرمجاز، تولید لاگ در سرور را بررسی کند.
۲ **تولید داده ممیزی ۲**
محصول باید برای هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید: • تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال (در صورتی که کاربرد داشته باشد) و نتیجه (موفقیت یا شکست) رویداد • [اختصاص: هر نوع اطلاعات قابل ممیزی دیگر از قبیل آدرس IP کاربر، نام و شناسه کاربری، نسخه سیستم‌عامل، زمان و تاریخ انجام فعالیت.] **اقدامات ارزیابی:** • **سند راهنمای محصول** ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل کند در سند مذکور، نحوه نمایش لاگ‌های ممیزی ذخیره‌شده در شکل و فرمت مناسب شرح داده شده است. • **آزمون‌ها** ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید بررسی کند برای لاگ ثبت شده در سرور، اطلاعات ذکر شده در این الزام وجود دارد یا خیر.
۳ **مرتبط نمودن هویت کاربر به رویداد ۱**

برای رویدادهای ممیزی حاصل از اقدامات کاربران شناسایی شده، محصول باید بتواند هویت کاربری که باعث ایجاد آن رویداد شده است را شناسایی و ثبت کند.

اقدامات ارزیابی:

- **بخش خلاصه مشخصات محصول**

در این بخش باید در صورت امکان روش‌هایی که باعث عدم انقیاد رویداد مرتبط با کاربری که آن را ایجاد کرده است، توضیح داده شود.

- **آزمون**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید رکوردهای ممیزی تولید شده را مطابقت دهد که آیا به نام همان کاربری که آن رویداد را ایجاد کرده، ذخیره شده است یا خیر. آزمون این الزام وابسته به الزام «تولید داده ممیزی ۱» است.

۴	**بازبینی داده ممیزی ۱**

محصول باید امکان خواندن [اختصاص: **فهرستی از اطلاعات ممیزی**] از کل رکوردهای ممیزی را برای [اختصاص: **کاربران مجاز**] فراهم نماید.

نکته کاربردی ۱:

به جای کاربران مجاز، با توجه به سازوکار کنترل دسترسی در محصول، کاربران و یا گروه کاربرانی که مجاز به قابلیت خواندن اطلاعات ممیزی هستند را اعلام نمایید.

به جای فهرستی از اطلاعات ممیزی، با توجه به سازوکار کنترل دسترسی در محصول، نوع اطلاعات ممیزی که کاربر مجاز قابلیت خواندن آن‌ها را دارد را اعلام نمایید.

اقدامات ارزیابی:

- **بخش خلاصه مشخصات محصول**

در این بخش از سند هدف امنیتی باید توضیح داده شود که چه مواقعی کاربر قادر به خواندن داده ممیزی است.

- **سند راهنمای محصول**

ارزیاب باید با بررسی سند راهنمای محصول تائید کند که در این سند در خصوص زمانی که کاربر امکان خواندن رکورد ممیزی دارد و از طریق کدام واسط‌ها این امکان فراهم می‌شود توضیحاتی ارائه شده است.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که تنها کاربر با دسترسی مجاز قادر به خواندن همه رکوردهای ممیزی در فرمت مناسب و قابل‌درک است.

آزمون دوم: ارزیاب باید بررسی کند که کاربران با توجه به نوع دسترسی، قادر به خواندن اطلاعات و رکوردهای ممیزی مناسب و خاص خود هستند.

۵	**بازبینی داده ممیزی ۲**

محصول باید رکوردهای ممیزی را طوری فراهم کند که کاربر بتواند آن‌ها را درک و اطلاعات این رکوردها را تفسیر کند.

اقدامات ارزیابی:

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که اطلاعات رکوردهای ممیزی فراهم شده قابل‌فهم هستند و محتویات فیلدهای یک رکورد قابل تفسیر هستند یا خیر.

۶	**بازبینی داده ممیزی محدود ۱**

محصول باید مانع دسترسی خواندن رکوردهای ممیزی توسط کلیه کاربران به غیر از کاربرانی که به صورت صریح مجاز به دسترسی خواندن هستند، گردد.

نکته کاربردی ۲:

در این الزام محدودیت‌های دسترسی که توسط سیستم‌عامل یا محیط ذخیره‌سازی اعمال می‌گردد یا قابل‌اعمال است، ملاک نیست. امکان اعمال محدودیت دسترسی در سطح برنامه کاربردی مدنظر است. این الزام، وابسته به الزام «بازبینی داده ممیزی ۱» است، زیرا در الزام مذکور کاربران مجاز تعریف می‌گردند.

اقدامات ارزیابی:

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که کاربر غیرمجاز قادر به خواندن رکوردهای ممیزی است یا خیر. ارزیاب باید اطمینان حاصل کند که برنامه کاربردی توانایی ممانعت بر اساس دسترسی را داشته باشد.

۷	**بازبینی داده ممیزی قابل انتخاب ۱**

محصول باید امکان انجام [اختصاص: متدهای انتخاب و مرتب‌سازی] رکوردهای ممیزی را به نحوی فراهم کند که کاربر مجاز بتواند آن رکوردها را بر اساس [اختصاص: حساب کاربری، تاریخ/زمان، مکان، روش اتصال کاربر، درجه اهمیت رکوردها، نوع رخداد و دیگر پارامترهای مورد نیاز] مرتب کند.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند که نحوه مرتب‌سازی داده‌های ممیزی بیان شده است و کدام واسطها این امکان را فراهم می‌کنند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید امکان مرتب‌سازی رکوردهای ممیزی را بر اساس چند مورد از پارامترهای ذکر شده در اختصاص دوم این الزام، بررسی کند.

آزمون دوم: ارزیاب باید امکان انتخاب گروهی از رکوردهای ممیزی یا انواعی از رکوردهای ممیزی را بررسی کند. در این آزمون ارزیاب باید از ترکیبی از پارامترهای ذکر شده در اختصاص دوم، استفاده کند.

۸	**انتخاب داده ممیزی ۱**

محصول باید قادر باشد بر اساس مشخصه‌های زیر، از مجموعه تمام رخدادهای قابل ممیزی، مجموعه‌ای از رخدادها را جهت ممیزی شدن، انتخاب کند:

- [انتخاب: هویت موجودیت فعال، نوع رخداد]

- [اختصاص: معیارهای انتخاب دیگر بیان شوند]

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل کند که لیستی از انواع رویدادها و مشخصه‌های قابل ممیزی وجود دارد که قابل انتخاب می‌باشند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید به ازای هر مشخصه و رویدادی که سند راهنمای محصول بیان شده است، قابل انتخاب بودن آن‌ها برای ممیزی را بررسی کند. ارزیاب باید با عدم انتخاب رویدادهای کم‌اهمیت، از ممیزی نشدن آن‌ها اطمینان حاصل کند.

آزمون دوم: ارزیاب باید چند مورد از لیست رویدادها را برای ممیزی انتخاب نموده و بررسی کند امکان انتخاب بر اساس مشخصه‌های بیان شده در این الزام، وجود دارد.

۹	**ذخیره‌سازی رویدادهای ممیزی ۱**

محصول باید رکوردهای ممیزی ذخیره شده در محل ذخیره‌سازی را، از حذف غیرمجاز حفاظت کند.

نکته کاربردی ۳:

در الزامات «ذخیره‌سازی رویدادهای ممیزی ۱» و «ذخیره‌سازی رویدادهای ممیزی ۲» محصول باید توانایی تشخیص تغییرات یا حذف رکوردهای ممیزی را داشته باشد. باید دقت شود که توانایی تشخیص در این الزامات به سطح برنامه کاربردی اشاره دارد نه سیستم‌عامل؛ بنابراین در صورتی که سیستم‌عامل نیز جزء حوزه آزمون باشد، باید رویکرد آن در جلوگیری از حذف یا تغییر غیرمجاز، در سند راهنمای محصول بیان گردد. در هر دو الزام، ارزیاب باید توانایی برنامه کاربردی در تشخیص هر کدام از اقدامات مربوطه را بررسی کند.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند و درخصوص بیان اینکه چه زمانی برای کاربر امکان حذف رکورد ممیزی داده می‌شود و کدام واسط این امکان را فراهم می‌کند اطمینان حاصل کند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که کاربر غیرمجاز قادر به حذف رکوردهای ممیزی است یا خیر.

آزمون دوم: ارزیاب باید بررسی کند که تلاش کاربر غیرمجاز برای حذف رکوردهای ممیزی، در لاگ ذخیره می‌شود.

۱۰	**ذخیره‌سازی رویدادهای ممیزی ۲**

محصول باید قادر به [انتخاب: تشخیص، جلوگیری] تغییرات غیرمجاز در رکوردهای ممیزی ذخیره شده، در محل ذخیره‌سازی آن‌ها باشد.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند و درخصوص بیان اینکه چه زمانی برای کاربر امکان تغییر رکورد ممیزی داده می‌شود و کدام واسط این امکان را فراهم می‌کند اطمینان حاصل کند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که کاربر غیرمجاز قادر به تغییر رکوردهای ممیزی است یا خیر.

آزمون دوم: ارزیاب باید بررسی کند که تلاش کاربر غیرمجاز برای اعمال تغییرات بر روی رکوردهای ممیزی، در لاگ ذخیره می‌شود.

۱۱	**اقدامات لازم در زمان از دست رفتن داده ممیزی ۱**

محصول در صورت تجاوز دنباله ممیزی از [اختصاص: یک محدودیت از پیش تعریف شده] باید با استفاده از [اختصاص: یک کانال ارتباطی، پیام کوتاه یا معادل آن، از طریق واسط‌های محصول کاربران مربوطه را] مطلع کند.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید اطمینان حاصل کند که در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی مقدار حجم ذخیره‌سازی رکوردهای ممیزی به صورت محلی بیان شده است. همچنین نوع رویدادی که در صورت پر شدن محل ذخیره‌سازی رخ می‌دهد و چگونگی محافظت از رکوردهای ممیزی در برابر دسترسی‌های غیرمجاز مشخص گردد. در این بخش، عملیاتی که بعد از پر شدن محل ذخیره‌سازی ممیزی صورت می‌گیرد و نوع اطلاعاتی که ممکن است از بین رود باید بیان شود. همچنین نوع تنظیماتی که مدیر سیستم باید بر روی محصول پیکربندی کند تا عملیات موردنظر فعال گردند، باید در این سند تعریف شود.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل کند که توضیحاتی در خصوص رویدادهایی که برای پیشگیری از دست رفتن رکوردهای ممیزی در صورت پر شدن محل ذخیره‌سازی در نظر گرفته شده، بیان شده است.

ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل کند که در خصوص رابطه بین رکوردهای ممیزی محلی و رکوردهای ممیزی ارسالی به لاگ سرور ممیزی توضیحاتی بیان شده باشد. برای مثال، اگر رکورد ممیزی تولید شده باشد، به‌طور هم‌زمان هم در سرور خارجی و هم در محل ذخیره‌سازی محلی ذخیره شود، یا محل ذخیره‌سازی محلی به عنوان بافر مورد استفاده قرار گیرد و با ارسال داده‌ها به طور دوره‌ای به سرور ممیزی، داده‌ها از محل ذخیره‌سازی محلی پاک گردد.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید با رساندن رکوردهای ممیزی به مقدار حد آستانه تعریف شده و تجاوز از آن، بررسی کند که در این شرایط رویدادهای ادعا شده صورت می‌گیرد.

۱۲	**پیشگیری از اتلاف و از بین رفتن داده ممیزی ۱**

محصول در صورت پر شدن دنباله ممیزی، باید [انتخاب: رویدادهای ممیزی را نادیده بگیرد، از ذخیره رویدادهای قابل ممیزی، به جز آن‌هایی که توسط کاربر مجاز و تحت حقوق خاص رخ می‌دهند جلوگیری کند، روی قدیمی‌ترین رکوردهای ممیزی ذخیره‌شده دوباره‌نویسی کند] و [اختصاص: یا دیگر اقدامات برای هشدار از پر شدن فضای ذخیره‌سازی].

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید با تولید داده ممیزی و پر کردن فضای ذخیره‌سازی در نظر گرفته شده برای رکوردهای ممیزی، بررسی کند که اقدامات ادعا شده، انجام می‌گیرند.

۶,۲ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱۳	**عملیات رمزنگاری ۱ (۱)**
محصول باید [اختصاص: برای وارسی صحت داده‌های ممیزی و داده‌های رکورد] بر اساس یک الگوریتم رمزنگاری مشخص [اختصاص: الگوریتم رمزنگاری] و اندازه کلید رمزنگاری [اختصاص: اندازه‌های کلید رمزنگاری]اجرا شود که مطابق با [اختصاص: لیستی از استانداردها]باشد. **نکته کاربردی ۴:** روش‌های اطمینان از صحت داده‌ی رکوردها و داده‌ی ممیزی بر عهده نویسنده سند هدف امنیتی است. نویسنده در صورت استفاده از مؤلفه‌های اضافی به منظور صحت داده‌ها باید آن‌ها را در سند هدف امنیتی اضافه کند. با توجه به روش بررسی صحت داده ممکن است نیاز به الزامات ذکر شده در «پیوست یک» باشد. همچنین در صورت استفاده از کلید رمزنگاری در محصول لازم است نویسنده سند هدف امنیتی الزامات مرتبط را از پیوست انتخاب نموده و به صورت تکمیل شده در سند هدف امنیتی ذکر کند. • **آزمون‌ها** ارزیاب باید اقدامات زیر را انجام دهد:	

آزمون اول: ارزیاب باید با بررسی سند هدف امنیتی، وجود کلید و الگوریتم رمزنگاری معتبر ادعا شده را در محصول تائید کند. الگوریتم و کلید باید مطابق استاندارد ارائه شده مربوط به الگوریتم باشد.

۱۴	**عملیات رمزنگاری ۱ (۲)**

محصول باید [اختصاص: برای تولید داده درهم‌سازی] بر اساس مجموعه الگوریتم‌های رمزنگاری مشخص [اختصاص: الگوریتم‌های رمزنگاری] و اندازه‌کلید رمزنگاری [اختصاص: هیچ‌کدام]اجرا شود که مطابق با [اختصاص: لیستی از استانداردها] باشد.

نکته کاربردی ۵:

از آنجائی که الگوریتم درهم‌سازی نیازی به کلید ندارد، محدودیتی برای اختصاص وجود ندارد. مجموعه الگوریتم‌های استاندارد قابل استفاده در پیوست یک؛ «الزامات اختیاری» بیان شده‌اند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید با بررسی سند هدف امنیتی، وجود و معتبر بودن الگوریتم درهم‌سازی ادعا شده را در محصول تائید کند.

۶,۳ کلاس حفاظت از داده کاربری

شماره الزام	نام الزام
۱۵	**خط‌مشی کنترل دسترسی ۱**

محصول باید [اختصاص: **خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال کند:

[اختصاص:

- موجودیت فعال: [اختصاص: مدیر سیستم، کاربر عادی، [اختصاص: دیگر موجودیت‌های فعال]]
- موجودیت غیرفعال:

- رکوردها، مستندات و فرا-داده[1]
- داده متعلق به کاربران
- داده احرازهویت
- داده با این معیارها: [اختصاص: معیارهای داده]
- [اختصاص: دیگر موجودیت‌های غیرفعال که شامل خط‌مشی کنترل دسترسی می‌باشند]

• عملیات:

- ایجاد موجودیت غیرفعال جدید
- حذف موجودیت غیرفعال
- تغییر دسترسی‌ها به موجودیت غیرفعال
- عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال
- [اختصاص: دیگر عملیات]

]

اقدامات ارزیابی:

• **خلاصه مشخصات محصول**

در این فصل از سند هدف امنیتی، باید سازوکار کنترل دسترسی محصول و مشخصه‌های امنیتی مورد استفاده در خط‌مشی کنترل دسترسی به طور خلاصه توضیح داده شود.

• **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی نموده و تائید کند توضیحاتی در خصوص خط‌مشی کنترل دسترسی و قوانین کنترل دسترسی برای مدیریت مشخصه‌های امنیتی ارائه شده است. همچنین ارزیاب باید این سند را در خصوص بیان چگونگی پیکربندی خط‌مشی کنترل دسترسی شامل مقداردهی پیش‌فرض مشخصه‌های امنیتی و انتساب مجوزهای مورد نیاز برای عملیات مدیریتی بررسی کند.

• **آزمون‌ها**

[1] Metadata

ارزیاب باید برای اقدامات زیر را انجام دهد: آزمون اول: بررسی تمام الگوریتم‌های کنترل دسترسی ذکر شده در سند هدف امنیتی آزمون دوم: برای هر الگوریتم کنترل دسترسی تمام شرایط ذکر شده در سند هدف امنیتی باید سنجیده شود (مانند شرایط منتهی شده به "yes" یا "no") آزمون سوم: آزمون و بررسی مجموعه ترکیباتی از تنظیمات مشخصه‌های امنیتی مورد استفاده در الگوریتم‌های کنترل دسترسی آزمون چهارم: آزمون و بررسی کارکردهای مدیریتی مورد استفاده برای مدیریت مشخصه‌های امنیتی (مشخصه‌های امنیتی که در الگوریتم کنترل دسترسی استفاده می‌شوند)
۱۶ **عملیات کنترل دسترسی ۱**
محصول باید [اختصاص: **خط‌مشی‌های کنترل دسترسی**] را با توجه به موارد زیر بر روی موجودیت‌های غیرفعال اعمال کند: [اختصاص: • هویت کاربر • نقش‌ها و مجوزهای کاربر مجاز • اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند • [اختصاص: دیگر مشخصه‌های موجودیت فعال]] **اقدامات ارزیابی:** الزامات عملیات کنترل دسترسی به الزام «خط‌مشی کنترل دسترسی ۱» وابسته است و همراه با آن الزام بررسی می‌شوند.
۱۷ **عملیات کنترل دسترسی ۲**
محصول باید قوانین زیر را اجرا کند تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز کند: [اختصاص: عملیات تنها به شرطی مجاز است که در لیست کنترل دسترسی، رکوردی وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد.]

اقدامات ارزیابی:

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید با کاربری که برای آن رکوردی بر مبنای دسترسی به موجودیت غیرفعال، وجود دارد، عملیات مجاز تعریف شده را آزمون کند. همچنین بررسی کند که در صورت عدم تعریف حق دسترسی، کاربر نمی‌تواند عملیاتی را بر روی موجودیت غیرفعال انجام دهد.

۱۸	**عملیات کنترل دسترسی ۳**

محصول باید بر اساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد:

[اختصاص:

- کاربران با مجوز مدیر سیستم به رکوردهای لازمه مدیریت سیستم و نیز روش ارائه شده توسط محصول، دسترسی دارند.
- کاربران غیرمجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل‌دسترس عموم، دسترسی دارند.
- [اختصاص: دیگر قوانین]

]

۱۹	**عملیات کنترل دسترسی ۴**

محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری کند:

[اختصاص:

- تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه[۱] از پیش تعریف شده،
- [اختصاص: دیگر قوانین]

]

اقدامات ارزیابی:

ارزیاب باید اقدامات زیر را انجام دهد:

[۱] Threshold

آزمون اول: ارزیاب باید برای یک کاربر مجاز چندین نشست هم‌زمان ایجاد کند و بررسی کند که محصول در صورت عبور تعداد نشست‌ها از حد آستانه، از دسترسی جلوگیری می‌کند.	
۲۰	**حفاظت کامل از اطلاعات باقیمانده در منابع ۱**
محصول باید تضمین کند در هنگام [انتخاب: تخصیص منابع به، آزادسازی منابع از] تمام موجودیت‌های غیرفعال استفاده شده، تمام محتوی اطلاعات قبلی آن منبع غیرقابل‌دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد. **اقدامات ارزیابی:** • **سند راهنمای محصول** در صورت امکان‌پذیری پیکربندی و مدیریت کارکردهای منابع در محصول، انتظار می‌رود که توضیحاتی در خصوص نحوه‌ی پیکربندی مدیریت منابع و استفاده مجدد از آن‌ها در سند راهنمای محصول بخش راهنمای مدیریتی محصول ارائه شده باشد. • **آزمون‌ها** ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید تمام واسطهایی که از منابع استفاده می‌کنند را بررسی کند. همچنین قابل‌دسترس بودن اطلاعات قبلی را در هنگام استفاده مجدد منابع، توسط موجودیت فعال دیگر (یک کاربر دیگر) تجزیه و تحلیل کند.	
۲۱	**ورود داده کاربری به محصول با مشخصه امنیتی ۱**
محصول باید هنگام دریافت داده کاربری، [اختصاص: خط‌مشی کنترل دسترسی] را اعمال کند. **اقدامات ارزیابی:** • **سند راهنمای محصول** ارزیاب باید در سند راهنمای محصول، ارائه توضیحاتی در خصوص نحوه‌ی کنترل و همچنین ورود داده کاربری را تائید کند. • **آزمون‌ها** ارزیاب باید اقدامات زیر را انجام دهد:	

آزمون اول: ارزیاب باید با توجه به پیکربندی و کنترل دسترسی که در راهنمای مدیریتی محصول آمده است، کاربری با مجوز ورود داده به داخل سیستم ایجاد کند و انجام درست عملیات را بررسی و تائید کند؛ همچنین با کاربری بدون مجوز وارد کردن داده، درستی یا عدم صحت عملیات بررسی گردد.

۲۲	**ورود داده کاربری به محصول با مشخصه امنیتی ۲**

محصول باید از مشخصه‌های امنیتی مرتبط با داده کاربری هنگام وارد کردن داده استفاده کند. مشخصات امنیتی شامل مواردی از این قبیل است: نوع داده، حجم و اندازه فایل، فرمت فایل، تعداد دفعات Import و از این قبیل موارد.

اقدامات ارزیابی:

- **آزمون‌ها**

این آزمون وابسته به الزام «ورود داده کاربری به محصول با مشخصه امنیتی ۱» است. همچنین ارزیاب هنگام ورود داده به سیستم باید اطمینان حاصل کند که تمامی مشخصه‌های امنیتی کاربر ذکر شده در راهنما همچون نام کاربری، امضاء دیجیتال و غیره نیز در نظر گرفته می‌شود. این بررسی در عملیاتی مانند «ثبت رکورد ممیزی عملیات ورود» با مشخصه امنیتی کاربر و همچنین «ذخیره داده وارد شده» با مشخصه امنیتی داده باید بررسی و تائید شود.

۲۳	**ورود داده کاربری به محصول با مشخصه امنیتی ۳**

محصول باید اطمینان دهد که پروتکل مورد استفاده برای انتقال داده، ارتباط و همبستگی شفافی را بین مشخصه‌های امنیتی و داده کاربری دریافت شده، فراهم می‌کند.

نکته کاربردی ۶:

هدف الزامات مربوط به «ورود داده کاربری به محصول»، ارائه کارکردهایی به منظور بررسی و صحت داده ورودی است. به عنوان مثال، محصول برای کنترل داده ورودی از سازوکاری همچون امضاء دیجیتال به منظور بررسی صحت استفاده کند.

اقدامات ارزیابی:

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید اطمینان حاصل کند ورود داده به داخل محصول، مطابق پروتکل ادعا شده در سند راهنمای محصول صورت می‌گیرد و در هنگام انتقال شنود و گم شدن داده وجود ندارد.

آزمون دوم: ارزیاب باید داده‌ای را مطابق با آنچه در سند راهنما محصول ذکر شده است به محصول ارسال نموده و بررسی کند که تمام اطلاعات و داده‌ها به طور صحیح و کامل انتقال داده شده است.

۲۴	**خروج داده کاربری از محصول با مشخصه امنیتی ۱**

محصول باید هنگام خروج داده کاربری به بیرون[۱] [اختصاص: خط‌مشی کنترل دسترسی] را اعمال کند.

اقدامات ارزیابی:

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید با توجه به پیکربندی و کنترل دسترسی که در سند راهنمای محصول آمده است، «کاربری دارای مجوز خروج داده از داخل سیستم» ایجاد نموده و صحت انجام عملیات را بررسی کند؛ سپس چگونگی انجام عملیات را با «کاربری بدون مجوز خروج داده از سیستم» بررسی کند.

۲۵	**خروج داده کاربری از محصول با مشخصه امنیتی ۲**

محصول باید به همراه داده کاربری خروجی (انتقال داده به بیرون از محصول)، مشخصه‌های امنیتی مرتبط با داده کاربری را نیز انتقال دهد.

نکته کاربردی ۷:

مشخصه‌های امنیتی داده کاربری می‌تواند شامل نوع داده، حجم داده، فرمت و اندازه فایل و غیره باشد.

اقدامات ارزیابی:

- **آزمون‌ها**

[۱] Export user data

این آزمون وابسته به الزام «خروج داده کاربری از محصول با مشخصه امنیتی ۱» است. ارزیاب هنگام خروج داده از سیستم باید اطمینان حاصل کند که مشخصه‌های امنیتی کاربر همانند نام کاربری، یا امضاء دیجیتال و غیره نیز در نظر گرفته می‌شود. همچنین باید بررسی گردد برای عملیات خروج با مشخصه امنیتی کاربر، رکورد ممیزی ثبت می‌گردد.	
۲۶	**خروج داده کاربری از محصول با مشخصه امنیتی ۴**
محصول باید هنگام خروج داده کاربری به بیرون (خارج از محصول)، قوانین زیر را اعمال کند: [اختصاص: مدیر سیستم باید خروج رکوردها را محدود کند، به طوری که کاربران محصول، قادر به خروج بدون هدف داده به بیرون از آن (خارج از محصول) نباشند.] **اقدامات ارزیابی:** ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید بعد از اعمال محدودیت بر روی داده کاربری، اقدام به خروج بدون هدف داده کند و سپس رفتار محصول را بررسی کند که آیا از این عمل جلوگیری می‌کند یا خیر.	
۲۷	**صحت داده کاربری ذخیره شده ۲**
محصول باید داده کاربری حساس و یا دارای بار حقوقی ذخیره شده در مکان تحت کنترل خود را برای تشخیص [اختصاص: خطاهای صحت داده] داده‌های رکورد و داده‌های ممیزی را بر اساس مشخصه‌های [اختصاص: درهم شده[۱] داده‌های کاربری ذخیره شده] پایش کند. **اقدامات ارزیابی:** • **خلاصه مشخصات محصول** در این فصل از سند هدف امنیتی باید در مورد پیاده‌سازی تشخیص خطای صحت توضیحاتی بیان شده باشد.	
۲۸	**صحت داده کاربری ذخیره شده ۳**
هنگام تشخیص خطای صحت داده، محصول باید [اختصاص: اقدام لازم] را صورت دهد.	

[۱] Hash

نکته کاربردی ۸:

محصول به منظور شناسایی خطای صحت داده‌ها باید مشخصه‌های داده کاربری را مانیتور کند تا در صورت تغییر و یا حذف، هشدار دهد. می‌توان برای تشخیص صحت داده‌ها از روش‌هایی همچون HMAC و یا ECC Checksum و دیگر روش‌های درهم‌سازی استفاده نمود.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

در این فصل از سند هدف امنیتی باید در مورد اقداماتی که در صورت تشخیص خطای صحت، صورت می‌گیرد، توضیحاتی بیان شده باشد.

۶,۴ کلاس شناسایی و احرازهویت

شماره الزام	نام الزام
۲۹	**مدیریت احرازهویت ناموفق ۱**
محصول باید بتواند با استفاده از [انتخاب: [اختصاص: یک عدد مثبت]، یک عدد مثبت قابل تنظیم توسط مدیر [اختصاص: بازه قابل قبولی از مقادیر]]، تلاش‌های ناموفق احرازهویت مرتبط با [اختصاص: لیستی از رویدادهای احرازهویت] را تشخیص دهد. **نکته کاربردی ۹:** به عنوان مثال در سومین اختصاص می‌توان به وارد نمودن کلمه عبور توسط کاربر برای احرازهویت شدن اشاره نمود. **اقدامات ارزیابی:** • **خلاصه مشخصات محصول**	

ارزیاب باید «خلاصه مشخصات محصول» از سند هدف امنیتی را بررسی نموده تا اطمینان حاصل کند توضیحاتی در خصوص روش‌های مورد پشتیبانی برای عملیات مدیریتی از راه‌دور و چگونگی تشخیص تلاش‌های موفق و ناموفق احراز هویت ارائه شده است.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل کند توضیحاتی در خصوص دستورات پیکربندی تعداد تلاش‌های موفق و ناموفق احرازهویت، ارائه شده است. همچنین در صورت استفاده از روش‌های مختلف احرازهویت از راه‌دور همانند SSH، توضیحات مربوطه باید در این سند شرح داده شود.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بر اساس حد آستانه تلاش موفق و ناموفق احرازهویت در سند راهنمای محصول، محصول را پیکربندی کند و هنگامی که تعداد تلاش احرازهویت به مقدار حد آستانه رسید، یک نام کاربری و کلمه عبور معتبر احرازهویت را بررسی کند که در این صورت محصول نباید اجازه ورود دهد.

۳۰	**مدیریت احرازهویت ناموفق ۲**

زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت [انتخاب: به حد تعیین شده رسید، بیشتر از حد تعیین شده رسید]، محصول باید [اختصاص: لیستی از اقدامات مقابله‌ای] را اجرا کند که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند و اطمینان حاصل کند، توضیحاتی در خصوص نحوه‌ی مدیریت احراز هویت در شرایطی که تعداد تلاش‌های ناموفق احرازهویت به بیش از حد آستانه (حد آستانه برای تلاش ناموفق نیز باید مشخص گردد) رسید ارائه شده باشد.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید ابتدا آزمون الزام «مدیریت احرازهویت ناموفق ۱» را انجام دهد، سپس بررسی کند که آیا محصول اقدام مقابله‌ای در جهت پیچیده‌تر کردن احرازهویت انجام می‌دهد یا خیر.	
۳۱	**تعریف مشخصات کاربر ۱**

محصول باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری نماید:

[اختصاص:

- شناسه کاربر
- متد احرازهویت مورد استفاده
- داده احرازهویت
- نقش کاربر
- وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)
- [اختصاص: **هر مشخصه امنیتی دیگر**]

]

نکته کاربردی ۱۰:

حداقل اطلاعات کاربری لازم برای شناسایی و احرازهویت باید وجود داشته باشد. این اطلاعات شامل نگهداری نمودن از هر مجوزی است که یک کاربر ممکن است دارا باشد.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید بررسی کند در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی مشخصه‌های امنیتی نگهداری شده برای هر کاربر تعریف شده باشد. البته ممکن است مشخصات لیست شده در خلاصه مشخصات محصول با لیست ذکر شده در این الزام (تعریف مشخصات کاربر ۱) متفاوت باشد. در این صورت، باید فصل «خلاصه مشخصات محصول» مشخصه‌های امنیتی مهم کاربر را پوشش دهد.

- **سند راهنمای محصول**

ارزیاب باید در راهنمای مدیریتی محصول از سند راهنمای محصول توضیحاتی در خصوص ایجاد، مشاهده، تغییر و یا حذف مشخصه‌های امنیتی کاربر (به عنوان مثال، تغییر کلمه عبور) مشاهده کند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید واسطهای مرتبط با مشخصه‌های امنیتی کاربر را بررسی کند و مشخصه‌های امنیتی تعریف شده برای کاربر را مشاهده کند و اطمینان یابد حداقل اطلاعات لازم برای شناسایی و احرازهویت را پوشش می‌دهد.

۳۲	**مدیریت کلمه عبور**

محصول باید قابلیت‌های مدیریت کلمه عبور را که در زیر ذکر شده‌اند برای کلمه‌های عبور مدیریتی فراهم کند:

۱. کلمه عبور باید بتوانند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص: [انتخاب: *"@"، "#"، "$"، "%"، "^"، "!" "&"، "*"، "(" ,")" [اختصاص: کاراکتر دیگر]]* باشد.

۲. حداقل طول کلمه عبور باید توسط مدیر امنیت، قابل تنظیم بوده و ۸ کاراکتر یا بیشتر باشد.

نکته کاربردی ۱۱:

نویسنده‌ی سند هدف امنیتی، کاراکترهای خاص پشتیبانی شده توسط محصول را انتخاب می‌کند. نویسنده این اختیار را دارد تا کاراکترهای خاص بیشتری را با استفاده از عبارت «اختصاص» لیست کند.

«کلمه عبور مدیریتی» به آن دسته از کلمه‌های عبور اشاره دارد که مدیران از آن‌ها در کنسول محلی یا پروتکل‌هایی که از «کلمه عبور» پشتیبانی می‌نمایند (مانند: SSH ,HTTPS)، استفاده می‌کنند.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید راهنمای محصول را بررسی نموده تا اطمینان حاصل کند در این سند توضیحات لازم در خصوص ایجاد کلمه‌های عبور قوی و تنظیم طول کلمه عبور برای مدیران بیان شده است.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید کلمه‌های عبور ضعیف و قوی ایجاد نموده و عکس‌العمل محصول در خصوص پشتیبانی از هر دو کلمه عبور را بررسی کند. آزمون دوم: ارزیاب باید اطمینان حاصل کند که تمام کاراکترها، قوانین و حداقل طول کلمه عبور که در سند راهنمای محصول آمده است پشتیبانی می‌گردد.
۳۳ **احرازهویت کاربر ۱**
محصول باید پیش از احرازهویت کاربر، اجازه اقدامات میانی زیر را به کاربر دهد: [انتخاب: • مشاهده راهنمای نحوه ورود به سیستم • شناسایی کاربر • بازیابی کلمه عبور • هیچ اقدامی • [اختصاص: دیگر اقدامات]] **اقدامات ارزیابی:** • **آزمون‌ها** ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید با استفاده از راهنمای محصول پیکربندی مناسبی برای احرازهویت تنظیم کند؛ بنابراین در اعتبارسنجی/روش احرازهویت باید جهت دسترسی به سیستم، اطلاعات صحیح مرتبط با احرازهویت فراهم شود. در حالی که در منع دسترسی به سیستم، اطلاعات نادرست فراهم می‌شود.
۳۴ **احرازهویت کاربر ۲**
محصول باید هر کاربر را پیش از آنکه امکان انجام اقدامات میانی دیگری داشته باشد، با موفقیت احرازهویت نماید. **نکته کاربردی ۱۲:**

ارزیاب باید در این الزام عملیاتی مانند فراموشی کلمه عبور و دیگر عملیاتی را که در اقدامات ذکر شده در الزام «احرازهویت کاربر ۱» مشاهده و بررسی کرده است، مورد آزمون قرار دهد؛ بنابراین لیستی از عملیاتی که باید قبل از امکان دسترسی و اجرای آن‌ها، کاربر شناسایی موفق شود، در سند راهنمای محصول ذکر گردد.

۳۵	**سازوکار احرازهویت چندگانه ۱**

محصول باید به منظور احرازهویت کاربر سازوکارهای زیر را فراهم آورد:

[انتخاب:

- نام کاربری و کلمه عبور
- امضاء دیجیتال
- [اختصاص: سایر شیوه‌های احرازهویت]

]

نکته کاربردی ۱۳:

برای احرازهویت کاربر، بیش از یک سازوکار احرازهویت می‌تواند در محصول به کاررفته باشد. به عنوان مثال، برای احرازهویت در محصول «نام کاربری و کلمه عبور، گواهی دیجیتال» استفاده می‌گردد. در این الزام همچنین سایر روش‌های احرازهویت امن طرف سوم دیگر مانند: Active directory, OAuth2 و ... می‌تواند در اختصاص قرار گیرد.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی بررسی کند که سازوکار احرازهویت معرفی شده باشد.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: برای آزمون این الزام، ابتدا باید الزام «احرازهویت کاربر ۱» به طور کامل مورد تائید قرار گرفته باشد. سپس ارزیاب باید همه سازوکارهای احرازهویت قابل‌دسترس را پیکربندی نموده و واسط‌های پشتیبان تمام سازوکارهای احرازهویت را بررسی کند.	
۳۶	**سازوکار احرازهویت چندگانه ۲**
محصول باید هر کاربر متقاضی احرازهویت را مطابق [اختصاص: کاربران از راه‌دور باید علاوه بر بررسی نام کاربری و کلمه عبور از روش احرازهویت چندگانه (مانند Dual factor authentication) استفاده کند، [اختصاص: OTP یا توکن و از این قبیل موارد]] احرازهویت کند. **اقدامات ارزیابی:** این الزام وابسته به الزام «سازوکار احرازهویت چندگانه ۱» وابسته است.	
۳۷	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱**
محصول باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری کند: [اختصاص: • شناسه کاربر • نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه • جزئیات واسط کلاینت • پیشینه احرازهویت (جزئیات تلاش برای احرازهویت موفق و ناموفق) • [اختصاص: لیست دیگر مشخصه‌های کاربری]] **نکته کاربردی ۱۴:** در اختصاص دوم می‌توان مواردی از قبیل آخرین دسترسی‌ها به موجودیت‌های غیرفعال را در نظر گرفت. **اقدامات ارزیابی:** • **خلاصه مشخصات محصول**	

ارزیاب باید مشخصه‌های امنیتی کاربر که در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی آمده است را با مشخصاتی که در واسط محصول وجود دارد مطابقت دهد تا نسبت به پشتیبانی این الزام اطمینان حاصل کند.

- **سند راهنمای محصول**

ارزیاب باید بخش راهنمای مدیریتی از سند راهنمای محصول را بررسی کند تا اطمینان حاصل کند که نحوه ایجاد موجودیت فعال و امکان تغییر مشخصه‌های امنیتی آن بیان شده باشد.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بتواند بر اساس سند راهنمای محصول، مشخصه‌های امنیتی را برای اجرای عملیات مقداردهی و ویرایش کند. سپس چگونگی اعمال این تغییرات (موفقیت‌آمیز یا عدم موفقیت) را بررسی کند. در برخی موارد این آزمون را باید همراه با کنترل دسترسی، محدودیت‌های مدیریتی امنیتی و یا در ممیزی صورت گیرد.

آزمون دوم: ارزیاب باید بتواند مشخصه‌های امنیتی را با توجه به راهنمای شرح محصول، با تمامی حداقل شرایط، مقداردهی و یا ویرایش کند. همچنین ارزیاب با دریافت خطا هنگام بررسی و اعمال مقادیر مختلف در مشخصه‌های امنیتی می‌تواند متوجه شود که تغییرات مشخصه‌های امنیتی به‌درستی اعمال نشده است. در برخی موارد باید این آزمون همراه با کنترل دسترسی، محدودیت‌های مدیریتی امنیتی و یا در ممیزی بررسی شود.

۳۸	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲**

محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه‌های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می‌کند، اعمال کند:

[اختصاص:

- زمانی که یک نشست جدید برقرار می‌شود، اعتبار نشست‌های قبلی باید از بین برود (به جزء مواردی که فعال بودن هم‌زمان چندین نشست مورد نیاز کارکردی برنامه باشد و هنگام فعال شدن نشست دوم و بیشتر در برنامه، باید به صفحه کاربر نشست اصلی (اول) اطلاع داده شود.)
- اطلاعات پیشینه احراز هویت باید به‌روزرسانی گردد
- [اختصاص: دیگر قوانین برای اتصال اولیه مشخصه‌ها]

]

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید در سند راهنمای محصول توضیحاتی در خصوص نحوه‌ی ایجاد موجودیت‌های فعال و اعمال تغییر در مشخصه‌های امنیتی مرتبط با موجودیت‌های فعال مشاهده کند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب ابتدا نشستی را با محصول آغاز کند و بعد از محصول خارج شود، ممکن است اطلاعات نشست به درستی منقضی نشده باشد لذا لازم است ارزیاب مجدد به سیستم ورود کند و بررسی کند که از شناسه نشست قبلی استفاده شده است یا خیر.

۳۹	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳**

محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال کند:

[اختصاص: هیچ تغییری در طول نشست فعال مجاز نیست، [اختصاص: دیگر قوانین حاکم بر تغییرات مشخصه‌ها]]

نکته کاربردی ۱۵:

منظور از تغییرات، به این معناست که هیچ‌یک از مشخصه‌های امنیتی کاربر تعریف شده در الزام «انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱» در طول نشست تغییر نکند. تغییر نقش کاربر نیاز به ورود مجدد دارد.

اقدامات ارزیابی:

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب ابتدا با یک نام کاربری مشخص نشستی را با محصول آغاز کند، سپس یکی از مشخصه‌های امنیتی کاربر مانند آدرس IP سیستم را تغییر دهد در این صورت باید نشست غیرفعال و خاتمه یابد.

آزمون دوم: ارزیاب ابتدا نشستی را با محصول با یک نام کاربری مشخص آغاز کند، سپس اطلاعات نشست را به سیستم دیگر انتقال داده و تلاش کند با همان اطلاعات نشست اتصال با محصول ادامه داشته باشد. در این حالت به دلیل تغییر سیستم و تغییر محیط ارتباطی (با استفاده از سازوکارهای http only و یا دیگر توکن‌های تصادفی در کنار نشست که همچنین برای جلوگیری از CSRF نیز است می‌توان استفاده کرد) سیستم کاربر باید نشست خاتمه یابد و مجدداً احرازهویت صورت گیرد. آزمون سوم: ارزیاب ابتدا از طریق نام کاربری و مرورگر مشخص یک نشست با محصول آغاز کند، سپس با مرورگر دیگری همان اطلاعات نشست را وارد نموده و تلاش کند اتصال با محصول با همان اطلاعات نشست ادامه داشته باشد. در این صورت باید نشست خاتمه یابد و مجدداً احرازهویت صورت گیرد.

۶,۵ کلاس مدیریت امنیت

شماره الزام	نام الزام
۴۰	**مدیریت کارکرد در محصول ۱**
محصول باید امکان [انتخاب: تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار] توابع [اختصاص: تمام کارکردهای مربوط به مدیریت محصول] را به [اختصاص: مدیر سیستم و هر کاربری که مجوز لازم را دارد، [اختصاص: دیگر نقش‌ها]] محدود کند. **نکته کاربردی ۱۶:** مثالی از این اختصاص: محصول باید امکان «تغییر رفتار» کارکرد جمع‌آوری داده‌های سیستم، آنالیز و عکس‌العمل را تنها به مدیران مجاز سیستم محدود نمایند. **اقدامات ارزیابی:**	

- **خلاصه مشخصات محصول**

ارزیاب باید در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی، هریک از کارکرد مدیریتی معرفی شده در راهنما (که از طریق واسط قابل‌دسترسی هستند) را بررسی و تائید کند.

- **سند راهنمای محصول**

ارزیاب باید لیست کارکردهای محصول را در این سند بررسی و تائید کند و همچنین ذکر چگونگی پیکربندی و تنظیمات کارکردها در محصول را بررسی کند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید یک‌بار با مجوز مدیر سیستم سعی در تغییر پیکربندی کارکردهای محصول مطابق با سند راهنمای محصول کند و بار دیگر با حساب کاربری غیرمجاز تلاش به غیرفعال نمودن و یا تغییر تنظیمات اعمال شده در کارکردها کند.

۴۱	**مدیریت مشخصه‌های امنیتی ۱**

محصول باید با اعمال [اختصاص: خط‌مشی کنترل دسترسی]، امکان تغییر پیش‌فرض، [انتخاب: پرس‌وجو، تغییر، حذف، [اختصاص: دیگر عملیات]] مشخصه‌های امنیتی [اختصاص: لیستی از مشخصه‌های امنیتی تعریف شده در الزام انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱] را به [اختصاص: مدیر سیستم و هر کاربری که مجوز لازم را دارد] محدود کند.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند و اطمینان حاصل کند در خصوص شرایطی که یک کاربر اجازه مدیریت مشخصه‌های امنیتی موجودیت‌های غیرفعال را دارد توضیحاتی ارائه شده است.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید تمامی واسط‌های مرتبط با مدیریت مشخصه‌های امنیتی موجودیت‌های غیرفعال و تمام مشخصه‌های امنیتی موجودیت‌های غیرفعال با مقداردهی آن‌ها (البته به عنوان بخشی از آزمون الگوریتم کنترل دسترسی در الزام قبل بررسی می‌شوند) را آزمون کند.

۴۲	**مدیریت داده محصول ۱**

محصول باید امکان [انتخاب: تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن، [اختصاص: دیگر کارکردها]] [اختصاص: لیستی از داده‌های محصول] را به [اختصاص: مدیر سیستم و هر کاربری که مجوز لازم را دارد] محدود کند.

نکته کاربردی ۱۷:

داده محصول می‌تواند شامل داده ممیزی، کلیدها و داده احرازهویت و از این نوع داده‌ها باشد.

مثالی از این الزام:

محصول امکان مدیریت داده‌های خود را تنها به مدیر امنیتی محدود می‌کند.

«مدیریت» در این الزام می‌تواند شامل موارد زیر باشد:

ایجاد، مقداردهی، مشاهده، تغییر پیش‌فرض، تغییر دادن، حذف کردن، پاک کردن و اضافه کردن

اقدامات ارزیابی:

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید با حساب کاربری دارای مجوز و حساب کاربری بدون مجوز، کارکردهای این الزام را برای داده محصول بررسی کند و از درستی مجاز بودن یا نبودن آن اطمینان حاصل کند.

۴۳	**کارکردهای مدیریتی محصول ۱**

محصول باید قادر به انجام [اختصاص: کارکردهای مدیریتی که در جدول زیر آمده است] باشد:

مؤلفه	عملیات مدیریتی
بازبینی داده ممیزی ۱	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
انتخاب داده ممیزی ۱	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی
اقدامات لازم در زمان از دست رفتن داده ممیزی ۱	پشتیبانی از حد آستانه و از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
پیشگیری از اتلاف و از بین رفتن داده‌های ممیزی ۱	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
عملیات کنترل دسترسی	مدیریت مشخصه‌های مورد استفاده برای ایجاد دسترسی و یا منع
حفاظت کامل از اطلاعات باقیمانده در منابع	انتخاب هنگام اجرای حفاظت از اطلاعات باقی‌مانده (برای مثال، تخصیص و یا آزادسازی) که می‌تواند در محصول قابل پیکربندی باشد.
ورود داده‌های کاربری به محصول با مشخصه امنیتی	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
صحت داده‌های کاربری ذخیره شده ۲	عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی باشد.
مدیریت احراز هویت ناموفق	مدیریت حد آستانه برای تلاش‌های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احرازهویت باید صورت گیرد.
تعریف مشخصات کاربر	مدیر مجاز باید قادر به تعریف مشخصه‌های امنیتی بیشتر برای کاربران باشد. [اختیاری]
مدیریت کلمه عبور	مدیریت تنظیمات و الزامات و قابلیت‌ها برای تنظیم کلمه عبورها
احراز هویت کاربر	مدیریت داده‌های احرازهویت توسط مدیر یا کاربر مرتبط مدیریت یکسری عملیاتی که قبل از احرازهویت کاربر انجام می‌شوند.
سازوکار احرازهویت چندگانه	مدیریت سازوکارهای احرازهویت مدیریت قوانین مرتبط با احرازهویت
شناسایی کاربر	مدیریت شناسایی کاربران]اختیاری[مدیریت تغییرات و فرایندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.

انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر	مدیر مجاز می‌تواند مشخصه‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف و تغییر دهد.
مدیریت مشخصه‌های امنیتی	مدیریت گروهی از نقش‌هایی که با مشخصه‌های امنیتی در تعامل هستند.
مقداردهی اولیه مشخصه‌ها	مدیریت گروهی از نقش‌هایی که مقادیر اولیه را مشخص می‌کنند. مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول
مدیریت داده‌های محصول ۱-مدیر سیستم	مدیریت گروهی از قوانینی مرتبط با داده‌های محصول
مدیریت داده‌های محصول ۱-کاربر عادی، واردکننده داده	مدیریت گروهی از قوانینی مرتبط با داده‌های محصول
نقش‌های امنیتی	مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند.
محدودیت بر روی چندین نشست هم‌زمان	مدیریت حداکثر نشست مجاز کاربران به طور هم‌زمان توسط مدیر
برقراری نشست	مدیریت شرایط آغاز نشست توسط مدیر مجاز
خاتمه دادن به نشست‌ها	تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد. تعیین زمان پیش‌فرض غیرفعال بودن کاربر که نشست خاتمه یابد.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

تمام کارکردهای امنیتی محصول به طور خلاصه باید در این بخش توضیح داده شود.

۴۴	**نقش‌های امنیتی ۱**

نقش‌های زیر در محصول باید تعریف شده باشد:

[انتخاب: مدیر سیستم، کاربر عادی، [اختصاص: دیگر نقش‌های مجاز معرفی شده]]

نکته کاربردی ۱۸:

از جمله نقش‌های مجاز می‌توان به «مدیر مجاز»، «مدیر تحلیلگر مجاز»، «اپراتورها» اشاره نمود، نویسنده سند هدف امنیتی در این الزام می‌تواند از نقش‌های مجاز دیگر نیز استفاده کند.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید در این فصل از سند هدف امنیتی بررسی و تائید کند توضیحاتی در خصوص نقش مدیریتی و نقش‌هایی با دسترسی پایین ارائه شده است.

- **سند راهنمای محصول**

ارزیاب باید بخش راهنمای مدیریتی از سند راهنمای محصول را بررسی نموده و در خصوص ارائه دستورالعمل‌هایی برای مدیریت محصول هم به‌طور محلی و از راه دور و همچنین پیکربندی‌هایی مورد نیاز برای مدیریت راه دور اطمینان حاصل کند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید اطمینان حاصل کند که نقش مدیریتی می‌تواند تمامی کارکردهای امنیتی محصول که در سند هدف امنیتی ذکر شده است را مدیریت کند. ارزیاب باید نقش مدیریتی و یا کاربر با یک نقش محدود را به طور محلی و یا از راه‌دور بر روی محصول آزمون کند.

۴۵	**نقش‌های امنیتی ۲**

محصول، باید قادر به مرتبط نمودن کاربران با نقش‌ها و دسترسی‌های مجاز تعریف شده باشند.

نکته کاربردی ۱۹:

لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد؛ اما ممکن است نقش‌ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.

۶,۶ کلاس حفاظت از توابع امنیتی محصول

شماره الزام	نام الزام
۴۶	**حفظ وضعیت امن در زمان شکست ۱**
محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند: [اختصاص: شکست‌های نرم‌افزاری، شکست‌های سخت‌افزاری] **نکته کاربردی ۲۰:** شکست نرم‌افزاری به معنی از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول است که در این صورت محصول باید در وضعیت امنی قرار گرفته و صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ کند. **اقدامات ارزیابی:** • **خلاصه مشخصات محصول** ارزیاب باید در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی، بررسی کند توضیحاتی در خصوص پیاده‌سازی شکست امن محصول، انواع مدهای شکست محصول و وضعیت امن هرکدام از شکست‌ها نیز ارائه شده باشد. • **آزمون‌ها** ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید انواع شکست‌ها را ایجاد و با وضعیت امن مقایسه و بررسی کند.	
۴۷	**انتقال داده امنیتی در داخل محصول ۱**

محصول باید توانایی داشته باشد که در صورت فراهم نمودن بستر و زیرساخت امن، از افشاء یا تغییر داده در هنگام انتقال بین بخش‌های مجزای خود که باهم ارتباط دارند، محافظت کند.

نکته کاربردی ۲۱:

منظور از بخش‌های مجزا به این معنی است که بخش‌های محصول بر روی دو سیستم مجزا قرار گرفته باشد، مانند وب سرور بر روی یک سیستم و بانک اطلاعاتی روی سیستم دیگر در یک شبکه عمومی باشد و یا دو بخش مجزای محصول یکی بر روی وب سرور و دیگری بر روی کلاینت باشد.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید در فصل «خلاصه مشخصات محصول» از سند هدف امنیتی بررسی کند در خصوص روش یا پروتکل‌های استفاده شده برای انتقال داده بین اجزای توزیع‌شده محصول توضیحاتی ارائه شده است.

- **سند راهنمای محصول**

ارزیاب باید با بررسی سند راهنمای محصول، نسبت به ارائه توضیحاتی در خصوص روش یا پروتکل ارتباطی بین اجزای محصول اطمینان حاصل کند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید روش ارتباطی ذکر شده در سند راهنمای محصول را آزمون کند.

آزمون دوم: ارزیاب باید اطمینان حاصل کند که داده‌ها بین اجزای محصول به‌صورت آشکار نمایش داده نشود.

آزمون سوم: ارزیاب باید اطمینان حاصل کند که ویرایش داده‌ها حین انتقال، توسط محصول تشخیص داده شود.

۴۸	**سازگاری داده امنیتی بین محصول و موجودیت امن ۱**

محصول در صورت استفاده از محصولات امن IT، باید تفسیر سازگار [اختصاص: لیستی از انواع داده امنیتی محصول] را در زمان اشتراک‌گذاری داده امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد.

نکته کاربردی ۲۲:

منظور از داده امنیتی محصول، داده‌های احرازهویت، کلید، امضای دیجیتال، داده‌های ممیزی و از این نوع داده‌ها است.

اقدامات ارزیابی:

- **سند راهنمای محصول**

در بخش راهنمای مدیریتی از سند راهنمای محصول باید توضیحاتی درخصوص انواع داده امنیتی محصول و داده اشتراک گذاشته شده یا دریافتی از دیگر محصولات امن IT ارائه شده باشد.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید با بررسی داده دریافتی از دیگر محصولات در داخل محصول نسبت به انطباق داده محصول با آنچه ادعای محصول است، اطمینان حاصل کند. ارزیاب باید همچنین از انطباق داده اشتراک گذاشته شده بین خود و دیگر محصولات امن IT اطمینان یابد.

۴۹	**مهرهای زمانی ۱**

محصول، باید قادر به ایجاد مهرهای زمانی قابل‌اطمینان باشند و یا این نیازمندی را از طریق سرورهای امن و سازوکار کارکردی صحیح برطرف کند.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید اطمینان حاصل کند در فصل «خلاصه مشخصات محصول» از سند هدف امنیت هریک از کارکردهای امنیتی استفاده‌کننده از زمان لیست شده باشد.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند تا در خصوص ارائه‌ی دستورالعمل‌هایی در مورد تنظیمات و پیکربندی زمان اطمینان حاصل کند.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را اجرا کند:

آزمون اول: ارزیاب باید مطابق سند راهنمای محصول، زمان را پیکربندی نموده و سپس با توجه به واسط مربوطه از صحت عملکرد آن اطمینان حاصل کند.

آزمون دوم: ارزیاب باید توسط کاربر غیرمجاز و با استفاده از واسط مربوط، سعی در تغییر پیکربندی زمان کند.

آزمون سوم: اگر محصول از سرور NTP پشتیبانی می‌کند باید کلاینت NTP را بر روی محصول پیکربندی نموده و زمان سرور و کلاینت را بررسی کند.

۵۰	**به‌روزرسانی امن ۲**

محصول مورد ارزیابی باید این امکان را برای مدیر سیستم امنیتی به همراه کارشناس شرکت تولیدکننده محصول فراهم کند که به‌روزرسانی نرم‌افزار و میان‌افزار محصول مورد ارزیابی را به صورت دستی آغاز کند و [انتخاب: از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند، از به‌روزرسانی‌های خودکار پشتیبانی کند، از سازوکار به‌روزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل به‌روزرسانی، از هیچ سازوکار به‌روزرسانی پشتیبانی نکند].

نکته کاربردی ۲۳:

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

۵۱	به‌روزرسانی امن ۳
محصول مورد ارزیابی باید در صورت استفاده از به‌روزرسانی به روش خودکار، پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از [انتخاب: سازوکار امضای دیجیتال، درهم‌ساز منتشرشده]، ابزاری را برای احراز هویت میان‌افزار آن‌ها در اختیار محصول مورد ارزیابی قرار دهد.	

۶,۷ کلاس تخصیص منابع

شماره الزام	نام الزام
۵۲	تحمل خطا ۱
محصول باید از عملکرد [اختصاص: تمام کارکردهای اصلی] هنگام رویداد شکست‌های زیر اطمینان حاصل کند: [اختصاص: شکست نرم‌افزاری، [اختصاص: انواع دیگر شکست‌ها]] **اقدامات ارزیابی:** • **آزمون‌ها** ارزیاب باید اقدامات زیر انجام دهد: آزمون اول: ارزیاب باید شکستی را ایجاد و سپس بررسی کند که کارکردهای اصلی (مانند ممیزی) به‌درستی کار می‌کنند یا خیر.	

۶,۸ کلاس دسترسی به محصول

شماره الزام	نام الزام

۵۳	**محدودیت بر روی چندین نشست هم‌زمان ۱**

محصول باید حداکثر تعداد نشست‌های هم‌زمان متعلق به یک کاربر را محدود کند.

نکته کاربردی ۲۴:

محصول می‌تواند انتخاب عملیاتی را که بعد از پر شدن نشست‌های هم‌زمان باید روی دهد را به مدیر سیستم و یا کاربر دارای مجوز بدهد.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل کند توضیحاتی در خصوص نحوه‌ی پیکربندی تعداد نشست هم‌زمان برای یک کاربر در راهنمای محصول ارائه شده است.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید با توجه به سند راهنمای محصول حداکثر نشست یک کاربر را پیکربندی کند و سپس با همان کاربر از چند سیستم به طور هم‌زمان سعی در ایجاد نشست کند. در این صورت اگر تعداد نشست بیش از مقدار مشخص شده باشد باید اجازه ایجاد نشست را ندهد.

۵۴	**خاتمه دادن به نشست‌ها توسط محصول ۱**

محصول باید کلیه نشست‌های تعاملی راه‌دور[۱] را پس از مدت‌زمان [اختصاص: **بازه زمانی که توسط مدیر تنظیم می‌شود**] غیرفعال بودن، خاتمه دهد.

اقدامات ارزیابی:

[۱] Remote

• **سند راهنمای محصول** در راهنمای محصول باید در خصوص نحوه‌ی پیکربندی زمان غیرفعال بودن نشست توضیحاتی بیان شده باشد. • **آزمون‌ها** ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید مطابق سند راهنمای محصول، مقادیر مختلف برای زمان غیرفعال بودن نشست تنظیم و پیکربندی کند که این مقادیر شامل حداقل و حداکثر زمان غیرفعال بودن طبق سند راهنما باشند. سپس ارزیاب برای هر زمان تنظیم شده نشستی از راه دور با محصول ایجاد و درستی زمان غیرفعال بودن نشست را بررسی کند که باعث خاتمه یافتن نشست می‌شود.
۵۵ **خاتمه دادن به نشست‌ها توسط کاربر ۱**
محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد. **اقدامات ارزیابی:** • **آزمون‌ها** ارزیاب باید اقدامات زیر را اجرا کند: آزمون اول: ارزیاب باید نشست محلی با محصول ایجاد نموده و سپس مطابق راهنما با استفاده از موارد "Exit" یا "Log out" از محصول خارج شود و بررسی کند که آیا نشست خاتمه یافته است. آزمون دوم: ارزیاب باید نشستی از راه‌دور با محصول ایجاد نموده و سپس مطابق راهنما با استفاده از موارد "Exit" یا "Log out" از محصول خارج شود و بررسی کند که آیا نشست خاتمه یافته است.
۵۶ **سوابق دسترسی به محصول ۱**
در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس [انتخاب: روز، زمان، [اختصاص: دیگر مشخصه‌ها]] باشد.
۵۷ **سوابق دسترسی به محصول ۲**

در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس [انتخاب: روز، زمان، [اختصاص: دیگر مشخصه‌ها]] و تعداد تلاش ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز باشد.

اقدامات ارزیابی:

- **سند راهنمای محصول**

باید در این سند در خصوص نحوه‌ی پیکربندی نمایش تعداد و آخرین تلاش ناموفق توضیحاتی ارائه شده باشد.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را اجرا کند:

آزمون اول: ارزیاب چندین بار با استفاده از یک نام کاربری با شرایطی غیرمجاز (مانند کلمه عبور نادرست) تلاش به برقراری نشست با محصول کند و سپس یک نشست موفقیت‌آمیزی را برقرار کند و بررسی کند که تعداد تلاش‌های ناموفق کاربر و زمان آخرین تلاش برای برقراری نشست در محصول ثبت شده باشد.

۵۸	**سوابق دسترسی به محصول ۳**

محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر از واسط کاربری پاک کند.

اقدامات ارزیابی

- **سند راهنمای محصول**

در صورت وجود امکان پیکربندی اطلاعات سوابق دسترسی، باید در بخش راهنمای مدیریتی از سند راهنمای محصول توضیحاتی ارائه شده باشد.

۵۹	**برقراری نشست ۱**

محصول باید قادر به ممانعت از ایجاد نشست بر اساس [انتخاب: مکان، شماره پورت، روز، زمان، [اختصاص: دیگر مشخصه‌ها]] باشد.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید با بررسی فصل «خلاصه مشخصات محصول» از سند هدف امنیتی نسبت به تعریف تمام مشخصه‌های کلاینتی که باید نشست آن منع شود، اطمینان حاصل کند.

- **راهنما**

ارزیاب باید در سند راهنمای محصول، بررسی کند توضیحاتی در خصوص پیکربندی هر مشخصه‌ای که در «خلاصه مشخصات محصول» آمده است (مشخصه‌هایی مانند آدرس IP ، زمان/تاریخ، آدرس فیزیکی و ...) ارائه شده است.

- **آزمون‌ها**

ارزیاب باید برای هر یک از مشخصه‌ها، آزمون زیر را انجام دهد:

آزمون اول: ارزیاب باید با یک کاربر یک نشست موفقیت‌آمیزی را ایجاد کند، سپس مطابق راهنما، مشخصه‌های کاربر را به گونه‌ای پیکربندی کند که از دسترسی آن کاربر به محصول ممانعت شود. ارزیاب باید تلاش در برقراری نشستی کند که مشخصه‌ای از آن (مانند آدرس IP و یا مکان کاربر) برای دسترسی منع شده باشد و سپس عدم موفقیت کاربر در تلاش برای دسترسی را مشاهده کند.

۶,۹ کلاس کانال‌های/مسیرهای مورد اعتماد

برای این کلاس، تعدادی الزام مبتنی بر انتخاب در «پیوست دو» ارائه شده است.

شماره الزام	نام الزام
۶۰	**مسیر امن ۱**
محصول باید قادر باشد در صورت فراهم بودن زیرساخت لازم با استفاده از پروتکل [انتخاب: TLS, HTTPS] مسیر ارتباطی امنی فراهم کند تا بدین ترتیب کانال ارتباطی بین خود و کاربران راه‌دور ایجاد شود که به طور منطقی از دیگر کانال‌ها متمایز بوده، کاربر مربوطه را احراز هویت نموده و از تغییر و افشاء داده‌های تبادلی حفاظت کند و تغییرات را تشخیص دهد.	

نکته کاربردی ۲۵: کاربر عمومی مجوز ورود به محصول را ندارد. نویسنده سند هدف امنیتی در صورت استفاده از TLS باید الزامات آن را از «پیوست دو» به سند هدف امنیتی اضافه کند.	
۶۱	**مسیر امن ۲**
محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.	
۶۲	**مسیر امن ۳**
محصول مورد ارزیابی باید استفاده از کانال امن را برای احرازهویت اولیه مدیر سیستم و تمام فعالیت‌های راه‌دور مدیر سیستم الزامی کند. **نکته کاربردی ۲۶:** این الزام اطمینان حاصل می‌کند که مدیران سیستم معتبر، تمام ارتباطات از راه دور را با محصول مورد ارزیابی، از طریق یک مسیر امن آغاز می‌کنند و در طی ارتباط با محصول مورد ارزیابی، همچنان از مسیر امن استفاده می‌نمایند. داده‌های منتقل شده از طریق این مسیر، با استفاده از پروتکل انتخاب شده در عبارت انتخاب، رمزگذاری می‌شوند.	

۷ الزامات تضمین امنیت

اهداف امنیتی تعریف شده در بخش ۵ جهت مقابله نمودن با تهدیدات معرفی شده در بخش ۴ در نظر گرفته شده‌اند. الزامات کارکردی در بخش ۶ بیان رسمی و استانداردی از «اهداف امنیتی» است. الزامات تضمین امنیتی که برگرفته از استاندارد ارزیابی امنیتی معیار مشترک می‌باشند تا بر اساس این الزامات ارزیابی، مستندات را ارزیابی و آزمون مستقل بر روی محصول انجام دهد.

مدل کلی ارزیابی محصول در برابر سند هدف امنیتی که مطابق این پروفایل حفاظتی است، به صورت زیر است:

پس از تائید سند هدف امنیتی برای ارزیابی، تولیدکننده محصول را در اختیار آزمایشگاه قرار می‌دهد و محیط آزمون آن را فراهم می‌کند؛ و سپس فعالیت‌های تضمین که در سند هدف امنیتی مطرح شده، توسط آزمایشگاه انجام می‌شود. نتایج این فعالیت‌ها مستند و برای اعتباربخشی به مرکز گواهی ارائه می‌شود.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Life cycle Support	ALC_CMC.1	برچسب‌گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول
Security Target	ASE_CCL.1	ادعاهای انطباق
	ASE_ECD.1	تعریف مؤلفه‌های توسعه‌یافته
	ASE_INT.1	معرفی هدف امنیتی
	ASE_OBJ.1	اهداف امنیتی
	ASE_REQ.1	الزامات امنیتی معین
	ASE_TSS.1	خلاصه مشخصات هدف ارزیابی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری

۷,۱ کلاس توسعه

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

مشخصات کارکردی:

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

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید مشخصات کارکردی را ارائه کند.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه کند. **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،

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

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

[۱]-SFR-enforcing TSFI

[۲]-SFR-supporting TSFI

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.3C)** **شرح مؤلفه:** مشخصات کارکردی باید برای دسته‌بندی ضمنی واسطهای غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه کند.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.4C)** **شرح مؤلفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسطهای کارکرد امنیتی در سند مشخصات کارکردی باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌کند.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2E)**

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: ارزیاب باید مشخص کند که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.

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

۷,۲ کلاس راهنمای کاربر

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

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

دستورالعمل نصب موفقیت‌آمیز محصول در محیط

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

دستورالعمل‌هایی که ارائه‌دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو است.

۷,۲,۱ راهنمای کاربردی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1D)**

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: توسعه‌دهنده باید راهنمای کاربردی ارائه کند.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف کند، همانند هشدارهای مناسب.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف کند که چگونه از واسط‌های در دسترس ارائه شده توسط محصول به صورت امن استفاده می‌گردد.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:**

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

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.7C)** **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل‌فهم باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌کند.

۷,۲,۲ راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱**

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

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه‌دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

مؤلفه‌های اقدامات ارزیاب	
راهنمای آماده‌سازی	**نام عنصر: راهنمای آماده‌سازی ۱**

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

۷,۳ 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 قابل‌مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه‌دهنده نقش کمرنگی در قابل‌اعتماد بودن محصول دارد، بلکه در این سطح اطمینان (EAL1) تنها به این اطلاعات نیاز است.

۷,۳,۱ قابلیت‌های پیکربندی

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

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

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

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

۷,۳,۲ حوزه پیکربندی

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

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

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

۷,۴ کلاس هدف امنیتی

ارزیابی سند هدف امنیتی برای اطمینان از شفاف بودن و نداشتن ناسازگاری داخلی لازم است. همچنین اگر سند هدف امنیتی از یک یا چند پروفایل حفاظتی استفاده کرده است، تضمین درست بودن آن و انتخاب‌های درست صورت گرفته شده در آن، لازم است.

۷,۴,۱ ادعاهای انطباق

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
ادعاهای انطباق **(ASE_CCL)**	**نام عنصر: ادعاهای انطباق ۱** **شماره مؤلفه: (ASE_CCL.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید یک ادعای انطباق تهیه کند.
	نام عنصر: ادعاهای انطباق ۱ **شماره مؤلفه: (ASE_CCL.1.2D)** **شرح مؤلفه:**

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	توسعه‌دهنده باید ارتباط منطقی ادعای انطباق تهیه کند.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
ادعاهای انطباق **(ASE_CCL)**	**نام عنصر: ادعاهای انطباق ۱** **شماره مؤلفه: (ASE_CCL.1.1C)** **شرح مؤلفه:** ادعای انطباق باید حاوی یک ادعای انطباق معیار مشترک باشد که نسخه‌ی معیار مشترک که سند هدف امنیتی و محصول ادعای انطباق با آن دارند را مشخص کند.
	نام عنصر: ادعاهای انطباق ۱ **شماره مؤلفه: (ASE_CCL.1.2C)** **شرح مؤلفه:** ادعای انطباق معیار مشترک باید انطباق سند هدف امنیتی به بخش ۲ انطباق یا توسعه معیار مشترک را توصیف کند.
	نام عنصر: ادعاهای انطباق ۱ **شماره مؤلفه: (ASE_CCL.1.3C)** **شرح مؤلفه:** ادعای انطباق معیار مشترک باید انطباق سند هدف امنیتی به بخش ۳ انطباق یا توسعه معیار مشترک را توصیف کند.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: ادعاهای انطباق ۱ **شماره مؤلفه: (ASE_CCL.1.4C)** **شرح مؤلفه:** ادعای انطباق معیار مشترک باید با تعریف مؤلفه‌های توسعه‌یافته سازگار باشد.
	نام عنصر: ادعاهای انطباق ۱ **شماره مؤلفه: (ASE_CCL.1.5C)** **شرح مؤلفه:** ادعای انطباق معیار مشترک باید تمامی پروفایل‌های حفاظتی و بسته‌های الزامات امنیتی که ادعاهای انطباق سند هدف امنیتی آن‌ها را بیان دارد را شناسایی کند.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
ادعاهای انطباق **(ASE_CCL)**	**نام عنصر: ادعاهای انطباق ۱** **شماره مؤلفه: (ASE_CCL.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.

۷,۴,۲ تعریف مؤلفه‌های توسعه‌یافته

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
تعریف مؤلفه‌های توسعه‌یافته **(ASE_ECD)**	**نام عنصر: تعریف مؤلفه‌های توسعه‌یافته ۱** **شماره مؤلفه: (ASE_ECD.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید یک اظهارنامه از الزامات امنیتی تهیه کند.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته ۱ **شماره مؤلفه: (ASE_ECD.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید یک تعریف مؤلفه‌های توسعه‌یافته تهیه کند.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
تعریف مؤلفه‌های توسعه‌یافته **(ASE_ECD)**	**نام عنصر: تعریف مؤلفه‌های توسعه‌یافته ۱** **شماره مؤلفه: (ASE_ECD.1.1C)** **شرح مؤلفه:** اظهارنامه الزامات امنیتی باید تمامی الزامات امنیتی توسعه‌یافته را مشخص کند.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته ۱ **شماره مؤلفه: (ASE_ECD.1.2C)**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: تعریف مؤلفه‌های توسعه‌یافته باید یک مؤلفه توسعه‌یافته برای هر الزام امنیتی توسعه‌یافته تعریف کند.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته ۱ **شماره مؤلفه: (ASE_ECD.1.3C)** **شرح مؤلفه:** تعریف مؤلفه‌های توسعه‌یافته باید توصیف کند که چگونه هر مؤلفه توسعه‌یافته به مؤلفه‌های معیار مشترک، خانواده‌ها و کلاس‌ها مرتبط می‌شود.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته ۱ **شماره مؤلفه: (ASE_ECD.1.4C)** **شرح مؤلفه:** تعریف مؤلفه‌های توسعه‌یافته باید از مؤلفه‌های معیار مشترک موجود، خانواده‌ها، کلاس‌ها و متدولوژی به عنوان یک مدل برای ارائه، استفاده کند.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته ۱ **شماره مؤلفه: (ASE_ECD.1.5C)** **شرح مؤلفه:** مؤلفه‌های توسعه‌یافته باید شامل المان‌های هدفمند و قابل‌اندازه‌گیری باشد، طوری که انطباق و عدم انطباق با این المان‌ها، قابل‌اثبات باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
تعریف مؤلفه‌های توسعه‌یافته **(ASE_ECD)**	**نام عنصر: تعریف مؤلفه‌های توسعه‌یافته ۱** **شماره مؤلفه: (ASE_ECD.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.
	نام عنصر: تعریف مؤلفه‌های توسعه‌یافته ۱ **شماره مؤلفه: (ASE_ECD.1.2E)** **شرح مؤلفه:** ارزیاب باید تائید کند که هیچ مؤلفه‌ی توسعه‌یافته‌ای به وسیله مؤلفه‌های موجود، به صورت شفاف قابل‌بیان نیست.

۷,۴,۳ معرفی هدف امنیتی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
معرفی هدف امنیتی **(ASE_INT)**	**نام عنصر: معرفی هدف امنیتی ۱** **شماره مؤلفه: (ASE_INT.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید یک سند معرفی هدف امنیتی تهیه کند.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
معرفی هدف امنیتی **(ASE_INT)**	**نام عنصر: معرفی هدف امنیتی ۱** **شماره مؤلفه: (ASE_INT.1.1C)** **شرح مؤلفه:** سند معرفی هدف امنیتی باید شامل مرجع هدف امنیتی، مرجع محصول، توصیف محصول و مرور کلی محصول باشد.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه: (ASE_INT.1.2C)** **شرح مؤلفه:** مرجع سند هدف امنیتی باید هدف امنیت را به‌صورت منحصربه‌فرد مشخص کند.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه: (ASE_INT.1.3C)** **شرح مؤلفه:** مرجع محصول باید محصول را مشخص کند.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه: (ASE_INT.1.4C)** **شرح مؤلفه:** مرور کلی محصول باید نحوه استفاده و ویژگی‌های اصلی محصول را به صورت خلاصه بیان کند.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه: (ASE_INT.1.5C)**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: مرور کلی محصول باید نوع محصول را معرفی کند.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه: (ASE_INT.1.6C)** **شرح مؤلفه:** مرور کلی محصول باید هر سخت‌افزار/نرم‌افزار/ثابت‌افزار غیر از محصول مورد ارزیابی را که به‌وسیله محصول استفاده می‌شود معرفی کند.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه: (ASE_INT.1.7C)** **شرح مؤلفه:** شرح محصول باید حوزه فیزیکی محصول را توصیف کند.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه: (ASE_INT.1.8C)** **شرح مؤلفه:** شرح محصول باید حوزه منطقی محصول را توصیف کند.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
معرفی هدف امنیتی	**نام عنصر: معرفی هدف امنیتی ۱**

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
(ASE_INT)	**شماره مؤلفه: (ASE_INT.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.
	نام عنصر: معرفی هدف امنیتی ۱ **شماره مؤلفه: (ASE_INT.1.2E)** **شرح مؤلفه:** ارزیاب باید تائید کند که مرور کلی محصول، مرجع محصول و خلاصه محصول با یکدیگر سازگار هستند.

۷,۴,۴ اهداف امنیتی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی **(ASE_OBJ)**	**نام عنصر: اهداف امنیتی ۱** **شماره مؤلفه: (ASE_OBJ.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید که اظهارنامه از اهداف امنیتی تهیه کند.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی **(ASE_OBJ)**	**نام عنصر: اهداف امنیتی ۱** **شماره مؤلفه: (ASE_OBJ.1.1C)** **شرح مؤلفه:** اظهارنامه اهداف امنیتی باید اهداف امنیتی برای محیط عملیاتی را توصیف کند.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی **(ASE_OBJ)**	**نام عنصر: اهداف امنیتی ۱** **شماره مؤلفه: (ASE_OBJ.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.

۷,۴,۵ الزامات امنیتی معین

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
الزامات امنیتی معین **(ASE_REQ)**	**نام عنصر: الزامات امنیتی معین ۱** **شماره مؤلفه: (ASE_REQ.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید که اظهارنامه از اهداف امنیتی تهیه کند.
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه: (ASE_REQ.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید ارتباط منطقی بین الزامات را تهیه کند.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
الزامات امنیتی معین **(ASE_REQ)**	**نام عنصر: الزامات امنیتی معین ۱** **شماره مؤلفه: (ASE_REQ.1.1C)** **شرح مؤلفه:** اظهارنامه الزامات امنیتی باید الزامات کارکردی و تضمین امنیت را توصیف کند.
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه: (ASE_REQ.1.2C)** **شرح مؤلفه:**

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
	تمامی موجودیت‌های فعال، غیرفعال، عملیات، مشخصه‌های امنیتی، موجودیت‌های خارجی و دیگر اصطلاحاتی که در الزامات کارکردی و تضمین امنیت استفاده می‌شوند، باید توصیف گردند.
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه: (ASE_REQ.1.3C)** **شرح مؤلفه:** اظهارنامه الزامات امنیتی باید تمامی عملیات بر روی الزامات امنیتی را معرفی کند.
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه: (ASE_REQ.1.4C)** **شرح مؤلفه:** تمامی عملیات باید به درستی انجام گیرند.
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه: (ASE_REQ.1.5C)** **شرح مؤلفه:** هر وابستگی بین الزامات امنیتی باید ارضاء گردد، یا ارتباط منطقی الزامات امنیتی نشان دهد که نیاز به ارضاء نیست.
	نام عنصر: الزامات امنیتی معین ۱ **شماره مؤلفه: (ASE_REQ.1.6C)** **شرح مؤلفه:** اظهارنامه الزامات امنیتی باید سازگاری داخلی داشته باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
اهداف امنیتی **(ASE_REQ)**	**نام عنصر: الزامات امنیتی معین ۱** **شماره مؤلفه: (ASE_REQ.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.

۷,۴,۶ خلاصه مشخصات هدف ارزیابی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
خلاصه مشخصات هدف ارزیابی **(ASE_TSS)**	**نام عنصر: خلاصه مشخصات هدف ارزیابی ۱** **شماره مؤلفه: (ASE_TSS.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید یک سند خلاصه مشخصات محصول تهیه کند.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
خلاصه مشخصات هدف ارزیابی **(ASE_TSS)**	**نام عنصر: خلاصه مشخصات هدف ارزیابی ۱** **شماره مؤلفه: (ASE_TSS.1.1C)** **شرح مؤلفه:** سند خلاصه مشخصات محصول باید تشریح کند که چگونه محصول الزامات کارکردی امنیت را برآورده می کند.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
خلاصه مشخصات هدف ارزیابی **(ASE_TSS)**	**نام عنصر: خلاصه مشخصات هدف ارزیابی ۱** **شماره مؤلفه: (ASE_TSS.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات تهیه شده، تمامی الزامات محتوایی را برآورده می‌سازد.
	نام عنصر: خلاصه مشخصات هدف ارزیابی ۱ **شماره مؤلفه: (ASE_TSS.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که خلاصه مشخصات محصول با مرور کلی محصول و خلاصه محصول سازگار است.

۷,۵ کلاس آزمون

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

۷,۵,۱ آزمون مستقل

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

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمودن، محصول را ارائه کند.

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

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

۷,۶ کلاس آسیب‌پذیری

این کلاس به پوشش آسیب‌پذیری‌های قابل بهره‌برداری که در توسعه و عملیات محصول ممکن وجود داشته باشد می‌پردازد.

۷,۶,۱ تحلیل آسیب‌پذیری

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

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

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:**

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

۸ پیوست یک: الزامات اختیاری

۸,۱ الزامات کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۶۳	**تولید کلید رمزنگاری ۱**
محصول باید کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم‌های تولید کلید استاندارد زیر تولید کنند. [انتخاب:	

• استفاده از طرح RSA با اندازه کلید 2048 بیت یا بیشتر که از این اسناد پیروی می‌کند: FIPS PUB 186-4، "Digital Signature Standard (DSS)"، Appendix B.3. • استفاده از طرح ECC "NIST curves" [انتخاب: P-256، P-384 ، P-521] که از اسناد زیر پیروی می‌کند: FIPS PUB 186-4، "Digital Signature Standard (DSS)"، Appendix B.4.]
نکته کاربردی ۲۷: نویسنده سند هدف امنیتی تمام طرح‌های تولید کلید که برای استقرار و احرازهویت کاربران استفاده می‌شود را انتخاب می‌کند. وقتی کلید تولید شده برای احرازهویت کاربران استفاده می‌شود، انتظار می‌رود کلید عمومی با یک گواهی X.509v3 مرتبط گردد.

۶۴	**تخریب کلید رمزنگاری ۱**
محصول باید بر اساس متد تخریب کلید رمزنگاری [اختصاص: متد تخریب کلید رمزنگاری] که بر اساس استاندارد [اختصاص: لیستی از استانداردها] باشد، کلیدهای رمزنگاری را از بین ببرد. **اقدامات ارزیابی:** • **خلاصه مشخصات محصول** ارزیاب باید این بخش را بررسی کند که در مورد همه کلیدهای محرمانه توضیحاتی بیان شده باشد. همچنین در مورد روش رویه تخریب کلید در حافظه (به عنوان مثال، بازنویسی با صفر و غیره) توضیحاتی را بیان کند.	

۶۵	**عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱(۳)**
محصول باید [رمزنگاری و رمزگشایی] را مطابق با الگوریتم رمزنگاری متقارن AES- XTSمطابق مستند,NIST SP 800- 38E AES-CBC مطابق سند NIST SP 800- 38A و [انتخاب:	

AES Key Wrap (KW مطابق سند NIST SP 800-38F, AES Key Wrap with Padding (KWP مطابق سند NIST SP 800-38F، AES-GCMمطابق سند NIST SP 800-38D, AES-CCM مطابق سند NIST SP 800-38C, و هیچ‌کدام] با اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی را انجام دهد. **نکته کاربردی ۲۸:** انتخاب یک نوع و یا چند نوع از الگوریتم‌های مذکور به معماری و طراحی تولیدکننده بستگی دارد.
۶۶ | **عملیات رمزنگاری ۱ (۴)**
محصول مورد ارزیابی باید خدمات امضای دیجیتال (تولید و تائید) را بر اساس الگوریتم‌های رمزنگاری زیر ارائه کند: [انتخاب: • الگوی RSA: اندازه کلیدهای [انتخاب: ۲۰۴۸ بیتی یا بزرگ‌تر] و بر اساس FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS» بخش ۴ • در مورد الگوی دیجیتال بیضوی ECDSA: اندازه کلیدهای [انتخاب: ۲۵۶ بیتی یا بزرگ‌تر] با استفاده از منحنی‌های NISTP-256 و P-384 و [انتخاب: P-521، هیچ منحنی دیگر]؛ بر اساس FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۵] **نکته کاربردی ۲۹:** نویسنده هدف امنیتی باید الگوریتم مورد استفاده برای اجرای امضای دیجیتال را تعیین کند. برای الگوریتم‌های انتخاب‌شده، نویسنده هدف امنیتی باید انتخاب‌ها و اختصاص‌های مناسب را انجام دهد و پارامترهای الگوریتم‌ها را به شکل مناسب تعیین کند.

۹ پیوست دو: الزامات مبتنی بر انتخاب

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. برای حفاظت از اتصال سرور ممیزی، مدیران راه‌دور و ... باید از یکی از پروتکل‌های ارتباطی امن (TLS، TLS/HTTPS) استفاده نمود.

۹,۱ الزامات پروتکل HTTPS

شماره الزام	نام الزام
۶۷	**الزامات پروتکل HTTPS (۱)**
محصول مورد ارزیابی باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کنند. **نکته کاربردی ۳۰:** نویسنده سند هدف امنیتی باید اطلاعات کافی را فراهم آورد و مشخص کند که پیاده‌سازی این پروتکل، مطابق استانداردهای تعریف‌شده است. برای انجام این کار می‌توان عناصری را به این مؤلفه افزود یا اطلاعاتی را به خلاصه مشخصات محصول اضافه کرد.	
۶۸	**الزامات پروتکل HTTPS (۲)**
محصول مورد ارزیابی باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	
۶۹	**الزامات پروتکل HTTPS (۳)**
درصورتی‌که گواهی‌نامه همتا ارائه شده، نامعتبر باشد، محصول مورد ارزیابی باید [انتخاب: اتصال را برقرار نکند، برای برقراری اتصال درخواست مجوز کند، هیچ اقدام دیگری انجام ندهد]. **نکته کاربردی ۳۱:** اگر در الزام FTP_ITC.1 یا FTP_TRP.1 پروتکل HTTPS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی‌نامه بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود.	

۹,۲ الزامات پروتکل TLS Client

شماره الزام	نام الزام
۷۰	**الزامات پروتکل TLS Client (۱)**
محصول باید [انتخاب: TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد کند. همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی کند: [انتخاب: o TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 o TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268 o TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268 o TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492 o TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 o TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246	

- TLS_RSA_WITH_AES_192_CBC_SHA256مطابق با RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_192_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS _RSA_WITH_AES_128_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_192_GCM_ SHA256مطابق با RFC 5288
- TLS _RSA_WITH_AES_256_GCM_ SHA384مطابق با RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384مطابق با RFC 5289

].

نکته کاربردی ۳۲:

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

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

۷۱	**الزامات پروتکل TLS Client (۲)**

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

نکته کاربردی ۳۳:

قوانین مربوط به تائید شناسه در بخش ۶ از RFC 6125 توضیح داده شده‌اند. شناسه مرجع توسط سرپرست (مثلاً واردکردن یک URL در مرورگر وب یا کلیک کردن روی یک لینک)، توسط پیکربندی (مثلاً پیکربندی نام یک سرور ایمیل یا سرور احرازهویت) یا توسط یک برنامه کاربردی (مثلاً یک پارامتر از یک API) بر اساس سرویس برنامه کاربردی، تعیین می‌شود. کلاینت بر مبنای دامنه منبع و نوع سرویس برنامه کاربردی (مثلاً؛ HTTP، SIP، LDAP) مربوط به یک شناسه مرجع منحصربه‌فرد، همه شناسه‌های مرجع قابل‌قبول؛ نظیر یک Common Name برای قسمت Name Subject از گواهی‌نامه و نام (حساس به بزرگ و کوچک بودن حروف) DNS، URI و سرویس برای قسمت Subject Alternative Name را منتشر می‌کند. سپس کلاینت لیست همه شناسه‌های مرجع قابل‌قبول را با شناسه‌های ارائه‌شده در گواهی سرور TLS مقایسه می‌کند.

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

۷۲	**الزامات پروتکل TLS Client (۳)**

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

نکته کاربردی ۳۴:

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

شماره الزام	نام الزام
۷۳	**الزامات پروتکل TLS Client (۴)**
محصول باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curve های [انتخاب: secp256r1, secp384r1, secp521r1] و هیچ منحنی دیگری] در پیام ClientHello ارائه دهد. **نکته کاربردی ۳۵:** اگر در الزام «الزامات پروتکل TLS Client (۱)» مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام «الزامات پروتکل TLS Client (۱)» هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب نگردد، عبارت «Supported Elliptic Curves Extension را ارائه نکند» باید انتخاب شود. این الزام مجموعه‌های رمز بیضوی مجاز برای احرازهویت و توافق کلید را به منحنی‌های NIST از الزام‌های FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌های که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.	

۹,۳ الزامات پروتکل TLS Server

با استفاده از پروتکل‌های زیر می‌توان تهدیدات مرتبط با به خطر افتادن کانال ارتباطی بین مدیران و دیگر بخش‌های محصول یا موجودیت‌های IT خارجی را کاهش داد.

شماره الزام	نام الزام
۷۴	**الزامات پروتکل TLS Server (۱)**
محصول باید [انتخاب: TLS 1.2 (RFC5246)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی کند: • [انتخاب:	

- TLS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256مطابق با RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289

- هیچ مجموعه رمز دیگری]].

نکته کاربردی ۳۶:

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

۷۵	**الزامات پروتکل TLS Server (۲)**
محصول باید اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0و [انتخاب: TLS1.1، هیچ‌کدام] دارند، رد کند. **نکته کاربردی ۳۷:** تمام نسخه‌های SSL و نسخه TLS 1.0 رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در «الزامات پروتکل TLS Server (۱)» انتخاب‌نشده است، در اینجا انتخاب شود.		

۷۶	**الزامات پروتکل TLS Server (۳)**
محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت و [انتخاب: ۳۰۷۲ بیت، ۴۰۹۶ بیت، یا هیچ اندازه دیگری] و [انتخاب: منحنی‌های NIST [انتخاب: secp256r1, secp384r1] و هیچ منحنی دیگری] ، [انتخاب: ۳۰۷۲ بیت، هیچ اندازه دیگری]] ایجاد کند. **نکته کاربردی ۳۸:** اگر در بخش «الزامات پروتکل TLS Server (۱)» سند هدف امنیتی مجموعه رمزهای DHE یا ECDHE لیست شده باشند، سند ST باید شامل Diffie-Hellmanیا منحنی‌هایNIST لیست شده در این الزام باشد.	

۹,۴ الزامات پروتکل TLS مشترک کلاینت و سرور

لازم به ذکر است که الزامات مربوط به پروتکل‌های TLS Server و TLS Client که در دو بخش قبل مطرح شده است، برای الزامات مربوط به احرازهویت TLS Server و TLS Client نیز مطرح می‌گردد. در این بخش چند الزام که برای احرازهویت این پروتکل‌ها مطرح می‌گردد و برای هردوی کلاینت و سرور نیز یکسان است و باید برای هر کدام مورد بررسی قرار گیرد، آورده شده است؛ بنابراین در هر الزام این نکته که الزام مطرح شده باید برای دیگری نیز بررسی گردد، بیان گردیده است.

شماره الزام	نام الزام
۷۷	**الزامات پروتکل TLS Server/ احرازهویت (۴)**
محصول باید احرازهویت دوطرفه کلاینت‌های TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی کند.	

توجه: این الزام فقط مختص به سرور نیست و برای کلاینت نیز مطرح می‌گردد. الزام مشترک کلاینت و سرور.	
۷۸	**الزامات پروتکل TLS Server/ احرازهویت (۵)**
محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد. اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات]]. **توجه: این الزام فقط مختص به سرور نیست و برای کلاینت نیز مطرح می‌گردد. الزام مشترک کلاینت و سرور.** **نکته کاربردی ۳۹:** استفاده از گواهی‌نامه‌های X509v3 برای پروتکل TLS در الزام FIA_X509_EXT.2.1 ارائه شده است. در این الزام بیان می‌شود که گواهی‌نامه‌های سمت کلاینت باید برای احرازهویت دوطرفه TLS پشتیبانی گردند. اگر در الزام FTP_TRP یا FTP_ITC پروتکل TLS انتخاب گردد، آنگاه اعتبار به‌وسیله تأییدیه شناسه، مسیر گواهی، تاریخ انقضاء و وضعیت ابطال مطابق با RFC 5280 تعیین می‌گردد. همچنین اعتبار گواهی بر اساس الزام FIA_X509_EXT.1/Rev آزموده می‌شود.	
۷۹	**الزامات پروتکل TLS Server/ احرازهویت (۶)**
محصول در صورت مطابقت نداشتن؛ نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه از شناساننده[۱] کلاینت انتظار بوده است، نباید کانال امن را برقرار سازد. **نکته کاربردی ۴۰:** شناساننده کلاینت ممکن است در فیلد subject یا افزونه نام دیگر فاعل مربوط به یک گواهی‌نامه باشد. شناساننده مورد انتظار باید پیکربندی گردد. این شناساننده ممکن است با نام دامنه، آدرس IP، یا آدرس ایمیل که توسط نظیر استفاده می‌گردد، مقایسه گردد. همچنین ممکن است این شناساننده برای مقایسه، به یک دایرکتوری سرور داده شود.	

۹,۵ الزامات شناسایی و احرازهویت

[۱] Identifier

شماره الزام	نام الزام
۸۰	**الزامات پروتکل X509 (۱) / ابطال**
محصول مورد ارزیابی باید گواهی‌نامه‌ها را بر اساس قوانین زیر تائید کند: • تائید گواهی‌نامه RFC 5280 و تائید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند. • مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد. • محصول مورد ارزیابی باید برای تائید یک مسیر گواهی‌نامه، اطمینان حاصل کند که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «True» تنظیم‌شده است • محصول مورد ارزیابی باید وضعیت فسخ گواهی‌نامه را با استفاده از [انتخاب: پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC 6960، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۶,۳، لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵، هیچ روش فسخ] تائید کند. • محصول مورد ارزیابی باید فیلد extendedKeyUsage را بر اساس قوانین زیر تائید کند: ○ گواهی‌نامه‌های مورداستفاده برای تائید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی، باید هدف «Code Signing» (id-kp 3 با OID 1.3.6.1.5.5.7.3.3) را در فیلد extendedKeyUsage خود داشته باشند ○ گواهی‌نامه‌های سرور ارائه‌شده برای TLS باید هدف "Server Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های کلاینت ارائه‌شده برای TLS باید هدف "Client Authentication" (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند. ○ گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ‌های OCSP باید هدف «OCSP Signing» (id-kp9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.	
۸۱	**الزامات پروتکل X509 (۲) / ابطال**

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

نکته کاربردی ۴۱:

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

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

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

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

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

الزام «الزامات پروتکل X509 (۲)/ ابطال» در مورد گواهی‌نامه‌هایی اعمال می‌شود که توسط محصول مورد ارزیابی بکار رفته و پردازش شده باشند. این الزام همچنین اضافه شدن گواهی‌نامه‌ها به لیست گواهی‌نامه‌های معتبر CA را محدود می‌کند.

۸۲	**الزامات پروتکل X509 (۳)**

محصول مورد ارزیابی باید جهت پشتیبانی احرازهویت برای [انتخاب: TLS, HTTPS] و [انتخاب: امضای کد برای به‌روزرسانی‌های نرم‌افزار سیستم، امضای کد برای تائید یکپارچگی، [اختصاص: سایر کاربردها]، هیچ کاربرد دیگر] از گواهی‌نامه‌های X.509v3 تعریف‌شده در RFC 5280 استفاده کند.