به نام خدا

پروفایل حفاظتی
توکن امنیتی OTP

نوع ۱

آذر ۹۶

نسخه ۱,۰

فهرست

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 ارائه‌شده‌اند، در محصول خود فراهم کنند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد. مرکز افتا با مشارکت سازمان فناوری اطلاعات این سند را در راستای این هدف تهیه کرده است. این پروفایل حفاظتی، به بیان الزامات توکن‌های امنیتی OTP می‌پردازد. این سند بر اساس سند طرح ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 تهیه گردیده است.

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 فعالی مشخص است. یک رکورد می‌تواند شامل دو یا چند مستند باشد.

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

داده‌های کاربری ذخیره‌شده: فایل‌های داده و اطلاعاتی هستند که توسط کاربر ایجاد و ذخیره می‌شوند. این داده‌ها می‌تواند شامل مستندات تولیدشده 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 می‌نماید 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 از قبیل نام کاربری، کلمه عبور، آدرس IP کاربر می‌تواند باشد.

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

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

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

۳ شرح محصول

به هر رشته‌ای از داده که برای اثبات مجوز ورود یا احراز هویت ارائه می‌شود یا ابزاری که این رشته از داده را تولید می‌کند توکن می‌گویند. در مباحث رمزنگاری و امنیت، توکن امنیتی بیشتر به ماژول سخت‌افزاری قابل حملی می‌گویند که کاربر برای کاربردهایی مانند ایمیل امن، ورود به شبکه اختصاصی، یا انجام عملیاتی که نیاز به مجوز خاصی دارد به کار می‌برد و از طرق مختلف مانند پورت USB یا ارتباطات بی‌سیم به سیستم‌ها متصل می‌گردند. توکن‌ها گاهی به صورت نرم‌افزاری نیز پیاده‌سازی می‌گردند.

توکن‌ها به عنوان مؤلفه «آنچه دارم» در احراز هویت به کار می‌رود و برای امنیت بیشتر باید با یکی از دو مؤلفه دیگر «آنچه میدانم» و «آنچه هستم» برای مثال با کلمه عبور یا روش‌های بیومتریک ترکیب شود. در این صورت از سوءاستفاده از توکن در صورت به سرقت رفتن آن جلوگیری می‌شود. رشته داده یا کلمه عبور ارائه‌شده توسط توکن می‌تواند برای هر کاربر ثابت باشد یا در هر بار استفاده تغییر کند. از آنجایی که ارائه کلمه عبور ثابت در برابر حمله تکرار آسیب‌پذیر و دارای امنیت پایینی است، در اغلب سازوکارهای امنیتی مکانیسمی برای ارائه کلمه عبور یک‌بار مصرف (OTP[1]) به کار گرفته می‌شود یا از رمزنگاری کلید عمومی و امضای دیجیتال استفاده می‌شود. کلمه عبور یک‌بار مصرف ممکن است در مدت زمان مشخصی مثلاً ۳۰ ثانیه اعتبار داشته باشد یا وابسته به شماره درخواست باشد و در هر بار درخواست تغییر کند.

[1] One Time Password

کاربر می‌تواند این کلمه‌های عبور را ذخیره کند یا مکانیسمی برای ساختن آن داشته باشد که توسط سرور قابل تصدیق باشد. ممکن است در هر بار درخواست احراز هویت کاربر، سرور توسط کانال دیگری رشته یا کلمه عبوری را برای کاربر ارسال کند. فرستادن کلمه عبور از طریق کانال دیگر معمول است و نسبت به کلمه عبور ثابت امنیت بالاتری دارد ولی از آنجایی که کانال‌های دیگر نیز ممکن است توسط مهاجم شنود شوند یا از دسترس خارج شوند در اغلب موارد برای امنیت بیشتر از کلمه عبور یک‌بار مصرف استفاده می‌شود. از آنجایی که ذخیره‌سازی تعداد زیاد کلمه عبور در یک توکن به حافظه زیادی نیاز دارد و امنیت پایینی دارد، بیشتر توکن‌های امنیتی با استفاده از یکی از روش‌های زیر اقدام به تولید کلمه عبور یک‌بار مصرف می‌کنند.

۳,۱ روش‌های مختلف احراز هویت در توکن‌های امنیتی

توکن‌ها از مکانیسم‌های مختلفی برای احراز هویت استفاده می‌کنند. در همه این روش‌ها رشته‌ای از داده که برای هر کاربر یکتا است به صورت امنی در توکن برای طولانی مدت ذخیره می‌شود و از آن برای تولید مجوزهای موقت برای ورود یا تولید امضا استفاده می‌شود به طوری که کلمه‌های عبور یا امضاهای تولیدشده کاملاً از هم مستقل باشند و مهاجم نتواند با استفاده از اطلاعاتی که در استفاده‌های مکرر بین توکن و سرور تبادل می‌گردد اطلاعاتی راجع به رشته داده سری کاربر به دست آورد. این رشته داده که باید با روش‌های سخت‌افزاری و نرم‌افزاری به شدت در توکن محافظت شود می‌تواند یک کلید متقارن یا زوج کلید برای رمزنگاری نامتقارن باشد. بر اساس نوع کلید سری و سازوکار توکن برای احراز هویت، توکن‌ها را به دو دسته کلی تقسیم می‌شوند:

- **توکن‌های PKI**: این توکن‌ها که می‌توانند در سطح گسترده و در شبکه‌های بزرگ مانند اینترنت استفاده شوند، بر اساس زیرساخت کلید عمومی و با استفاده از گواهی‌های دیجیتال کار می‌کنند. در زیرساخت کلید عمومی هویت هر موجودیت زوج کلید عمومی و خصوصی است که کلید عمومی از طریق سازوکار گواهی‌های الکترونیک ارائه می‌شود و کلید خصوصی به طور امنی ذخیره‌سازی می‌گردد. یکی از مهم‌ترین کارکردهای توکن‌های امنیتی ذخیره امن و استفاده از کلید خصوصی است به طوری که کلید خصوصی هرگز از آن خارج نشود و عملیات رمزنگاری مانند امضای دیجیتال با استفاده از آن در داخل توکن انجام شود.
- **توکن‌های OTP**: در این توکن‌ها به جای استفاده از زوج کلید و گواهینامه از کلید سری استفاده می‌شود که توسط سرور تولیدشده است و در زمان راه‌اندازی توکن به طوری در آن ذخیره‌شده است که به راحتی قابل استخراج از آن نباشد. این کلید در سرور نیز ذخیره‌شده است. از این کلید سری به روش‌های متفاوتی کلمه‌های عبور یک‌بار مصرف برای هر بار استفاده ساخته می‌شود. به طوری که اگر کلمه عبوری که کاربر برای ورود

استفاده می‌کند، آشکار گردد، مهاجم قادر به استفاده مجدد از آن نباشد؛ به عبارت دیگر کلمات عبور باید مستقل از یکدیگر باشند. برای ساختن این کلمات عبور یک‌بار مصرف در روش‌های مختلف از یک پارامتر متغیر مانند زمان یا یک عدد تصادفی و همچنین از الگوریتم‌های رمزنگاری برای ترکیب آن‌ها با کلید سری استفاده می‌شود.

۳,۲ مکانیسم‌های OTP

روش مبتنی بر زمان: در این روش از ترکیب یک کلید ذخیره‌شده ثابت بر روی توکن و زمان و استفاده از یک تابع رمزنگاری مانند توابع درهم‌ساز، در هر بار استفاده کلمه عبور یک‌بار مصرف جدید تولید می‌شود. این روش نیاز به انطباق زمانی سرور و توکن دارد و از آنجایی که توکن نیاز به باتری دارد طول عمر استفاده از آن محدود است. انطباق زمانی سرور و توکن در زمان راه‌اندازی توکن انجام می‌شود و در بعضی از توکن‌ها در هر بار استفاده چک می‌شود. این روش یکی از متداول‌ترین روش‌هاست و اغلب توکن‌هایی که مبتنی بر این روش هستند، برای تولید و نمایش کلمه عبور یک‌بار مصرف نیازی به اتصال یا ارتباط با سرور یا رایانه کاربر ندارند.

روش مبتنی بر شماره مرتبه استفاده از توکن: در این روش با استفاده از یک کلید ثابت ذخیره‌شده و چند بار استفاده از یک تابع رمزنگاری مانند یک تابع درهم‌ساز، در هر بار استفاده کلمه عبور جدیدی وابسته به مرتبه استفاده از توکن ساخته می‌شود. مثلاً در دفعه اول صدبار از کلید ثابت درهم‌ساز گرفته می‌شود، در بار دوم ۹۹ بار، در بار سوم ۹۸ بار و ...؛ و به این ترتیب این توکن تا صدبار می‌تواند کلمه عبور جدید تولید کند و از آنجایی که توابع درهم‌ساز توابع یک‌طرفه هستند با داشتن کلمه‌های عبور قبلی نمی‌توان به کلمه عبور جدید رسید و امنیت آن وابسته به امنیت کلید ثابت ذخیره‌شده است. این روش هزینه پایین و پیاده‌سازی نسبتاً آسانی دارد و نیاز به انطباق زمانی با سرور ندارد.

روش مبتنی بر چالش و پاسخ: در این روش لازم است توکن حتماً با سرور ارتباط برقرار کند و خود را معرفی کند. هر توکن با توجه به شناسه‌ای که در سرور دارد دارای کلید سری ثابت از پیش ذخیره‌شده یا زوج کلید ثابتی است. در صورتی که دارای کلید سری باشد، سرور در آغاز هر ارتباط عدد تصادفی تولید می‌کند و برای کاربر ارسال می‌کند. توکن با استفاده از کلید سری مختص به خود و این عدد تصادفی و یک تابع رمزنگاری یک‌طرفه مانند تابع درهم‌ساز، کلمه عبور جدید را می‌سازد و برای سرور ارسال می‌کند و سرور از طریق آن هویت کاربر را تصدیق می‌کند. در صورتی که از زوج کلید استفاده شده باشد، عددی تصادفی توسط سرور تولید و با کلید عمومی کاربر رمز می‌شود و برای کاربر فرستاده می‌شود. در این حالت کلید خصوصی کاربر در توکن

ذخیره‌شده است و کاربر با استفاده از آن عدد تصادفی رمز شده را رمزگشایی می‌کند و برای سرور ارسال می‌کند و به این ترتیب احراز هویت می‌شود. این روش یکی از امن‌ترین روش‌ها است و توکن حتماً باید توسط رابطی مانند usb یا دیگر رابط‌های ممکن، به سیستم کاربر متصل شود.

۳,۳ حوزه کاربرد

محصول با توجه به مسائل امنیتی که برای مقابله با آن‌ها طراحی شده است دارای اهداف امنیتی مشخصی است و با مجموعه‌ای از تهدیدات مقابله می‌کند. الزامات با توجه به اهداف امنیتی تعریف می‌شوند. مصرف‌کنندگان با توجه به شرایط و سیاست‌های امنیتی و نیازمندی‌های خود، از بین محصولات، محصولی که اهداف امنیتی آن‌ها را برآورده می‌کند انتخاب می‌کنند.

توکن‌های تولید کلمه عبور یک‌بار مصرف ممکن است به عنوان فاکتور دوم برای احراز هویت (احراز هویت ۲ فاکتوری) و یا به عنوان تنها فاکتور احراز هویت استفاده شوند. مصرف‌کنندگان باید متناسب با نیاز خود و اهداف امنیتی مورد نظر، یکی از توکن‌های نوع ۱، نوع ۲ و نوع ۳ را استفاده کنند. همان‌گونه که در جدول ۳-۱ قابل مشاهده است، توکن نوع ۳ دارای سخت‌ترین و نوع ۱ دارای ساده‌ترین اهداف امنیتی هستند؛ بنابراین توکن نوع ۳ دارای بیشترین الزامات امنیتی است و بالاترین سطح امنیت را برآورده می‌کند. مصرف‌کنندگانی که نیاز به توکن با اهداف امنیتی پایینی، برای عامل دوم احراز هویت خود دارند می‌توانند از توکن نوع ۱ استفاده کنند. مصرف‌کنندگانی که می‌خواهند از توکن به عنوان تنها عامل احراز هویت استفاده کنند یا کاربرد مورد نظرشان دارای حساسیت بالایی است باید از توکن نوع ۲ و ۳ استفاده کنند.

این پروفایل حفاظتی به بیان الزامات مربوط به توکن نوع ۱ می‌پردازد و در آن الزامات مربوط به احراز هویت کاربران برای توکن و مقاومت در برابر حملات فیزیکی و کانال جانبی و خودآزمون‌ها وجود ندارد. هدف امنیتی در این نوع از توکن‌ها تولید کلمه‌های عبور مستقل از هم است به طوری که مهاجم نتواند ارتباطی بین آن‌ها یا پارامترهای متغیر بیابد و اطلاعاتی درباره آن‌ها به‌جز طولشان به دست آورد. از آنجایی که این نوع از توکن‌ها دارای سازوکار احراز هویت کاربر برای توکن نیستند مهاجم با توان پایین نیز می‌تواند با در اختیار داشتن آن‌ها از آن‌ها سوءاستفاده کند؛ بنابراین باید صرفاً به عنوان عامل دوم احراز هویت و نه به عنوان تنها عامل احراز هویت استفاده شوند.

جدول ۳-۱ اهداف امنیتی انواع توکن

حوزه کاربرد	نوع محصول	اهداف امنیتی	تهدیدات	دسترسی و توان مهاجم
به عنوان فاکتور دوم احراز هویت	نوع ۱	مستقل بودن OTP ها از هم	حدس زدن کلمات عبور با استفاده از ارتباط آن‌ها با هم و نقص در مکانیسم OTP	بدون دسترسی فیزیکی به توکن
احراز هویت برای دسترسی‌های نیمه حساس	نوع ۲	▪ مستقل بودن OTP ها از هم ▪ احراز هویت افراد و کنترل دسترسی نقش‌ها به کارکردهای توکن	▪ نقص در مکانیسم ساخت OTP ▪ سوءاستفاده از توکن توسط فرد غیرمجاز	دسترسی محدود (مهاجم با توان پایین)
احراز هویت برای دسترسی‌های حساس	نوع ۳	• مستقل بودن OTP ها از هم ▪ احراز هویت افراد و کنترل دسترسی نقش‌ها به کارکردهای توکن ▪ آشکارسازی حملات فیزیکی و مقاومت در برابر آن‌ها	▪ نقص در مکانیسم ساخت OTP ▪ سوءاستفاده از توکن توسط فرد غیرمجاز ▪ حملات فیزیکی	دسترسی نامحدود (مهاجم با توان بالا)

۴ مسائل امنیتی

۴,۱ تهدیدات

جدول ۴-۱ تهدیدات محصول

تهدیدات	توضیحات
حدس زدن کلمات عبور با استفاده از ارتباط آن‌ها با هم و نقص در مکانیسم OTP	ممکن است به دلیل انتخاب روش یا الگوریتم یا پارامترهای نامناسب کلمات عبور یک‌بار مصرف به گونه‌ای باهم ارتباط داشته باشند که مهاجم بتواند با کمک کلمات عبور قبلی اطلاعاتی درباره کلمات عبور آینده به دست آورد.
سوءاستفاده از نقایص موجود در الگوریتم‌های رمزنگاری و درهم‌سازی یا پیاده‌سازی‌های آن‌ها	ممکن است از نقایص موجود در الگوریتم‌ها یا پیاده‌سازی‌های آن‌ها مهاجم بتواند به اطلاعات محرمانه دسترسی پیدا کند.

۵ اهداف امنیتی

۵,۱ اهداف امنیتی برای محصول

جدول ۵-۱ اهداف امنیتی محصول

هدف امنیتی	توضیحات

هدف امنیتی	توضیحات
تصادفی بودن کلمات عبور یک‌بار مصرف	برای مقابله با تهدید سوءاستفاده مهاجمین از ارتباط کلمات عبور یک‌بار مصرف با یکدیگر و یا ارتباط آن‌ها با پارامترهای آشکار، مکانیسم تولید آن‌ها باید طوری طراحی و پیاده‌سازی شود که کلمات عبور یک‌بار مصرف کاملاً مستقل از هم و تصادفی به نظر بیایند و مشاهده کلمات عبور قبلی هیچ اطلاعاتی درباره کلید سری و کلمات عبور آینده در اختیار مهاجمین نگذارد.

۶ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول ۶-۱ هستند. در ادامه هر یک از الزامات شرح و بسط داده شده‌اند.

جدول ۶-۱ الزامات کارکرد امنیتی

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	مدیریت کلید رمزنگاری ۲	FCS_CKM.2.1
۲	مدیریت کلیدهای رمزنگاری ۴	FCS_CKM.4.1
۳	عملیات رمزنگاری ۱ (۱)	FCS_COP.1.1 (1)
۴	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1 (3)
۵	عملیات رمزنگاری ۱ (۳)	FCS_COP.1.1 (4)
۶	تولید کلمه عبور یک‌بار مصرف ۱	FCS_OTP_EXT.1.1

۶,۱ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱	**مدیریت کلید رمزنگاری ۲**

محصول مورد ارزیابی باید استقرار کلید[۱] رمزنگاری را بر اساس یک روش خاص استقرار کلید رمزنگاری انجام دهد: [انتخاب:

- الگوهای استقرار کلید RSA که این الزامات را رعایت کنند: انتشار ویژه NIST 800-56B بازبینی ۱، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری فاکتورگیری عدد صحیح»[۲]؛
- الگوهای استقرار کلید منحنی بیضوی[۳] که این الزامات را رعایت کنند: انتشار ویژه NIST 800-56A بازبینی ۲، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته»[۴]؛
- الگوهای استقرار کلید میدانی[۵] که این الزامات را رعایت کنند: انتشار ویژه NIST 800-56A بازبینی ۲، «توصیه‌هایی برای الگوهای استقرار جفت کلید با استفاده از رمزنگاری لگاریتم گسسته».
- الگوی استقرار کلید با استفاده از دیفی-هلمن گروه ۱۴ که این الزامات را رعایت کنند: RFC 3526، بخش ۳؛

نکته کاربردی ۱:

این عنصر درواقع نسخه اصلاح‌شده الزام «مدیریت کلید رمزنگاری ۲»[۶] در استاندارد ISO 15408 است که به‌جای توزیع کلید، به استقرار کلید می‌پردازد.

---

۱ Key establishment

۲ Integer factorization cryptography

۳ Elliptic curve-based

۴ Discrete logarithm cryptography

۵ Finite filed-based

۶ FCS_CKM.2.1

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

الگوهای استقرار کلید مبتنی بر RSA در بخش ۹، بازبینی ۱، مربوط به NIST SP 800-56B تشریح شده‌اند؛ اما این بخش وابسته به پیاده‌سازی موارد مذکور در سایر بخش‌های بازبینی ۱ مربوط به SP 800-56B است. اگر محصول مورد ارزیابی در الگوی استقرار کلید به‌عنوان گیرنده عمل کند، نیازی نخواهد بود که محصول، الگوی تولید کلید RSA را اجرا نماید.

ورود کلید باید به روش دستی یا الکترونیک انجام شود. دقت ورود، کلیدهایی که دستی وارد می‌شوند باید بررسی شود. در زمان ورود دستی کلیدها مقادیر واردشده ممکن است به طور موقت نشان داده شوند تا چک شوند. اگر کلید به صورت رمز شده وارد می‌شود مقادیر رمز نشده کلید نباید حین ورود نمایش داده شود.

کلیدهای سری که به صورت رمز شده به هدف ارزیابی وارد می‌شوند و در مدهای تائید شده مورد استفاده قرار می‌گیرد باید با استفاده از الگوریتم‌های تائید شده رمز شوند. هدف ارزیابی باید کلیدهای واردشده را به موجودیتی (کاربر، گروه یا پروسه) که کلید به آن اختصاص‌یافته است مربوط کند. نویسنده هدف ارزیابی باید همه روش‌های ورود کلید به هدف ارزیابی را توصیف کند.

۲	**مدیریت کلید رمزنگاری ۴**

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

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

[۱] Volatile Storage

[۲] Invocation

○ یک بخشی از توابع امنیتی محصول را برای نابودی انتزاع معرف کلید، می‌سازد] انجام شود.] **نکته کاربردی ۲:** در قسمت مربوط به انتخاب در گزینه دوم از اولین اختصاص، جایی که کلیدها برای نابودی به‌وسیله «یک بخشی از توابع امنیتی محصول» شناسایی می‌شوند، خلاصه مشخصات محصول باید «بخش» مربوطه و واسط مرتبط با آن را تعریف نماید. واسط اشاره‌شده در الزام می‌تواند در محصولات مختلف، شکل متفاوتی داشته باشد. شاید مشهودترین شکل آن یک برنامه کاربردی روی یک سیستم‌عامل باشد. وقتی که روش‌های تخریب مختلفی برای کلیدهای مختلف و/یا موقعیت‌های تخریب مختلف استفاده می‌شود، این روش‌ها و کلیدها/موقعیت‌های متفاوت بکار گرفته‌شده، در خلاصه مشخصات محصول توصیف می‌شوند. خلاصه مشخصات محصول همه کلیدهای مرتبط استفاده شده در پیاده‌سازی الزامات کارکرد امنیتی را توصیف می‌نماید، همچنین مواردی که محل ذخیره شدن کلیدها به‌صورت متن آشکار است را شامل می‌شود. در بعضی از اختصاص‌های بالا، از «شامل هیچ CSP نباشد» استفاده شده است. این جمله به این معنی است که محصول از برخی داده خاص استفاده می‌کند که شامل هیچ‌کدام از مقادیر تولیدشده توسط تولیدکننده بیت تصادفی موجود در الزام FCS_RBG_EXT (در صورت پشتیبانی توسط محصول) یا مقادیر مشخص لیست شده در این الزام، مثلاً موارد لیست شده در اولین انتخاب از اولین اختصاص این الزام نیست. در واقع وجود عبارت «شامل هیچ CSP نباشد» برای مطمئن شدن از این موضوع است که حتماً بازنویسی داده با دقت انتخاب شده است. هدف ارزیابی باید روش‌هایی برای صفر سازی همه کلیدهای سری و عمومی رمز نشده و سایر پارامترهای امنیتی رمز نشده داشته باشد. صفر سازی کلیدها یا پارامترهای امنیتی رمز شده یا کلیدهایی که به صورت فیزیکی یا منطقی درون ماژول ارزیابی‌شده‌ای محافظت می‌شوند نیاز نیست. هدف ارزیابی باید روش امحای کلید به‌کاررفته در هدف ارزیابی را توصیف کند.
۳ | عملیات رمزنگاری ۱ (۱)
محصول مورد ارزیابی باید رمزگذاری و رمزگشایی را بر اساس الگوریتم‌های رمزنگاری خاص [اختصاص: الگوریتم AES که در حالت [انتخاب: CBC، GCM، CTR] و در اندازه‌های کلید [انتخاب: ۱۲۸ بیتی، ۱۹۲ بیتی، ۲۵۶ بیتی] استفاده می‌شوند] و با توجه به [اختصاص: استاندارد AES که در ISO 18033-3 تعریف‌شده است، [انتخاب: CBC که در ISO 10116 تعریف‌شده است، GCM که در ISO 19772 تعریف‌شده است، CTR که در ISO 10116 تعریف شده است]] انجام دهد. **نکته کاربردی ۳:**

در مورد نخستین انتخاب این الزام، نویسنده هدف امنیتی حالت یا حالت‌های کارکردی AES را انتخاب می‌کند. در مورد دومین انتخاب، نویسنده هدف امنیتی اندازه کلیدهای پشتیبانی شده توسط این کارکرد را انتخاب می‌کند. حالت‌ها و اندازه کلیدهای انتخاب‌شده در این مرحله، متناظر با انتخاب مجموعه رمز[۱] در الزامات کانال امن هستند.	
۴	**عملیات رمزنگاری ۱ (۳)**
محصول مورد ارزیابی باید خدمات درهم‌سازی رمزنگاری را بر اساس یک الگوریتم رمزنگاری مشخص [انتخاب: SHA-1، SHA-256، SHA-384، SHA-512] و اندازه‌های خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیتی که [اختصاص: ISO/IEC 10118-3:2004] را رعایت کند، ارائه نماید. **نکته کاربردی ۴:** به تولیدکنندگان اکیداً توصیه می‌شود که از پروتکل‌های به‌روزرسانی شده‌ای که از خانواده SHA-2 پشتیبانی می‌نمایند، استفاده کنند. تا زمانی که پروتکل‌های به‌روز شده پشتیبانی شوند، این پروفایل حفاظتی اجازه پشتیبانی از SHA-1 را بر اساس SP 800-131A فراهم می‌کند. طبق SP 800-131 A الگوریتم SHA-1 فقط می‌تواند برای عملیات غیر از امضای دیجیتال همچون درهم سازی کلمه عبور و ... استفاده شود. در نسخه‌های آتی این پروفایل حفاظتی، SHA-256 کمینه الزام برای محصولات خواهد بود. انتخاب درهم‌ساز باید بر اساس قدرت کلی الگوریتم مورداستفاده برای الزام «عملیات رمزنگاری ۱(۱)» و الزام «عملیات رمزنگاری ۱(۲)» انجام شود (مثلاً SHA 256 برای کلیدهای ۱۲۸ بیتی). انتخاب الگوریتم درهم‌سازی باید متناسب با اندازه خلاصه پیام باشد، به طور مثال اگر الگوریتم SHA-1 انتخاب شده است، تنها انتخاب، اندازه خلاصه پیام قابل‌قبول ۱۶۰ بیت خواهد بود. در صورتی که از هر الگوریتمی به‌جز الگوریتم‌های استاندارد نام برده شده استفاده شده باشد، آن الگوریتم باید مورد ارزیابی و تائید قرار گیرد.	
۵	**عملیات رمزنگاری ۱ (۴)**
محصول مورد ارزیابی باید احراز هویت پیام مبتنی بر کلید درهم‌سازی شده[۱] را بر اساس الگوریتم رمزنگاری خاص [انتخاب:HMAC-SHA-1, HMAC-SHA-256,HMAC-SHA-384, HMAC-SHA-512] و با استفاده از اندازه‌های کلید [اختصاص: اندازه کلید مورداستفاده در HMAC (بر حسب بیت)]	

[۱] Cipher suite

و اندازه‌های خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیت و با توجه به موارد مطرح‌شده در [اختصاص: بخش هفتم ISO/IEC 9797-2:2011 با نام «الگوریتم MAC ۲»] انجام دهد.

نکته کاربردی ۵:

اندازه کلید k در عبارت «اختصاص» بین L1 و L2 خواهد بود (که در ISO/IEC 10118 مربوط به توابع درهم‌ساز تعریف شده است). به عنوان مثال، در مورد SHA-256 داریم: L1=512, L2=256 که L2<=k<=L1.

در صورتی که از هر الگوریتمی به‌جز الگوریتم‌های استاندارد نام برده شده استفاده شده باشد، آن الگوریتم باید مورد ارزیابی و تائید قرار گیرد. انتخاب الگوریتم درهم‌سازی باید متناسب با اندازه خلاصه پیام باشد، به طور مثال اگر HMAC-SHA-256 انتخاب شده است، تنها انتخاب، اندازه خلاصه پیام قابل‌قبول ۲۵۶ بیت خواهد بود.

اندازه خلاصه پیام‌های بالا متناسب با الگوریتم درهم‌سازی مورد استفاده است. کوتاه شدن خروجی HMAC پس از محاسبه درهم‌سازی گام مناسب در طیفی از برنامه‌های کاربردی است. کوتاه شدن پیام، اندازه خروجی نهایی و استانداردی که پیام کوتاه شده منطبق بر آن است باید در سند هدف امنیتی بیان گردد.

۶	**تولید کلمه عبور یک‌بار مصرف ۱**

هدف ارزیابی باید کلمه عبور یک‌بار مصرف را مطابق با یکی از استانداردهای زیر:

- RFC 4226: HOTP: An HMAC-Based One-Time Password Algorithm
- RFC 6238: TOTP: Time-Based One-Time Password Algorithm
- RFC 6287: OATH Challenge-Response Algorithm

و یا [اختصاص: هر الگوریتم تولید تائید شده دیگر] تولید نماید.

نکته کاربردی ۶:

کلمه‌های عبورِ یک‌بار مصرفِ تولیدشده باید کاملاً مستقل از هم باشند به‌گونه‌ای که با داشتن کلمه‌های عبور پیشین و پارامتر متغیر الگوریتم نتوان اطلاعاتی راجع به کلمه عبور جدید به دست آورد. در صورتی که از هر الگوریتمی به‌جز الگوریتم‌های استاندارد نام برده شده استفاده شده باشد، آن الگوریتم باید مورد ارزیابی و تائید قرار گیرد. کلید سری و پارامتر متغیر باید دارای طول کافی باشند و کلید سری به طور امنی تولید و وارد توکن شود.

[۱] Keyed-hash message authentication

۷ الزامات تضمین امنیت

اهداف امنیتی تعریف شده در بخش ۵ جهت مقابله نمودن با تهدیدات معرفی‌شده در بخش ۴ در نظر گرفته‌شده‌اند. 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 می‌نماید؛ و سپس فعالیت‌های تضمین که در سند هدف امنیتی مطرح‌شده، 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
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب‌گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

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

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

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

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1C)** **شرح مؤلفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجراکننده کارکرد امنیتی[۱] و پشتیبان کننده‌ی الزام کارکرد امنیتی[۲] توصیف نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2C)** **شرح مؤلفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجراکننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.3C)**

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

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

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2E)** **شرح مؤلفه:** ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.

مستندات «مشخصات کارکردی» جهت پشتیبانی از ارزیابی الزامات کارکردی و اقدامات لازم در کلاس‌های «راهنما»، «آزمون» و «آسیب‌پذیری» ارائه‌شده 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 نماید) ارائه می‌شود.

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

- دستورالعمل نصب موفقیت‌آمیز محصول در محیط
- دستورالعمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگ‌تر
- دستورالعمل‌هایی که ارائه‌دهنده قابلیت مدیریتی محافظت‌شده 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)** **شرح مؤلفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای	**نام عنصر: راهنمای کاربردی ۱**

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
کاربردی (AGD_OPE)	**شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه‌شده توسط محصول به صورت امن استفاده می‌گردد.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های در دسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل توابع امنیتی محصول.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.5C)** **شرح مؤلفه:** سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آن‌ها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.6C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.7C)** **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

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

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه‌شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۷,۲,۲ راهنمای آماده‌سازی

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

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای 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.

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

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

۷,۳ کلاس آزمون

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

۷,۳,۱ آزمون مستقل

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

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

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱**

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

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

۷,۴ کلاس آسیب‌پذیری

۷,۴,۱ تحلیل آسیب‌پذیری

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

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

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری	**نام عنصر: آسیب‌پذیری ۱**

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
(AVA_VAN)	**شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.2E)** **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.3E)** **شرح مؤلفه:** ارزیاب باید بر اساس آسیب‌پذیری‌های بالقوه شناسایی‌شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۷,۵ کلاس پشتیبانی از چرخه حیات

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

۷,۵,۱ قابلیت‌های پیکربندی

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

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

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

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**

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

۷,۵,۲ حوزه پیکربندی

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

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

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

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