**به نام خدا**

# پروفایل حفاظتی گذرنامه الکترونیک

دی ۹۴

نسخه ۱,۰

## فهرست

## ۱- مقدمه

این سند که در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک توسط مرکز مدیریت راهبردی افتا و سازمان فناوری اطلاعات ایران تهیه و نهایی شده است، برای بیان الزامات کارکرد امنیتی هر محصول لازم است. 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 خودفراهم کنند وبه خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد.

در این سند الزامات امنیتی پروفایل حفاظتی‌گذرنامه الکترونیک که یک سند مسافرتی قابل خواندن توسط ماشین[۱] (MRTD) بارگذاری شده بر روی تراشه‌ی مدار مجتمع[۲] (IC) همراه با ملزومات آن است تبیین می‌شود.

این پروفایل حفاظتی شامل حداقل الزامات امنیتی است و اطلاعاتی در مورد مدل پیاده‌سازی محصول ارائه نمی‌دهد. در واسطه با مسائل امنیتی که با توجه به مدل پیاده‌سازی محصول احتمال دارد رخ دهد، نویسنده هدف امنیتی باید مسئله امنیتی، اهداف امنیتی و الزامات امنیتی اضافی را تعریف کند.

توسعه‌دهندگان محصولات و یا بازاریابان می‌توانند اهداف امنیتی را با انطباق با تمام مفاهیم تعریف شده در این پروفایل حفاظتی ترسیم کنند و کاربران می‌توانند از آن‌ها برای انتخاب، به‌کارگیری و مدیریت محصول استفاده نمایند.

احراز هویت فعال[۳] (AA) در مشخصات کنترل دسترسی توسعه‌یافته (EAC) اختیاری است. بنابراین، نویسنده‌ی هدف امنیتی می‌تواند ساز و کار امنیتی احراز هویت فعال را با توجه به خط‌مشی صدور گذرنامه الکترونیک اضافه کند. در صورت افزودن ساز و کار امنیتی نویسنده‌ی هدف امنیتی باید تعریف مسئله امنیتی، اهدف امنیتی و الزامات امنیتی را نیز تعریف کند.

---

[۱] machine readable travel documents

[۲] integrated circuit

[۳] active authentication

چرخه حیات محصول، ساز و کار احراز هویت عامل شخصی‌سازی و غیره ممکن است با توجه به خط‌مشی صدور گذرنامه الکترونیک متفاوت باشند. بنـابراین نویسنده‌ی هدف امنیتی ممکن است مرور کلی محصول، تعریف مسئله امنیتی، اهداف و الزامات امنیتی را با در نظر گرفتن این جزئیات افزوده یا تغییر دهد.

## ۲- فرهنگ اصطلاحات

- **احراز هویت فعال**

ساز و کار امنیتی که تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) با امضای عدد تصادفی انتقال یافته از سامانه بازرسی (IS) اصـل آن را بـه سامانه بازرسی (IS) نشان می‌دهد و سامانه بازرسی (IS) اصل بودن تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) را با درستی‌سنجی با استفاده از مقادیر امضا شده تأیید می‌کند.

- **کنترل دسترسی پایه (BAC)**

ساز و کار امنیتی جهت پیاده‌سازی پروتکل موجودیت مبتنی بر کلید متقارن مبتنی برای احراز هویت دو طرفه‌ی تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و سامانه بازرسی (IS)و پروتکل توزیع کلید مبتنی بر کلید متقارن برای تولید کلیـدهای نشسـت ضـروری در برقـراری پیام‌رسـانی امـن بـرای تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و سامانه بازرسی (IS)

- **کلید احراز هویت کنترل دسترسی پایه (BAC)**

کلید رمزگذاری احراز هویت کنترل دسترسی پایه (BAC) و کلید کد احراز هویت پیام (MAC) احراز هویت کنترل دسترسی پایـه (BAC) تولیـد شـده بـا استفاده از ساز و کار اشتقاق کلید (KDM) از ناحیه قابل خواندن توسط ماشین (MRZ) (شماره گذرنامه، رقم حواله‌ی شماره گذرنامه، تاریخ تولد، رقـم حوالـه‌ی

تاریخ تولد، تاریخ اعتبار، رقم حواله‌ی تاریخ اعتبار) برای احراز هویت دو طرفه‌ی تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و سامانه بازرسی (IS)

- **احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC)**

احراز هویت دو طرفه‌ی تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و سامانه بازرسی (IS) طبق پروتکل احراز هویت موجودیت مبتنی بر کلید متقارن استاندارد ISO 9798-2

- **پیام‌رسانی امن کنترل دسترسی پایه (BAC)**

کانال ارتباطی برای فراهم آوردن محرمانگی و یکپارچگی داده منتقل شده توسط رمزگذاری داده منتقل شده با کلید رمزگذاری نشست کنترل دسترسی پایه (BAC) و تولید کردن، و در نتیجه انتقال بعد از تولید مقدار احراز هویت پیام با کلید کد احراز هویت پیام (MAC) نشست کنترل دسترسی پایه (BAC)

- **کلید نشست کنترل دسترسی پایه(BAC)**

کلید رمزنگاری نشست کنترل دسترسی پایه (BAC) و کلید کد احراز هویت پیام (MAC) نشست کنترل دسترسی پایه (BAC) تولید شده برای آن، با استفاده از ساز و کار اشتقاق کلید (KDM) از اعداد تصادفی برای تولید کلیدهای نشست به اشتراک گذاشته شده در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC)

- **داده زیست‌سنجی دارنده گذرنامه الکترونیک**

اثر انگشت و یا داده عنبیه‌ی دارنده گذرنامه الکترونیک ذخیره شده در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) در ساختار منطقی داده (LDS)

- **سامانه بازرسی کنترل دسترسی پایه(BAC)**

سامانه بازرسی (IS) پیاده‌سازی شده با کنترل دسترسی پایه (BAC) و ساز و کارهای امنیتی احراز هویت غیر فعال (PA)

- **گواهی**

داده الکترونیکی ایجاد شده توسط امضای دیجیتال بر روی کلید درستی‌سنجی امضای دیجیتال توسط مرجع صلاحیت دار صدور گواهی (CA) به منظور بررسی و نشان دادن این موضوع که کلید تولید امضای دیجیتال تنها متعلق فردی است که کلید را دارد.

- **حمله تنها به متن رمز**

حمله توسط عامل تهدید برای رمزگشایی متن رمز جمع‌آوری شده

- **مرجع صلاحیت دار امضا کننده گواهی کشور (CSCA)**

مرجع صلاحیت دار صدور گواهی (CA) اصلی که گواهی مرجع صلاحیت دار امضا کننده گواهی کشور(CVCA) و گواهی تأیید کننده سند (DV) را با تولید امن کلید امضای دیجیتال در PA-PKI برای پشتیبانی از ساز و کارهای امنیتی کنترل احراز هویت غیر فعال (PA) تولید و صادر می‌کند.

- **گواهی مرجع صلاحیت دار امضا کننده گواهی کشور (CSCA)**

گواهی برای نشان دادن اعتبار کلید درستی‌سنجی امضای دیجیتال برای کلید تولید امضای دیجیتال مرجع صلاحیت دار صدور گواهی (CA) اصلی PA-PKI

با امضا بر روی کلید درستی‌سنجی امضای دیجیتال با کلید تولید امضای دیجیتال مرجع صلاحیت دار صدور گواهی (CA) اصلی PA-PKI

- **مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA)**

مرجع صلاحیت دار صدور گواهی (CA) اصلی که گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) و گواهی تأیید کننده سند (DV) را با تولید امن کلید امضای دیجیتال در EAC-PKI برای پشتیبانی از ساز و کارهای امنیتی کنترل دسترسی توسعه یافته (EAC) را تولید و صادر می‌کند.

- **گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA)**

این گواهی شامل مقدار امضای دیجیتال مرجع صلاحیت دار صدور گواهی (CA) اصلی EAC-PKI با کلید تولید امضای دیجیتال مرجع صلاحیت دار صدور گواهی (CA) اصلی EAC-PKI بر روی کلید درستی‌سنجی امضای دیجیتال است که نشان دهنده‌ی اعتبار گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) و گواهی تأیید کننده سند (DV) است.

- **گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA)**

این گواهی شامل مقدار امضای دیجیتال مرجع صلاحیت دار صدور گواهی (CA) اصلی EAC-PKI با کلید تولید امضای دیجیتال است که با گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) قبلی بعد از تولید گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) جدید قبل از انقضای تاریخ اعتبار گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) مطابقت دارد.

- **گواهی امضاء کننده سند (DS)**

گواهی عامل شخصی‌سازی امضا شده با کلید تولید امضای دیجیتال مرجع صلاحیت دار صدور گواهی (CA) اصلی PA-PKI مورد استفاده توسط سامانه بازرسی (IS) جهت تأیید سند موجودیت غیر فعال امنیتی (SOD) ساز و کار امنیتی احراز هویت غیر فعال (PA)

- **تایید کننده سند(DV)**

مرجع صلاحیت دار صدور گواهی (CA) که گواهی سامانه بازرسی (IS) را تولید و صادر می‌کند.

- **گواهی تأیید کننده سند (DV)**

گواهی‌ای است که شامل مقدار امضای دیجیتال بر روی کلید درستی‌سنجی امضای دیجیتال سامانه بازرسی (IS) با کلید تولید امضای دیجیتال تأیید کننده سند (DV) به منظور نشان دادن اعتبار کلید درستی‌سنجی امضای دیجیتال سامانه بازرسی (IS) است.

- **کنترل دسترسی توسعه یافته – احراز هویت تراشه (EAC-CA)**

ساز و کار امنیتی برای پیاده‌سازی پروتکل توزیع کلیدزودگذر- ایستای دیفی – هلمن (DH) (PKCS#3، ANSI X.42 و...)، برای فعال کردن احراز هویت تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) توسط سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) از طریق بررسی کلید برای عمومی احراز هویت تراشه‌ی کنترل دسترسی توسعه یافته (EAC) و کلید خصوصی تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و کلید عمومی و خصوصی موقت در سامانه بازرسی کنترل دسترسی توسعه یافته (EIS)

- **کنترل دسترسی توسعه یافته–احرازهویت پایانه (EAC-TA)**

ساز و کار امنیتی که در آن سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) مقادیر امضای دیجیتال را با کلید تولید امضای دیجتال خودش به کلید عمومی موقت استفاده شده در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) انتقال می‌دهد و تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) با استفاده از گواهی سامانه بازرسی (IS) امضای دیجیتال را تأیید می‌کند. این ساز و کار امنیتی پروتکل احراز هویت پاسخ به چالش مبتنی بر امضای دیجیتال را از طریق احراز هویت سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) توسط تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) پیاده‌سازی می‌کند.

- **کنترل دسترسی توسعه یافته (EAC)**

ساز و کارهای امنیتی متشکل از کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) برای تراشه احراز هویت و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) جهت احراز هویت سامانه بازرسی (IS) است که تنها امکان خواندن داده زیست‌سنجی دارنده گذرنامه الکترونیک جهت کنترل دسترسی به داده زیست‌سنجی دارنده گذرنامه الکترونیک ذخیره شده در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) را برای کنترل دسترسی توسعه‌یافته (EAC) پشتیبانی کننده از سامانه بازرسی فراهم می‌آورد.

- **کلید عمومی و خصوصی احراز هویت تراشه‌ی کنترل دسترسی توسعه یافته (EAC)**

مجموعه‌ای از کلیدهای دیفی –هلمن (DH) مورد استفاده توسط تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) برای احراز هویت خودش برای کنترل دسترسی توسعه یافته (EAC) پشتیبانی کننده از سامانه بازرسی (IS) در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA)، که حاوی داده ثبت شده توسط عامل شخصی‌سازی در فاز شخصی‌سازی است.

- **سامانه بازرسی کنترل دسترسی توسعه یافته (EIS)**

سامانه بازرسی (IS) برای پیاده‌سازی کنترل دسترسی پایه (BAC)، احراز هویت غیر فعال (PA) و ساز و کارهای امنیتی کنترل دسترسی توسعه یافته (EAC) و احراز هویت فعال (AA) به عنوان یک گزینه

- **کلید نشست کنترل دسترسی توسعه یافته (EAC)**

کلید نشست استفاده شده برای برقراری پیام‌رسانی امن برای انتقال محافظت شده‌ی داده زیست‌سنجی دارنده گذرنامه الکترونیک که شامل کلید رمزگذاری نشست کنترل دسترسی توسعه یافته (EAC) و کلید کد احراز هویت پیام (MAC) نشست کنترل دسترسی توسعه یافته (EAC) تولید شده با استفاده از تابع اشتقاق کلیدی (KDF) است که کلیدهای به اشتراک گذاشته شده با سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) از طریق پروتکل توزیع کلید دیفی – هلمن (DH) ایستای زودگذر در کنترل دسترسی توسعه یافته – احراز هویت تراشه (EAC-CA) به عنوان نقطه‌ی آغاز تصادفی (Seed) استفاده شده‌اند.

- **EF.COM**

شامل اطلاعات برچسب گروه داده و اطلاعات نسخه ساختارداده‌منطقی (LDS)

- **EF.CVCA**

قالب فایل ابتدایی (EF) برای مشخص کردن حق خواندن و فهرستی از کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) مورد نیاز برای درستی‌سنجی اعتبار گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA)

- **کلید رمزگذاری**

کلید استفاده شده در الگوریتم رمزگذاری متقارن برای داده رمزگذاری شده به منظور جلوگیری از افشای داده

- **گذرنامه الکترونیک**

گذرنامه تعبیه شده در تراشه‌ی مدار مجتمع (IC) که داده هویتی و دیگر داده‌های دارنده گذرنامه الکترونیک مطابق با استانداردهای سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) و سازمان بین‌المللی استاندارد (ISO) ذخیره شده است.

- **داده احراز هویت گذرنامه الکترونیک**

داده ذخیره شده در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) با قالب ساختار منطقی داده (LDS) برای پشتیبانی از ساز و کار امنیتی گذرنامه الکترونیک که شامل PA SOD، کلید عمومی احراز هویت تراشه‌ی EAC، کلید عمومی احراز هویت تراشه احراز هویت فعال (AA) و غیره است.

- **داده هویتی گذرنامه الکترونیک**

شامل داده شخصی و زیست‌سنجی دارنده گذرنامه الکترونیک

- **زیرساخت کلید عمومی (PKI)گذرنامه الکترونیک**

داده منحصر به فرد امضا شده‌ی بر روی گذرنامه الکترونیک توسط عامل شخصی‌سازی با کلید تولید امضای دیجیتال صادر شده در سامانه زیرساخت کلید عمومی (PKI) به منظور صدور و بررسی گذرنامه پردازش شده به صورت الکترونیکی

- **سامانه زیرساخت کلید عمومی (PKI) گذرنامه الکترونیک**

سامانه‌ای برای ارائه‌ی اقدامات مرتبط با گواهی مانند صدور گواهی‌های لازم در امضای دیجیتال گذرنامه و مدیریت سوابق مرتبط با گواهی و غیره

- **حمله استاد بزرگ شطرنج (Grandmaster Chess)**

حمله با تغییر ظاهر به عنوان تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) استفاده کننده از تراشه‌ی مدار مجتمع (IC) برای تجمع امواج رادیویی[۴] کانال ارتباطی بین تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و سامانه بازرسی (IS)

- **ICAO-PKD**

انبارش گواهی تأیید کننده سند (DV) به کار گرفته شده و مدیریت شده توسط سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) که در صورتی که سامانه بازرسی داخلی یا خارج از کشورخواستار گواهی امضاء کننده سند (DS) کشور مکاتبه کننده باشد، به صورت برخط عرضه می‌شود.

- **بازرسی**

روش اجرایی که در آن اداره‌ی مهاجرت هویت دارنده گذرنامه الکترونیک را با بازرسی تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) ارائه شده توسط دارنده گذرنامه الکترونیک، و سپس تأیید اصل بودن تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) مورد بررسی قرار می‌دهد.

- **سامانه بازرسی (IS)**

---

[۴] hookup

به عنوان یک سیستم اطلاعاتی که تابع خواندن ناحیه قابل خواندن توسط ماشین (MRZ) دیداری و ساز و کار امنیتی (امنیتی کنترل دسترسی پایه (BAC)، احراز هویت غیر فعال (PA)، کنترل دسترسی توسعه یافته (EAC)، احراز هویت فعال (AA) و غیره) را پیاده‌سازی می‌کند. سامانه بازرسی (IS) برای پشتیبانی از بازرسی گذرنامه الکترونیک، در بر گیرنده‌ی پایانه‌ای است که ارتباط فرکانس رادیویی (RF) را با تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و سیستم انتقال دهنده‌ی تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) از طریق این پایانه را برقرار کرده و پاسخ دستورات را پردازش می‌کند.

- **گواهی سامانه بازرسی (IS)**

گواهی مورد استفاده توسطتراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) به منظور بررسی امضای دیجیتال انتقال یافته توسط سامانه بازرسی (IS) در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA). تأیید کننده سند (DV) امضای دیجیتالی را بر روی کلید احراز هویت امضای دیجیتال سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) با کلید تولید امضای دیجیتال انجام می‌دهد.

- **تابع کلید اشتقاق (KDF)**

تابعی برای تولید کلید رمزگذاری و کلید کد احراز هویت پیام (MAC) با استفاده از الگوریتم با استفاده از الگوریتم چکیده‌ساز از نقطه‌ی آغاز تصادفی (Seed)

- **ساز و کار کلید اشتقاق (KDM)**

ساز و کاری برای تولید کلید رمزگذاری و کلید کد احراز هویت پیام (MAC) با استفاده از الگوریتم چکیده‌ساز از نقطه‌ی آغاز تصادفی (Seed)

- **ساختار داده منطقی (LDS)**

ساختار منطقی داده تعریف شده در سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) به منظور ذخیره کردن داده کاربر در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD)

- **کلیدکد احراز هویت پیام (MAC) (کلیدی برای کد احراز هویت پیام)**

کلید استفاده شده توسط الگوریتم رمزنگاری متقابل بر طبق ISO9797 برای تولید کد احراز هویت پیام به منظور جلوگیری از جعل و تخریب داده

- **سند مسافرتی قابل خواندن توسط ماشین (MRTD)**

سند مسافرتی قابل خواندن توسط ماشین مانند گذرنامه، ویزا یا سند رسمی هویت مورد پذیرش مقاصد سفر

- **برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD)**

برنامه‌ای برای بارگذاری در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) است که توسط ساختار منطقی داده (LDS) سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) برنامه‌نویسی شده و ساز و کارهای امنیتی کنترل دسترسی پایه (BAC)، احراز هویت غیر فعال (PA)، کنترل دسترسی توسعه یافته (EAC) و غیره را فراهم می‌آورد.

- **داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD)**

شامل داده کاربر، داده‌امنیتی (TSF) سند مسافرتی قابل خواندن توسط ماشین (MRTD) است.

- **تراشه سند مسافرتی قابل خواندن توسط ماشین (MRTD)**

تراشه‌ی مدار مجتمع (IC) بدون تماس که در برگیرنده‌ی برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و سیستم عامل تراشه‌ی مدار مجتمع (IC) مورد نیاز در عملکرد برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) است که از پروتکل‌های ارتباطی با استاندارد ISO/IEC 14443 پشتیبانی می‌کند.

- **احراز هویت غیر فعال (PA)**

ساز و کار امنیتی برای نشان دادن این که داده ثبت شده در گذرنامه الکترونیک مورد جعل و تخریب قرار نگرفته است، به گونه‌ای که سامانه بازرسی (IS) با گواهی امضاء کننده سند (DS)، امضای دیجیتال را در سند موجودیت غیر فعال امنیتی (SOD) و مقادیر چکیده‌ی داده کاربر مطابق حق خواندن خط‌مشی کنترل دسترسی گذرنامه الکترونیک بررسی می‌کند.

- **داده شخصی دارنده گذرنامه الکترونیک**

داده دیداری قابل شناسایی چاپ شده بر روی صفحه اطلاعات هویتی گذرنامه الکترونیک و دیگر داده‌های هویتی ذخیره شده در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) در ساختار منطقی داده (LDS)

- **عامل شخصی‌سازی**

عاملی که داده هویتی گذرنامه الکترونیک را از سازمان پذیرنده دریافت کرده و سند موجودیت غیر فعال امنیتی (SOD) را با امضای دیجیتال داده تولید می‌کند. پس از ثبت آن‌ها در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) عامل شخصی‌سازی داده امنیتی (TSF) را تولید کرده و آن را در حافظه‌ی امن تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) ذخیره می‌کند. همچنین به اجرای PA-PKI و یا EAC-PKI می‌پردازد.

- **کاوش**

حمله به کاوش داده با قرار دادن پین جستجو در تراشه‌ی مدار مجتمع (IC)

- **مهندسی معکوس**

برای شناسایی و تولید مجدد مفهوم طراحی پایه‌ای و فناوری‌های به کار گرفته شده‌ی محصول از طریق تحلیل مفصل محصول تکمیل شده است.

- **سند موجودیت غیر فعال امنیتی (SOD)** [۵]

سند موجودیت غیر فعال امنیتی (SOD) اشاره به داده هویتی گذرنامه الکترونیک و داده احراز هویت گذرنامه الکترونیک ثبت شده در فاز شخصی‌سازی توسط عامل شخصی‌سازی دارد که با کلید تولید امضای دیجیتال توسط عامل شخصی‌سازی امضا شده است. سند موجودیت غیر فعال امنیتی (SOD) موجودیت غیر فعال پیاده‌سازی شده با نوع داده امضا شده‌ی "نحو پیام رمزنگاری RFC 3369، 2002.8" و از کد خارج شده با روش DER است.

- **داده امنیتی** (TSF data)

[۵] Security Object of Document

داده ذخیره شده در حافظه‌ی امن تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) برای پشتیبانی از ساز و کارهای امنیتی گذرنامه الکترونیک هستند.

- **داده کاربری** (User data)

شامل داده هویتی گذرنامه الکترونیک و داده احراز هویت گذرنامه الکترونیک هستند.

## ۳- شرح محصول

### ۳-۱- نوع محصول

محصول تعریف شده در این پرو فایل حفاظتی، نوعی سیستم عامل تراشه‌ی مدار مجتمع (IC) (COS) و برنامه‌ی کاربردی اسناد مسافرتی قابل خواندن توسط ماشین (برنامه‌ی کاربردی MRTD) به غیر از عناصر سخت‌افزاری تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (تراشه‌ی MRTD) است.

نرم افزار سند مسافرتی قابل خواندن توسط ماشین، الزامات قسمت ۱ جلد ۲ سند ۹۳۰۳ سند مسافرتی قابل خواندن توسط ماشین سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) [۱] (سند ICAO) و کنترل دسترسی توسعه‌یافته V1.11– ساز و کارهای امنیتی پیشرفته‌ی BSIسند مسافرتی قابل خواندن توسط ماشین 2008.02 (مشخصات کنترل دسترسی توسعه‌یافته (EAC)) را برآورده می‌سازد.

گذرنامه الکترونیک، گذرنامه تعبیه شده در تراشه‌ی مدار مجتمع (IC) بدون تماسی است که در آن هویت و دیگر داده‌های دارنده‌گذرنامه الکترونیک مطابق سازمان بین‌المللی هواپیمایی غیر نظامی (سازمان بین‌المللی هواپیمایی غیر نظامی ICAO[۶]) و سازمان بین‌المللی استاندارد(ISO)[۷] ذخیره شده است. تراشه‌ی

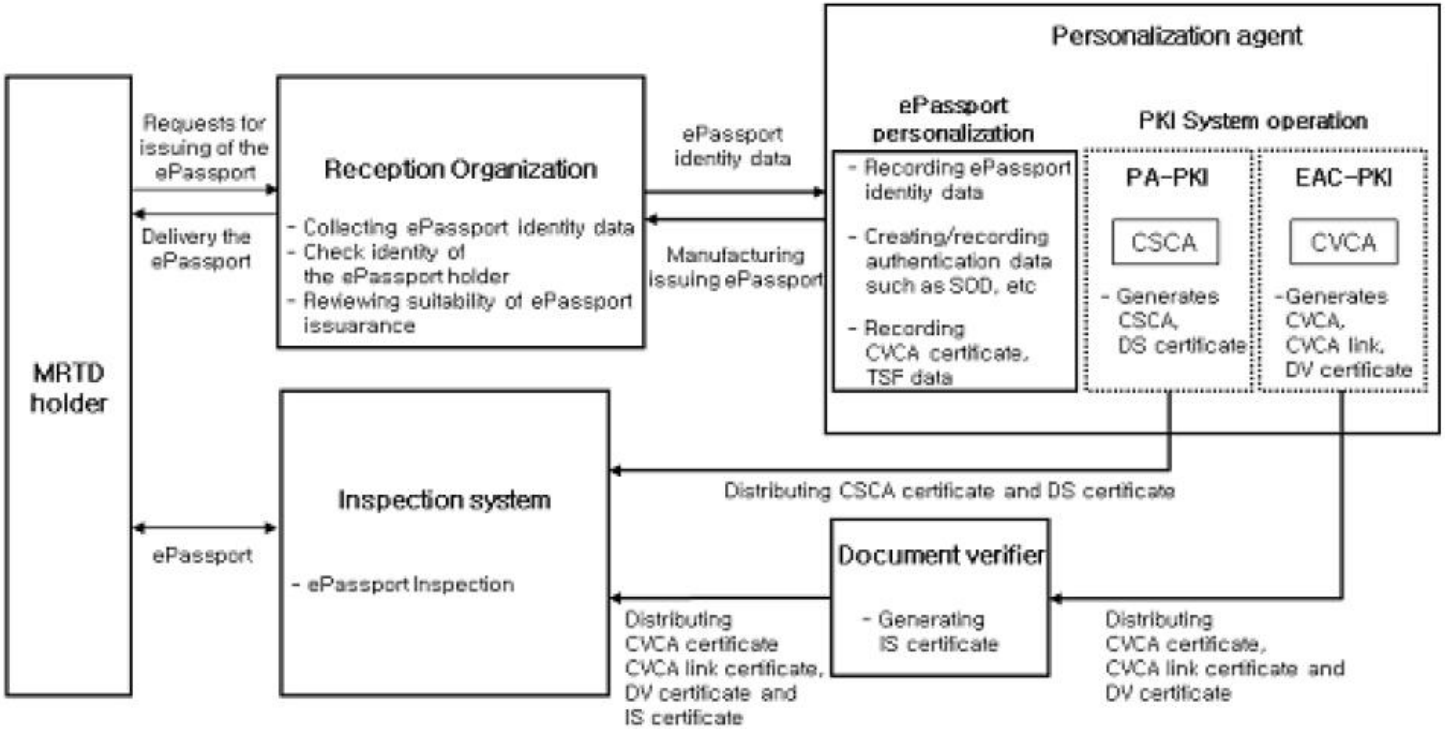
[۶] International Civil Aviation Organization

[۶] The International Standard Organization

مدار مجتمع (IC) بدون تماس مورد استفاده در گذرنامه الکترونیک به عنوان تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) نامیده می‌شود. تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) توسط برنامه‌ی کاربردی تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و سیستم عامل تراشه‌ی مدار مجتمع (IC) (COS) بارگذاری می‌شود تا از فناوری اطلاعات و فناوری‌های امنیتی اطلاعات برای ذخیره‌سازی، پردازش و ساماندهی الکترونیک داده‌های هویتی گذرنامه الکترونیکی پشتیبانی کند.

### ۳-۲- سامانه گذرنامه الکترونیک

در شکل ۱، پیکربندی کلی سامانه گذرنامه الکترونیکی نشان داده شده‌است.




**شکل ۱- پیکربندی کلی سامانه گذرنامه الکترونیک**

دارنده گذرنامه‌ی الکترونیک برای صدور گذرنامه الکترونیک درخواست می‌دهد و گذرنامه الکترونیک صادر شده مطابق با خط‌مشی صدور گذرنامه الکترونیک را دریافت می‌کند. دارنده‌گذرنامه الکترونیک، گذرنامه را به مأمور مهاجرت نشان می‌دهد تا گذرنامه الکترونیک در بخش کنترل مهاجرت بازرسی شود. برای کنترل مهاجرت، گذرنامه الکترونیک توسط مأمور مهاجرت یا یک سامانه بازرسی خودکار طبق خط‌مشی کنترل مهاجرت گذرنامه الکترونیک هر کشور مورد تأیید قرار می‌گیرد.

سازمان پذیرنده، اطلاعات شخصی و زیست‌سنجی دارنده گذرنامه الکترونیک را جمع‌آوری کرده و هویت دارنده گذرنامه را با همکاری با سازمان‌های مربوطه مانند نهادملی پلیس بررسی کرده و این اطلاعات جمع‌آوری شده را برای صدور گذرنامه الکترونیک به عامل شخصی‌سازی می‌فرستد.

عامل شخصی‌سازی موجودیت غیرفعال، امنیت سند (از این به بعد در اینجا SOC[۸]) را با امضای دیجیتال بر روی داده کاربر (هویت و داده‌های احراز هویت) ایجاد می‌کند و آن را در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) با داده‌های هویتی گذرنامه ارسال شده از سازمان پذیرنده ثبت می‌نماید. همچنین پس از ثبت داده‌امنیتی (TSF) در یک حافظه‌ی امن، عامل شخصی‌سازی به تولید و صدور گذرنامه الکترونیک تعبیه شده در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) برای گذرنامه می‌پردازد.

عامل شخصی‌سازی، کلید امضای دیجیتال را برای بررسی جعل و تخریب داده ذخیره شده‌ی کاربر در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) تولید می‌کند. سپس، مطابق با بیانیه‌ی شیوه صدور گواهی[۹] (CPS) سامانه زیرساخت کلید عمومی (PKI) گذرنامه الکترونیک، عامل شخصی‌سازی گواهی مرجع صلاحیت دار امضا کننده گواهی کشور (CSCA) و گواهی امضاء کننده سند (DS) را تولید، صادر و مدیریت می‌کند. مطابق با خط‌مشی صدور گذرنامه الکترونیک، عامل شخصی‌سازی برای بررسی حقوق دسترسی به داده زیست‌سنجی دارنده‌گذرنامه الکترونیک در صورت پشتیبانی ساز و کار امنیتکنترل

[۸] document security object

[۹] Certification Practice Statement

دسترسی توسعه‌یافته(EAC) کلید امضای دیجیتال را تولید می‌کند. سپس، عامل شخصی‌سازی گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) و گواهی تأیید کننده سند (DV) را تولید، صادر و مدیریت می‌کند. جزئیات مربوط به سامانه زیرساخت کلید عمومی (PKI) گذرنامه الکترونیک و شیوه صدور گواهی‌نامه، مانند سرور صدور گواهی‌نامه، افزاره‌های تولید کلید و اقدامات امنیتی رویه‌ای فیزیکی[۱۰] و غیره، به خط‌مشی صدور گذرنامه الکترونیک بستگی دارد.

تأیید کننده سند، با استفاده از گواهی‌های مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) و تأیید کننده سند (DV) به تولید گواهیسامانه بازرسی[۱۱] (IS) می‌پردازد، سپس این گواهی‌ها را به سامانه بازرسی ارائه می‌دهد.

انواع گواهی‌های مورد استفاده در سامانه‌گذرنامه الکترونیک در جدول ۱، نشان داده شده است.

**جدول ۱- انواع گواهی**

| کاربری | سامانه زیرساخت کلید عمومی (PKI) گذرنامه الکترونیکی | موضوع | گواهی |
|---|---|---|---|
| برای بررسی جعل و تخریب داده کاربر | PA-PKI | مرجع صلاحیت دار امضا کننده گواهی کشور (CSCA) | گواهی CSCA |
| | | عامل شخصی‌سازی | گواهی DC |
| برای بررسی حق دسترسی به داده زیست‌سنجی دارنده | EAC-PKI | مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA) | گواهی CVCA |
| | | | گواهی پیوند CVCA |

[۱۰] procedural

[۱۱] Inspection System

| | | | |
|---|---|---|---|
| گذرنامه الکترونیکی | | تأیید کننده سند | گواهی تأیید کننده سند (DV) |
| | | کنترل دسترسی توسعه یافته (EAC) پشتیبانی کننده از سامانه بازرسی | گواهی سامانه بازرسی (IS) |

نکته‌ی کاربردی: عامل شخصی‌سازی گواهی‌هایی برای احراز هویت غیر فعال[۱۲] (PA) وکنترل دسترسی توسعه‌یافته(EAC) تولید و صادر کرده و مطابق خط‌مشی صدور گذرنامه الکترونیک، گواهی‌ها را به صورت برخط[۱۳] و یا برون خط[۱۴] توزیع می‌کند. در صورتی که حالت صادر کننده گذرنامه الکترونیک به ICAO-PKDمتصل شود، ممکن است گواهی امضاء کننده سند (DS) ثبت شده و به صورت برخط توزیع گردد. همچنین تأیید کننده سند، گواهی سامانه بازرسی (IS) را مطابق با خط‌مشی صدور گذرنامه الکترونیک تولید کرده و به سامانه بازرسی توزیع می‌کند.

### ۳-۳- دامنه‌ی کاربرد محصول

این پروفایل حفاظتی چرخه حیات محصول را از قبیل توسعه، ساخت، شخصی‌سازی و استفاده عملیاتی از گذرنامه الکترونیک را تعریف کرده و محیط محصول و دامنه‌ی فیزیکی یا منطقی محصول را به صورت زیر تعریف می‌کند:

#### ۳-۳-۱- چرخه حیات و محیط محصول

##### ۳-۳-۱-۱- چرخه حیات تراشه‌یسند مسافرتی قابل خواندن توسط ماشین (MRTD) و محصول

[۱۲] Passive Authentication

[۱۳] online

[۱۴] offline

جدول ۲، چرخه حیات تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و محصول را نشان می‌دهد. در این جدول فرایند انتقال حذف شده است. در چرخه حیات نشان داده شده در جدول ۲، فرایند توسعه‌ی محصول مربوط به فاز۱ (توسعه) و فاز۲ (ساخت) است، در حالی که محیط عملیاتی محصول مربوط به فاز ۳ (شخصی‌سازی) و فاز ۴ (استفاده عملیاتی) است.

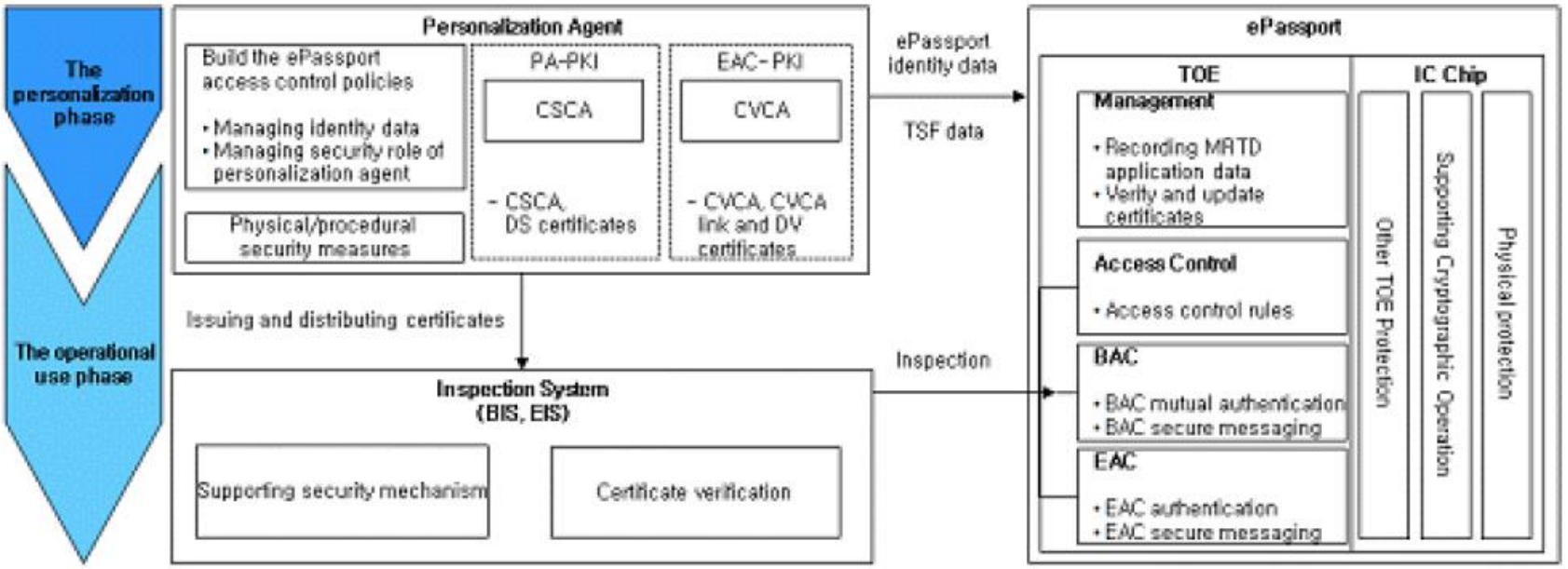
**جدول ۲- چرخه حیات تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و محصول**

| فاز | چرخه حیات تراشه‌ی (MRTD) | چرخه حیات محصول |
|---|---|---|
| فاز ۱ (توسعه) | (۱) توسعه دهنده‌ی تراشه‌ی مدار مجتمع (IC) برای طراحی تراشه‌ی مدار مجتمع (IC) و توسعه تراشه‌ی مدار مجتمع (IC) S/Wتخصیص یافته | |
| | | (۲) توسعه‌دهنده S/W برای توسعه محصول (سیستم عامل تراشه‌ی (COS) برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD)) با استفاده از تراشه‌ی مدار مجتمع (IC) و S/Wتخصیص یافته |
| فاز ۲ (ساخت) | (۳) سازنده‌ی تراشه‌ی مدار مجتمع (IC) برای پوشش محصول در حافظه‌ی فقط خواندنی (ROM)، برای ثبت شناسه تراشه‌ی مدار مجتمع (IC) و برای تولید تراشه‌ی مدار مجتمع (IC) | |
| | | (۴) سازنده‌ی گذرنامه ی الکترونیک برای ایجاد فضای انبارش داده کاربر مطابق با قالب ساختار منطقی داده (LDS) یا سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) و برای ثبت آن در حافظه‌ی فقط خواندنی قابل پاک کردن و قابل برنامه‌نویسی به صورت الکترونیکی (EEPROM)<br>(۵) سازنده‌ی گذرنامه الکترونیک برای ثبت اطلاعات شناسایی و احراز هویت عامل شخصی‌سازی در حافظه‌ی فقط خواندنی قابل پاک کردن و قابل برنامه‌نویسی به صورت الکترونیکی (EEPROM)<br>(۶) سازنده‌ی گذرنامه الکترونیک برای تعبیه تراشه‌ی مدار مجتمع (IC) در دفترچه‌ی گذرنامه |

| | | |
|---|---|---|
| فاز ۳<br>(شخصی) | | (۷) عامل شخصی‌سازی برای ایجاد سند موجودیت غیر فعال امنیتی (SOD) با یک امضای دیجیتال بر روی داده شناسه‌ی گذرنامه الکترونیک<br>(۸) عامل شخصی‌سازی برای ثبت داده هویتی گذرنامه الکترونیک، داده احراز هویت (از جمله SOD) و داده‌امنیتی در محصول |
| فاز ۴<br>(استفاده عملیاتی) | | (۹) سامانه بازرسی برای تأیید گذرنامه الکترونیک و بررسی هویت دارنده‌گذرنامه الکترونیک بوسیله برقراری ارتباط با محصول |

**۳-۳-۱-۲- محیط عملیاتی محصول**

شکل ۲، محیط عملیاتی محصول را در فازهای شخصی‌سازی و استفاده عملیاتی گذرنامه الکترونیک، از طریق ارتباط با توابع مهم امنیتی محصول و موجودیت‌های خارجی (عامل شخصی‌سازی، سامانه بازرسی ) نشان می‌دهد که با محصول در تعامل هستند.

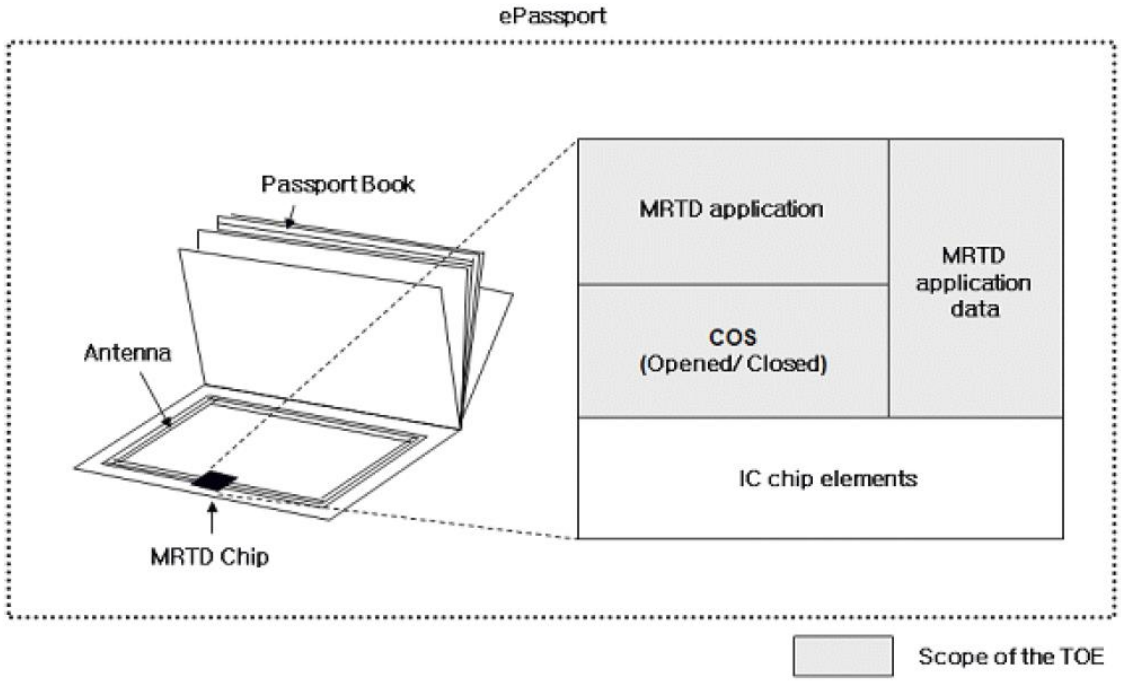



**شکل ۲- محیط عملیاتی محصول**

### ۳-۳-۲-  دامنه‌ی فیزیکی محصول

**شکل ۳دامنه‌ی کاربرد محصول**

، دامنه کاربرد محصول را نشان می‌دهد.




**شکل ۳دامنه‌ی کاربرد محصول**

گذرنامه الکترونیک به دفتر گذرنامه، تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و آنتن تعبیه شده در جلد دفتر گذرنامه اشاره دارد. تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) شامل سیستم عامل تراشه‌ی مدار مجتمع (IC)، برنامه‌ی کاربردی سند مسافرتی قابل خواندن

توسط ماشین (MRTD)، داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و عناصر تراشه‌ی مدار مجتمع (IC) است. عناصر تراشه‌ی مدار مجتمع (IC)، شامل پردازنده‌ی مرکزی (CPU)، کمک پردازنده[۱۵]، پورت ورودی و خروجی، حافظه (حافظه‌ی دستیابی تصادفی (RAM)، حافظه‌ی فقط خواندنی (ROM)، حافظه‌ی فقط خواندنی قابل پاک کردن و قابل برنامه‌نویسی به صورت الکترونیکی (EEPROM)) و واسط‌های بدون تماس و غیره است.

در این پروفایل حافظتی، محصول با سیستم عامل تراشه‌ی مدار مجتمع (IC) (COS)، برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) تعریف شده است. عناصر تراشه‌ی مدار مجتمع (IC)از دامنه محصول حذف شده است.

سیستم عامل تراشه‌ی مدار مجتمع (IC) (COS)، کارکردهایی برای اجرای برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و مدیریت داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) مانند پردازش دستورات، مدیریت فایل‌ها و غیره را ارائه می‌دهد. که در استاندارد ISO/IEC 7816-4،8 و 9 تعریف شده است. در این پروفایل حفاظتی هم سیستم عامل تراشه‌ی مدار مجتمع (IC) باز و هم بسته پذیرفته شده است.

برنامه‌ی کاربردی تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD)، برنامه‌ی کاربردی تراشه‌ی مدار مجتمع (IC) است که توابعی را برای ذخیره و پردازش داده هویتی گذرنامه الکترونیک مطابق با قالب ساختار منطقی داده[۱۶] (LDS) تعریف شده در سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) و ساز و کارهای امنیتی برای محافظت امن از توابع پیاده‌سازی می‌کند. همچنینبه دلیل گنجانده شدن داده زیست‌سنجی دارنده‌گذرنامه الکترونیک در داده هویتی گذرنامه الکترونیک، ساز و کارهای امنیتی کنترل دسترسی توسعه‌یافته (EAC)را با مشخصات کنترل دسترسی توسعه‌یافته (EAC) به برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) افزوده است.

---

[۱۵] Co-processor

[۱۶] Logical Data Structure

داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) متشکل از داده کاربر مانند داده هویتی گذرنامه الکترونیک و غیره و داده امنیتی مورد نیاز در ساز و کار امنیتی است.

ممکن است محصول برای انجام عملیات، نیازمند به عناصر تراشه‌ی مدار مجتمع (IC)، سخت‌افزار، نرم‌افزار یا دیواره‌ی آتش اضافی باشد. این پروفایل حفاظتی برای انعکاس محصول توسعه یافته است که در اشکال مختلف پیاده‌سازی شده است. زمانی که یک نویسنده‌ی هدف امنیتی این پروفایل حفاظتی را مدعی می‌شود باید تمام نرم افزار یا دیواره‌ی آتشی که بخشی از محصول نیستند اما برای انجام کارکردهای محصول مورد نیاز هستند را در هدف امنیتی توضیح دهد.

### ۳-۳-۳- دامنه‌ی منطقی محصول

محصول مطابق با پروتکل انتقالی تعریف شده در استاندارد ISO/IEC 14443-4 با سامانه بازرسی ارتباط برقرار می‌کند. محصول ساز و کارهای امنیتی تعریف شدهدر سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) و مشخصات کنترل دسترسی توسعه‌یافته (EAC) را پیاده‌سازی می‌کند و کنترل دسترسی و توابع مدیریت امنیتی را ارائه می‌دهد. همچنین، محصول توابع حفاظت توابع هدف امنیتی (TSF)، مانند خود آزمایی توابع هدف امنیتی (TSF)، محافظت از حالت امن و غیره را فراهم می‌آورد.

### ۳-۴- مشخصه‌های امنیتی محصول

#### ۳-۴-۱- سازوکار امنیتی

محصول، مشخصه‌های امنیتی مانند محرمانگی، یکپارچگی، کنترل دسترسی و احراز هویت را به منظور محافظت از داده‌امنیتی (TSF)، داده کاربر از داده هویتی گذرنامه الکترونیکی و داده احراز هویت گذرنامه الکترونیک و غیره را فراهم می‌آورد. این مشخصه‌های امنیتی با ساز و کار BAC از سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) و ساز و کار EAC از مشخصات کنترل دسترسی توسعه‌یافته (EAC) پیاده‌سازی می‌شوند. علاوه بر آن محصول، سند موجودیت

غیر فعال امنیتی (SOD) برای سامانه بازرسی کنترل دسترسی پایه (BAC) و سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) فراهم آورده و سامانه بازرسی جعل و تخریب داده کاربر را از طریق درستی‌سنجی امضای دیجیتال سند موجودیت غیر فعال امنیتی (SOD) تشخیص می‌دهد.

**۳-۴-۱-۱-کنترل دسترسی پایه(BAC)**

کنترل دسترسی پایه[۱۷] (BAC)، محرمانگی و یکپارچگی داده فردی دارنده‌گذرنامه الکترونیک را با پیام‌رسانی امن در هنگام کنترل دسترسی به داده فردی دارنده‌گذرنامه الکترونیک ذخیره شده در محصول و انتقال آن به سامانه بازرسی با رعایت حق خواندن فراهم می‌آورد، کنترل دسترسی پایه (BAC) شامل احراز هویت دو طرفه کنترل دسترسی پایه (BAC)، توزیع کلید کنترل دسترسی پایه (BAC) و پیام‌رسانی امنکنترل دسترسی پایه (BAC) است.

محصول مقادیر تصادفی را یا با تولید کلید احراز هویت کنترل دسترسی پایه (BAC) از داده MRZDG1 یا با استفاده از کلید احراز هویت کنترل دسترسی پایه (BAC) ذخیره شده و سامانه بازرسی پشتیبان کنترل دسترسی پایه (BAC) با استفاده از کلید احراز هویتکنترل دسترسی پایه (BAC) از خواندن نوری (Optically) ناحیه قابل خواندن توسط ماشین (MRZ) تولید می‌کند. پس از آن، محصول وسامانه‌بازرسی رمزگذاری اعداد تصادفی تولید شده را انجام داده و آن‌ها را مبادله می‌کنند. محصول و سامانه بازرسی پشتیبان کنترل دسترسی پایه (BAC) احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) را با بررسی اعداد تصادفی مبادله شده اجرا می‌کنند. در صورتی که احراز هویت دو طرفه با شکست روبرو شود نشست به پایان می‌رسد.

به منظور انتقال امن داده شخصی دارنده‌گذرنامه الکترونیک، محصول پس از بررسی حق خواندن سامانه بازرسی برای داده شخصی دارنده‌گذرنامه الکترونیک از طریق احراز هویت متقابل کنترل دسترسی پایه (BAC)، پیام‌رسانی امن کنترل دسترسی پایه (BAC) را با رمزگذاری بوسیله‌ی کلید نشست کنترل دسترسی پایه (BAC) به اشتراک گذاشته شده از طریق توزیع کلید کنترل دسترسی پایه (BAC)و تولید کد احراز هویت پیام (MAC) ایجاد می‌کند.

**۳-۴-۱-۲- کنترل دسترسی توسعه یافته(EAC)**

[۱۷] basic access control

کنترل دسترسی توسعه یافته[۱۸] (EAC)، محرمانگی و یکپارچگی داده زیست‌سنجی دارنده‌گذرنامه الکترونیک را فراهم می‌آورد. این کار از طریق پیام‌رسانی امن هنگام کنترل دسترسی به داده زیست‌سنجی دارنده‌گذرنامه الکترونیک ذخیره شده در محصول و انتقال آن به سامانه بازرسی دارای حق خواندن صورت می‌پذیرد. کنترل دسترسی توسعه یافته (EAC)، شامل کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA)، پیام‌رسانی امن کنترل دسترسی توسعه یافته (EAC) و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) است.

در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA)، برای پیاده‌سازی پروتکل توزیع کلید ایستای زودگذر دیفی-هلمن(DH)، برای توزیع کلید نشست EAC و احراز هویت تراشه است. محصول، کلید عمومی احراز هویت تراشه‌ی کنترل دسترسی توسعه یافته (EAC) را به گونه‌ای انتقال می‌دهد که سامانه بازرسی خود را احراز هویت کرده و پروتکل توزیع کلید را با استفاده از کلید عمومی موقت دریافت شده از سامانه بازرسی اجرا می‌کند. در صورت شکست در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA)، نشست به پایان می‌رسد. در صورت موفقیت در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA)، محصول پیام‌رسان امن کنترل دسترسی توسعه یافته (EAC) را با استفاده از کلید نشست کنترل دسترسی توسعه یافته (EAC) ایجاد می‌کند.

در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) برای محصول جهت پیاده‌سازی پروتکل احراز هویت چالش - پاسخ مبتنی بر امضای دیجیتالی TOEبه منظور احراز هویت سامانه بازرسی پشتیبانی کننده از کنترل دسترسی توسعه یافته (EAC) است. محصول سامانه بازرسی بررسی‌کننده‌ی مقادیر امضای دیجیتال با سامانه بازرسی در کلید عمومی موقت استفاده شده برای در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) با استفاده از گواهی سامانه بازرسی (IS) را احراز هویت می‌کند. محصول هنگام دریافت گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، گواهی تأیید کننده سند (DV) و گواهی سامانه بازرسی از سامانه بازرسی پشتیبانی کننده از کنترل دسترسی توسعه یافته (EAC)، گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) را با استفاده از کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) در حافظه امن

[۱۸]extended access control

بررسی می‌کند. سپس محصول، با چک کردن تاریخ معتبر در گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA)، کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) و تاریخ جاری را در صورت لزوم به روزرسانی می‌کند. پس از بررسی گواهیسامانه بازرسی (IS)، محصول اجازه دسترسی سامانه بازرسی پشتیبانی کننده از کنترل دسترسی توسعه یافته (EAC) را برای خواندن داده زیست‌سنجی دارنده‌گذرنامه الکترونیک را صادر می‌کند و داده را از طریق پیام‌رسان امن کنترل دسترسی توسعه یافته (EAC) انتقال می‌دهد.

جدول ۳، ساز و کار امنیتی گذرنامه الکترونیک را خلاصه کرده است.

**جدول ۳ ساز و کار امنیتی گذرنامه الکترونیک**

| ساز و کار امنیت گذرنامه الکترونیک | | | | |
|---|---|---|---|---|
| **ساز و کار امنیتی** | **مشخصه‌های امنیتی** | **رمزنگاری** | **نوع کلید یا گواهی رمزنگاری** | **مشخصه‌های امنیتی فناوری اطلاعات محصول** |
| **احراز هویت غیر فعال (PA)** | احراز هویت داده کاربر | N/A | N/A | کنترل دسترسی برای سند موجودیت غیر فعال امنیتی (SOD)<br>حق خواندن: BIS و EIS<br>حق نوشتن: عامل شخصی‌سازی |
| **کنترل دسترسی پایه (BAC)** | احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) | پروتکل احزار هویت موجودیت مبتنی بر کلید متقارن<br>TDES-CBC<br>SHA<br>MAC | کلید احراز هویت کنترل دسترسی پایه (BAC) (کلید رمزگذاری، کلید کد احراز هویت پیام (MAC)) | محصول حق دسترسی سامانه بازرسی را با رمزگشایی و عملیات کد احراز هویت پیام (MAC) برای مقادیر انتقال یافته از سامانه بازرسی بررسی می کند.<br>محصول پس از رمزگشایی و عملیات کد احراز هویت پیام (MAC) برای احراز هویت به سامانه بازرسی انتقال می‌دهد. |
| | توزیع کلید کنترل دسترسی پایه (BAC) | پروتکل توزیع کلید مبتنی بر کلید متقارن<br>TDES-CBC<br>SHA<br>MAC | کلید نشست کنترل دسترسی پایه (BAC) (کلید رمزگذاری، کلید کد احراز هویت پیام (MAC)) | تولید کلید نشست کنترل دسترسی پایه (BAC) با استفاده از تابع اشتقاق کلید (KDF) از عدد تصادفی کلید به اشتراک گذاری شده‌ی تبادل یافته از پروتکل توزیع کلید مبتنی بر استاندارد رمزگذاری داده سه گانه۱۹ (TDES) |

[۱۹] Triple-DES

| | | | | |
|---|---|---|---|---|
| | پیام‌رسان امن کنترل دسترسی پایه (BAC) | پیام‌رسان امن | کلید نشست کنترل دسترسی پایه (BAC) (کلید رمزگذاری، کلید MAC) | انتقال پیام‌ها با ایجاد کد احراز هویت پیام (MAC) بعد از رمزگذاری با کلید نشست کنترل دسترسی پایه (BAC)<br>دریافت پیام‌ها با رمزگشایی آن پس از تایید کد احراز هویت پیام (MAC) با کلید نشست کنترل دسترسی پایه (BAC) |
| **EAC** | در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) | پروتکل توزیع کلید DH پروتکل توزیع کلید منحنی بیضوی دیفی– هلمن (ECDH) | کلید عمومی احراز هویت تراشه‌ی کنترل دسترسی توسعه یافته (EAC)<br>کلید خصوصی احراز هویت تراشه‌ی کنترل دسترسی توسعه یافته (EAC) | محصول پروتکل توزیع کلید ایستای زودگذردیفی–هلمن (DH) را اجرا می کند. |
| | پیام‌رسانی امن کنترل دسترسی توسعه یافته (EAC) | پیام‌رسان امن | کلید نشست کنترل دسترسی توسعه یافته (EAC) (کلید رمزنگاری، کلید کد احراز هویت پیام (MAC)) | پیام‌رسانی امن با استفاده از کلید نشست کنترل دسترسی توسعه یافته (EAC) به اشتراک گذاری شده در در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) |

| | | | | |
|---|---|---|---|---|
| | کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) | RSAPSS<br>ECDSA | گواهی CVCA<br>گواهی پیوند CVCA<br>گواهی تأیید کننده سند (DV)<br>گواهی سامانه بازرسی (IS) | بررسی گواهی سامانه بازرسی (IS) با استفاده از زنجیره گواهی و گواهی پیوند.<br>بررسی امضای دیجیتال برای پیام‌های انتقال یافته سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) برای احراز هویت سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) |

### ۳-۴-۲- کنترل دسترسی و مدیریت امنیت محصول

محصول قوانین کنترل دسترسی و توابع مدیریتی برای داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) براساس مشخصه‌های امنیتی کاربر در فازهای شخصی‌سازی و استفاده عملیاتی ارائه می‌دهد.

محصول امکان نوشتن توابع بر روی داده کاربر و داده‌امنیتی (TSF) در فاز شخصی‌سازی را برای عامل شخصی‌سازی مجاز فراهم می‌آورد. همچنین محصول تابع کنترل دسترسی بر روی حق خواندن داده کاربر را بر اساس حق دسترسی‌های سامانه بازرسی داده شده از طریق اجرای ساز و کارهای امنیتی در فاز استفاده عملیاتی ارائه می‌دهد.

محصول تنها به عامل شخصی‌سازی مجاز اجازه‌ی مدیریت مشخصه‌های امنیتی کاربر، داده کاربر و داده‌امنیتی (TSF) را در فازهای شخصی‌سازی و استفاده عملیاتی داده و آن را به عنوان نقش امنیتی تعریف می‌کند. علاوه بر آن توابع هدف امنیتی (TSF) خود برخی از توابع مدیریت امنیت را مانند به روز رسانی گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، تاریخ جاری و مقدار دهی اولیه شناسه پیام‌رسان امن و غیره را اجرا می‌کند.

### ۳-۴-۳- دیگرحفاظت‌های محصول

محصول توابعی را جهت شناسایی، اقدام به اصلاح داده انتقال یافته و اجرای خود آزمایی برای بررسی یکپارچگی داده ذخیره شده‌ی توابع هدف امنیتی (TSF) و توابع هدف امنیتی (TSF) اجرا می‌کند. همچنین، چنانچه اگر تشخیص از طریق خود آزمایی یا عملیات غیرطبیعی در تراشه‌ی مدار مجتمع (IC) با شکست همراه باشد، محصول از حالت امن محافظت می‌کند تا از انواع خرابی در توابع هدف امنیتی (TSF) (سوء عمل) جلوگیری کند.

محصول اطمینان حاصل می‌کند که داده مرتبط با رمزنگاری از طریق بهره‌برداری از پدیده‌ی فیزیکی عملیات رمزنگاری قابل دستیابی نیستند (تغییر جریان، ولتاژ و الکترومغناطیس و غیره).

## ۴-مسائل امنیتی

### ۴-۱- دارایی‌ها

به منظور حفاظت از دارایی‌های محصول که درجدول ۴ نمایش داده شده است، محصول توابع امنیتی مانند محرمانگی، یکپارچگی، احراز هویت و کنترل دسترسی و غیره را ارائه می‌دهد.

**جدول ۴- دارایی‌های محصول**

| رده‌بندی | | | توضیحات | فضای انبارش |
|---|---|---|---|---|
| داده کاربر | داده هویتی گذرنامه الکترونیکی | داده شخصی دارنده‌گذرنامه الکترونیکی | داده ذخیره شده در EF.DG1، EF.DG2، EF.DG 15 و EF.DG5~EF.DG13 | فایل ابتدایی (EF) |
| | | داده زیست‌سنجی دارنده گذرنامه الکترونیکی | داده ذخیره شده در EF.DG3 و EF.DG4 | |
| | داده احراز هویت گذرنامه الکترونیکی | | سند موجودیت غیر فعال امنیتی (SOD)، کلید عمومی احراز هویت تراشه‌یEAC و غیره | |
| | EF.CVCA | | در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA)، | |

| | | | |
|---|---|---|---|
| | | فهرست شناسه‌ی درستی‌سنجی امضای دیجیتالی مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA) برای احراز هویت سامانه بازرسی مورد استفاده محصول قرار می‌گیرد | |
| | EF.COM | اطلاعات نسخه‌ی ساختار منطقی داده (LDS)، فهرست برچسب DG استفاده شده و غیره | |
| داده‌امنیتی (TSF) | کلید خصوصی احراز هویت تراشه‌ی کنترل دسترسی توسعه یافته (EAC) | در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA)، کلید خصوصی تراشه‌ی برای نشان دادن عدم جعل در تراشه MRTD مورد استفاده‌محصول قرار می‌گیرد. | حافظه‌ی امن |
| | گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA) | در فاز شخصی‌سازی، گواهی ریشه‌ی احراز هویت تراشه (CA) در EAC-PKI صادر می‌شود. | |
| | کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA) | پس از فاز شخصی‌سازی، کلید عمومی گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA) با به روزرسانی گواهی از نو ایجاد می شود. | |
| | تاریخ جاری | در فاز شخصی‌سازی تاریخ صدور گذرنامه الکترونیکی ثبت شده است. با این حال، در فاز استفاده عملیاتی، محصول به صورت داخلی آن را به عنوان آخرین تاریخ در میان تاریخ‌های صدور گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA)، گواهی تأیید کننده سند (DV) و یا حالت صدور گواهی سامانه بازرسی (IS) به روز رسانی می‌کند | |
| | کلید احراز هویت BAC | کلید رمزنگاری احراز هویت BAC، کلید کد احراز هویت پیام (MAC) احراز هویت BAC | |
| | کلید نشست BAC | کلید رمزنگاری نشست BAC، کلید کد احراز هویت پیام (MAC) نشست BAC | |
| | کلید نشست EAC | کلید رمزنگاری نشست EAC، کلید کد احراز هویت پیام (MAC) نشست EAC | |

**نکته‌ی کاربردی**: داده زیست‌سنجی به دست آمده از دارنده‌گذرنامه الکترونیک شامل چهره، اثر انگشت و عنبیه است. اطلاعات چهره مطابق با سند سازمان بین‌المللی هواپیمایی غیرنظامی (ICAO) به صورت اجباری گنجانده می‌شود. اطلاعات اثر انگشت و عنبیه با توجه به خط‌مشی صدور گذرنامه الکترونیک به صورت اختیاری ذخیره می‌شود. این پروفایل حفاظتی در برگیرنده‌ی الزامات کارکرد امنیتی برای مشخصات کنترل دسترسی توسعه‌یافته (EAC) است با این فرض که باید اطلاعات اثر انگشت گنجانده شود. نویسنده‌ی هدف امنیتی ممکن است علاوه بر این اطلاعات عنبیه را در گروه داده ۴ (DG4) تعریف کند.

**نکته‌ی کاربردی**: کلید احراز هویت کنترل دسترسی پایه (BAC) در حال حاضر در فاز شخصی‌سازی توسط روش پیاده‌سازی تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) تولید شده و در حافظه‌ی امن تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) ثبت شده یا محصول خود کلید را در کنترل دسترسی پایه (BAC) فاز استفاده عملیاتی تولید می‌کند.

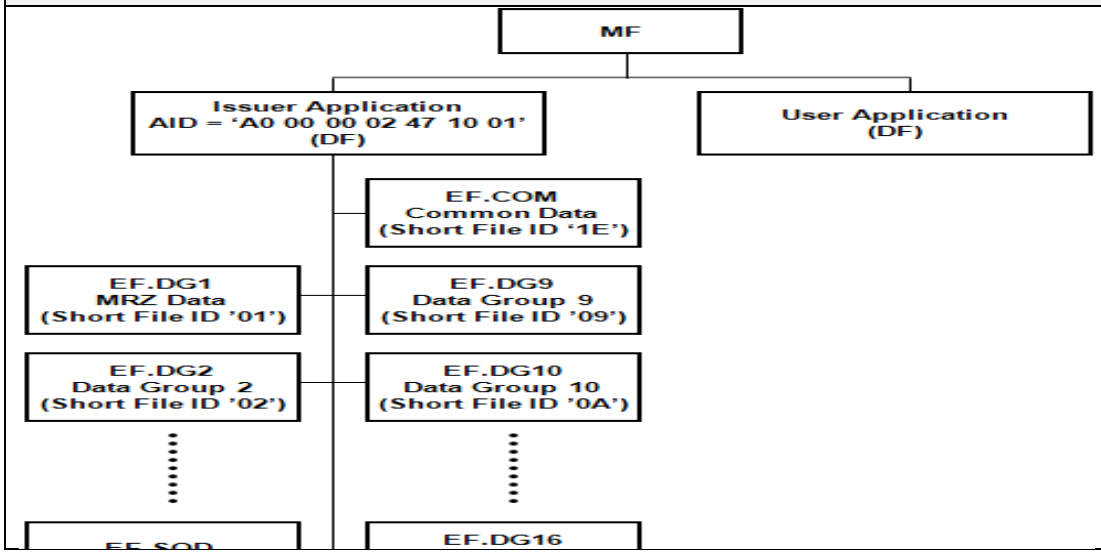
**نکته‌ی کاربردی**: به منظور حمایت از کنترل دسترسی توسعه‌یافته (EAC)، عامل شخصی‌سازی کلید عمومی و خصوصی احراز هویت تراشه‌ی کنترل دسترسی توسعه‌یافته (EAC)را تولید و آن‌ها را در محصول ثبت می‌کند. کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA)، از طریق گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA) مطابق با مشخصات کنترل دسترسی توسعه‌یافته (EAC)به روز رسانی می‌شود. با این حال، اولین کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) برای تأیید گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) باید در حافظه‌ی امن تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) در فاز شخصی‌سازی ثبت شود. وقتی که کلید درستی‌سنجی امضای دیجیتال به روز رسانی شد، نا معتبر کردن یا حذف کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) به خط‌مشی‌های صدور گذرنامه الکترونیک بستگی دارد.

ساختار منطقی داده‌ای (LDS) که داده کاربر در آن ذخیره شده است ساختار فایل‌های فایل اصلی[۲۰] (MF)، فایل تخصیص یافته[۲۱] (DF) و فایل ابتدایی[۲۲] (EF) را تعریف می‌کند. جدول ۵۵، محتوایی از EF.DG1~EF.DG16 که در آن بخش‌هایی از داده کاربر ذخیره شده است را نشان می‌دهد.

---

[۲۰] Master File

**جدول ۵- محتوای ساختار منطقی داده که داده کاربر در آن ذخیره می‌شود**

| دسته | DG | محتوا | ساختار LSD |
|---|---|---|---|
| جزییات ثبت شده در ناحیه قابل خواندن توسط ماشین (MRZ) | DG1 | نوع سند<br>حالت صدور<br>نام دارنده<br>شماره سند<br>رقم حواله - شماره سند<br>ملیت<br>تاریخ تولد<br>رقم حواله - تاریخ تولد<br>جنسیت<br>تاریخ اعتبار یا انقضا<br>رقم حواله - تاریخ اعتبار یا انقضا |  |

[۲۱]Dedicated File

[۲۲]Elementary File

| | | | |
|---|---|---|---|
| | | رقم حواله ترکیبی | |
| ویژگی‌های شناسایی کد گذاری شده | DG2 | چهره کدگذاری شده | |
| | DG3 | انگشت کدگذاری شده | |
| | DG4 | چشم کدگذاری شده | |
| سایر | DG5 | تصویر (عکس صورت) نمایش داده شده | |
| | DG6 | - | |
| | DG7 | امضا نمایش داده شده | |
| | DG8 | - | |
| | DG9 | - | |
| | DG10 | - | |
| | DG11 | جزئیات فردی اضافی | |
| | DG12 | جزئیات سند اضافی | |
| | DG13 | - | |
| | DG14 | کلید عمومی احراز هویت تراشه‌یEAC | |
| | DG15 | کلید درستی‌سنجی امضای دیجیتال احراز هویت فعال (AA) (اختیاری) | |
| | DG16 | اطلاع‌رسانی به فرد یا افراد | |

### ۴-۲- موجودیت‌های فعال، موجودیت‌های غیر فعال، عملیات و مشخصه‌های امنیتی

این پروفایل حفاظتی همه‌ی موجودیت‌های فعال، موجودیت‌های غیر فعال، عملیات، مشخصه‌های امنیتی به کار رفته شده در الزامات امنیتی را به گونه‌ای که در جدول ۶ نشان داده شده است تعریف می‌کند. همچنین، این پروفایل حفاظتی شمارنده دنباله ارسال[۲۳] (SSC) را با مشخصه‌های امنیتی نشست مرتبط با برقراری پیام‌رسانی امن تعریف می‌کند.

**جدول ۶- تعریف موجودیت فعال، موجودیت غیرفعال، مشخصه‌های امنیتی مرتبط و عملیات**

<table>
<tr><th>موجودیت فعال</th><th>مشخصه‌های امنیتی موجودیت فعال</th><th>موجودیت غیر فعال</th><th>مشخصه‌های امنیتی موجودیت غیر فعال</th><th>عملیات</th></tr>
<tr>
<td>
<table>
<tr><th>موجودیت‌های فعال</th><th>مشخصه‌های امنیتی موجودیت فعال</th></tr>
<tr><td>BIS</td><td>مجوز BAC</td></tr>
<tr><td>EIS</td><td>مجوز BAC،<br>مجوز EAC</td></tr>
<tr><td>عامل شخصی سازی</td><td>عامل شخصی‌سازی صادر کننده مجوز</td></tr>
</table>
</td>
<td></td>
<td>
<table>
<tr><th rowspan="2">موجودیت‌های غیر فعال</th><th colspan="2">مشخصه‌های امنیتی</th></tr>
<tr><th>مشخصه های امنیتی عملیات موجودیت غیر فعال</th><th>مشخصه‌های امنیتی حق دسترسی موجودیت غیر فعال</th></tr>
<tr><td rowspan="2">داده شخصی دارنده گذرنامه الکترونیک</td><td>حق خواندن</td><td>مجوز BAC،<br>مجوز EAC</td></tr>
<tr><td>حق نوشتن</td><td>عامل شخصی‌سازی صادر کننده مجوز</td></tr>
<tr><td rowspan="2">داده زیست‌سنجی دارنده گذرنامه الکترونیک</td><td>حق خواندن</td><td>مجوز EAC</td></tr>
<tr><td>حق نوشتن</td><td>عامل شخصی‌سازی صادر کننده مجوز</td></tr>
</table>
</td>
<td>- خواندن<br>- نوشتن</td>
</tr>
</table>

[۲۳] Send Sequence Counter

| | | | | |
|---|---|---|---|---|
| | داده احراز هویت گذرنامه الکترونیک | حق خواندن | مجوز BAC، مجوز EAC | |
| | | حق نوشتن | عامل شخصی‌سازی صادر کننده مجوز | |
| | EF.CVCA | حق خواندن | مجوز BAC، مجوز EAC | |
| | | حق نوشتن | عامل شخصی‌سازی صادر کننده مجوز | |
| | EF.COM | حق خواندن | مجوز BAC، مجوز EAC | |
| | | حق نوشتن | عامل شخصی‌سازی صادر کننده مجوز | |

نویسنده‌ی هدف امنیتی باید موجودیت فعال، موجودیت غیر فعال، عملیات، مشخصه‌های امنیتی، موجودیت‌های بیرونی را که به صراحت در این پروفایل حفاظتی توضیح داده نشده‌اند تعریف کند.

### ۴-۳- تهدیدات

گذرنامه الکترونیکی می‌تواند با در اختیار داشتن افراد بدون افزاره‌های کنترل شده فیزیکی مورد استفاده قرار گیرد، بنابراین امکان وقوع هر دو تهدید فیزیکی و منطقی در این فرایند وجود خواهد داشت. عامل تهدید یک موجودیت خارجی است که برای دسترسی غیر قانونی به دارایی‌های حفاظت شده توسط محصول با هر دو روش فیزیکی و منطقی بیرون از محصول تلاش می‌کند.

در این پروفایل حفاظتی تراشه‌ی مدار مجتمع (IC)، کارکردهای حفاظت فیزیکی را به منظور محافظت TOE مطابق با A.IC_Chip فراهم می‌آورد. بنابراین، خود تهدید فیزیکی تراشه‌ی مدار مجتمع (IC) با عامل تهدید سطح بالا مد نظر نیست.

بنابراین، عامل تهدید این محصول در سطح متوسطی از تخصص، منابع و انگیزه برخوردار است.

### ۴-۳-۱-تهدیدات محصول در فاز شخصی‌سازی

| تهدیدات | توضیحات |
|---|---|
| T.TSF_Data_Modification<br>تغییر و تبدیل داده امنیتی | عامل تهدید ممکن است با استفاده از واسط خارجی از طریق سامانه بازرسی، به داده‌های ذخیره شده‌ی توابع هدف امنیتی دسترسی پیدا کند. |

### ۴-۳-۲- تهدیدات مرتبط با کنترل دسترسی پایه (BAC) در فاز استفاده از محصول

| تهدیدات | توضیحات |
|---|---|
| T.Eavesdropping<br>استراق سمع | عامل تهدید ممکن است به منظور پیدا کردن اطلاعات شخصی دارنده‌گذرنامه الکترونیک، با استفاده از پایانه‌ی مستعد ارتباطات فرکانس رادیویی (RF) داده‌های انتقال یافته را استراق سمع کند. |
| T.Forgery_Corruption_ Personal_ Data<br>جعل و تخریب داده شخصی | عامل تهدید ممکن است برای خواندن داده کاربر به منظور جعل و تخریب داده شخصی دارنده‌گذرنامه الکترونیک که در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) ذخیره شده است، با استفاده از سامانه بازرسی غیر مجاز برای دسترسی تلاش کند. |

| | |
|---|---|
| T.BAC_Authentication_Key_Disclose<br>افشای کلید احراز هویت | به منظور پیدا کردن داده شخصی دارنده‌گذرنامه الکترونیک، عامل تهدید ممکن است حق خواندن کلید احـراز هویـت کنترل دسترسی پایه (BAC) جاسازی شده در محصول را به دست آورده و اطلاعات مربوطه را افشا کند.<br>**نکته کاربردی ۱:** کلید احراز هویت کنترل دسترسی پایه (BAC) ممکن است توسط عامل شخصی‌سازی در فاز شخصی‌سازی و یا توسط محصول در فاز استفاده عملیاتی تولید شود. با توجه به روش تولید کلید احراز هویت کنترل دسترسی پایه (BAC)، نویسنده هدف امنیتی باید تهدید افشای کلید احراز هویت کنترل دسترسی پایه (BAC) ذخیره شده در حافظه امن و موقت تراشه سند مسافرتی قابل خواندن توسط ماشین (MRTD) را در مورد قبلی در نظر بگیرد. در مورد بعدی، نویسنده هدف امنیتی باید تهدید افشای کلید احراز هویت کنترل دسترسی پایه (BAC) از اطلاعات باقی مانده در حافظه موقت را نیز مد نظر قرار دهد. (مراجعه شود به ‘تهدید اطلاعات باقیمانده(T.Residual_Info)’. |
| T.BAC_ReplayAttack<br>حمله بازپخش | عامل تهدید ممکن است احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) را بـا پاسـخ پـس از متوقـف شـدن داده انتقال یافته توسط محصول و سامانه بازرسی در فاز اولیه احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) دور بزند.<br>**نکته کاربردی ۲:** محصول عدد تصادفی از متن خام را مطابق با دستورالعمل 'get_Challenge'سامانه بازرسی در کنترل دسترسی پایه (BAC) به سامانه بازرسی تحویل می‌دهد. بنابراین عامل تهدید می‌تواند با متوقف کردن عدد تصادفی و مقادیر سامانه بازرسی و انتقال مجدد مقادیر پاسخ سامانه بازرسی به نشست بعدی احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) را دور بزند. همچنین عامل تهدید ممکن است داده انتقالی را به عنوان عامل تهدیدی تعریف کند که می‌تواند کلید نشست کنترل دسترسی پایه (BAC) را پس از کسب کلید احراز هویت کنترل دسترسی پایه (BAC) توسطافشای کلید احراز هویت(T.BAC_Authentication_Key_Disclose) تولید کند. |

### ۳-۳-۴- تهدید در فاز استفاده عملیاتی مربوط به کنترل دسترسی توسعه یافته (EAC)

| تهدیدات | توضیحات |
|---|---|
| T.Damage_to_Biometric_Data<br>آسیب به داده بیومتریک | عامل تهدید ممکن است، با استفاده از پایانه‌ی مستعد ارتباط فرکانس رادیویی (RF) غیرمجاز و غیره،داده زیست‌سنجی دارنده‌گذرنامه الکترونیک را افشا، جعل و یا تخریب کند.<br>**نکته کاربردی ۳:** تنها سامانه بازرسی کنترل دسترسی توسعه یافته‌ای (EIS) که به کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) نائل آمده است می‌تواند به حق خواندن داده زیست‌سنجی از دارنده‌گذرنامه الکترونیک دسترسی داشته باشد، بنابراین عامل تهدید ممکن است برای بدست آوردن داده زیست‌سنجی با استفاده از سامانه بازرسی غیر مجاز و سامانه بازرسی کنترل دسترسی پایه (BAC) و غیره تلاش کند. |
| T.EAC-CA_ByPass<br>دور زدن کنترل دسترسی توسعه یافته - احراز هویت تراشه | عامل تهدید ممکن است احراز هویت سامانه بازرسی را به گونه‌ای دور بزند که در طول کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) با استفاده از عامل تهدید کلید عمومی در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) تولید شده برود. |
| T.IS_Certificate_Forgery<br>جعل گواهی سامانه بازرسی | عامل تهدید ممکن است، به منظور به دست آوردن حق دسترسی به داده زیست‌سنجی دارنده‌گذرنامه الکترونیک، تلاش کند تا با جعل گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، گواهی تأیید کننده سند (DV) و گواهی سامانه بازرسی (IS) و درخواست درستی‌سنجی گواهی‌ها برای محصول کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) را دور بزند. |

### ۴-۳-۴- تهدیدات مرتبط با کنترل دسترسی پایه (BAC) و کنترل دسترسی توسعه یافته (EAC) در فاز استفاده عملیاتی

| تهدیدات | توضیحات |
| --- | --- |
| T.SessionData_Reuse<br>استفاده مجدد از داده نشست | عامل تهدید ممکن است کلید نشست را از تعدادی از متون ارتباطی رمزنگاری جمع‌آوری شده با استفاده از پایانه‌ی مستعد در محدوده‌ی گسترده‌ای از ارتباطات فرکانس رادیویی (RF) به منظور کشف داده انتقال یافته از طریق پیام‌رسانی امن استنتاج کند.<br>**نکته کاربردی ۴:** هنگامی که محصول و سامانه بازرسی از کلید احراز هویت کنترل دسترسی پایه (BAC) به عنوان کلید نشست کنترل دسترسی پایه (BAC) استفاده می‌کند، ممکن است در معرض حمله متن رمزی قرار گیرند که تنها به عنوان همان کلید نشستی مبادرت به حمله می‌کند که در هر کنترل دسترسی پایه (BAC) مورد استفاده قرار گرفته است. زمانی که کلید نشست کنترل دسترسی پایه (BAC) با همان عدد تصادفی مورد استفاده احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) تولید شود، اطلاعات مهم ضروری در استخراج کلید نشست ممکن است به مهاجم به عنوان اولین عدد تصادفی محصول به عنوان یک متن رمز ارائه شود. در صورتی که سامانه بازرسی کنترل دسترسی توسعه یافته (EIS)، کلید عمومی موقت را به در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) انتقال می‌دهد و عدد تصادفی را در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) به همان شیوه به نشست‌های دیگر انتقال می‌دهد و محصول استفاده از آن‌ها را ادامه می‌دهد، ممکن است در معرض حمله متن رمزی قرار گیرد که تنها حمله می‌کند. |

| | |
|---|---|
| T.Skimming<br>دستکاری | عامل تهدید ممکن است، اطلاعات ذخیره شده در تراشه‌ی مدار مجتمع (IC) را با ارتباط برقرار کردن با تراشه‌ی سند مسافرت قابل خواندن توسط ماشین (MRTD) از طریق پایانه‌ی ارتباطی غیر مجاز فرکانس رادیویی (RF) بخواند بدون اینکه دارنده‌گذرنامه الکترونیک متوجه شود. |

### ۴-۳-۵- تهدیدات مرتبط با پشتیبانی تراشه‌ی مدار مجتمع (IC)

| تهدیدات | توضیحات |
|---|---|
| T.Malfunction<br>اختلال در عملکرد | عامل تهدید ممکن است موجب بد عمل کردن محصول در فشار محیطی خارج از شرایط عملیاتی عادی بصورت غیر عادی شود تا توابع امنیتی را دور زده و یا به توابع هدف امنیتی (TSF) و داده‌امنیتی (TSF) ذخیره شده در محصول آسیب برساند. |

### ۴-۳-۶- سایر تهدیدات در فاز استفاده عملیاتی

| تهدیدات | توضیحات |
|---|---|
| T.Leakage_CryptographicKey_Info<br>نشت اطلاعات کلید رمزنگاری | عامل تهدید ممکن است با استفاده از توان برق و افزاره‌های تحلیل موج، اطلاعات کلیدی استفاده شده در روش‌های رمزنگاری به کار رفته در ساز و کارهای امنیتی گذرنامه الکترونیکی را با تحلیل اطلاعات توان برق و امواج منتشر شده در جریان عملیات محصول بدست آورد. |
| T.ePassport_Reproduction<br>تکثیر گذرنامه الکترونیک | عامل تهدید ممکن است، با تولید مجدد داده برنامه‌ی کاربردی سند مسافرت قابل خواندن توسط ماشین (MRTD) که در محصول ذخیره شده است و جعل اطلاعات هویتی صفحه‌ی گذرنامه الکترونیک خود را به عنوان دارنده گذرنامه الکترونیک مبدل سازد. |

| | |
|---|---|
| T.Residual_Info<br>اطلاعات باقیمانده | عامل تهدید ممکن است با بازیابی اطلاعات باقیمانده، اطلاعات مهم را افشا کند در حالی‌که داده‌امنیتی (TSF) از قبیل کلید احراز هویت کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی توسعه یافته (EAC)، گواهی تأیید کننده سند (DV) و گواهی سامانه بازرسی (IS) و غیره ثبت شده و در حافظه‌ی موقت استفاده شده است. |

### ۴-۴- خط‌مشی‌های امنیت سازمانی

محصول باید خط‌مشی‌های امنیت سازمانی[۲۴] (OSP) زیر را به عنوان قوانین امنیتی، روش‌های اجرایی، اقدامات و راهنمایی‌های که توسط سازمان بر عملیاتش تحمیل شده است را برآورده کند.

| خط‌مشی‌های امنیتی سازمان | توضیحات |
|---|---|
| P.International_Compatibility<br>سازگاری بین المللی | عامل شخصی‌سازی باید از سازگاری بین ساز و کارهای امنیتی صدور گذرنامه الکترونیک و ساز و کارهای امنیتی سامانه بازرسی هنگام مهاجرت اطمینان حاصل کند.<br>**نکته کاربردی ۵:** سازگاری بین‌المللی باید با توجه به سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) و مشخصات کنترل دسترسی توسعه‌یافته (EAC) تضمین شود. |

[۲۴] Organisational Security Policies

| | |
|---|---|
| **P.Security_Mechanism_**Application_**Procedures**<br>روش‌های کاربرد مکانیسم امنیتی | محصول باید از روش‌های کاربرد سازوکار امنیتی با توجه به نوع سامانه بازرسی به گونه‌ای اطمینان یابد که خط‌مشی‌های کنترل دسترسی عامل شخصی‌سازی به گذرنامه الکترونیک را نقض نکند.<br>**نکته کاربردی ۶:** جریان عملیات محصول با توجه به نوع سازوکارهای امنیتی پشتیبانی شده توسط سامانه بازرسی متفاوت است. جریان عملیات اصلی وابسته به روش اجرایی استاندارد بازرسی گذرنامه الکترونیک بخش ۲-۱-۱- و روش اجرایی پیشرفته‌ی گذرنامه الکترونیک بخش ۲-۱-۲ مشخصات کنترل دسترسی توسعه‌یافته (EAC) است. |
| P.Application_Program_Install<br>نصب برنامه کاربردی | عامل شخصی‌سازی بعد از اینکه بررسی کرد برنامه‌ی کاربردی(App) بارگذاری شده در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) بر محصول امن اثر نگذاشته است، باید نصب برنامه‌ی کاربردی (App) را تأیید کند.<br>**نکته کاربردی ۷:** نصب برنامه کاربردی (App) می‌تواند توسط سازمان دارنده همان مجوز به عنوان عامل شخصی‌سازی انجام شود. |
| P.Personalization_Agent<br>عامل شخصی‌سازی | عامل شخصی‌سازی باید گذرنامه الکترونیک را به روش امنی صادر کند، تا تصدیق نماید که موجودیت فعال در حال صدور تغییر نیافته است و باید بعد از بررسی این موضوع که داده درون تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) پس از صدور به شکل نرمالی کار می‌کند محصول را به فاز استفاده عملیاتی تحویل دهد. عامل شخصی‌سازی باید تابع نوشتن روی تراشه را قبل از تحویل محصول به فاز استفاده عملیاتی غیرفعال کند. |

| | |
|---|---|
| P.ePassport_Access_Control<br>کنترل دسترسی به گذرنامه الکترونیک | عامل شخصی‌سازی و محصول، باید خط‌مشی‌های کنترل دسترسی به گذرنامه الکترونیک را بـه منظـور حفاظـت از داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) ایجاد کند. همچنین، محصول باید نقش کاربران را تعریف و تنظیم نماید.<br>**نکته کاربردی ۸:** محصول باید خط‌مشی‌های کنترل دسترسی را با توجه به سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) و مشخصات کنترل دسترسی توسعه‌یافته (EAC) ایجاد کند. |
| P.PKI<br>زیرساخت کلید عمومی | حالت صادر کننده گذرنامه الکترونیک باید روش صدور گواهی را برای تولید و مدیریت کلیـد امضـای دیجیتـال و بـرای تولید، صدور، به کار گرفتن، تخریب گواهی‌ها به صورت امن با توجه به CPS با پیاده‌سـازی PA-PKI و EAC-PKI مطـابق بـا سامانه زیرساخت کلید عمومی (PKI) گذرنامه الکترونیک، اجرا کند.<br>همچنین حالت صادر کننده گذرنامه الکترونیک باید با توجه به خط‌مشـی‌هایی بـرای مـدیریت تـاریخ معتبـر گواهی‌هـا، گواهی‌ها را به روز رسانی کند، سپس به صورت امنی آن‌ها را برای بررسی حالت و سامانه بازرسی تحویل دهـد. هنگـامی که کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA)، گواهی‌هـای پیونـد CVCA، تأییـد کننـده سـند (DV) و سامانه بازرسی (IS) را برای محصول فراهم می‌کند، بعد از آن کـه سـامانه بازرسـی، اطلاعـات EF.CVCA ذخیـره شـده در محصول را به دست آورد، محصول باید به صورت داخلی گواهی‌ها را با بررسی اعتبار گواهی به روز رسانی کند. |
| P.Range_RF_Communication<br>محدوده ارتباط فرکانس رادیویی | فاصله ارتباط فرکانس رادیویی (RF) بین تراشه‌ی سند مسافرتی قابل خواندن توسط ماشـین (MRTD) و سـامانه بازرسـی باید کمتر از ۵ سانتیمتر باشد و اگر صفحه گذرنامه الکترونیک پیوست شده با تراشه‌ی مدار مجتمع (IC) باز نباشد، کانال ارتباط فرکانس رادیویی (RF) نباید برقرار شود. |

**جدول ۷- خط‌مشی کنترل دسترسی گذرنامه الکترونیک**

| لیست موجودیت فعال | لیست اهداف | | اهداف | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | مشخصه‌ی امنیتی / مشخصه‌ی امنیتی | | داده شخصی دارنده گذرنامه الکترونیک | | داده زیست‌سنجی دارنده گذرنامه الکترونیک | | داده احراز هویت گذرنامه الکترونیک | | EF.CVCA | | EF.COM | |
| | | | حق خواندن | حق نوشتن | حق خواندن | حق نوشتن | حق خواندن | حق نوشتن | حق خواندن | حق نوشتن | حق خواندن | حق نوشتن |
| موجودیت فعال | سامانه بازرسی BAC | احراز هویت BAC | بلی | خیر | خیر | خیر | بلی | خیر | بلی | خیر | بلی | خیر |
| | سامانه بازرسی EAC | احراز هویت BAC | بلی | خیر | خیر | خیر | بلی | خیر | بلی | خیر | بلی | خیر |
| | | احراز هویت EAC | بلی | خیر | بلی | خیر | بلی | خیر | بلی | خیر | بلی | خیر |
| | عامل شخصی سازی | احراز هویت شخصی‌سازی | بلی | بلی | بلی | بلی | بلی | بلی | بلی | بلی | بلی | بلی |

### ۴-۵- مفروضات

مفروضات جنبه‌های امنیت محیطی که در آن محصول مورد استفاده قرار خواهد گرفت یا برای استفاده در نظر گرفته شده است را توضیح می‌دهد تا دامنه‌ی ملاحظات امنیتی را محدود کند.

| مفروضات | توضیحات |
| --- | --- |
| A.Certificate_Verification<br>تایید گواهی | سامانه بازرسی مانند سامانه بازرسی کنترل دسترسی پایه (BAC) و سامانه بازرسی کنترل دسترسی توسعه یافته (EIS)، بعد از بررسی اعتبار زنجیره‌ی گواهی برای احراز هویت غیر فعال (PA)، سند موجودیت غیر فعال امنیتی (SOD) را بررسی می‌کند (گواهی مرجع صلاحیت دار امضا کننده گواهی کشور (CSCA)←گواهی امضاء کننده سند (DS)). این کار به منظور بررسی جعل و تخریب داده هویتی گذرنامه الکترونیک ثبت شده در محصول انجام می‌شود. برای این، گواهی امضاء کننده سند (DS) و CRL باید به صورت دوره‌ای بررسی شوند.<br>سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) باید کلید تولید امضای دیجیتال را که با گواهی سامانه بازرسی (IS) مطابقت دارد به صورت امنی حفظ کند و باید برای محصول گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، گواهی تأیید کننده سند (DV) و گواهی سامانه بازرسی (IS) در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) را فراهم آورد.<br>**نکته کاربردی ۹:** روش‌های سامانه بازرسی به منظور بررسی زنجیره‌ی گواهی برای احراز هویت غیرفعال (PA)، و جهت توزیع گواهی سامانه بازرسی (IS) و کلید تولید امضای دیجیتال ممکن است به خط‌مشی صدور گذرنامه الکترونیک وابسته باشد. بنابراین، نویسنده‌ی هدف امنیتی می‌تواند محیط امنیتی را با توجه به خط‌مشی صدور گذرنامه الکترونیک تعریف کند. |

| | |
|---|---|
| **A.Inspection_System**<br>**سامانه بازرسی** | سامانه بازرسی باید سازوکارهای امنیتی برای احراز هویت غیر فعال (PA)، کنترل دسترسی پایه (BAC) و کنترل دسترسی توسعه یافته (EAC)، مطابق سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) و مشخصات کنترل دسترسی توسعه یافته (EAC) بر اساس خط‌مشی تأیید گذرنامه الکترونیک برای دارنده گذرنامه الکترونیک پیاده‌سازی کند.<br>همچنین، بعد از پایان نشست، سامانه بازرسی کنترل دسترسی پایه (BAC) و سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) باید به صورت امنی تمامی اطلاعات مورد استفاده در ارتباطات و محصول (مانند کلید نشست کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی توسعه یافته (EAC)، اطلاعات نشست و غیره) را تخریب کنند.<br>**نکته کاربردی ۱۰:** محصول درخواست دسترسی به EF.SOD را توسط سامانه بازرسی که احراز هویت دو طرفه کنترل دسترسی پایه (BAC) را رد کرده است، انکار می‌کند.<br>همانطور که سامانه بازرسی کنترل دسترسی پایه (BAC)، از ساز و کارهای امنیتی کنترل دسترسی پایه (BAC) و احراز هویت غیر فعال (PA) پشتیبانی می‌کند، در صورتی که احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) با استفاده از کلید احراز هویت کنترل دسترسی پایه (BAC) با موفقیت همراه باشد، حق خواندن داده شخصی و احراز هویت دارنده گذرنامه الکترونیک را به دست می‌آورد. سپس، با برقراری پیام‌رسان امن کنترل دسترسی پایه (BAC) با کلید نشست کنترل دسترسی پایه (BAC)، از محرمانگی و یکپارچگی تمامی داده‌های انتقال یافته اطمینان حاصل می‌کند. سامانه بازرسی کنترل دسترسی پایه (BAC) با اجرای احراز هویت غیر فعال (PA) پس از کنترل دسترسی پایه (BAC)، SOD را تأیید می‌کند. پس از آن، با محاسبه و مقایسه مقدار چکیده پیام داده شخصی و احراز هویت دارنده‌گذرنامه الکترونیک، جعل و تخریب داده شخصی و احراز هویت دارنده‌گذرنامه الکترونیک را بررسی می‌کند.<br>هنگامی که سامانه بازرسی کنترل دسترسی توسعه یافته (EIS)، از ساز و کارهای امنیتی کنترل دسترسی پایه (BAC) و احراز هویت غیر فعال (PA) پشتیبانی می‌کند، حق خواندن داده شخصی، احراز هویت و داده زیست‌سنجی دارنده گذرنامه الکترونیک را به دست می‌آورد. زمانی که احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) و پیام‌رسانی امن با موفقیت انجام گرفت، سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) با استفاده از خواندن کلید عمومی احراز هویت تراشه‌ی کنترل دسترسی توسعه یافته (EAC) درون کنترل دسترسی پایه (BAC)، کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) را اجرا می‌کند تا محصول اصل را تأیید کند. سپس به منظور بررسی کلید عمومی احراز |

| | |
|---|---|
| A.IC_Chip<br>تراشه‌ی مدار مجتمع | تراشه‌ی مدار مجتمع (IC) که بستره‌ی زیرین محصول است، تولید اعداد تصادفی و عملیات رمزنگاری را برای پشتیبانی از توابع هدف امنیتی ارائه می‌دهد. همچنین بد عمل کردن‌های محصول خارج از شرایط عملیاتی عادی را تشخیص داده و توابع حفاظت فیزیکی برای محافظت از محصول از حملات فیزیکی با استفاده از اکتشاف و تحلیل مهندسی معکوس را ارائه می‌دهد.<br>**نکته کاربردی ۱۱:** برای اطمینان از محیط امن محصول، تراشه‌ی مدار مجتمع (IC) باید یک محصول گواهی شده از CCRA EAL4+(SOF - high) یا سطح بالاتری از آن باشد. عملیات رمزنگاری پشتیبانی شده توسط تراشه‌ی مدار مجتمع (IC) ممکن است در کمک پردازنده‌ی تراشه‌ی مدار مجتمع (IC) و یا کتابخانه‌های رمزنگاری بارگذاری شده در تراشه‌ی مدار مجتمع (IC)، ارائه شده باشد. |
| A.MRZ_Entropy<br>آنتروپی ناحیه قابل خواندن توسط ماشین | برای اطمینان از کلید احراز هویت کنترل دسترسی پایه (BAC) امن، نقطه‌ی آغاز تصادفی (seed)کلید احراز هویت کنترل دسترسی پایه (BAC) از آنتروپی ناحیه قابل خواندن توسط ماشین (MRZ) استفاده می‌کند.<br>**نکته کاربردی ۱۲:** به منظور مقاومت در برابر عامل تهدید با سطح متوسط، آنتروپی برای شماره گذرنامه، تاریخ تولد، تاریخ انقضا یا تاریخ اعتبار تا تاریخ مشخص و رقم حواله‌ی استفاده شده به عنوان نقطه‌ی آغاز تصادفی (seed)کلید احراز هویت کنترل دسترسی پایه (BAC) در آنتروپی ناحیه قابل خواندن توسط ماشین (MRZ) در سطح تکنولوژی فعلی باید حداقل ۵۶ بیت باشد. نویسنده‌ی هدف امنیتی ممکن است با توجه به سطح عامل تهدید آنتروپی ناحیه قابل خواندن توسط ماشین (MRZ) را تغییر دهد. |

## ۵- اهداف امنیتی

### ۵-۱- کلیات

این پروفایل حفاظتی اهداف امنیتی را با دسته‌بندی آن‌ها برای محصول و محیط تعریف می‌کند. اهداف امنیتی برای محصول به طور مستقیم توسط محصول به کار گرفته می‌شود. اهداف امنیتی برای محیط توسط ابزارهای مرتبط با فرایند یا فنی پشتیبانی شده‌ی محیط فناوری اطلاعات به منظور فراهم آوردن دقیق قابلیت‌های کارکرد امنیتی محصول به کار گرفته می‌شوند.

### ۵-۲- اهداف امنیتی برای محصول

موارد زیر اهداف امنیتی هستند که به طور مستقیم توسط محصول بکار گرفته شده است.

| اهداف امنیتی | توضیحات |
|---|---|
| O.Management<br>مدیریت | محصول باید ابزاری برای مدیریت داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) در مرحله شخصی‌سازی، برای عامل شخصی‌سازی مجاز فراهم آورد.<br>**نکته کاربردی ۱۳:** در مرحله شخصی‌سازی، عامل شخصی‌سازی باید تابع نوشتن را پس از ثبت داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) غیرفعال کند. |

| | |
|---|---|
| O.Security_Mechanism_Application_Procedures<br>روش‌های کاربرد مکانیسم امنیتی | محصول باید با توجه به روش‌های اجرایی بازرسی گذرنامه الکترونیک در مشخصاتی EAC، از جریان دستورات اطمینان حاصل کند.<br>**نکته کاربردی ۱۴:** محصول باید اطمینان حاصل کند که ترتیب کاربرد سازوکارهای امنیتی احراز هویت غیر فعال (PA)، کنترل دسترسی پایه (BAC) و کنترل دسترسی توسعه یافته (EAC) مطابق با روش اجرایی بازرسی گذرنامه الکترونیک استاندارد ۲,۱,۱ و روش اجرایی گذرنامه الکترونیک پیشرفته ۲,۱,۲ از مشخصات کنترل دسترسی توسعه‌یافته (EAC) است و نباید به درخواست‌هایی از سامانه بازرسی که مطابق با ترتیب کاربرد ساز و کارهای امنیتی نیست اجازه دهد. در صورت پیاده‌سازی متفاوت با روش‌های اجرایی مشخصات کنترل دسترسی توسعه‌یافته (EAC)، نویسنده‌ی هدف امنیتی باید از پایایی و امن بودن که منطبق با مشخصات کنترل دسترسی توسعه‌یافته (EAC) است، اطمینان حاصل کند. |
| **O.Session_Termination**<br>خاتمه نشست | محصول باید در صورت شکست احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC)، شکست در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) و یا شناسایی تغییر در داده امنیتی (TSF) انتقال یافته، نشست را خاتمه دهد. |
| **O.Secure_Messaging**<br>پیام‌رسانی امن | محصول باید برای محافظت از داده‌امنیتی (TSF) و داده انتقال یافته کاربر از محرمانگی و یکپارچگی داده‌ها اطمینان حاصل کند |
| **O.Certificate_Verification**<br>تایید گواهی | محصول باید به طور خودکار، گواهی و تاریخ فعلی را با بررسی تاریخ اعتبار بر اساس گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA) ارائه شده توسط سامانه بازرسی، به روز رسانی کند. |
| **O.Secure_State**<br>حالت امن | محصول باید از حالت امن در تلاش برای تغییر در توابع هدف امنیتی (TSF) و داده راه‌اندازی محافظت کند. |
| **O.Deleting_Residual_Info**<br>حذف اطلاعات باقی‌مانده | در هنگام تخصیص منابع، محصول باید ابزارهایی ارائه دهد تا اطمینان یابد اطلاعات مرتبط با امنیت قبلی (مثلاً کلید نشست کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی توسعه یافته (EAC) و غیره) را شامل نمی‌شود. |

| | |
|---|---|
| **O.Replay_Prevention**<br>پیشگیری از بازپخش | محصول باید از تولید و استفاده از اعداد تصادفی مختلف در هر نشست برای اطلاعات مرتبط با رمزنگاری امن مورد استفاده در سازوکارهای امنیتی اطمینان یابد.<br>**نکته کاربردی ۱۵:** محصول باید داده انتقال یافته به سامانه بازرسی را در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) را تولید کرده و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) در هر نشست متفاوت بوده و نباید از کلید احراز هویت کنترل دسترسی پایه (BAC) به عنوان کلید نشست کنترل دسترسی پایه (BAC) استفاده کند. همچنین، محصول نباید اطلاعات مهم ضروری در استخراج کلید نشست را با تولید کلید نشست کنترل دسترسی پایه (BAC) با همان اعداد تصادفی استفاده شده در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) ارائه دهد. |
| **O.Access_Control**<br>کنترل دسترسی | محصول باید توابع کنترل دسترسی را به گونه‌ای ارائه دهد که اجازه‌ی دسترسی به داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD)، تنها با اعطای حقوق دسترسی به موجودیت‌های خارجی مطابق با خط‌مشی‌های کنترل دسترسی گذرنامه الکترونیک عامل شخصی‌سازی داده شود.<br>**نکته کاربردی ۱۶:** تنها عامل شخصی‌سازی مجاز در مرحله شخصی‌سازی می‌تواند داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) را ثبت کند. همچنین، خط‌مشی‌های کنترل دسترسی برای حق خواندن با توجه به نوع سامانه بازرسی در مرحله‌استفاده عملیاتی ایجاد می‌شود. |

| | |
|---|---|
| O.Handling_Info_Leakage<br>ساماندهی نشت اطلاعات | محصول باید اقدامات احتیاطی را به منظور جلوگیری از بهره‌برداری از اطلاعات نشتی در طول عملیات رمزنگاری برای توابع هدف امنیتی (TSF) پیاده‌سازی کند.<br>**نکته کاربردی ۱۷:** در صورتی که کمک پردازنده تراشه‌ی مدار مجتمع (IC) یا کتابخانه‌ی رمزنگاری بارگذاری شده در تراشه‌ی مدار مجتمع (IC)، اقدامات احتیاطی را برای برآوردن این اهداف امنیتی ارائه دهد، نویسنده‌ی هدف امنیتی باید آن را به عنوان اهداف امنیتی برای محیط مشخص کند. |
| **O.BAC**<br>کنترل دسترسی پایه | محصول احراز هویت دو طرفه کنترل دسترسی پایه (BAC) سامانه بازرسی را با پیاده‌سازی سازوکار امنیتی کنترل دسترسی پایه (BAC) محصول اجرا می‌کند تا حق خواندن داده شخصی دارنده گذرنامه الکترونیک را تنها برای سامانه بازرسی مجاز ارائه دهد. همچنین، محصول کلید نشست کنترل دسترسی پایه (BAC) مورد استفاده برای پیام‌رسانی امن کنترل دسترسی پایه (BAC) را تولید می‌کند. |
| **O.EAC**<br>کنترل دسترسی توسعه‌یافته | محصول با پیاده‌سازی سازوکارهای امنیتی کنترل دسترسی توسعه یافته (EAC)، (درون کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) و درون کنترل دسترسی توسعه یافته - احراز هویت پایانه (EAC-TA)) سامانه بازرسی را احراز هویت کرده تا حق خواندن داده زیست‌سنجی دارنده گذرنامه الکترونیک را تنها برای سامانه بازرسی مجاز ارائه دهد. همچنین محصول کلید نشست کنترل دسترسی توسعه یافته (EAC) مورد استفاده برای پیام رسانی امن کنترل دسترسی توسعه یافته (EAC) را تولید می‌کند. |

### ۵-۳- اهداف امنیتی محیط عملیاتی

اهداف امنیتی زیر توسط ابزارهای مرتبط با روش اجرایی یا فنی پشتیبانی شده‌ی محیط فناوری اطلاعات به منظور فراهم آوردن دقیق قابلیت‌های کارکرد امنیتی محصول به کار گرفته می‌شوند.

| هدف امنیتی محیط عملیاتی | توضیحات |
|---|---|
| OE.ePassport_Manufacturing_Security<br>امنیت تولید گذرنامه | اقدامات امنیتی فیزیکی (چاپ امن و غیره) برای گذرنامه الکترونیک باید به منظور شناسایی تولید مجدد تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و تلاش حمله استاد بزرگ شطرنج، جایگزینی تصویر چهره و اصلاح داده ناحیه قابل خواندن توسط ماشین (MRZ) و غیره آماده شود. |
| OE.Procedures_of_ePassport_holder_Check<br>رویه بررسی دارنده گذرنامه | مأمور مهاجرت روش‌های اجرایی را برای بررسی هویت دارنده گذرنامه الکترونیک بر اساس صفحه اطلاعات هویتی چاپ شده‌ی گذرنامه الکترونیک آماده کند. |
| OE.Application_Program_Install<br>نصب برنامه کاربردی | عامل شخصی‌سازی باید بعد از بررسی عدم تأثیر برنامه‌های کاربردی (App) بارگذاری شده در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) بر امنیت محصول،بارگذاری برنامه کاربردی (App) را تأیید کند. |

| | |
|---|---|
| **OE.Certificate_Verification**<br>تأیید گواهی | سامانه بازرسی مانند سامانه بازرسی کنترل دسترسی پایه (BAC) و سامانه بازرسی کنترل دسترسی توسعه یافته (EIS)، پس از بررسی اعتبار زنجیره‌ی گواهی احراز هویت غیر فعال (PA) (گواهی مرجع صلاحیت دار امضا کننده گواهی کشور (CSCA)←گواهی امضاء کننده سند (DS))، سند موجودیت غیر فعال امنیتی (SOD) را بررسی می‌کند تا جعل و تخریب داده هویتی گذرنامه الکترونیک ثبت شده در محصول را بررسی کند. برای این،گواهی امضاء کننده سند (DS) و CRL باید به صورت دوره‌ای بررسی شوند.<br>سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) باید کلید تولید امضای دیجیتال را که منطبق بر گواهی سامانه بازرسی (IS) است، به صورت امنی حفظ کرده و برای محصول گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، گواهی تأیید کننده سند (DV) و گواهی سامانه بازرسی (IS) را درون کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) فراهم آورد. |
| OE.Personalization_Agent<br>عامل شخصی‌سازی | عامل شخصی‌سازی باید گذرنامه الکترونیک را به شیوه امنی صادر کند به گونه‌ای که تصدیق نماید، موجودیت فعال در حال صدور تغییر نکرده است و باید بعد از تأیید عملکرد عادی و سازگار گذرنامه الکترونیک محصول را به مرحله‌استفاده عملیاتی تحویل دهد. عامل شخصی‌سازی باید تابع نوشتن را قبل از تحویل محصول به مرحله استفاده عملیاتی غیر فعال کند. |
| OE.Inspection_System<br>سیستم بازرسی | سامانه بازرسی باید ساز و کارهای امنیتی را با توجه به نوع سامانه بازرسی پیاده‌سازی کند به گونه‌ای که خط‌مشی‌های کنترل دسترسی گذرنامه الکترونیک عامل شخصی‌سازی را نقض نکند و از ترتیب کاربرد اطمینان یابد. همچنین، سامانه بازرسی باید پس از اتمام نشست تمامی اطلاعات استفاده شده در ارتباط با محصول را به صورت امنی تخریب کند. |
| **OE.IC_Chip**<br>**تراشه‌ی مدار مجتمع** | تراشه‌ی مدار مجتمع (IC)، که بستره زیرین محصول است، تولید اعداد تصادفی و عملیات رمزنگاری را جهت پشتیبانی از توابع هدف امنیتی ارائه می‌دهد. همچنین بد عمل کردن‌های محصول خارج از شرایط عملیاتی عادی را تشخیص داده و توابع حفاظت فیزیکی برای محافظت از محصول از حملات فیزیکی با استفاده از اکتشاف و تحلیل مهندسی معکوس ارائه می‌دهد. |

| | |
|---|---|
| **OE.MRZ_Entropy**<br>**آنتروپی ناحیه قابل خواندن توسط ماشین** | عامل شخصی‌سازی باید از آنتروپی ناحیه قابل خواندن توسط ماشین (MRZ) اطمینان حاصل کند تا از کلید احراز هویت کنترل دسترسی پایه (BAC) امن اطمینان حاصل کند. |
| **OE.PKI**<br>**زیرساخت کلید عمومی** | حالت صادر کننده‌ی گذرنامه الکترونیک باید روش صدور گواهی را برای تولید و مدیریت کلید امضای دیجیتال، و برای تولید، صدور، به کار گرفتن، تخریب گواهی‌ها به صورت امن با توجه به CPS با پیاده‌سازی PA-PKI و EAC-PKI مطابق با سامانه زیرساخت کلید عمومی (PKI) گذرنامه الکترونیک، اجرا کند.<br>همچنین، حالت صادر کننده گذرنامه الکترونیک باید با توجه به خط‌مشی‌هایی برای مدیریت تاریخ معتبر گواهی‌ها، گواهی‌ها را به روز رسانی کند، سپس به صورت امنی آن‌ها را برای بررسی حالت و سامانه بازرسی تحویل دهد. |
| **OE.Range_RF_Communication**<br>**محدوده ارتباط فرکانس رادیویی** | فاصله ارتباط فرکانس رادیویی (RF) بین تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و سامانه بازرسی باید کمتر از ۵ سانتیمتر باشد و اگر صفحه گذرنامه الکترونیک پیوست شده با تراشه‌ی مدار مجتمع (IC) باز نباشد، کانال ارتباط فرکانس رادیویی (RF) نباید برقرار شود. |

## ۵-۴- منطق اهداف امنیتی

منطق اهداف امنیتی نشان می‌دهد که اهداف امنیتی مشخص شده برای ردیابی مسائل امنیتی کافی و مناسب هستند و بیشتر ضروری هستند تا بیش از حد.

منطق اهداف امنیتی موارد زیر را نشان می‌دهد:

هر مفروضات، تهدید یا خط‌مشی امنیتی سازمان حداقل یک هدف امنیتی برای ردیابی دارد.

هر هدف امنیتی حداقل یک مفروض، تهدید یا خط‌مشی امنیتی سازمانی را ردیابی می‌کند.

جدول ۸۸، نگاشت بین تعریف مسئله‌ی امنیتی و اهداف امنیتی را نشان می‌دهد

**جدول ۸- نگاشت بین تعریف مشکل امنیتی و اهداف امنیتی**

| اهداف امنیتی / تعریف مسئله‌ی امنیتی | اهداف امنیتی محصول | | | | | | | | | | | | اهداف امنیتی برای محیط | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | O.Management | O.Session_Termination<br>O.Security_Mechanism_Application_Procedures | O.Secure_Messaging | O.Certificate_Verification | O.Secure_State | O.DDeleting_Residua_Info | O.Replay_Prevention | O.Access_Control | O.Handling_Info_Leakage | O.BAC | O.EAC | OE.ePassport_Manufacturing_Security | OE.Procedures_of_ePassport_Holder_Check | OE.Application_Program_Install | OE.Certification_Verification | OE.Personalization_Agent | OE.Inspection_System | OE.IC_Chip | OE.MRZ_Entropy | OE.PKI | OE.Range_RF_Communication |
| T.TSF_DATA_MODIFICATION | × | | × | | | | | × | | | | | | | | × | | | | | | |
| T.Eavesdropping | | | | × | | | | | | | | | | | | | × | | | | | |
| T.Forgery_Corruption_Personal Data | | | × | | | | | × | | × | | | | | | | × | | | | | |
| T.BAC_Authentication_Key_Disclose | × | | × | | | | × | × | | | | | × | | | | | | | | | |
| T.BAC_ReplayAttack | | | | | | | × | | | | | | | | | | | | | | | |
| T.Damage_to_Biometric_Data | | | × | × | × | | | × | | | × | | | | × | | × | | × | | | |
| T.EAC-CA_Bypass | | × | | | | | | | | | | | × | | × | | × | | | | | |
| T.IS_Certificate_Forgery | × | | | | × | | | | | | | | | | × | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T.SessionData_Reuse | | | | | | | | × | | | | | | | | | × | | | | |
| T.Skimming | | | | | | | | | × | | × | × | | | | | | × | | | | × |
| T.Malfuction | | | | | | × | | | | | | | | | | | | | × | | | |
| T.T.Leakage_Cryptographickey_Info | | | | | | | | | | × | | | | | | | | | | | | |
| T.ePassport_Reproduction | | | | | | | | | | | | | × | × | | | | | | | | |
| T.Residual_Info | | | | | | | × | | | | | | | | | | | | | | | |
| P.International_Compatibility | | | | | | | | | | | | | | | | | | × | | | | |
| P.Security_Mechanism_Application_Procedures | | × | | | | | | | | | | | | | | | | | × | | | |
| P.Application_Program_Install | | | | | | | | | | | | | | | | × | | | | | | |
| P.Personalization_Agent | × | | | | | | | | | | | | | | | | | × | | | | |
| P.ePassport_Access_Control | × | | | | | | | | | × | | × | × | | | | | × | × | | | |
| P.PKI | | | | | × | | | | | | | | | | | | | | | | × | |
| P.Range_RF_Communication | | | | | | | | | | | | | | | | | | | | | | × |
| A.Certificate_Verification | | | | | | | | | | | | | | | | × | × | | | | × | |
| A.Inspection System | | | | | | | | | | | | | | | | | | × | | | | |
| A.Ic_Chip | | | | | | | | | | | | | | | | | | | × | | | |
| A.MRZ_Entropy | | | | | | | | | | | | | | | | | | | | × | | |

### ۵-۴-۱-منطق اهداف امنیتی برای محصول

| هدف امنیتی | توضیحات |
| --- | --- |
| **O.Management**<br>**مدیریت** | این هدف امنیتی اطمینان حاصل می‌کنند که محصول ابزارهایی برای نوشتن داده کاربر در دامنه‌ی فایل ابتدایی (EF) و ابزارهایی برای نوشتن داده‌امنیتی (TSF) در حافظه امن را تنها برای عامل شخصی‌سازی در مرحله شخصی‌سازی فراهم اورده و از دسترسی غیر مجاز با استفاده از واسطهای خارجی از طریق غیر فعال کردن تابع نوشتن داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) در مرحله‌استفاده عملیاتی جلوگیری می‌کند. بنابراین، این هدف امنیتی برای مقابله با تهدیدات تغییر و تبدیل داده امنیتی (T.TSF_Data_Modification) وافشای کلید احراز هویت (T.BAC_Authentication_Key_Disclose) و برای به اجرا در آوردن خط‌مشی‌های امنیت سازمانی کنترل دسترسی به گذرنامه الکترونیک (P.ePassport_Access_Control) و عامل شخصی‌سازی (P.Personalization_Agent) مورد نیاز است.<br>همچنین، این اهداف امنیتی ابزارهایی جهت ثبت گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) در حافظه امن در فاز شخصی‌سازی برای عامل شخصی‌سازی ارائه می‌دهند، بنابراین لازم است برای مقابله با تهدید جعل گواهی سامانه بازرسی (T.IS_Certificate_Forgery) مورد نیاز است. |

| | |
|---|---|
| O.Security_Mechanism_Application_Procedures<br>روش‌های کاربرد مکانیسم امنیتی | این هدف امنیتی برای به برای به اجرا در آوردن خط‌مشی امنیت سازمانی،روش‌های کاربرد مکانیسم امنیتی (P.Security_Mechanism_Application_Procedures)مورد نیاز است تا محصول اطمینان حاصل کند که ترتیب کاربرد ساز و کارهای احراز هویت غیر فعال (PA)، کنترل دسترسی پایه (BAC)، کنترل دسترسی پیشرفته (EAC)مطابق به روش اجرایی بازرسی گذرنامه الکترونیک استاندارد ۲،۱،۱ و روش اجرایی گذرنامه الکترونیک پیشرفته ۲،۱،۲ در مشخصات کنترل دسترسی توسعه‌یافته (EAC) است و به درخواست‌هایی از سامانه بازرسی که مطابق ترتیب کاربرد ساز و کار امنیتی نیستند اجازه دسترسی نمی‌دهد.<br>همچنین، این هدف امنیتی مستلزم مقابله با تهدید دور زدن T.EAC-C با حذف موارد نشان دهنده‌ی محصول اصل به سامانه بازرسی غیر مجاز است به طوری که اطمینان حاصل کند که ترتیب کاربرد ساز و کارهای امنیتی به گونه‌ای است که اجرای در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) را تنها به سامانه بازرسی‌ای می‌دهد که دارای حق دسترسی کلید عمومی احراز هویت تراشه‌ی کنترل دسترسی توسعه یافته (EAC) از طریق اجرای کنترل دسترسی پایه (BAC) است. |
| O.Session_Termination<br>خاتمه نشست | این هدف امنیتی اطمینان حاصل می‌کند که محصول از تلاش‌های احراز هویت مداوم احراز هویت به منظو جعل یا تخریب داده شخصی یا زیست‌سنجی دارنده‌گذرنامه الکترونیک جلوگیری کرده و در صورت شناسایی تغییر داده‌امنیتی (TSF) انتقال یافته به نشست خاتمه می‌دهد. بنابراین، این هدف امنیتی مستلزم مقابله با تهدیدات T.Forgery_Corruption_Personal_Data، T.Damage_to_Bometric_Data، افشای کلید احراز هویت (T.BAC_Authentication_Key_Disclose) و تغییر و تبدیل داده امنیتی (T.TSF_Data_Modification) است. |

| | |
|---|---|
| O.Secure_Messaging<br>پیام‌رسانی امن | این هدف امنیتی اطمینان حاصل می‌کند که محصول پیام‌رسانی امنی برای BAC یا EAC برقرار می‌کند تا انتقال داده شخصی و زیست‌سنجی دارنده‌گذرنامه الکترونیک به سامانه بازرسی به صورت امن صورت گیرد، و محرمانگی و یکپارچگی داده شخصی و زیست‌سنجی دارنده‌گذرنامه الکترونیک را فراهم می‌کند. بنابراین، این هدف امنیتی برای مقابله با تهدیدآسیب به داده بیومتریک (T.Damage_to_Biometric_Data) مورد نیاز است. |
| O.Certificate_Verification<br>تایید گواهی | این هدف امنیتی برای اجرای خط‌مشی‌های امنیت سازمانی P.PKI نیاز دارد تا به محصول اطمینان دهد که تاریخ اعتبار بر اساس گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) ارائه شده توسط سامانه بازرسی بررسی شده، بنابراین به صورت خودکار گواهی و تاریخ جاری به روز رسانی می‌شود.<br>این هدف امنیتی برای مقابله با تهدیداتآسیب به داده بیومتریک(T.Damage_to_Biometric_Data) و جعل گواهی سامانه بازرسی (T.IS_Certificate_Forgery) نیاز است تا هنگامی که محصول اعتبار گواهی پیوندمرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، گواهی تأیید کننده سند (DV) و گواهی سامانه بازرسی (IS) را در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA)بررسی می‌کند وضعیت جعل را تعیین کند. |
| O.Secure_State<br>حالت امن | این هدف امنیتی برای مقابله با تهدید اختلال در عملکرد (T.Malfunction) نیاز است، هنگامی که محصول تغییر در توابع هدف امنیتی (TSF) و داده را از طریق خود آزمایی تشخیص می‌دهد، و از خود محصول از طریق حفظ داده امن محافظت می‌کند به گونه‌ای که سوء عمل در توابع هدف امنیتی (TSF) اتفاق نیفتد. |

| | |
|---|---|
| O.Deleting_Residual_Info<br>حذف اطلاعات باقی‌مانده | این هدف امنیتی برای مقابله با تهدید اطلاعات باقیمانده (T.Residual_Info)که حذف کننده همه‌ی اطلاعات مرتبط با امنیت قبلی (کلید نشست کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی توسعه یافته(EAC) و غیره) می‌باشد، نیاز است، بنابراین در صورت تخصیص یا عدم تخصیص منابع حافظه توسط محصول شامل اطلاعات نمی‌شود و درنتیجه اطمینان می‌یابد که اطلاعات در دسترس نیستند.<br>این هدف امنیتی برای مقابله با تهدید افشای کلید احراز هویت (T.BAC_Authentication_Key_Disclose) با ارائه‌ی ابزاری برای اطمینان از این موضوع که اطلاعات باقیمانده در حافظه‌ی موقت در دسترس نیستند مورد نیاز است. |
| O.Replay_Prevention<br>پیشگیری از بازپخش | این هدف امنیتی برای مقابله با تهدید حمله بازپخش (T.BAC_ReplayAttack) نیاز است تا اطمینان حاصل کند که محصول مقادیر مختلفی را در هر نشست تولید می‌کند که به سامانه بازرسی در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) انتقال یافته است. همچنین،این هدف امنیتی برای مقابله با تهدید استفاده مجدد از داده نشست (T.SessionData_Reuse) مورد نیاز است تا اطمینان حاصل کند که اعداد تصادفی مختلفی تولید شده و در هر نشست از سازوکار امنیتی مورد استفاده قرار می‌گیرند تا محصول اطمینان حاصل کند که کلید احراز هویت کنترل دسترسی پایه (BAC) به عنوان کلید نشست کنترل دسترسی پایه (BAC) در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC ) مورد استفاده قرار نگرفته است و کلید نشست کنترل دسترسی پایه (BAC) با همان عدد تصادفی مورد استفاده در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) تولید نشده است و وضعیت جواب عدد تصادفی انتقال یافته توسط سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) در EAC را بررسی می‌کند. |

| | |
|---|---|
| O.Access_Control<br>کنترل دسترسی | این هدف امنیتی برای مقابله با تهدیدات T. Forgery_Corruption_Personal، آسیب به داده بیومتریک(T.Damage_to_Biometric_Data) و دستکاری(T.Skimming) مورد نیاز است و خط‌مشی‌های امنیت سازمانی کنترل دسترسی به گذرنامه الکترونیک (P.ePassport_Access_Control) را با پیاده‌سازی قوانین اجازه یا رد سامانه بازرسی برای خواندن داده کاربر مطابق با خط‌مشی‌های کنترل دسترسی گذرنامه الکترونیک توسط عامل شخصی‌سازی اعمال می‌کند.<br>این هدف امنیتی برای مقابله با تهدیدات تغییر و تبدیل داده امنیتی (T.TSF_Data_Modification) وافشای کلید احراز هویت (T.BAC_Authentication_Key_Disclose) مورد نیاز است به طوری که به عامل شخصی‌سازی مجاز دارنده حق نوشتن داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) در مرحله شخصی‌سازی اجازه‌ی دسترسی می‌دهد و در مرحله‌استفاده عملیاتی دسترسی عامل شخصی‌سازی را انکار می‌کند. |
| O.Handling_Info_Leakage<br>ساماندهی نشت اطلاعات | این هدف امنیتی برای مقابله با تهدید فاش شدن (نشت) اطلاعات کلید رمزنگاری (T.Leakage_CryptographicKey_Info) مورد نیاز است، به گونه‌ای که محصول ابزاری برای جلوگیری از تحلیل اطلاعات منتشر شده (توان برق و امواج و غیره) را در طول عملیات رمزنگاری، و به دست آوردن اطلاعات کلید فراهم می‌آورد. |

| | |
|---|---|
| O.BAC<br>کنترل دسترسی پایه | ایـن هـدف امنیتـی، بـرای بـه اجـرا در آوردن خطمشـی‌های امنیـت سـازمانی کنتـرل دسترسـی بـه گذرنامـه الکترونیـک (P.ePassport_Access_Control)، مورد نیاز است به گونه‌ای که محصول سازوکارهای امنیت کنترل دسترسـی پایـه (BAC) را برای کنترل دسترسی به داده شخصی دارنده گذرنامه الکترونیک پیاده‌سازی می‌کند، بنابراین، حق خواندن اطلاعات شخصی دارنده گذرنامه الکترونیک را تنها به سامانه بازرسی مجازی می‌دهد که احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) را با موفقیت انجام داده باشد.<br>این هدف امنیتی برای مقابله با تهدیدات T.Forgery_Corruption_Personal Data و دستکاری (T.Skimming) مورد نیاز است. به طوری که محصول حق خواندن داده شخصی دارنده گذرنامه الکترونیک را با تولید کلیـد نشسـت کنتـرل دسترسـی پایـه (BAC) در طول احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) تنها به سامانه بازرسـی مجـاز داده و دسترسـی سـامانه بازرسی را که حق خواندن ندارد، انکار می‌کند. |

| | |
|---|---|
| O.EAC<br>کنترل دسترسی توسعه‌یافته | این هدف امنیتی برای به اجـرا در آوردن خط‌مشـی‌های امنیـت سـازمانی P.ePassport_Access_Control مـورد نیـاز اسـت هنگامی که محصول در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) را برای کنترل دسترسی به داده‌زیست‌سنجی دارنده گذرنامـه الکترونیـک پیاده‌سـازی می‌کنـد، حـق دسترسی به داده زیست‌سنجی دارنده‌گذرنامه الکترونیک را تنها به سامانه بازرسی مجازی می‌دهد که کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) را با موفقیت انجام داده است.<br>این هدف امنیتی برای مقابله با تهدیدآسیب به داده بیومتریک(T.Damage_to_Biometric_Data) و دسـتکاری (T.Skimming) مورد نیاز است، به طوری که محصول حق خواندن داده‌زیست‌سنجی دارنده‌گذرنامه الکترونیک را را از طریق کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) با تولید کلید نشسـت کنتـرل دسترسـی توسـعه یافتـه (EAC) در طـول کنتـرل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) تنها به سامانه بارزسی مجاز می‌دهد و دسترسی با سـامانه بازرسـی‌ای که حق خواندن ندارد را رد می‌کند. |

### ۵-۴-۲- منطق اهداف امنیتی برای محیط عملیاتی

| هدف امنیتی برای محیط عملیاتی | توضیحات |
|---|---|
| OE.ePassport_Manufacturing_Security<br>امنیت تولید گذرنامه | این هدف امنیتی محیطی جهت مقابله با تهدید تکثیر گذرنامه الکترونیک(T.ePassport_Reproduction) مورد نیاز است ایـن کار از طریق حصول اطمینان از آمادگی اقدامات امنیتی فیزیکی (چاپ امن و غیره)گذرنامه الکترونیک جهت تشخیص تولیـد دوباره‌ی تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و تلاش حمله استاد بزرگ شـطرنج، جـایگزینی تصـویر چهره و تغییر داده ناحیه قابل خواندن توسط ماشین (MRZ) و غیره صورت می‌پذیرد. |

| | |
|---|---|
| OE.Procedures_of_ePassport_Holder_Check<br>رویه بررسی دارنده گذرنامه | این هدف امنیتی محیطی جهت مقابله با تهدیدات تکثیر گذرنامه الکترونیک(T.ePassport_Reproduction)، افشای کلید احراز هویت (T.BAC_Authentication_Key_Disclose) و T.EAC-CA_Bypass مورد نیاز است، این کار با پیاده‌سازی با اجرای اقدامات امنیتی رویه‌ای در فرایند مهاجرت، از جمله روش‌های اجرایی برای بررسی صفحه اطلاعات هویتی چاپ شده‌ی گذرنامه الکترونیک و تعیین وضعیت جعل دفترچه‌ی گذرنامه الکترونیک و غیره انجام می‌شود |
| OE.Application_Program_Install<br>نصب برنامه کاربردی | این هدف امنیتی محیطی، جهت اجرای خط‌مشی امنیت سازمانی نصب برنامه کاربردی (P.Application_Program_Install) مورد نیاز است تا اطمینان حاصل کند که تنها برنامه‌های برنامه‌ی کاربردی (App) در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) به شیوه امنی توسط عامل شخصی‌سازی بارگذاری شده‌اند. |
| OE.Certificate_Verification<br>تأیید گواهی | این هدف امنیتی محیطی، پس از بررسی منظم گواهی‌های امضاء کننده سند (DS) و CRL، برای سامانه بازرسی، مانند سامانه بازرسی کنترل دسترسی پایه (BAC) و سامانه بازرسی کنترل دسترسی توسعه یافته (EIS)، سند موجودیت غیر فعال امنیتی (SOD) را مورد بررسی قرار می‌دهد تا جعل و تخریب داده هویتی گذرنامه الکترونیک ثبت شده در محصول را بررسی کند. همچنین، این هدف امنیتی محیطی اطمینان می‌یابد که سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) به صورت امنی کلید امضای دیجیتالی که منطبق بر گواهی سامانه بازرسی (IS) را نگهداری می‌کند و برای محصول گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، گواهی تأیید کننده سند (DV) و گواهی سامانه بازرسی (IS) را در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) ارائه می‌دهد. بنابراین، این هدف امنیتی محیطی برای مقابله با تهدیدات آسیب به داده بیومتریک (T.Damage_to_Biometric_Data)، T. EAC-CA Bypass، جعل گواهی سامانه بازرسی (T.IS_Certificate_Forgery) و پشتیبانی از A.Certificate_Verification مورد نیاز است. |

| | |
|---|---|
| OE.Personalization_Agent<br>عامل شخصی‌سازی | این هدف امنیتی محیطی جهت اجرای خط‌مشی‌های امنیت سازمانی، سازگاری بین المللی (P.International_Compatibility) و عامل شخصی‌سازی (P.Personalization_Agent)مورد نیاز است. این هدف با حصول اطمینان از اینکه محصول پس از صدور امن گذرنامه الکترونیک در فاز استفاده عملیاتی، به گونه‌ای تحویل داده شده است که عامل شخصی‌سازی با تأیید عملکرد عادی و سازگار گذرنامه الکترونیک در فاز شخصی‌سازی و غیر فعال کردن تابع نوشتن بتواند بررسی کند که صدور موجودیت فعال تغییر نیافته است. این هدف امنیتی محیطی همچنین برای به اجرا در آوردن خط‌مشی امنیت سازمانی کنترل دسترسی به گذرنامه الکترونیک (P.ePassport_Access_Control)مورد نیاز است که نقش عامل شخصی‌سازی را تعریف می‌کند. همچنین این هدف امنیتی محیطی برای پشتیبانی از مفروضات A.Certificate_Verification مورد نیاز است چرا که عامل شخصی‌سازی گواهی‌های ضروری در احراز هویت غیر فعال (PA) را ایجاد کرده و پشتیبانی کنترل دسترسی توسعه یافته (EAC) برای سامانه بازرسی در دسترس است.<br>این هدف امنیتی محیطی برای مقابله با تهدید تغییر و تبدیل داده امنیتی (T.TSF_Data_Modification) مورد نیاز است چرا که عامل شخصی‌سازی تابع نوشتن را در مرحله استفاده عملیاتی غیر فعال می‌کند، بنابر این، تابع نوشتن برای تغییر داده‌امنیتی (TSF) غیر فعال می‌شود. |

| | |
|---|---|
| OE.Inspection_System<br>سیستم بازرسی | هدف امنیتی محیطی برای پشتیبانی از مفروضات سامانهA.Inspection و اجـرای خط‌مشـی‌های امنیـت سـازمانی روش‌هـای کاربرد مکانیسم امنیتی<br>(P.Security_Mechanism_Application_Procedures)وePassport_Access_Control مـورد نیـاز اسـت هنگـامی کـه سـامانه بازرسی سازوکارهای امنیتی را پیاده‌سازی می‌کند و از ترتیب کاربرد سازوکارهای امنیتـی منطبـق بـر نـوع سـامانه بازرسـی اطمینان می‌یابد به گونه‌ای که خط‌مشی‌های کنترل دسترسـی گذرنامـه الکترونیـک عامـل شخصی‌سـازی را نقـض نکنـد و اطمینان می‌یابد که اطلاعات استفاده شده در محصول به شیوه امنی پس از اتمام نشست از بین می‌روند.<br>این هدف امنیتی محیطی برای مقابله با تهدید استراق سمع (T.Eavesdropping) مورد نیاز است به گونـه‌ای کـه بـا برقـراری پیام‌رسانی امن کنترل دسترسی پایه (BAC) بعد از تولید کلید نشستکنترل دسترسی پایه (BAC) از طریق توزیع کلیـدکنترل دسترسی پایه (BAC) هنگامی که سامانه بازرسی با محصول ارتباط برقرار می‌کند از محرمانگی و یکپارچگی داده‌هـای انتقـال یافته اطمینان حاصل می‌کند.<br>ایـن هـدف امنیتـی محیطـی بـرای مقابلـه بـا تهدیـد T. Forgery_Corruption_Personal Data، آسـیب بـه داده بیومتریـک (T.Damage_to_Biometric_Data)، دستکاری (T.Skimming) و T.EAC-CA_Bypass مورد نیاز است هنگامی که سامانه بازرسی از احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) کنترل دسترسی توسعه یافته (EAC) و احـراز هویـت غیـر فعـال (PA) پشتیبانی می‌کند.<br>این هدف امنیتی محیطی برای مقابله با تهدید استفاده مجدد از داده نشست (T.SessionData_Reuse) مـورد نیـاز اسـت بـه طوری که سامانه بازرسی، کلیدهای عمومی موقت مختلفی را درهر نشست جهت انتقال به محصول دردرون کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) تولید می‌کند. |

| | |
|---|---|
| OE.IC_Chip<br>تراشه‌ی مدار مجتمع | این هدف امنیتی محیطی برای پشتیبانی از مفروضاتA.IC_Chip مورد نیاز است به گونه‌ای که از تراشه‌ی مدار مجتمع (IC) (EAL4+(SOF-high استفاده می‌کند که عدد تصادفی تولید کرده و عملیات رمزنگاری را به منظور پشتیبانی از توابع هدف امنیتی ارائه داده و آشکارسازی سوء عمل‌ها و حفاظت‌های فیزیکی را فراهم می‌آورد. همچنین، این هدف امنیتی محیط برای مقابله با تهدیداختلال در عملکرد (T.Malfunction) مورد نیاز است چنانکه تراشه‌ی مدار مجتمع (IC) بد عمل کردن‌ها را خارج از شرایط عادی عملیات تشخیص می‌دهد. |
| OE.MRZ_Entropy<br>آنتروپی ناحیه قابل خواندن توسط ماشین | این هدف امنیتی محیطی، برای پشتیبانی از آنتروپی مفروض ناحیه قابل خواندن توسط ماشین(A.MRZ_Entropy) با ارائه آنتروپی ناحیه قابل خواندن توسط ماشین (MRZ) برای شخصی‌سازی جهت اطمینان از کلید احراز هویت کنترل دسترسی پایه (BAC) امن مورد نیاز است. |
| OE.PKI<br>زیرساخت کلید عمومی | این هدف امنیتی محیطی برای به اجرا درآوردن خط‌مشی‌های امنیت سازمانی P. PKI مورد نیاز است و با پیاده‌سازی و به-کارگیری سامانه زیرساخت کلید عمومی (PKI) گذرنامه الکترونیک که اقدامات صدور گواهی را مطابق با CPS مانند تولید کلید امضای دیجیتال و تولید، صدور و توزیع گواهی ضروری در پشتیبانی از سازوکارهای امنیتی احراز هویت غیر فعال (PA) و کنترل دسترسی توسعه یافته (EAC) اجرا می‌کند از مفروضات تأیید گواهی(A.Certificate_Verification) پشتیبانی می‌کند. این هدف امنیتی محیطی برای مقابله با تهدید آسیب به داده بیومتریک(T.Damage_to_Biometric_Data) با تولید، صدور و توزیع گواهی ضروری در EAC از طریق پیاده‌سازی EAC-PKI، مورد نیاز است. |

| | |
|---|---|
| OE.Range_RF_Communication<br>محدوده ارتباط فرکانس رادیویی | این هدف امنیتی محیطی، برای مقابله با تهدید دستکاری (T.Skimming) و اجرای خط‌مشی‌های امنیت سازمانی محدوده ارتباط فرکانس رادیویی(P.Range_RF_Communication) با حصول اطمینان از کمتر از ۵ سانتیمتر بودن فاصله ارتباط فرکانس رادیویی (RF) بین تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) و سامانه بازرسی و عدم برقراری کانال ارتباطی فرکانس رادیویی (RF) در صورت بسته بودن صفحه‌ی گذرنامه الکترونیک پیوست شده به تراشه‌ی مدار مجتمع (IC) مورد نیاز است. |

## ۶-الزامات کارکرد امنیتی

الزامات امنیتی الزامات کارکردی و تضمین امنیتی را مشخص می‌کند که باید توسط محصول که ادعای انطباق با این پروفایل حفاظتی را دارد برآورده شود. در این پروفایل حفاظتی، موجودیت‌های خارجی مشخص شده در الزامات امنیتی شامل عامل شخصی‌سازی، سامانه بازرسی کنترل دسترسی توسعه یافته (EIS)، سامانه بازرسی کنترل دسترسی پایه (BAC) و تراشه‌ی مدار مجتمع (IC) گذرنامه الکترونیک است.

معیار مشترک اجازه‌ی اجرای عملیات مختلف بر روی الزامات کارکردی را می‌دهد. این عملیات عبارتند از: اختصاص[۲۵]، تکرار[۲۶]، پالایش[۲۷] و انتخاب[۲۸]. هر یک از این عملیات در این پروفایل حفاظتی مورد استفاده قرار گرفته است.

**۱. تکرار**

[۲۵] Assignment

[۲۶] Iteration

[۲۷] Refinement

[۲۸] Selection

این عملیات موقعی مورد استفاده قرار می‌گیرد که یک مؤلفه[۲۹] با تغییر عملیات تکرار می‌شود. نتیجه تکرار، با شماره تکرار داخل پرانتز به دنبال شناسه‌ی مؤلفه مشخص می‌شود. به عنوان مثال (شماره‌ی تکرار).

**۲. انتخاب**

این عملیات موقعی مورد استفاده قرار می‌گیرد که یک یا چند آیتم از فهرست ارائه شده توسط معیار مشترک در بیان یک الزام انتخاب شده باشد. نتیجه‌ی انتخاب با متن *زیرخط دار و مورب* نشان داده می‌شود.

**۳. پالایش**

این عملیات موقعی مورد استفاده قرار می‌گیرد که جزئیاتی به یک الزام اضافه شده و در نتیجه بیشتر یک الزام محدودتر می‌شود. نتیجه‌ی پالایش با **متن پر رنگ** نشان داده می‌شود.

**۴. اختصاص**

این عملیات موقعی مورد استفاده قرار می‌گیرد که مقادیر خاصی به پارامترهای نامشخصی (مانند طول کلمه‌عبور) اختصاص داده شود. نتیجه‌ی اختصاص در براکت نشان داده می‌شود. به عنوان مثال [مقدار اختصاص].

**نکته کاربردی ۱۸:** برای کمک به روشن شدن هدف الزام، شناسایی انتخاب‌های پیاده‌سازی و یا برای تعریف معیارهای "پذیرش/ رد" یک الزام ارائه شده‌اند. نکته کاربردی الزامات مرتبط را در هر جا که مناسب بود دنبال خواهند کرد.

الزامات کارکرد امنیتی برای این پروفایل حفاظتی شامل مؤلفه‌های بخش ۲ معیار مشترک جهت برآوردن الزامات امنیتی شناسایی شده در فصل ۴ است، و در جدول ۹، به طور خلاصه بیان شده است.

**جدول ۹- الزامات کارکرد امنیتی**

[۲۹] component

| شماره الزام | نام الزام | تطابق الزام با استاندارد |
|---|---|---|
| ۱ | تولید کلید رمزنگاری (ساز و کار استخراج کلید) ۱ | FCS_CKM.1.1 |
| ۲ | توزیع کلید رمزنگاری (توزیع نقطه‌ی آغاز تصادفی (seed) تابع اشتقاق کلید (KDF) برای تولید کلید نشست (BAC) ۱ | FCS_CKM.2(1) |
| ۳ | توزیع کلید رمزنگاری (توزیع نقطه‌ی آغاز تصادفی (seed) تابع اشتقاق کلید (KDF) برای تولید کلید نشست (EAC) ۱ | FCS_CKM.2(2) |
| ۴ | تخریب کلید رمزنگاری ۱ | FCS_CKM.4 |
| ۵ | عملیات رمزنگاری (عملیات رمزنگاری کلید متقارن) ۱ | FCS_COP.1(1) |
| ۶ | عملیات رمزنگاری (کد احراز هویت پیام (MAC)) ۱ | FCS_COP.1(2) |
| ۷ | عملیات رمزنگاری (تابع چکیده‌ساز) | FCS_COP.1(3) |
| ۸ | عملیات رمزنگاری (درستی‌سنجی امضای دیجیتال برای درستی‌سنجی گواهی) ۱ | FCS_COP.1(4) |
| ۹ | کنترل دسترسی زیر مجموعه ۱ | FDP_ACC.1.1 |
| ۱۰ | ویژگی امنیتی مبتنی بر کنترل دسترسی ۱ | FDP_ACF.1.1 |
| ۱۱ | ویژگی امنیتی مبتنی بر کنترل دسترسی ۲ | FDP_ACF.1.2 |
| ۱۲ | ویژگی امنیتی مبتنی بر کنترل دسترسی ۳ | FDP_ACF.1.3 |
| ۱۳ | ویژگی امنیتی مبتنی بر کنترل دسترسی ۴ | FDP_ACF.1.4 |
| ۱۴ | حفاظت از اطلاعات باقیمانده‌ی زیر مجموعه ۱ | FDP_RIP.1.1 |
| ۱۵ | محرمانگی تبادل داده اولیه ۱ | FDP_UCT.1.1 |
| ۱۶ | یکپارچگی تبادل داده ۱ | FDP_UIT.1.1 |
| ۱۷ | یکپارچگی تبادل داده ۲ | FDP_UIT.1.2 |
| ۱۸ | ساماندهی شکست احراز هویت ۱ | FIA_AFL.1.1 |
| ۱۹ | ساماندهی شکست احراز هویت ۲ | FIA_AFL.1.2 |
| ۲۰ | زمان‌بندی احراز هویت (احراز هوست دو طرفه‌ی BAC) ۱ | FIA_UAU.1(1) (FIA_UAU.1.1) |

| | | |
|---|---|---|
| ۲۱ | زمان‌بندی احراز هویت (احراز هوست دو طرفه‌ی BAC) ۲ | FIA_UAU.1(1)<br>(FIA_UAU.1.2) |
| ۲۲ | زمان‌بندی احراز هویت (کنترل دسترسی توسعه یافته –احراز هویت پایانه (EAC-TA)) ۱ | FIA_UAU.1(2)<br>(FIA_UAU.1.1) |
| ۲۳ | زمان‌بندی احراز هویت (کنترل دسترسی توسعه یافته –احراز هویت پایانه (EAC-TA)) ۲ | FIA_UAU.1(2)<br>(FIA_UAU.1.2) |
| ۲۴ | ساز و کار احراز هویت تک کاربردی ۱ | FIA_UAU.4.1 |
| ۲۵ | ساز و کار احراز هویت چند گانه ۱ | FIA_UAU.5.1 |
| ۲۶ | ساز و کار احراز هویت چند گانه ۲ | FIA_UAU.5.2 |
| ۲۷ | زمان‌بندی شناسایی ۱ | FIA_UID.1.1 |
| ۲۸ | زمان‌بندی شناسایی ۲ | FIA_UID.1.2 |
| ۲۹ | مدیریت رفتار توابع امنیتی | FMT_MOF.1.1 |
| ۳۰ | مدیریت مشخصه‌های امنیتی | FMT_MSA.1.1 |
| ۳۱ | مقدار دهی اولیه مشخصه‌ی ایستا ۱ | FMT_MSA.3.1 |
| ۳۲ | مقدار دهی اولیه مشخصه‌ی ایستا ۲ | FMT_MSA.3.2 |
| ۳۳ | مدیریت داده امنیتی (TSF) (اطلاعات درستی‌سنجی گواهی ۱ | FMT_MTD.1(1)<br>(FMT_MTD.1.1) |
| ۳۴ | مدیریت داده امنیتی (TSF) (مقداردهی اولیه SSC) ۱ | FMT_MTD.1(2)<br>(FMT_MTD.1.1) |
| ۳۵ | داده امنیتی (TSF) امن ۱ | FMT_MTD.3.1 |
| ۳۶ | مشخصات توابع مدیریتی ۱ | FMT_SMF.1.1 |
| ۳۷ | نقش‌های امنیتی ۱ | FMT_SMR.1.1 |
| ۳۸ | نقش‌های امنیتی ۲ | FMT_SMR.1.2 |
| ۳۹ | غیر قابل مشاهده بودن ۱ | FPR_UNO.1 |
| ۴۰ | خرابی با حفظ حالت امن ۱ | FPT_FLS.1.1 |
| ۴۱ | آشکارسازی تغییر درون توابع هدف امنیتی ۱ | FPT_ITI.1.1 |
| ۴۲ | آشکارسازی تغییر درون توابع هدف امنیتی ۲ | FPT_ITI.1.2 |

| | | |
|---|---|---|
| **۴۳** | **آزمون توابع هدف امنیتی (TSF) ۱** | FPT_TST.1.1 |
| **۴۴** | **آزمون توابع هدف امنیتی (TSF) ۲** | FPT_TST.1.2 |
| **۴۵** | **آزمون توابع هدف امنیتی (TSF)۳** | FPT_TST.1.3 |

### ۶-۱- پشتیبانی رمزنگاری

| شماره الزام | نام الزام |
|---|---|
| **۱** | **تولید کلید رمزنگاری (ساز و کار استخراج کلید) ۱** |
| وراثت از هیچ مؤلفه دیگر ندارد.<br>وابستگی: FCS_CKM.2[ توزیع کلید رمزنگاری یا FCS_COP.1 عملیات رمزنگاری ]، FCS_CKM.4 تخریب کلید رمزنگاری<br>توابع هدف امنیتی (TSF) باید کلیدهای رمزگذاری و کلید کد احراز هویت پیام (MAC) را مطابق با الگوریتم تولید کلید رمزنگاری مشخص شده [پیوست ۵,۱ سازوکار استخراج کلید] و اندازه‌های کلید رمزنگاری مشخص شده [۱۱۲ بیت] تولید کند که مورد زیر را برآورده می‌سازد [سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO)].<br>**نکته کاربردی ۱۹:** محصول، کلید احراز هویت کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی پایه (BAC) و کلید نشست کنترل دسترسی توسعه یافته (EAC) را با استفاده از سازوکار استخراج کلید تولید می‌کند. اگر عامل شخصی‌سازی کلید احراز هویت کنترل دسترسی پایه (BAC) را تولید کند و آن را در فاز شخصی‌سازی با توجه به خط‌مشی صدور گذرنامه الکترونیک در محصول ثبت کند، محصول نمی‌تواند کلید احراز هویت کنترل دسترسی پایه (BAC) را تولید کند. | |
| **۲** | **توزیع کلید رمزنگاری (توزیع نقطه‌ی آغاز تصادفی (seed) (تابع اشتقاق کلید (KDF)برای تولید کلید نشست کنترل دسترسی پایه (BAC)) ۱** |
| وابستگی: [FDP_ITC.1، ورود داده کاربر بدون مشخصه‌های امنیتی، یا FDP_ITC.2 ورود داده کاربر با مشخصه‌های امنیتی،یاFCS_CKM.1 تولید کلید رمزنگاری]، FCS_CKM.4 تخریب کلید رمزنگاری<br>توابع هدف امنیتی (TSF) باید نقطه‌ی آغاز تصادفی (seed) تابع اشتقاق کلید (KDF) را برای تولید کلید نشست کنترل دسترسی پایه (BAC) مطابق با روش توزیع کلید | |

| | |
|---|---|
| رمزنگاری مشخص شده [[انتخاب: ساز و کار برقراری کلید ۶،[*اختصاص: دیگر روش‌های توزیع کلید رمزنگاری*]] تولید کندکه مورد زیر را برآورده می‌سازد: [[انتخاب: ISO/IEC 11770-2، [*اختصاص: استانداردهای دیگر*]] | |
| **۳** | **توزیع کلید رمزنگاری (توزیع نقطه‌ی آغاز تصادفی (seed) (تابع اشتقاق کلید (KDF)برای تولید کلید نشست کنترل دسترسی توسعه یافته (EAC)) ۱** |
| وابستگی‌ها : [FDP_ITC.1، ورود داده کاربر بدون مشخصه‌های امنیتی،یا FDP_ITC.2 ورود داده کاربر با مشخصه‌های امنیتی،یا FCS_CKM.1 تولید کلید رمزنگاری]، FCS_CKM.4 تخریب کلید رمزنگاری<br>توابع هدف امنیتی (TSF) باید نقطه‌ی آغاز تصادفی (seed) تابع اشتقاق کلید (KDF) را برای تولید کلید نشست کنترل دسترسی توسعه یافته (EAC) مطابق با روش توزیع کلید رمزنگاری مشخص شده [[انتخاب: پروتکل توافق کلید دیفی–هلمن (DH)، پروتکل توافق کلید دیفی-هلمن منحنی بیضوی، [اختصاص: دیگر روش‌های توزیع کلید رمزنگاری]] تولید کند که مورد زیر را برآورده می‌سازد: [[انتخاب: PKCS#3، ANSI X9.4، ISO/IEC 15946-3، [اختصاص: استانداردهای دیگر]] | |
| **۴** | **تخریب کلید رمزنگاری** |
| وابستگی‌ها: [ FDP_ITC.1، ورود داده کاربر بدون مشخصه‌های امنیتی،یا FDP_ITC.2ورود داده کاربر با مشخصه‌های امنیتی،یا FCS_CKM.1 تولید کلید رمزنگاری]<br>توابع هدف امنیتی (TSF) بایدکلیدهای رمزنگاری و کد احراز هویت پیام (MAC) رامطابق با روش تخریب کلید رمزنگاری مشخص شده [*اختصاص: روشتخریب کلید رمزنگاری*]] از بین ببردکه مورد زیر را برآورده می‌سازد: [*اختصاص: فهرستی از استانداردها*]]<br>**نکته کاربردی ۲۰:** نویسنده‌ی هدف امنیتی باید روشی را برای تخریب امن کلیدهای تولید شده توسط ساز و کار استخراج کلید مشخص کند. چنانچه فهرستی از استانداردها برای ارجاع وجود نداشته باشد، می‌توان «هیچ»[۳۰] را اختصاص داد. | |
| **۵** | عملیات رمزنگاری (عملیات رمزنگاری کلید متقارن) ۱ |
| وابستگی‌ها: [FDP_ITC.1، ورود داده کاربر بدون مشخصه‌های امنیتی،یا FDP_ITC.2 ورود داده کاربر با مشخصه‌های امنیتی،یا FCS_CKM.1 تولید کلید رمزنگاری]، FCS_CKM.4 تخریب کلید رمزنگاری | |

[۳۰] none’

| |
|---|
| توابع هدف امنیتی (TSF) باید [رمزگذاری پیام، عملیات رمزگشایی] را مطابق با الگوریتم رمزنگاری مشخص شده [[انتخاب: استاندارد رمزگذاری داده سه گانه (TDES)، [*اختصاص: دیگرالگوریتم‌های رمزنگاری*]] و اندازه‌های کلید رمزنگاری [انتخاب: ۱۱۲ بیت، [اختصاص: *دیگر اندازه‌های کلید رمزنگاری*] اجرا کند که مورد زیر را برآورده می‌سازد: [انتخاب: ISO/IEC 18033-3، [*اختصاص:استانداردهای دیگر*]]<br>**نکته کاربردی ۲۱:** محصول از الگوریتم رمزنگاری استاندارد رمزگذاری داده سه گانه (TDES) برای حفاظت از محرمانگی داده انتقال یافته پیام‌رسانی امن کنترل دسترسی پایه (BAC) یا کنترل دسترسی توسعه یافته (EAC)، جهت احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) و برای توزیع کلیدکنترل دسترسی پایه (BAC) استفاده می‌کند. برای مد عملیاتی الگوریتم رمزنگاری مورد استفاده، مد CBC با IV=0 همانگونه که در ISO/IEC 10116 تعریف شده است مورد استفاده قرار می‌گیرد. در صورتی که محصول نتواند این الزام را پیاده‌سازی کند، این الزام می‌تواند در محیط محصول (کمک پردازنده‌ی تراشه‌ی مدار مجتمع (IC) گواهی شده یا کتابخانه‌های رمزنگاری بارگذاری شده در تراشه‌ی مدار مجتمع (IC) گواهی شده) پشتیبانی شود. |
| **۶** **عملیات رمزنگاری (کد احراز هویت پیام (MAC)) ۱** |
| وابستگی‌ها: [FDP_ITC.1، ورود داده کاربر بدون مشخصه‌های امنیتی، یا FDP_ITC.2ورود داده کاربر با مشخصه‌های امنیتی،یا FCS_CKM.1 تولید کلید رمزنگاری]، FCS_CKM.4 تخریب کلید رمزنگاری<br>توابع هدف امنیتی (TSF) باید [عملیات کد احراز هویت پیام (MAC)] را مطابق با الگوریتم رمزنگاری مشخص شده [[انتخاب: کد احراز هویت پیام (MAC) جزئی، [*اختصاص: دیگرالگوریتم‌های رمزنگاری*]] و اندازه‌های کلید رمزنگاری [انتخاب: ۱۱۲ بیت، [اختصاص: *دیگر اندازه‌های کلید رمزنگاری*] اجرا کند که مورد زیر را برآورده می‌سازد: [انتخاب: ISO/IEC 9797-1، [*اختصاص:استانداردهای دیگر*]]<br>**نکته کاربردی ۲۲:**محصول از الگوریتم کد احراز هویت پیام (MAC) جزئی برای حفاظت از یکپارچگی برای حفاظت از محرمانگی داده انتقال یافته پیام‌رسانی امن کنترل دسترسی پایه (BAC) یا کنترل دسترسی توسعه یافته (EAC) و برای احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) استفاده می‌کند. کد احراز هویت پیام (MAC) جزئی از الگوریتم MAC 3، استاندارد رمزگذاری داده (DES) رمز قالبی، شمارنده‌ی پیام دنباله و مد لایه‌گذاری ۲ تعریف شده در ISO/IEC 9797-1 استفاده می‌کند. با این حال، در صورتی که محصول نتواند این الزام را پیاده‌سازی کند، این الزام می‌تواند در محیط محصول (کمک پردازنده‌ی تراشه‌ی مدار مجتمع (IC) گواهی شده یا |

| | |
|---|---|
| کتابخانه‌های رمزنگاری بارگذاری شده در تراشه‌ی مدار مجتمع (IC) گواهی شده) پشتیبانی شود. | |
| **۷** | عملیات رمزنگاری (تابع چکیده‌ساز)۱ |
| وابستگی‌ها: [FDP_ITC.1، ورود داده کاربر بدون مشخصه‌های امنیتی، یا FDP_ITC.2 ورود داده کاربر با مشخصه‌های امنیتی، یا FCS_CKM.1 تولید کلید رمزنگاری]، FCS_CKM.4 تخریب کلید رمزنگاری<br>توابع هدف امنیتی (TSF) باید [عملیات چکیده‌سازی] را مطابق با الگوریتم رمزنگاری مشخص شده [[انتخاب: SHA-1، [*اختصاص: دیگرالگوریتم‌های رمزنگاری*]] و اندازه‌های کلید رمزنگاری [هیچ] اجرا کند که مورد زیر را برآورده می‌سازد: [انتخاب: ISO/IEC 10118-3، [*اختصاص:استانداردهای دیگر*]]<br>**نکته کاربردی ۲۳:** در ساز و کار استخراج کلید سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO)، SHA-1 به عنوان یک تابع چکیده‌سازجهت تولید کلید نشست مورد استفاده در پیام‌رسانی امن کنترل دسترسی پایه (BAC) یا کنترل دسترسی توسعه یافته (EAC) استفاده شده است. با این حال، در صورتی که محصول نتواند این الزام را پیاده‌سازی کند، این الزام می‌تواند در محیط محصول (کمک پردازنده‌ی تراشه‌ی مدار مجتمع (IC) گواهی شده یا کتابخانه‌های رمزنگاری بارگذاری شده در تراشه‌ی مدار مجتمع (IC) گواهی شده) پشتیبانی شود. | |
| **۸** | **عملیات رمزنگاری (درستی‌سنجی امضای دیجیتال برای درستی‌سنجی گواهی‌ها)۱** |
| وابستگی‌ها: [FDP_ITC.1، ورود داده کاربر بدون مشخصه‌های امنیتی،یا FDP_ITC.2 ورود داده کاربر با مشخصه‌های امنیتی،یا FCS_CKM.1 تولید کلید رمزنگاری] FCS_CKM.4 تخریب کلید رمزنگاری<br>توابع هدف امنیتی (TSF) باید [اختصاص: *فهرستی از عملیات رمزنگاری*] را مطابق با الگوریتم رمزنگاری مشخص شده [[انتخاب: RSASSA_PKCS1_V1.5-SHA-256، RSASSA-PSS_SHA-256، ECDSA-SHA-224، ECDSA-SHA-256، [*اختصاص: دیگرالگوریتم‌های رمزنگاری*]] و اندازه‌های کلید رمزنگاری [اختصاص: *اندازه‌های کلید رمزنگاری*] اجرا کند که مورد زیر را برآورده می‌سازد: [انتخاب: PKCS#1، ISO/IEC 15946-2]]<br>**در پیوست ۳ احراز هویت پایانه‌ی مشخصات کنترل دسترسی توسعه‌یافته (EAC)، الگوریتم امضای دیجیتال، الگوریتم چکیده‌ساز و اندازه‌های کلید امضای دیجیتال به شکل زیر تعریف** | |

**امضای دیجیتال به شکل زیر تعریف شده‌اند. نویسنده‌ی هدف امنیتی باید با مراجعه به**

**نکته کاربردی ۲۴:** جدول ۱۰، اندازه‌های کلید رمزنگاری را به گونه‌ای مشخص کند به مهاجمان دارای پتانسیل حمله‌ی متوسط پاسخ مورد نیاز AVA_VAN.4 را بدهد. با این حال، در صورتی که محصول نتواند این الزام را پیاده‌سازی کند، این الزام می‌تواند در محیط محصول (کمک پردازنده‌ی تراشه‌ی مدار مجتمع (IC) گواهی شده یا کتابخانه‌های رمزنگاری بارگذاری شده در تراشه‌ی مدار مجتمع (IC) گواهی شده) پشتیبانی شود.

**جدول ۱۰- جزئیات امضای دیجیتال در پروفایل EAC**

| الگوریتم امضای دیجیتال | الگوریتم چکیده‌ساز | اندازه‌های کلید امضای دیجیتال |
|---|---|---|
| RSASSA-PKCS1-V1.5 | SHA-1, SHA-256 | ۱۰۲۴،۱۲۸۰،۱۵۳۶،۲۰۴۸،۳۰۷۲ بیت |
| RSASSA-PSS | SHA-1, SHA-256 | ۱۰۲۴،۱۲۸۰،۱۵۳۶،۲۰۴۸،۳۰۷۲ بیت |
| ECDSA | SHA-1, SHA-224/SHA-256 | ۱۶۰، ۱۹۲،۲۲۴، ۲۵۶ بیت |

### ۶-۲- حفاظت از داده کاربر

| شماره الزام | نام الزام |
|---|---|
| **۹** | **کنترل دسترسی زیر مجموعه ۱** |

وراثت از هیچ مؤلفه دیگر ندارد.

وابستگی: FDP_AC.1 مشخصه‌های امنیتی مبتنی بر کنترل دسترسی

FCS_CKM.4 تخریب کلید رمزنگاری

توابع هدف امنیتی (TSF) باید [خط‌مشی کنترل دسترسی گذرنامه الکترونیک] را روی موارد زیر اعمال کند: [

أ. موجودیت‌های فعال

(۱) عامل شخصی‌سازی

(۲) سامانه بازرسی کنترل دسترسی پایه (BAC)

(۳) سامانه بازرسی کنترل دسترسی توسعه یافته (EIS)

(۴) [اختصاص: *فهرستی از موجودیت‌های فعال دیگر*]

ب. موجودیت‌های غیر فعال

(۱) داده شخصی دارنده‌گذرنامه الکترونیک

: EF.DG1، EF.DG2، EF.DG5~EF.DG13، EF.DG16

(۲) داده زیست‌سنجی دارنده‌گذرنامه الکترونیک

: EF.DG3، EF.DG4

(۳) داده احراز هویت گذرنامه الکترونیک

: EF.DG14، EF.DG15، EF.SOD

(۴) EF.CVCA

(۵) EF.COM

(۶) [اختصاص: *فهرستی از موجودیت‌های غیر فعال دیگر*]

ج. عملیات

(۱) خواندن

(۲) نوشتن

(۳) [اختصاص: *فهرستی از موجودیت‌های غیر فعال دیگر*]

| ۱۰ | **ویژگی امنیتی مبتنی بر کنترل دسترسی ۱** |
|---|---|

وابستگی: FDP_ACC.1کنترل دسترسی زیر مجموعه

FMT_MSA.3مقدار دهی اولیه ایستا

توابع هدف امنیتی (TSF) باید [خط‌مشی کنترل دسترسی گذرنامه الکترونیک] را روی موجودیت‌های غیر فعال بر اساس موارد زیر اعمال کند: [[جدول ۱۱]، [جدول ۱۲]، [اختصاص: *مشخصه‌های امنیتی مرتبط با فهرست افزوده‌ی اختصاص یافته‌ی موجودیت‌های فعال، موجودیت‌های غیر فعال و عملیات در FDP_ACC.1*]].

**نکته کاربردی ۲۵:** مجوز کنترل دسترسی پایه (BAC) حقی است که به کاربر شناسایی شده با سامانه بازرسی داده می‌شود که هنگامی که احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) با موفقیت انجام می‌شود، از برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) به وسیله FIA_UID.1 را پشتیبانی می‌کند.

مجوز کنترل دسترسی توسعه یافته (EAC) حق دسترسی است که هنگامی که سامانه بازرسی با احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) در در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) با موفقیت روبرو می‌شود، داده می‌شود و حق خواندن داده زیست‌سنجی در همه‌ی تمامی گواهی‌های مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، تأیید کننده سند (DV) و سامانه بازرسی (IS) حفظ شده توسط سامانه بازرسی گنجانده شده است. حتی هنگامی که در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) با موفقیت انجام می‌شود، چنانچه گواهی‌ها شامل حق خواندن نباشند، سامانه بازرسی تنها مجوز کنترل دسترسی پایه (BAC) را دارد.

عامل شخصی‌سازی صادر کننده‌ی مجوز حق اعطا شده‌ای است که عامل شخصی‌سازی با موفقیت در فاز شخصی‌سازی احراز هویت شده است.

| ۱۱ | **ویژگی امنیتی مبتنی بر کنترل دسترسی ۲** |
|---|---|

| | |
|---|---|
| توابع هدف امنیتی (TSF) باید قوانین زیر را برای تعیین اینکه آیا یک عملیات در بین موجودیت‌های فعال کنترل شده و موجودیت‌های غیر فعال کنترل شده اجازه داده شده است اعمال کنند: [<br>أ. اجرای این عملیات، تنها زمانی مجاز است که مشخصه‌های امنیتی موجودیت‌های فعال موجود در مشخصه‌های امنیتی حق دسترسی موجودیت‌های غیر فعال و عملیات با مشخصه‌های امنیتی عملیات موجودیت‌های غیر فعال متناظر باشد.<br>ب. [اختصاص: قوانین حاکم بر دسترسی موجودیت‌های فعال کنترل شده و موجودیت‌های غیر فعال کنترل شده با استفاده از عملیات کنترل شده روی موجودیت‌های فعال کنترل شده].<br>].<br>**نکته کاربردی ۲۶:** نویسنده‌ی هدف امنیتی باید قوانین کنترل دسترسی را با ارجاع به جدول ۶ کنترل دسترسی به گذرنامه الکترونیک (P.ePassport_Access_Control) به منظور اجرای خط‌مشی‌های کنترل دسترسی گذرنامه الکترونیک پیاده‌سازی کند. | |
| **ویژگی امنیتی مبتنی بر کنترل دسترسی ۳** | **۱۲** |
| توابع هدف امنیتی (TSF) بایدصریحاً اجازه‌ی دسترسی موجودیت‌های فعال به موجودیت‌های غیر فعال را بر اساس قوانین افزوده‌ی زیر تفویض نماید: [اختصاص: *قوانین، بر اساس مشخصه‌های امنیتی، که صریحاً اجازه دسترسی موجودیت‌های فعال به موجودیت‌های غیر فعال را تفویض می‌نمایند*]. | |
| **ویژگی امنیتی مبتنی بر کنترل دسترسی ۴** | **۱۳** |
| توابع هدف امنیتی (TSF) بایدصریحاً اجازه‌ی دسترسی موجودیت‌های فعال به موجودیت‌های غیر فعال را بر اساس قوانین افزوده‌ی زیر انکار نماید:<br>أ. چنانچه ترتیب دستورالعمل‌های سامانه بازرسی درست نباشد صریحاً اجازه‌ی دسترسی موجودیت‌های فعال به موجودیت‌های غیر فعال را انکار نماید تا از ترتیب کاربرد ساز و کارهای امنیتی، طبق روش‌های اجرایی بازرسی بخش ۲,۱ مشخصات کنترل دسترسی توسعه‌یافته (EAC) اطمینان حاصل کند.<br>ب. چنانچه در گواهی سامانه بازرسی (IS) سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) که مجوز کنترل دسترسی توسعه یافته (EAC) را دارد حق خواندن | |

| | |
|---|---|
| داده‌زیست‌سنجی وجود ندارد خواندن داده زیست‌سنجی توسط موجودیت‌های فعال را صراحتاً رد کند.<br>ج. دسترسی (خواندن، نوشتن و غیره) سامانه بازرسی غیر مجاز به تمام موجودیت‌های غیر فعال را صراحتاً رد کند.<br>[اختصاص: قوانین، بر اساس مشخصه‌های امنیتی دیگر، که صریحاً اجازه دسترسی موجودیت‌های فعال به موجودیت‌های غیر فعال را انکار می‌نمایند]. | |
| **حفاظت از اطلاعات باقیمانده زیر مجموعه ۱** | **۱۴** |
| توابع هدف امنیتی (TSF) باید اطمینان حاصل کند که هر گونه محتوای اطلاعاتی قبلی از منابع بر اساس [انتخاب: *اختصاص منابع به، عدم اختصاص منابع از*] موجودیت‌های غیر فعال زیر غیر قابل دسترس شده است: [<br>أ. کلید نشست کنترل دسترسی پایه (BAC)<br>ب. کلید نشست کنترل دسترسی توسعه یافته (EAC)<br>ج. کلید احراز هویت کنترل دسترسی پایه (BAC)<br>د. [*اختصاص: فهرستی ازموجودیت‌های غیر فعال دیگر*]<br>].<br>**نکته کاربردی ۲۷:** پس از اتمام یک نشست، توابع هدف امنیتی (TSF)نباید کلید نشست کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی توسعه یافته (EAC) و اعداد تصادفی و غیره را در حافظه موقت باقی بگذارند. کلید نشست کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی توسعه یافته (EAC) و کلید احراز هویت کنترل دسترسی پایه (BAC) و غیره را می‌توان با استفاده از روش تعریف شده در FCS_CKM.4 تخریب کرد تا از عدم دسترسی آن‌ها اطمینان حاصل کرد. نویسنده‌ی هدف امنیتی باید با در نظر گرفتن اعداد تصادفی مورد استفاده عملیات *اختصاص* را کامل کند. | |
| **محرمانگی تبادل داده اساسی ۱** | **۱۵** |
| وابستگی: [FTP_ITC.1 کانال قابل اعتماد درونی توابع هدف امنیتی (TSF)، یا | |

FTP_TRO.1 مسیر قابل اعتماد]

[FDP_ACC کنترل دسترسی زیر مجموعه، یا

FDP_IFC.1 کنترل جریان اطلاعات زیرمجموعه]

توابع هدف امنیتی (TSF) باید [خط‌مشی کنترل دسترسی به گذرنامه الکترونیک] را برای *انتقال، دریافت* موجودیت‌های غیر فعال به روشی محافظت شده از افشای غیر مجاز اعمال کند.

**نکته کاربردی ۲۸:** هنگامی که سامانه بازرسی احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) را با موفقیت انجام داد، توابع هدف امنیتی (TSF) با استفاده از کلید رمزنگاری نشست کنترل دسترسی پایه (BAC) از افشای اطلاعات محافظت می‌کند. هنگامی که در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) با موفقیت اجرا شد، بعد از آن از افشای داده انتقال یافته با استفاده از کلید رمزگذاری نشست کنترل دسترسی توسعه یافته (EAC) اطلاعات محافظت می‌شود.

| ۱۶ | **یکپارچگی تبادل داده ۱** |
|---|---|

وابستگی‌ها: [FDP_ACC.1 کنترل دسترسی زیر مجموعه، یا

FDP_IFC.1 کنترل جریان اطلاعات زیر مجموعه]

[FTP_ITC.1 کانال قابل اعتماد درونی توابع هدف امنیتی (TSF)، یا

FTP_TRO.1 مسیر قابل اعتماد]

توابع هدف امنیتی (TSF) باید [خط‌مشی کنترل دسترسی به گذرنامه الکترونیک] را برای انتقال، دریافت داده کاربر به روشی محافظت شده از خطاهای [انتخاب: تغییر، حذف، درج، انتشار] اعمال کند.

| ۱۷ | **یکپارچگی تبادل داده ۲** |
|---|---|

توابع هدف امنیتی (TSF) باید بتواند مشخص کند در دریافت داده کاربر [انتخاب: *تغییر، حذف، درج، انتشار*] چه روی داده است.

**نکته کاربردی ۲۹:** توابع هدف امنیتی (TSF) با استفاده از کلید کد احراز هویت پیام (MAC) برای نشست کنترل دسترسی پایه (BAC) و یا نشست کنترل دسترسی توسعه یافته (EAC) از یکپارچگی داده انتقال یافته محافظت می‌کند. این روش، محافظت در برابر تغییر، حذف و درج داده کاربر را فراهم می‌آورد. نویسنده‌ی هدف امنیتی باید درصورت انتخاب «انتشار» در عملیات انتخاب، ساز و کار امنیتی افزوده‌ای را پیاده‌سازی کند.

**جدول ۱۱موجودیت‌های فعال مرتبط با مشخصه‌های امنیتی**

| موجودیت‌های فعال | مشخصه‌های امنیتی |
|---|---|
| سامانه بازرسی کنترل دسترسی پایه (BAC) | مجوز BAC |
| سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) | مجوز BAC، مجوز EAC |
| عامل شخصی‌سازی | عامل شخصی‌سازی صادر کننده‌ی مجوز |

**جدول ۱۲- موجودیت‌های غیر فعال مرتبط با مشخصه‌های امنیتی**

| موجودیت‌های غیر فعال | مشخصه‌های امنیتی عملیات موجودیت‌های غیر فعال | مشخصه‌های امنیتی حق دسترسی موجودیت‌های غیر فعال |
|---|---|---|
| داده شخصی دارنده‌گذرنامه الکترونیک | حق خواندن | مجوز BAC، مجوز EAC |
| | حق نوشتن | عامل شخصی‌سازی صادر کننده‌ی مجوز |
| داده زیست‌سنجی دارنده گذرنامه الکترونیک | حق خواندن | مجوز EAC |
| | حق نوشتن | عامل شخصی‌سازی صادر کننده‌ی مجوز |
| داده احراز هویت گذرنامه الکترونیک | حق خواندن | مجوز BAC، مجوز EAC |
| | حق نوشتن | عامل شخصی‌سازی صادر کننده‌ی مجوز |
| EF.CVCA | حق خواندن | مجوز BAC، مجوز EAC |
| | حق نوشتن | عامل شخصی‌سازی صادر کننده‌ی مجوز |
| EF.COM | حق خواندن | مجوز BAC، مجوز EAC |
| | حق نوشتن | عامل شخصی‌سازی صادر کننده‌ی مجوز |

### ۶-۳- شناسایی و احراز هویت

| شماره الزام | نام الزام |
|---|---|
| ۱۸ | **ساماندهی شکست احراز هویت ۱** |
| وراثت: از هیچ مؤلفه دیگر ندارد.<br>وابستگی: FIA_UAU.1 زمان‌بندی احراز هویت<br>توابع هدف امنیتی (TSF) باید زمانی که تلاش‌های احراز هویت [انتخاب: *[اختصاص: عدد صحیح مثبت]*، *عدد صحیح مثبت قابل پیکربندی مدیرسیستم همراه با [اختصاص: گستره‌ای از مقادیر قابل قبول]*] مرتبط با موارد زیر اتفاق می‌افتد را تشخیص دهد: [<br>أ. احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC)<br>ب. کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA)<br>ج. *[اختصاص: فهرستی از رویدادهای دیگر احراز هویت]*] | |
| ۱۹ | **ساماندهی شکست احراز هویت ۲** |
| هنگامی که تعداد تعریف شده‌ی تلاش احراز هویت نا موفق [انتخاب: برآورده شد یا فراتر رفت] توابع هدف امنیتی (TSF)باید [پایان نشست کاربر] را اعمال کند.<br>**نکته کاربردی ۳۰:** در صورت شکست احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) یا کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA)، توصیه می‌شود پیام‌رسانی امن کنترل دسترسی پایه (BAC) یا کنترل دسترسی توسعه یافته (EAC) خاتمه یابد. با این حال، نویسنده‌ی هدف امنیتی می‌تواند آن را با ساز و کار معادل دیگری جایگزین کند. نویسنده‌ی هدف امنیتی باید تعداد تلاش‌های احراز هویت ناموفق را با توافق عامل شخصی‌سازی *اختصاص* دهد. | |
| ۲۰ | **زمان‌بندی احراز هویت(احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC)) ۱** |
| وابستگی: FIA_UAU.1 زمان‌بندی شناسایی | |

| | |
|---|---|
| توابع هدف امنیتی (TSF) باید اجازه دهد [<br>أ. نشانه‌ای که از سازوکار کنترل دسترسی پایه (BAC) پشتیبانی کند<br>ب. [*اختصاص: فهرستی از دیگر اقدامات واسطه شده توسط توابع هدف امنیتی (TSF)*]<br>] قبل از اینکه کاربر احراز هویت شود، در طرف کاربر انجام شود. | |
| **۲۱** | **زمان‌بندی احراز هویت(احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC)) ۲** |
| توابع هدف امنیتی (TSF) باید مستلزم این باشد که قبل از اینکه اجازه‌ی هر اقدام واسطه شده توسط توابع هدف امنیتی (TSF) در طرف هر کاربر داده شود، آن کاربر به طور موفقیت آمیز احراز اصالت شود. | |
| **۲۲** | **زمان‌بندی احراز هویت(کنترل دسترسی توسعه یافته–احرازهویت پایانه (EAC-TA)) ۱** |
| وابستگی: FIA_UAU.1(1)زمان‌بندی احراز هویت (احراز هویت دو طرفه‌یکنترل دسترسی پایه (BAC))<br>توابع هدف امنیتی (TSF) باید اجازه دهد [<br>أ. کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) اجرا شود<br>ب. داده کاربر به جز داده زیست‌سنجی دارنده‌گذرنامه الکترونیک خوانده شود<br>ج. [*اختصاص: فهرستی از دیگر اقدامات واسطه شده توسط توابع هدف امنیتی (TSF)*]<br>] قبل از اینکه کاربر احراز هویت شود، در طرف کاربر انجام شود. | |
| **۲۳** | **زمان‌بندی احراز هویت(کنترل دسترسی توسعه یافته–احرازهویت پایانه (EAC-TA)) ۲** |
| توابع هدف امنیتی (TSF) باید مستلزم این باشد که قبل از اینکه اجازه‌ی هر اقدام واسطه شده توسط توابع هدف امنیتی (TSF) در طرف هر کاربر داده شود، آن کاربر به طور موفقیت آمیز احراز هویت شود. | |

| ۲۴ | **ساز و کارهای احراز هویت تک کاربره ۱** |
|---|---|

توابع هدف امنیتی (TSF) باید از استفاده مجدد از داده‌احراز هویت مرتبط با موارد زیر جلوگیری کند [

أ. احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC)

ب. کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA)

ج. [*اختصاص: دیگر ساز و کارهای احراز هویت*]

| ۲۵ | **ساز و کارهای احراز هویت چندگانه ۱** |
|---|---|

توابع هدف امنیتی (TSF) باید [

أ. احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC)

ب. کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA)

ج. [*اختصاص: دیگر ساز و کارهای احراز هویت*]

] را جهت پشتیبانی از احراز هویت کاربر ارائه دهد.

| ۲۶ | **ساز و کارهای احراز هویت چندگانه ۲** |
|---|---|

توابع هدف امنیتی (TSF) باید هر هویت کاربر ادعا شده را مطابق با موارد زیر احراز هویت کند [

أ. سامانه بازرسی کنترل دسترسی پایه (BAC) یا سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) باید در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) با موفقیت همراه باشد تا مجوز کنترل دسترسی پایه (BAC) را داشته باشد.

ب. سامانه بازرسی کنترل دسترسی توسعه یافته (EIS)، به منظور احراز هویت کنترل دسترسی توسعه یافته (EAC) باید در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC)، در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) و کنترل دسترسی توسعه یافته –احراز هویت پایانه (EAC-TA) با

| |
|---|
| موفقیت همراه بوده و حق خواندن داده زیست‌سنجی را در همه‌ی گواهی‌های مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA)، تأیید کننده سند (DV)، سامانه بازرسی (IS) بگنجاند. بدین منظور، توابع هدف امنیتی (TSF)باید در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA) را ارائه دهد.<br>ج. [*اختصاص*: قوانین *دیگر ساز و کارهای احراز هویت*] |

| **۲۷** | **زمانبندی شناسایی ۱** |
|---|---|
| توابع هدف امنیتی (TSF) باید اجازه دهد [<br>أ. برقراری کانال ارتباطی بر اساس ISO/IEC 14443-4<br>] قبل از اینکه کاربر شناسایی شود، در طرف کاربر انجام شود. | |

| **۲۸** | **زمانبندی شناسایی ۲** |
|---|---|
| توابع هدف امنیتی (TSF) باید مستلزم این باشد که قبل از اینکه اجازه‌ی هر اقدام واسطه شده توسط توابع هدف امنیتی (TSF) در طرف هر کاربر داده شود، آن کاربر به طور موفقیت آمیز احراز هویت شود.<br>**نکته کاربردی ۳۱:** هنگامی که موجودیت‌های بیرونی ارتباط برقرار کرده با محصول درخواست استفاده از برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) را دارند، محصول آن را با سامانه بازرسی شناسایی می‌کند. | |

### ۶-۴- مدیریت امنیت

| شماره الزام | نام الزام |
|---|---|
| **۲۹** | **مدیریت رفتار توابع امنیتی۱** |
| وراثت از هیچ مؤلفه دیگر ندارد. | |

| | |
|---|---|
| وابستگی‌ها: FMT_SMR.1 قوانین امنیتی ، FMT_SMF.1مشخصات توابع مدیریتی<br>توابع هدف امنیتی (TSF) باید توانایی *غیر فعال کردن* توابع [تابع نوشتن] را برای [عامل شخصی‌سازی در فاز شخصی‌سازی] محدود کنند.<br>**نکته کاربردی ۳۲:** عامل شخصی‌سازی، گذرنامه الکترونیک را با غیر فعال کردن تابع نوشتن بعد از ثبت داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) در فاز شخصی‌سازی به فاز استفاده عملیاتی تحویل می‌دهد. | |
| **مدیریت مشخصه‌های امنیتی ۱** | **۳۰** |
| وابستگی‌ها: [FDP_ACC.1، کنترل دسترسی زیرمجموعه، یا FDP_IFC.1، کنترل جریان اطلاعات زیر مجموعه]، FMT_SMR.1، قوانین امنیتی، FMT_SMF.1، مشخصات توابع مدیریتی<br>توابع هدف امنیتی (TSF) باید [خط‌مشی کنترل دسترسی گذرنامه الکترونیک] را اعمال کند تا توانایی [*مقدار دهی اولیه*/مشخصه‌های امنیتی [مشخصه‌های امنیتی موجودیت‌های فعال تعریف شده در FDP_ACF.1] را برای [توابع هدف امنیتی (TSF)] محدود کند.<br>**نکته کاربردی ۳۳:** اگر توابع هدف امنیتی (TSF) تغییر داده انتقال یافته توابع هدف امنیتی (TSF) را در FPT_ITI.1 تشخیص داد، به عنوان یک اقدامی که باید اتخاذ شود، توابع هدف امنیتی (TSF) باید مشخصه‌های امنیتی موجودیت‌های فعال تعریف شده در FDP_ACF.1 را مجدداً تنظیم کند. | |
| **مقدار دهی اولیه‌ی مشخصه‌ی ایستا ۱** | **۳۱** |
| وابستگی‌ها: FMT_SMF.1، مشخصات توابع مدیریتی، FMT_SMR.1، قوانین امنیتی<br>توابع هدف امنیتی (TSF) باید [خط‌مشی کنترل دسترسی گذرنامه الکترونیک] را اعمال کند تا مقادیر پیش فرض *محدود کننده*برای مشخصه‌های امنیتی ارائه دهد که برای اجرای خط‌مشی کارکرد امنیتی(SFP) به کار می‌روند. | |
| **مقدار دهی اولیه‌ی مشخصه‌ی ایستا ۲** | **۳۲** |
| توابع هدف امنیتی (TSF)باید به [عامل شخصی‌سازی] اجازه دهد تا هنگامی که موجودیت‌های غیر فعال یا اطلاعات ایجاد شدند، مقادیر اولیه جایگزینی را مشخص کند | |

که مقادیر پیش‌فرض را باطل می‌کند.

**نکته کاربردی ۳۴:** هنگام تولید داده کاربر (EF.DG1~16، EF.SOD، EF.COM، EF.CVCA) در فاز شخصی‌سازی عامل شخصی‌سازی باید مشخصه‌های امنیتی عملیات موجودیت‌های غیر فعال و حق دسترسی‌های موجودیت‌های غیر فعال جدول ۱۰ در .FDP_ACF.1.1 را تعریف کند.

| ۳۳ | **مدیریت داده‌امنیتی (TSF) (اطلاعات درستی‌سنجی گواهی) ۱** |
|---|---|

وابستگی‌ها: FMT_SMR.1، قوانین امنیتی، FMT_SMF.1، مشخصات توابع مدیریتی

توابع هدف امنیتی (TSF) باید توانایی *[نوشتن در حافظه‌ی امن]*این موارد را [

أ. کلید خصوصی احراز هویت تراشه‌ی کنترل دسترسی توسعه یافته (EAC)

ب. تاریخ جاری اولیه

ج. گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA) اولیه

د. کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA) اولیه

ه. *[اختصاص: فهرستی از داده‌های دیگر توابع هدف امنیتی (TSF)]*

] برای [عامل شخصی‌سازی در فاز شخصی‌سازی] محدود کند.

| ۳۴ | **مدیریت داده‌امنیتی (TSF) (مقدار دهی اولیهSSC) ۱** |
|---|---|

وابستگی‌ها: FMT_SMR.1، قوانین امنیتی، FMT_SMF.1، مشخصات توابع مدیریتی

توابع هدف امنیتی (TSF) باید توانایی *تغییر*[SSC (شمارش‌گر دنباله‌ی ارسال)] را برای [توابع هدف امنیتی (TSF)] محدود کند.

**نکته کاربردی ۳۵:** توابع هدف امنیتی (TSF)باید مقدار اولیه SCC را «صفر» قرار دهد تا قبل از برقراری پیام‌رسانی امن کنترل دسترسی توسعه یافته (EAC) بعد از تولید کلید نشست کنترل دسترسی توسعه یافته (EAC) پیام‌رسانی امن کنترل دسترسی پایه (BAC) را خاتمه دهد.

| ۳۵ | **داده‌امنیتی (TSF) امن ۱** |
|---|---|

وابستگی‌ها: FMT_MTD.1، مدیریت داده‌امنیتی(TSF)

توابع هدف امنیتی (TSF) باید اطمینان حاصل کند که تنها مقادیر امن برای [*اختصاص: فهرستی از داده‌های توابع هدف امنیتی (TSF)*] پذیرفته شده‌اند.

**نکته کاربردی ۳۶:** داده امنیتی (TSF) باید تنها از مقادیر امن به عنوان اعداد تصادفی استفاده کند تا به حمله‌ی متوسط بالقوه پاسخ دهد. داده‌امنیتی (TSF) باید با بررسی داده معتبر گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA)، گواهی تأیید کننده سند (DV) و گواهی سامانه بازرسی (IS) ارائه شده توسط سامانه بازرسی کنترل دسترسی توسعه یافته (EIS) هنگام اجرای کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) و به روز رسانی داخلی گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور (CVCA)، کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، داده جاری و EF.CVCA در صورت لزوم از مقادیر امن محافظت کند.

| ۳۶ | **مشخصات توابع مدیریتی ۱** |
|---|---|

وابستگی: ندارد

توابع هدف امنیتی (TSF) باید قادر به انجام توابع مدیریت امنیت زیر باشد: [

أ. تابع برای نوشتن داده کاربر و داده‌امنیتی (TSF) بایددر فاز شخصی‌سازی

ب. تابع به منظور بررسی و به روز رسانی گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) و داده‌های جاری در فاز استفاده عملیاتی

ج. [*اختصاص: دیگر توابع مدیریت امنیتی*]

].

| ۳۷ | **نقش‌های امنیتی ۱** |
|---|---|

| |
|---|
| وابستگی:FIA_UID.1 زمان‌بندی شناسایی<br>توابع هدف امنیتی (TSF) باید نقش‌های امنیتی زیر را حفظ کنند [<br>أ. عامل شخصی‌سازی<br>[*اختصاص: نقش‌های دیگر*]. |

| **۳۸** | **نقش‌های امنیتی ۲** |
|---|---|

توابع هدف امنیتی (TSF) باید بتواند بین کاربران و نقش‌ها ارتباط برقرار کند.

**نکته کاربردی ۳۷:** نکته کاربردی: عامل شخصی‌سازی به عنوان نقشی برای اجرای

أ. توابع مدیریت امنیت EMT_SMF.1. و توابع هدف امنیتی (TSF) توابع مدیریا امنیت را برای FMT_MTD.1(2) اجرا می‌کنند.

ب) FMT_SMF.1

تعریف می‌شود، هر چند، توابع هدف امنیتی (TSF) تا زمانی که یک کاربر نباشد، به عنوان نقش تعریف نمی‌شود.

### ۶-۵- حریم خصوصی

| شماره الزام | نام الزام |
|---|---|
| **۳۹** | **غیر قابل مشاهده بودن ۱** |

وراثت از هیچ مؤلفه دیگر ندارد.

وابستگی: ندارد

توابع هدف امنیتی (TSF) باید اطمینان حاصل کند که [موجودیت خارجی] قادر به مشاهده عملیات زیر نیستند [

أ. FCS_COP.1(1)، عملیات رمزنگاری (عملیات رمزنگاری کلید متقارن)

ب. FCS_COP.1، عملیات رمزنگاری (کد احراز هویت پیام (MAC))

ج. FCS_COP.1(4)، عملیات رمزنگاری (درستی‌سنجی امضای دیجیتالی برای درستی‌سنجی گواهی)

د. [*اختصاص: فهرستی از عملیات دیگر*]

] بر روی [

أ. کلید احراز هویت کنترل دسترسی پایه (BAC)

ب. کلید نشست کنترل دسترسی پایه (BAC)

ج. کلید نشست کنترل دسترسی توسعه یافته (EAC)

د. کلید احراز هویت خصوصی تراشه کنترل دسترسی توسعه یافته (EAC)

ه. [*اختصاص: فهرستی از موجودیت‌های غیر فعال دیگر*] توسط [توابع هدف امنیتی (TSF)]

**نکته کاربردی ۳۸:** موجودیت بیرونی ممکن است داده مرتبط با رمزنگاری را از پدیده‌های فیزیکی (تغییر جریان، ولتاژ، الکترومغناطیس و غیره)، هنگامی که توابع هدف امنیتی (TSF) عملیات رمزنگاری را انجام می‌دهد، یافته و مورد بهره‌برداری قرار دهد. توابع هدف امنیتی (TSF)، ابزارهایی برای رویارویی با حملات فراهم می‌آورد از جمله تحلیل تفاضلی نیرو[۳۱] (DPA) و تحلیل نیروی ساده[۳۲] (SPA) و غیره. با این حال در مواردی که اقدامات برای رویارویی با حملاتی مانند تحلیل تفاضلی نیرو (DPA و تحلیل نیروی ساده (SPA) و غیره به طور کامل توسط محصول پیاده‌سازی نشود، می‌تواند از محیط محصول ارائه شود (تراشه‌ی مدار مجتمع (IC) گواهی شده یا کتابخانه‌های رمزنگاری بارگذاری شده در تراشه‌ی مدار مجتمع (IC) گواهی شده).

[۳۱] Differential Power Analysis

[۳۲] simple power analysis

### ۶-۶- حفاظت از توابع هدف امنیتی

| شماره الزام | نام الزام |
|---|---|
| ۴۰ | **خرابی در حفظ حالت امن ۱** |
| وراثت از هیچ مؤلفه دیگر ندارد.<br>وابستگی: ندارد<br>توابع هدف امنیتی (TSF) باید حالت امنی را هنگام وقوع انواع خرابی‌های زیر حفظ نماید [<br>أ. الف) خرابی تشخیص داده شده در خود آزمایی توسط FPT_TST.1<br>ب. شرایط غیر عادی عملکرد توابع هدف امنیتی (TSF) تشخیص داده شده توسط تراشه‌ی مدار مجتمع (IC)<br>ج. [*اختصاص:فهرستی از انواع خرابی‌های دیگر در توابع هدف امنیتی (TSF)*]<br>]. | |
| ۴۱ | **آشکارسازی تغییر درون توابع هدف امنیتی ۱** |
| وابستگی: ندارد<br>توابع هدف امنیتی (TSF) باید قابلیت شناسایی تغییر تمامی داده‌های توابع هدف امنیتی (TSF)رادرطول انتقال بین توابع هدف امنیتی (TSF) و یک محصول فناوری اطلاعات قابل اعتماد از راه دور را در متریک زیر داشته باشد: [استحکام کد احراز هویت پیام (MAC) جزئی]. | |
| ۴۲ | **آشکارسازی تغییر درون توابع هدف امنیتی ۲** |
| توابع هدف امنیتی (TSF)باید قابلیت بررسی یکپارچگی تمام داده‌های توابع هدف امنیتی (TSF)انتقال یافته توابع هدف امنیتی (TSF) و یک محصول فناوری اطلاعات قابل اعتماد از راه دور را داشته باشد و موارد زیر را اجرا کند [ | |

| | |
|---|---|
| أ. خاتمه دادن به پیام‌رسانی امن کنترل دسترسی پایه (BAC) و یا پیام‌رسانی امن کنترل دسترسی توسعه یافته (EAC)<br>ب. حذف کلید نشست کنترل دسترسی پایه (BAC) و یا کلید نشست کنترل دسترسی توسعه یافته (EAC)<br>ج. اقدام مدیریتی مشخص شده در FMT_MSA.1<br>د. [*اختصاص: اقدامات دیگری که باید اتخاذ شود*]<br>] چنانچه تغییراتی تشخیص داده شد.<br>**نکته کاربردی ۳۹:** استحکام کد احراز هویت پیام (MAC) جزئی معادل استحکام کد احراز هویت پیام (MAC) جزئی امن مشخص شده در FCS_COP.1(2) است. | |
| **آزمون توابع هدف امنیتی (TSF) ۱** | **۴۳** |
| وابستگی: ندارد<br>توابع هدف امنیتی (TSF) باید، مجموعه‌ای از خود آزمایی‌ها را [انتخاب: *در طی راه‌اندازی مقداردهی اولیه، در حین عملیات عادی دوره‌ای، به درخواست کاربر مجاز، بر اساس شرایطی* [*اختصاص: شرایطی که تحت آن باید خود آزمایی رخ دهد*] برای نشان دادن عملکرد درست عملیات [انتخاب: [*اختصاص: قسمتی ازداده‌امنیتی (TSF)*]، *داده‌امنیتی (TSF)*] اجرا کند. | |
| **آزمون توابع هدف امنیتی (TSF) ۲** | **۴۴** |
| توابع هدف امنیتی (TSF) باید برای کاربران مجاز قابلیت بررسی یکپارچگی [انتخاب: [*اختصاص: قسمتی ازداده‌امنیتی (TSF)*]، *داده‌امنیتی(TSF)*] را فراهم آورد. | |
| **آزمون توابع هدف امنیتی (TSF) ۳** | **۴۵** |
| توابع هدف امنیتی (TSF) باید برای کاربران مجاز قابلیت بررسی یکپارچگی [انتخاب: [اختصاص: قسمتی از داده‌امنیتی (TSF)]، داده‌امنیتی (TSF)] را فراهم آورد. | |

## ۷- الزامات تضمین امنیت هدف ارزیابی

الزامات تضمین امنیت در این پروفایل حفاظتی شامل مؤلفه‌های زیر از قسمت ۳ معیار مشترک هستند که در جدول ۱۳، به صورت خلاصه آورده شده است. سطح اطمینان ارزیابی EAL4+(ADV_IMP.2, ATE_DPT.2, AVA_VAN.4) است.

مؤلفه‌های تضمین طبق موارد زیر تکمیل شده‌اند:

- ADV_IMP.2، نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی (TSF)؛
- آزمون ATE_DPT.2: واحدهای اعمال کننده امنیت؛
- AVA_VAN.4، تحلیل آسیب‌پذیری نظام‌مند.

**جدول ۱۳- تضمین الزامات امنیتی**

| نام کلاس | نام الزام | توضیحات |
|---|---|---|
| Security Target(ASE) | ASE_CCL.1 | ادعاهای انطباق |
| | ASE_ECD.1 | تعریف مؤلفه‌های توسعه یافته |
| | ASE_INT.1 | معرفی هدف امنیتی |
| | ASE_OBJ.2 | اهداف امنیتی |
| | ASE_REQ.2 | الزامات امنیتی مشتق شده |
| | ASE_SPD.1 | تعریف مشکلات امنیتی |
| | ASE_TSS.1 | خلاصه مشخصات محصول |
| Development(ADV) | ADV_FSP.1 | مشخصات کارکرد ابتدایی |

| | | |
|---|---|---|
| توصیف معماری امنیتی | ADV_ARC.1 | |
| مشخصات کارکرد کامل | ADV_FSP.4 | |
| نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی (TSF) | ADV_IMP.2 | |
| راهنمای کاربری | AGD_OPE.1 | Guidance Documents(AGD) |
| راهنمای آماده‌سازی | AGD_PRE.1 | |
| تحلیل پوشش | ATE_COV.2 | Tests(ATE) |
| آزمون: واحدهای اجرا کننده امنیت | ATE_DPT.2 | |
| آزمون کارکردی | ATE_FUN.1 | |
| آزمون مستقل – انطباق | ATE_IND.2 | |
| تحلیل آسیب‌پذیری روشمند | AVA_VAN.4 | Vulnerability Assessment(AVA) |
| پشتیبانی تولید، پذیرش روش‌های اجرایی و خودکار سازی | ALC_CMC.4 | Life cycle Support(ALC) |
| پوشش CM ردیابی مسئله | ALC_CMS.4 | |
| روش اجرایی تحویل | ALC_DEL.1 | |
| شناسایی اقدامات امنیتی | ALC_DVS.1 | |
| مدل چرخه حیات تعریف شده توسط توسعه‌دهنده | ALC_LCD.1 | |
| ابزار توسعه خوب تعریف شده | ALC_TAT.1 | |

### ۷-۱- کلاس ارزیابی هدف امنیتی (ASE)

#### ۷-۱-۱- ادعای انطباق(ASE_CCL.1)

**وابستگی:**

ASE_INT.1، معرفی هدف امنیتی

ASE_ECD.1، تعریف مؤلفه‌های توسعه یافته

ASE_REQ.1، الزامات امنیتی بیان شده

**مؤلفه‌های اقدامات توسعه‌دهنده**

| نام خانواده | عنصر امنیتی |
|---|---|
| ادعای انطباق (**ASE_CCL**) | **نام عنصر:** ادعای انطباق ۱<br>**شماره مؤلفه:** (ASE_CCL.1.1D)<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید ادعای انطباق را ارائه دهد. |
| | **نام عنصر**: ادعای انطباق ۲<br>**شماره مؤلفه: (ASE_CCL.1.2D)** |

**مؤلفه‌های اقدامات توسعه‌دهنده**

| نام خانواده | عنصر امنیتی |
| --- | --- |
| | **شرح مؤلفه:**<br><br>توسعه‌دهنده باید منطقی برای ادعای انطباق ارائه دهد. |

**مولفه‌های محتوایی**

| مولفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| ادعای انطباق (**ASE_CCL**) | **نام عنصر: ادعای انطباق ۱**<br>**شماره مؤلفه: (ASE_CCL.1.1C)**<br>**شرح مؤلفه:**<br>ادعای انطباق شامل ادعای انطباق با معیار مشترک است که نسخه‌ای از معیار مشترک را که هدف امنیتی و محصول ادعای انطباق دارند مشخص می‌نماید. |
| | **نام عنصر: ادعای انطباق ۲**<br>**شماره مؤلفه: (ASE_CCL.1.2C)**<br>**شرح مؤلفه:**<br>ادعای انطباق معیار مشترک باید انطباق هدف امنیتی با قسمت دوم معیار مشترک را به گونه‌ای نشان دهد که یا منطبق[۳۳] بر قسمت دوم معیار مشترک است یا قسمت دوم معیار مشترک را توسعه داده [۳۴]است. |

[۳۳] conformant

[۳۴] Extended

| مولفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: ادعای انطباق ۳**<br>**شماره مؤلفه: (ASE_CCL.1.3C)**<br>**شرح مؤلفه:**<br>ادعای انطباق معیار مشترک باید ادعای انطباق هدف امنیتی با قسمت سوم معیار مشترک به گونه‌ای نشان دهد که یا منطبق بر قسمت سوم معیار مشترک است یا قسمت سوم معیار مشترک را توسعه داده است. |
| | **نام عنصر: ادعای انطباق ۴**<br>**شماره مؤلفه: (ASE_CCL.1.4C)**<br>**شرح مؤلفه:**<br>ادعای انطباق معیار مشترک باید با تعریف مؤلفه‌های توسعه یافته سازگار باشد. |
| | **نام عنصر: ادعای انطباق ۵**<br>**شماره مؤلفه: (ASE_CCL.1.5C)**<br>**شرح مؤلفه:** |

| مولفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | ادعای انطباق باید تمامی نمایه‌های حفاظتی و بسته‌های الزامات امنیتی که هدف امنیتی ادعای انطباق دارد را شناسایی کند. |
| | **نام عنصر: ادعای انطباق ۶**<br>**شماره مؤلفه: (ASE_CCL.1.6C)**<br>**شرح مؤلفه:**<br>ادعای انطباق باید هر گونه انطباق هدف امنیتی را با بسته توضیح دهد که منطبق بر بسته است یا بسته را تکمیل کرده[۳۵] است. |
| | **نام عنصر: ادعای انطباق ۷**<br>**شماره مؤلفه: (ASE_CCL.1.7C)**<br>**شرح مؤلفه:**<br>منطق ادعای انطباق باید نشان دهد که نوع محصول با نوع محصول در نمایه‌های حفاظتی‌ای که ادعای انطباق با آن‌ها شده است سازگار است. |
| | **نام عنصر: ادعای انطباق ۸** |

[۳۵] augmented

| مولفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **شماره مؤلفه: (ASE_CCL.1.8C)**<br><br>**شرح مؤلفه:**<br><br>منطق ادعای انطباق باید نشان دهد که بیانیه‌ی تعریف مسئله‌ی امنیتی با بیانیه‌ی مسئله‌ی امنیتی در نمایه‌های حفاظتی‌ای که ادعای انطباق با آن‌ها شده است سازگار است. |
| | **نام عنصر: ادعای انطباق ۹**<br><br>**شماره مؤلفه: (ASE_CCL.1.9C)**<br><br>**شرح مؤلفه:**<br><br>منطق ادعای انطباق باید نشان دهد که بیانیه‌ی هدف امنیتی با بیانیه‌ی هدف امنیتی در نمایه‌های حفاظتی‌ای که ادعای انطباق با آن‌ها شده است سازگار است. |
| | **نام عنصر: ادعای انطباق ۱۰**<br><br>**شماره مؤلفه: (ASE_CCL.1.10C)**<br><br>**شرح مؤلفه:** |

| مولفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | منطق ادعای انطباق باید نشان دهد که بیانیه‌ی الزامات امنیتی با بیانیه‌ی الزامات امنیتی در نمایه‌های حفاظتی‌ای که ادعای انطباق با آن‌ها شده است سازگار می‌باشد. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | |
| ادعای انطباق (**ASE_CCL**) | **نام عنصر: ادعای انطباق ۱**<br>**شماره مؤلفه:** (ASE_CCL.1.1E)<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

**۷-۱-۲-تعریف مؤلفه‌های توسعه یافته (ASE_ECD.1)**

**وابستگی:** بدون وابستگی

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| تعریف مؤلفه‌های توسعه یافته (**ASE_ECD**) | **نام عنصر: تعریف مؤلفه‌های توسعه یافته ۱**<br>**شماره مؤلفه: (ASE_ECD.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید بیانیه‌ای از الزامات امنیتی ارائه دهد. |
| | **نام عنصر: تعریف مؤلفه‌های توسعه یافته ۲**<br>**شماره مؤلفه: (ASE_ECD.1.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید تعریفی از مؤلفه‌های توسعه یافته ارائه دهد. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| تعریف مؤلفه‌های | **نام عنصر: تعریف مؤلفه‌های توسعه یافته ۱** |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| توسعه یافته<br>**(ASE_ECD)** | **شماره مؤلفه: (ASE_ECD.1.1C)**<br>**شرح مؤلفه:**<br>بیانیه الزامات امنیتی، باید تمامی الزامات امنیتی توسعه یافته را شناسایی کند. |
| | **نام عنصر: تعریف مؤلفه‌های توسعه یافته ۲**<br>**شماره مؤلفه: (ASE_ECD.1.2C)**<br>**شرح مؤلفه:**<br>تعریف مؤلفه‌های توسعه یافته باید تعریفی از مؤلفه‌های توسعه یافته برای هر الزام امنیتی توسعه یافته ارائه دهد. |
| | **نام عنصر: تعریف مؤلفه‌های توسعه یافته ۳**<br>**شماره مؤلفه: (ASE_ECD.1.3C)**<br>**شرح مؤلفه:**<br>تعریف مؤلفه‌های توسعه یافته باید توضیح دهد که چگونه هر مؤلفه‌ی توسعه یافته با مؤلفه‌ها، خانواده‌ها و کلاس‌های موجود در معیار مشترک مرتبط می‌شود. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: تعریف مؤلفه‌های توسعه یافته ۴**<br>**شماره مؤلفه: (ASE_ECD.1.4C)**<br>**شرح مؤلفه:**<br>تعریف مؤلفه توسعه یافته باید از مؤلفه‌ها، خانواده‌ها، کلاس‌ها و روش‌های موجود در معیار مشترک به‌عنوان مدل برای ارائه استفاده کند. |
| | **نام عنصر: تعریف مؤلفه‌های توسعه یافته ۵**<br>**شماره مؤلفه: (ASE_ECD.1.5C)**<br>**شرح مؤلفه:**<br>مؤلفه‌های توسعه یافته باید شامل عناصر قابل اندازه‌گیری و عینی‌ای باشد که انطباق یا عدم انطباق این عناصر قابل نشان دادن باشد. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| تعریف مؤلفه‌های توسعه یافته | **نام عنصر: تعریف مؤلفه‌های توسعه یافته ۱**<br>**شماره مؤلفه: (ASE_ECD.1.1E)** |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| (ASE_ECD) | **شرح مؤلفه:**<br><br>ارزیاب باید تأیید کند تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |
| | **نام عنصر: تعریف مؤلفه‌های توسعه یافته ۲**<br><br>**شماره مؤلفه: (ASE_ECD.1.2E)**<br><br>**شرح مؤلفه:**<br><br>ارزیاب باید تأیید کند هیچ مؤلفه‌ی توسعه‌یافته‌ای با استفاده از مؤلفه‌های موجود نمی‌تواند به وضوح بیان شود. |

**۷-۱-۳-معرفی هدف امنیتی (ASE_INT.1)**

**وابستگی**: بدون وابستگی

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| معرفی هدف امنیتی **(ASE_INT)** | **نام عنصر: معرفی هدف امنیتی ۱**<br>**شماره مؤلفه: (ASE_INT.1.1D)**<br>**شرح مؤلفه:**<br>توسعه دهنده باید معرفی از هدف امنیتی ارائه دهد. |

| مؤلفه‌های محتوایی و ارائه | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| معرفی هدف امنیتی **(ASE_INT)** | **نام عنصر: معرفی هدف امنیتی ۱**<br>**شماره مؤلفه: (ASE_INT.1.1C)**<br>**شرح مؤلفه:**<br>معرفی هدف امنیتی باید شامل مرجع هدف امنیتی، مرجع محصول، مرور کلی محصول و شرح محصول باشد. |

| مؤلفه‌های محتوایی و ارائه | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: معرفی هدف امنیتی ۲**<br>**شماره مؤلفه: (ASE_INT.1.2C)**<br>**شرح مؤلفه:**<br>هدف امنیتی به شکل منحصر به فردی هدف امنیتی را بشناساند. |
| | **نام عنصر: معرفی هدف امنیتی ۳**<br>**شماره مؤلفه: (ASE_INT.1.3)**<br>**شرح مؤلفه:**<br>مرجع هدف امنیتی باید هدف امنیتی را شناسایی کند. |
| | **نام عنصر: معرفی هدف امنیتی ۴**<br>**شماره مؤلفه: (ASE_INT.1.4C)**<br>**شرح مؤلفه:**<br>مرور کلی محصول کاربری و مشخصه‌های امنیتی مهم محصول را خلاصه کند. |

| مؤلفه‌های محتوایی و ارائه | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: معرفی هدف امنیتی ۵**<br>**شماره مؤلفه: (ASE_INT.1.5C)**<br>**شرح مؤلفه:**<br>مرور کلی محصول باید نوع محصول را شناسایی کند. |
| | **نام عنصر: معرفی هدف امنیتی ۶**<br>**شماره مؤلفه: (ASE_INT.1.6C)**<br>**شرح مؤلفه:**<br>مرور کلی محصول باید هرگونه سخت‌افزار، نرم‌افزار و میان‌افزار به غیر از محصول را که مورد نیاز آن است شناسایی کند. |
| | **نام عنصر: معرفی هدف امنیتی ۷**<br>**شماره مؤلفه: (ASE_INT.1.7.C)**<br>**شرح مؤلفه:**<br>شرح محصول، باید دامنه فیزیکی محصول را توصیف کند |

| مؤلفه‌های محتوایی و ارائه | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: معرفی هدف امنیتی ۸**<br>**شماره مؤلفه: (ASE_INT.1.8C)**<br>**شرح مؤلفه:**<br>شرح محصول ، باید دامنه منطقی محصول را توصیف کند. |
| **مؤلفه‌های اقدامات ارزیاب** | |
| **نام خانواده** | **عنصر امنیتی** |
| معرفی هدف امنیتی **(ASE_INT)** | **نام عنصر: معرفی هدف امنیتی ۱**<br>**شماره مؤلفه: (ASE_INT.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تصدیق کند که اطلاعات فراهم شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |
| | **نام عنصر: معرفی هدف امنیتی ۱**<br>**شماره مؤلفه: (ASE_INT.1.2E)** |

| مؤلفه‌های محتوایی و ارائه | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **شرح مؤلفه:**<br><br>ارزیاب باید تصدیق کند که مرجع محصول، مرور کلی محصول و توصیف محصول با یکدیگر سازگار هستند. |

**۷-۱-۴-اهداف امنیتی (ASE_OBJ.2)**

**وابستگی: ASE_SPD.1** تعریف مسئله امنیتی

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| اهداف امنیتی (**ASE_OBJ**) | **نام عنصر: اهداف امنیتی ۱**<br><br>**شماره مؤلفه: (ASE_OBJ.2.1D)**<br><br>**شرح مؤلفه:**<br><br>توسعه‌دهنده باید بیانیه‌ای از اهداف امنیتی ارائه دهد. |
| | **نام عنصر: اهداف امنیتی ۲**<br><br>**شماره مؤلفه: (ASE_OBJ.2.2D)** |

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **شرح مؤلفه:**<br><br>توسعه‌دهنده باید یک منطقی برای اهداف امنیتی ارائه دهد. |

| مؤلفه‌های اقدامات محتوایی و ارائه | | |
|---|---|---|
| **نام خانواده** | **عنصر امنیتی** | |
| اهداف امنیتی<br>(**ASE_OBJ**) | **نام عنصر: اهداف امنیتی ۱**<br><br>**شماره مؤلفه: (ASE_OBJ.2.1C)**<br><br>**شرح مؤلفه:**<br><br>بیانیه اهداف امنیتی باید اهداف امنیتی محصول و اهداف امنیتی محیط عملیاتی را توضیح دهد. | |
| | **نام عنصر: اهداف امنیتی ۲**<br><br>**شماره مؤلفه: (ASE_OBJ.2.2C)**<br><br>**شرح مؤلفه:** | |

| مؤلفه‌های اقدامات محتوایی و ارائه | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | منطق اهداف امنیتی باید هر هدف امنیتی برای محصول را تا تهدیدات مقابله شده با آن هدف امنیتی و خط‌مشی‌های امنیت سازمانی (OSP) اعمال شده توسط این اهداف امنیتی ردیابی کند. |
| | **نام عنصر: اهداف امنیتی ۳**<br>**شماره مؤلفه: (ASE_OBJ.2.3C)**<br>**شرح مؤلفه:**<br>منطق اهداف امنیتی، باید هر هدف امنیتی برای محیط عملیاتی را تا تهدیدات مقابله شده با آن هدف امنیتی و خط‌مشی‌های امنیت سازمانی (OSP) اعمال شده توسط این اهداف امنیتی ردیابی کند. |
| | **نام عنصر: اهداف امنیتی ۴**<br>**شماره مؤلفه: (ASE_OBJ.2.4C)**<br>**شرح مؤلفه:**<br>منطق اهداف امنیتی باید نشان دهد که اهداف امنیتی با تمام تهدیدات مقابله می‌کنند. |
| | **نام عنصر: اهداف امنیتی ۵** |

| مؤلفه‌های اقدامات محتوایی و ارائه | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **شماره مؤلفه: (ASE_OBJ.2.5C)**<br><br>**شرح مؤلفه:**<br><br>منطق اهداف امنیتی باید نشان دهد که اهداف امنیتی همه‌ی خط‌مشی‌های امنیت سازمانی (OSP) را به کار می‌برند. |
| | **نام عنصر: اهداف امنیتی ۶**<br><br>**شماره مؤلفه: (ASE_OBJ.2.6C)**<br><br>**شرح مؤلفه:**<br><br>منطق اهداف امنیتی باید نشان دهد که اهداف امنیتی برای محیط عملیاتی همه‌ی مفروضات را مورد حمایت قرار می‌دهد. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| اهداف امنیتی (**ASE_OBJ**) | **نام عنصر: اهداف امنیتی ۱**<br>**شماره مؤلفه: (ASE_OBJ.2.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

**۷-۱-۵-الزامات امنیتی استنتاج شده (ASE_REQ.2)**

**وابستگی:**

ASE_OBJ.2 اهداف امنیتی

ASE_ECD.1 تعریف مؤلفه‌های توسعه یافته

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| الزامات امنیتی استنتاج شده **(ASE_REQ)** | **نام عنصر: الزامات امنیتی استنتاج شده ۱**<br>**شماره مؤلفه: (ASE_REQ.2.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید بیانیه‌ای از الزامات امنیتی ارائه دهد. |
| | **نام عنصر: الزامات امنیتی استنتاج شده ۲**<br>**شماره مؤلفه: (ASE_REQ.2.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید منطقی برای الزامات امنیتی فراهم آورد. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| الزامات امنیتی استنتاج شده (**ASE_REQ**) | **نام عنصر: الزامات امنیتی استنتاج شده ۱**<br>**شماره مؤلفه: (ASE_REQ.2.1C)**<br>**شرح مؤلفه:**<br>بیانیه‌ی الزامات امنیتی باید الزامات کارکرد امنیتی و الزامات تضمین امنیتی را توضیح دهند. |
| | **نام عنصر: الزامات امنیتی استنتاج شده ۲**<br>**شماره مؤلفه: (ASE_REQ.2.2C)**<br>**شرح مؤلفه:**<br>تمامی موجودیت‌های فعال، موجودیت‌های غیر فعال، عملیات، مشخصه‌های امنیتی، موجودیت‌های بیرونی و اصطلاحات دیگری که در الزامات کارکرد امنیتی و الزامات تضمین امنیتی استفاده شده‌اند باید تعریف شود. |
| | **نام عنصر: الزامات امنیتی استنتاج شده ۳**<br>**شماره مؤلفه: (ASE_REQ.2.3C)**<br>**شرح مؤلفه:** |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | بیانیه‌ی الزامات امنیتی، باید تمامی عملیات بر روی الزامات امنیتی را مشخص کند. |
| | **نام عنصر: الزامات امنیتی استنتاج شده ۴**<br>**شماره مؤلفه: (ASE_REQ.2.4C)**<br>**شرح مؤلفه:**<br>تمامی عملیات باید به درستی انجام پذیرد. |
| | **نام عنصر: الزامات امنیتی استنتاج شده ۵**<br>**شماره مؤلفه: (ASE_REQ.2.5C)**<br>**شرح مؤلفه:**<br>هر وابستگی از الزامات امنیتی، یا باید برآورده شده باشد یا منطق الزامات امنیتی باید استدالالی برای وابستگی‌هایی که برآورده نشده‌اند ارائه دهد. |
| | **نام عنصر: الزامات امنیتی استنتاج شده ۶**<br>**شماره مؤلفه: (ASE_REQ.2.6C)** |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **شرح مؤلفه:**<br><br>منطق الزامات امنیتی باید هر الزام کارکرد امنیتی را تا اهداف امنیتی محصول ردیابی کند. |
| | **نام عنصر: الزامات امنیتی استنتاج شده ۷**<br><br>**شماره مؤلفه: (ASE_REQ.2.7C)**<br><br>**شرح مؤلفه:**<br><br>منطق الزامات امنیتی باید نشان دهد که الزامات کارکرد امنیتی همه‌ی اهداف امنیتی محصول را برآورده می‌سازد. |
| | **نام عنصر: الزامات امنیتی استنتاج شده ۸**<br><br>**شماره مؤلفه: (ASE_REQ.2.8C)**<br><br>**شرح مؤلفه:**<br><br>منطق الزامات امنیتی باید توضیح دهد که چرا الزامات تضمین امنیتی انتخاب شده‌اند. |
| | **نام عنصر: الزامات امنیتی استنتاج شده ۹**<br><br>**شماره مؤلفه: (ASE_REQ.2.9C)** |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **شرح مؤلفه:**<br><br>بیانیه‌ی الزامات امنیتی باید سازگاری داخلی داشته باشند. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| الزامات امنیتی استنتاج شده **(ASE_REQ)** | **نام عنصر: الزامات امنیتی استنتاج شده ۲**<br>**شماره مؤلفه: (ASE_REQ.2.1E)**<br>**شرح مؤلفه:**<br><br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

**۷-۱-۶- تعریف مسئله امنیتی (ASE_SPD.1)**

**وابستگی:** بدون وابستگی

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| تعریف مسئله امنیتی **(ASE_SPD)** | **نام عنصر: تعریف مسئله امنیتی ۱**<br>**شماره مؤلفه: (ASe_SPD.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید یک تعریف برای مسئله امنیتی فراهم کند. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| تعریف مسئله امنیتی **(ASE_SPD)** | **نام عنصر: تعریف مسئله امنیتی ۱**<br>**شماره مؤلفه: (ASE_SPD.1.1C)**<br>**شرح مؤلفه:**<br>تعریف مسئله‌ی امنیتی، باید تهدیدات را توصیف کند. |
| | **نام عنصر: تعریف مسئله امنیتی ۲** |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **شماره مؤلفه: (ASE_SPD.1.2C)**<br><br>**شرح مؤلفه:**<br><br>تمامی تهدیدات باید از دیدگاه یک عامل تهدید، یک دارایی، و یک اقدام مقابله‌ای توصیف شوند. |
| | **نام عنصر: تعریف مسئله امنیتی ۳**<br><br>**شماره مؤلفه: (ASE_SPD.1.3C)**<br><br>**شرح مؤلفه:**<br><br>تعریف مسئله امنیتی، باید خط‌مشی‌های امنیت سازمانی (OSP) را توصیف کند. |
| | **نام عنصر: تعریف مسئله امنیتی ۴**<br><br>**شماره مؤلفه: (ASE_SPD.1.4C)**<br><br>**شرح مؤلفه:**<br><br>تعریف مسئله امنیتی باید مفروضاتی را درباره‌ی محیط عملیاتی محصول بیان کند. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| تعریف مسئله امنیتی **(ASE_SPD)** | **نام عنصر: تعریف مسئله امنیتی ۱**<br>**شماره مؤلفه: (ASE_SPD.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

### ۷-۱-۷-خلاصه مشخصات محصول (ASE_TSS.1)

**وابستگی:**

ASE_INT.1، معرفی هدف امنیتی

ASE_REQ.1، الزامات امنیتی بیان شده

ADV_FSP.1، مشخصات کارکردی اساسی

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| خلاصه مشخصات محصول (**ASE_TSS**) | **نام عنصر: خلاصه مشخصات محصول ۱**<br>**شماره مؤلفه: (ASE_TSS.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید خلاصه‌ای از مشخصات محصول را ارائه دهد. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| خلاصه مشخصات محصول (**ASE_TSS**) | **نام عنصر: خلاصه مشخصات محصول ۱**<br>**شماره مؤلفه: (ASE_TSS.1.1C)**<br>**شرح مؤلفه:**<br>خلاصه مشخصات محصول باید توضیح دهد که چگونه محصول هر الزام کارکرد امنیتی را براورده می‌سازد. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| خلاصه مشخصات محصول (ASE_TSS) | **نام عنصر: خلاصه مشخصات محصول ۱**<br>**شماره مؤلفه: (ASE_TSS.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |
| | **نام عنصر: خلاصه مشخصات محصول ۲**<br>**شماره مؤلفه: (ASE_TSS.1.2E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تأیید کند که خلاصه مشخصات محصول با مرور کلی خلاصه مشخصات محصول و توضیحات خلاصه مشخصات محصول سازگار است. |

### ۷-۲- کلاس توسعه (ADV)

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 ناست، اما در صورت وجود باید محتوای آن با الزمات کارکردی مرتبط بوده و مورد تائید توسعه دهندگان محصول باشد.

**۷-۲-۱-شرح معماری امنیتی (ADV_ARC.1)**

**وابستگی:**

ADV_FSP.1، مشخصات کارکردی پایه‌ای

ADV_TDS.1، طراحی پایه‌ای

| **مؤلفه‌های اقدامات توسعه دهنده** | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| شرح معماری امنیتی (ADV_ARC) | **نام عنصر: شرح معماری امنیتی ۱**<br>**شماره مؤلفه: (ADV_ARC.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید محصول را به گونه‌ای طراحی و پیاده‌سازی کند که مشخصه‌های امنیتی توابع هدف امنیتی (TSF) قابل دور زدن نباشد. |
| | **نام عنصر: شرح معماری امنیتی ۲**<br>**شماره مؤلفه: (ADV_ARC.1.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهندهباید محصول را به گونه‌ای طراحی و پیاده‌سازی کند که تا بتواند از خود در مقابل دستکاری توسط موجودیت‌های فعال نامطمئن حفاظت کند. |

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: شرح معماری امنیتی ۳**<br>**شماره مؤلفه: (ADV_ARC.1.3D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید توصیفی از معماری امنیتی توابع هدف امنیتی (TSF) ارائه دهد. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| شرح معماری امنیتی (**ADV_ARC**) | **نام عنصر: شرح معماری امنیتی ۱**<br>**شماره مؤلفه: (ADV_ARC.1.1C)**<br>**شرح مؤلفه:**<br>شرح معماری امنیتی باید در سطحی از جزئیات همراه با توصیف خلاصه‌های اعمال کننده الزامات کارکرد امنیتی توضیح داده شده در سند طراحی محصول باشد. |
| | **نام عنصر: شرح معماری امنیتی ۱** |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **شماره مؤلفه: (ADV_ARC.1.2C)**<br><br>**شرح مؤلفه:**<br><br>شرح معماری امنیتی، باید دامنه‌های امنیتی حفظ شده توسط توابع هدف امنیتی (TSF) سازگار با الزامات کارکرد امنیتی را توضیح دهد. |
| | **نام عنصر: شرح معماری امنیتی ۱**<br><br>**شماره مؤلفه: (ADV_ARC.1.3C)**<br><br>**شرح مؤلفه:**<br><br>شرح معماری امنیتی باید توضیح دهد که چگونه فرایند مقداردهی اولیه توابع هدف امنیتی (TSF) امن است. |
| | **نام عنصر: شرح معماری امنیتی ۱**<br><br>**شماره مؤلفه: (ADV_ARC.1.4C)**<br><br>**شرح مؤلفه:**<br><br>شرح معماری امنیتی باید نشان دهد که توابع هدف امنیتی (TSF) از خودش در مقابل دستکاری محافظت می‌کند. |
| | **نام عنصر: شرح معماری امنیتی ۱** |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **شماره مؤلفه: (ADV_ARC.1.5C)**<br><br>**شرح مؤلفه:**<br><br>شرح معماری امنیتی باید نشان دهد که توابع هدف امنیتی (TSF) از دور زدن قابلیت‌های کارکردی اعمال کننده الزامات کارکرد امنیتی جلوگیری می‌کند. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| شرح معماری امنیتی **(ADV_ARC)** | **نام عنصر: شرح معماری امنیتی ۱**<br>**شماره مؤلفه: (ADV_ARC.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

### ۷-۲-۲- مشخصات کارکردی کامل (ADV_FSP.4 )

**وابستگی:** **ADV_TDS.1**، طراحی پایه‌ای

| **مؤلفه‌های اقدامات توسعه دهنده** | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| مشخصات کارکردی کامل (**ADV_FSP**) | **نام عنصر: مشخصات کارکردی کامل ۱**<br>**شماره مؤلفه: (ADV_FSP.4.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید مشخصات کارکردی ارائه دهد. |
| | **نام عنصر: مشخصات کارکردی کامل ۲**<br>**شماره مؤلفه: (ADV_FSP.4.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید یک ردیابی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه دهد. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| مشخصات کارکردی کامل (**ADV_FSP**) | **نام عنصر: مشخصات کارکردی کامل ۱**<br>**شماره مؤلفه: (ADV_FSP.4.1C)**<br>**شرح مؤلفه:**<br>مشخصات کارکردی باید به طور کامل توابع هدف امنیتی را نشان دهد. |
| | **نام عنصر: مشخصات کارکردی کامل ۲**<br>**شماره مؤلفه: (ADV_FSP.4.2C)**<br>**شرح مؤلفه:**<br>مشخصات کارکردی باید هدف و روش استفاده را برای تمامی TSFIها توصیف کند. |
| | **نام عنصر: مشخصات کارکردی کامل ۳**<br>**شماره مؤلفه: (ADV_FSP.4.3C)**<br>**شرح مؤلفه:**<br>مشخصات کارکردی باید تمامی پارامترهای مربوط به TSFI شناسایی و توصیف کند. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: مشخصات کارکردی کامل ۴**<br><br>**شماره مؤلفه: (ADV_FSP.4.4C)**<br><br>**شرح مؤلفه:**<br><br>مشخصات کارکردی باید تمامی اقدامات مربوط به هر TSFI را توصیف کند. |
| | **نام عنصر: مشخصات کارکردی کامل ۵**<br><br>**شماره مؤلفه: (ADV_FSP.4.5C)**<br><br>**شرح مؤلفه:**<br><br>مشخصات کارکردی باید تمام پیام‌های خطای مستقیم که ممکن است منجر به فراخوانی هر TSFI شود، را توصیف کند. |
| | **نام عنصر: مشخصات کارکردی کامل ۶**<br><br>**شماره مؤلفه: (ADV_FSP.4.6C)**<br><br>**شرح مؤلفه:**<br><br>ردیابی باید نشان دهد که الزامات کارکرد امنیتی تا TSFIها در مشخصات کارکردی ردگیری می‌شود. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| مشخصات کارکردی کامل (**ADV_FSP**) | **نام عنصر: مشخصات کارکردی کامل ۱**<br>**شماره مؤلفه: (ADV_FSP.4.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |
| | **نام عنصر: مشخصات کارکردی کامل ۲**<br>**شماره مؤلفه: (ADV_FSP.4.2E)**<br>**شرح مؤلفه:**<br>ارزیاب باید مشخص کند که مشخصات کارکردی نمونه‌ی کامل و دقیقی از الزامات کارکرد امنیتی است. |

### ۷-۲-۳- نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی (TSF) (ADV_IMP.2)

**وابستگی:**

ADV_TDS.3، طراحی پیمانه‌ای پایه‌ای

ALC_TAT.1، ابزار توسعه به خوبی تعریف شده

ALC_CMC.5، پشتیبانی پیشرفته

| **مؤلفه‌های اقدامات توسعه دهنده** | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی (**ADV_IMP**) | **نام عنصر: نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی ۱**<br>**شماره مؤلفه: (ADV_IMP.2.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید مشخصات کارکردی ارائه دهد. |
| | **نام عنصر: نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی ۲**<br>**شماره مؤلفه: (ADV_IMP.2.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید نگاشتی بین توصیف طراحی محصول و همه‌ی بازنمایی پیاده‌سازی ارائه دهد. |

| **مؤلفه‌های اقدامات محتوایی** | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی (**ADV_IMP**) | **نام عنصر: نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی ۱**<br>**شماره مؤلفه: (ADV_IMP.2.1.C)**<br>**شرح مؤلفه:**<br>بازنمایی پیاده‌سازی باید توابع هدف امنیتی (TSF) را با سطحی از جزئیات تعریف کنند تا توابع هدف امنیتی (TSF) بتواند بدون تصمیمات طراحی بیشتر تولید شود. |
| | **نام عنصر: نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی ۲**<br>**شماره مؤلفه: (ADV_IMP.2.2.C)**<br>**شرح مؤلفه:**<br>بازنمایی پیاده‌سازی باید در قالب استفاده شده توسط پرسنل توسعه باشد. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی۳**<br>**شماره مؤلفه: (ADV_IMP.2.3.C)**<br>**شرح مؤلفه:**<br>نگاشت بین توضیحات طراحی محصول و کل بازنمایی پیاده‌سازی باید تناظر بین آن‌ها را بیان کند. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی **(ADV_IMP)** | **نام عنصر: نگاشت کامل بازنمایی پیاده‌سازی توابع هدف امنیتی ۱**<br>**شماره مؤلفه: (ADV_IMP.2.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تأیید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

### ۷-۲-۴- طراحی پیمانه‌ای[۳۶] پایه‌ای (ADV_TDS.3)

**وابستگی:** **ADV_FSP.4**، مشخصات کارکردی کامل

| **مؤلفه‌های اقدامات توسعه دهنده** | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| طراحی پیمانه‌ای پایه‌ای (**ADV_TDS**) | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۱**<br>**شماره مؤلفه: (ADV_TDS.3.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید طراحی از محصول ارائه دهد. |
| | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۲**<br>**شماره مؤلفه: (ADV_TDS.3.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید نگاشتی از TSFI مشخصات کارکردی به به پایین‌ترین سطح تجزیه‌ی موجود در طراحی هدف ارزیابی ارائه دهد. |

| **مؤلفه‌های اقدامات محتوایی** |
|---|

[۳۶] modular

| نام خانواده | عنصر امنیتی |
| --- | --- |
| طراحی پیمانه‌ای پایه‌ای (**ADV_TDS**) | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۱**<br>**شماره مؤلفه: (ADV_TDS.3.1C)**<br>**شرح مؤلفه:**<br>طراحی باید ساختار محصول را از دیدگاه زیر سیستم‌ها توصیف کند. |
| | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۲**<br>**شماره مؤلفه: (ADV_TDS.3.2C)**<br>**شرح مؤلفه:**<br>طراحی باید توابع هدف امنیتی (TSF) را از دیدگاه پیمانه[۳۷]ها توصیف کند. |
| | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۳**<br>**شماره مؤلفه: (ADV_TDS.3.3C)**<br>**شرح مؤلفه:**<br>طراحی باید تمام زیرسیستم‌های توابع هدف امنیتی (TSF) را شناسایی کند. |

[۳۷] module

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۴**<br><br>**شماره مؤلفه: (ADV_TDS.3.4C)**<br><br>**شرح مؤلفه:**<br><br>طراحی باید شرحی از هر یک از زیرسیستم‌های توابع هدف امنیتی (TSF) ارائه دهد. |
| | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۵**<br><br>**شماره مؤلفه: (ADV_TDS.3.5C)**<br><br>**شرح مؤلفه:**<br><br>طراحی باید توصیفی از تعاملات میان همه‌ی زیرسیستم‌های توابع هدف امنیتی (TSF) ارائه دهد. |
| | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۶**<br><br>**شماره مؤلفه: (ADV_TDS.3.6C)**<br><br>**شرح مؤلفه:**<br><br>طراحی باید نگاشتی از زیرسیستم توابع هدف امنیتی (TSF) به پیمانه‌های توابع هدف امنیتی (TSF) ارائه دهد. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۷**<br>**شماره مؤلفه: (ADV_TDS.3.7C)**<br>**شرح مؤلفه:**<br>طراحی باید هر پیمانه‌ی اجرا کننده الزامات کارکرد امنیتی را از دیدگاه هدف و ارتباط با پیمانه‌های دیگر توصیف کند. |
| | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۸**<br>**شماره مؤلفه: (ADV_TDS.3.8C)**<br>**شرح مؤلفه:**<br>طراحی باید هر پیمانه‌ی اجرا کننده الزامات کارکرد امنیتی را از دیدگاه واسط‌های مرتبط با الزامات کارکرد امنیتی، مقادیر بازگشتی از این واسط‌ها، تعاملات با دیگر پیمانه‌ها و واسط‌های مرتبط با الزامات کارکرد امنیتیی فراخوانی شده به دیگر پیمانه های اجرا کننده الزامات کارکرد امنیتی را توصیف کند. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۹**<br>**شماره مؤلفه: (ADV_TDS.3.9C)**<br>**شرح مؤلفه:**<br>طراحی باید هر پیمانه‌ی پشتیبانی کننده از الزامات کارکرد امنیتی یا الزامات کارکرد امنیتی غیر مداخله کننده را از دیدگاه هدف و تعامل با دیگر پیمانه‌ها توصیف کند. |
| | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۱۰**<br>**شماره مؤلفه: (ADV_TDS.3.10C)**<br>**شرح مؤلفه:**<br>نگاشت باید تمام ردیابی‌های TSFIها را به رفتار توصیف شده در طراحی محصول که آن‌ها فراخوانی می‌کنند نشان دهد. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| طراحی پیمانه‌ای پایه‌ای (**ADV_TDS**) | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۱**<br>**شماره مؤلفه: (ADV_TDS.3.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |
| | **نام عنصر: طراحی پیمانه‌ای پایه‌ای ۲**<br>**شماره مؤلفه: (ADV_TDS.3.2E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تعیین کند که طراحی نمونه‌ای دقیق و کامل از همه‌ی الزامات کارکرد امنیتی است. |

### ۷-۳- مستندات راهنما (AGD)

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 سیستم (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 و راه‌اندازی موفقیت آمیز محصول در محیط
- دستورالعمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگتر
- دستورالعمل‌هایی که ارائه دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو است.

**۷-۳-۱-راهنمای کاربری (AGD_OPE.1)**

**وابستگی: ADV_FSP.1** مشخصات کارکردی پایه‌ای

| **مؤلفه‌های اقدامات توسعه دهنده** | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| راهنمای کاربری (**AGD_OPE**) | **نام عنصر: راهنمای کاربری ۱**<br>**شماره مؤلفه: (ADV_TDS.3.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید راهنمای کاربری را فراهم آورد. |

| **مؤلفه‌های اقدامات محتوایی** | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| راهنمای کاربری (**AGD_OPE**) | **نام عنصر: راهنمای کاربری ۱**<br>**شماره مؤلفه: (AGD_OPE.1.1C)**<br>**شرح مؤلفه:**<br>راهنمای کاربری باید برای هر نقش کاربری، توابع قابل دسترس کاربر و امتیازات ویژه‌ای که باید در محیط پردازشی امن کنترل شود از جمله هشدارهای مناسب را توصیف کند. |
| | **نام عنصر: راهنمای کاربری ۲**<br>**شماره مؤلفه: (AGD_OPE.1.2C)**<br>**شرح مؤلفه:**<br>راهنمای کاربری باید برای هر نقش کاربری توضیح دهد که چگونه از واسط‌های موجود فراهم شده توسط محصول به روش امنی استفاده کنند. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: راهنمای کاربری ۳**<br>**شماره مؤلفه: (AGD_OPE.1.3C)**<br>**شرح مؤلفه:**<br>راهنمای کاربری باید برای هر نقش کاربری توابع و واسطهای در دسترس را به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر نشان دهنده‌ی مقادیر امن مناسب، توضیح دهد. |
| | **نام عنصر: راهنمای کاربری۴**<br>**شماره مؤلفه: (AGD_OPE.1.4C)**<br>**شرح مؤلفه:**<br>راهنمای کاربری باید برای هر نقش کاربر، به وضوح انواع رویدادهای مرتبط با امنیت مربوط به توابع قابل دسترس کاربر را که لازم است انجام شود از جمله تغییر مشخصه‌های امنیتی موجودیت‌ها تحت کنترل توابع هدف امنیتی (TSF) تعریف کند. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: راهنمای کاربری ۵**<br><br>**شماره مؤلفه: (AGD_OPE.1.5C)**<br><br>**شرح مؤلفه:**<br><br>راهنمای کاربری باید تمامی مدهای ممکن از عملکرد محصول (از جمله عملیات دنبال کننده خرابی یا خطای عملیاتی)، عواقب و پیامدهای آن‌ها را جهت حفظ عملیات امن شناسایی کند. |
| | **نام عنصر: راهنمای کاربری ۶**<br><br>**شماره مؤلفه: (AGD_OPE.1.6C)**<br><br>**شرح مؤلفه:**<br><br>راهنمای کاربری باید برای هر نقش کاربر، اقدامات امنیتی را که باید برای برآوردن اهداف امنیتی برای محیط عملیاتی که در هدف امنیتی توضیح داده‌شده است دنبال شود توضیح دهد. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: راهنمای کاربری ۷**<br>**شماره مؤلفه: (AGD_OPE.1.7C)**<br>**شرح مؤلفه:**<br>راهنمای کاربری باید واضح و منطق‌پذیر باشد. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| راهنمای کاربری (**AGD_OPE**) | **نام عنصر: راهنمای کاربری ۱**<br>**شماره مؤلفه: (AGD_OPE.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

**۷-۳-۲- راهنمای آماده‌سازی (AGD_PRE.1)**

**وابستگی:** بدون وابستگی

**مؤلفه‌های اقدامات توسعه دهنده**

| نام خانواده | عنصر امنیتی |
|---|---|
| راهنمای آماده‌سازی (**AGD_PRE**) | **نام عنصر: راهنمای آماده‌سازی ۱**<br>**شماره مؤلفه: (AGD_PRE.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید محصول را با راهنمای آماده‌سازی‌اش فراهم آورد. |

**مؤلفه‌های اقدامات محتوایی**

| نام خانواده | عنصر امنیتی |
|---|---|
| راهنمای آماده‌سازی (AGD_PRE) | **نام عنصر: راهنمای آماده‌سازی ۱**<br>**شماره مؤلفه: (AGD_PRE.1.1C)**<br>**شرح مؤلفه:**<br>راهنمای آماده‌سازی باید تمام گام‌های لازم برای پذیرش امن محصول تحویل داده شده مطابق با روش‌های اجرایی تحویل توسعه‌دهنده را شرح دهد. |

| نام خانواده | عنصر امنیتی |
| --- | --- |
| | **نام عنصر: راهنمای آماده‌سازی ۲**<br>**شماره مؤلفه: (AGD_PRE.1.2C)**<br>**شرح مؤلفه:**<br>روندهای مقدماتی باید تمام مراحل لازم برای نصب و راه‌اندازی امن محصول و آماده‌سازی امن محیط عملیاتی مطابق با اهداف امنیتی محیط عملیاتی توصیف شده در هدف امنیتی را شرح دهد |
| **مؤلفه‌های اقدامات ارزیاب** | |
| **نام خانواده** | **عنصر امنیتی** |
| راهنمای آماده‌سازی **(AGD_PRE)** | **نام عنصر: راهنمای آماده‌سازی ۱**<br>**شماره مؤلفه: (AGD_PRE.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تائید کند که اطلاعات ارائه شده تمام الزامات محتوا و ارائه شواهد را فراهم می‌آورد. |
| | **نام عنصر: راهنمای آماده‌سازی ۲**<br>**شماره مؤلفه: (AGD_PRE.1.2E)** |

| نام خانواده | عنصر امنیتی |
| --- | --- |
| | **شرح مؤلفه:**<br><br>ارزیاب باید راهنمای آماده‌سازی را به کار برد تا تائید کند که محصول می‌تواند به صورت امنی برای عملیات آماده شود. |

**۷-۴- پشتیبانی چرخه حیات (ALC)**

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

**۷-۴-۱-پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی (ALC_CMC.4)**

**وابستگی:**

ALC_CMS.1، پوشش CM محصول

ALC_DVS.1، شناسایی اقدامات امنیتی

ALC_LCD.1، اهداف مدل چرخه حیات تعریف شده توسط توسعه‌دهنده

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی (**ALC_CMC**) | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۱**<br>**شماره مؤلفه: (ALC_CMC.4.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید محصول و یک مرجع برای محصول ارائه دهد. |
| | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۲**<br>**شماره مؤلفه: (ALC_CMC.4.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید اسناد و مدارک CM را فراهم آورد. |
| | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۳**<br>**شماره مؤلفه: (ALC_CMC.4.3D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید از یک سیستم CM استفاده کند. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی (**ALC_CMC**) | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۱**<br>**شماره مؤلفه: (ALC_CMC.4.1C)**<br>**شرح مؤلفه:**<br>محصول باید مرجع منحصربفرد خودش برچسب‌گذاری شود. |
| | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۲**<br>**شماره مؤلفه: (ALC_CMC.4.2C)**<br>**شرح مؤلفه:**<br>اسناد و مدارک CM، باید روش استفاده شده برای شناسایی منحصر به فرد اقلام پیکربندی را توصیف کند. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| نام خانواده | عنصر امنیتی |
| | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۳**<br>**شماره مؤلفه: (ALC_CMC.4.3C)**<br>**شرح مؤلفه:**<br>سیستم CM باید تمامی اقلام پیکربندی را به شکل منحصربفردی شناسایی کند. |
| | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۴**<br>**شماره مؤلفه: (ALC_CMC.4.4C)**<br>**شرح مؤلفه:**<br>سیستم CM باید اقدامات خودکاری را فراهم آورد تا تنها تغییرات مجاز در اقلام پیکربندی ایجاد شود. |
| | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۵**<br>**شماره مؤلفه: (ALC_CMC.4.5C)**<br>**شرح مؤلفه:**<br>سیستم CM باید از تولید محصول با ابزار خودکار پشتیبانی کند. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| نام خانواده | عنصر امنیتی |
| | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۶**<br>**شماره مؤلفه: (ALC_CMC.4.6C)**<br>**شرح مؤلفه:**<br>اسناد CM باید شامل طرح CM نیز باشد.. |
| | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۷**<br>**شماره مؤلفه: (ALC_CMC.4.7C)**<br>**شرح مؤلفه:**<br>طرح CM توضیح دهد که چگونه سیستم CM برای توسعه محصول به کار گرفته می‌شود. |
| | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۸**<br>**شماره مؤلفه: (ALC_CMC.4.8C)**<br>**شرح مؤلفه:**<br>طرح CM باید روش‌های اجرایی مورد استفاده برای پذیرش تغییر یا اقلام پیکربندی جدید به عنوان قسمتی از محصول را توصیف کند. |

| مؤلفه‌های اقدامات محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۹**<br>**شماره مؤلفه: (ALC_CMC.4.9C)**<br>**شرح مؤلفه:**<br>شواهد باید نشان دهد که همه‌ی اقلام پیکربندی، تحت سیستم CM نگهداری می‌شوند. |
| | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۱۰**<br>**شماره مؤلفه: (ALC_CMC.4.10C)**<br>**شرح مؤلفه:**<br>شواهد باید نشان دهد که سیستم CM مطابق طرح CM به کار گرفته می‌شود. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| پشتیبانی از تولید، | **نام عنصر: پشتیبانی از تولید، روش‌های اجرایی پذیرش و خودکارسازی ۱** |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| روش‌های اجرایی پذیرش و خودکارسازی (**ALC_CMC**) | **شماره مؤلفه: (ALC_CMC.4.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد |

### ۷-۴-۲- پوشش CMردیابی مسئله (ALC_CMS.4)

**وابستگی:** بدون وابستگی

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| پوشش CMردیابی مسئله (**ALC_CMS**) | **نام عنصر: پوشش CMردیابی مسئله ۱**<br>**شماره مؤلفه: (ALC_CMS.4.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید فهرست پیکربندی محصول را فراهم آورد. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| پوشش CMردیابی مسئله (**ALC_CMS**) | **نام عنصر: پوشش CMردیابی مسئله ۱**<br>**شماره مؤلفه: (ALC_CMS.4.1C)**<br>**شرح مؤلفه:**<br>فهرست پیکربندی باید شامل موارد زیر باشد: خود محصول، شواهد ارزیابی مورد نیاز الزامات تضمین امنیت، قسمت‌هایی که محصول را تشکیل می‌دهند، بازنمایی پیاده‌سازی، گزارش نقص امنیتی و وضعیت رفع مشکل. |
| | **نام عنصر: پوشش CMردیابی مسئله ۲**<br>**شماره مؤلفه: (ALC_CMS.4.2C)**<br>**شرح مؤلفه:**<br>فهرست پیکربندی باید برای اقلام پیکربندی را به شکل منحصر بفردی شناسایی کند. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: پوشش CMردیابی مسئله ۳**<br>**شماره مؤلفه: (ALC_CMS.4.3C)**<br>**شرح مؤلفه:**<br>برای هر اقلام پیکربندی مرتبط با توابع هدف امنیتی، فهرست پیکربندی باید توسعه‌دهنده آیتم را نشان دهد. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| پوشش CMردیابی مسئله (**ALC_CMS**) | **نام عنصر: پوشش CMردیابی مسئله ۱**<br>**شماره مؤلفه: (ALC_CMC.4.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

**۷-۴-۳- روش‌های اجرایی تحویل (ALC_DEL.1)**

**وابستگی:** بدون وابستگی

| **مؤلفه‌های اقدامات توسعه دهنده** | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| روش‌های اجرایی تحویل (**ALC_DEL**) | **نام عنصر: روش‌های اجرایی تحویل ۱**<br>**شماره مؤلفه: (ALC_DEL.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده، باید روش‌های اجرایی برای تحویل محصول یا قسمت‌هایی از آن را برای مصرف کننده مستند کرده و ارائه دهد. |
| | **نام عنصر: روش‌های اجرایی تحویل ۲**<br>**شماره مؤلفه: (ALC_DEL.1.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید از روش‌های اجرایی تحویل استفاده کند. |

| **مؤلفه‌های محتوایی** | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| روش‌های اجرایی تحویل (**ALC_DEL**) | **نام عنصر: روش‌های اجرایی تحویل ۱**<br>**شماره مؤلفه: (ALC_DEL.1.1C)**<br>**شرح مؤلفه:**<br>مستندات تحویل باید تمام روش‌های اجرایی را که برای حفظ امنیت در هنگام توزیع نسخه محصول به مصرف‌کننده ضروری است توضیح دهد. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| روش‌های اجرایی تحویل (**ALC_DEL**) | **نام عنصر: روش‌های اجرایی تحویل ۱**<br>**شماره مؤلفه: (ALC_DEL.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

### ۷-۴-۴- شناسایی اقدامات امنیتی (ALC_DVS.1)

**وابستگی:** بدون وابستگی

| **مؤلفه‌های اقدامات توسعه دهنده** | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| شناسایی اقدامات امنیتی (**ALC_DVS**) | **نام عنصر: شناسایی اقدامات امنیتی ۱**<br>**شماره مؤلفه: (ALC_DVS.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید مستندات توسعه امنیت را تولید کرده و ارائه دهد. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| شناسایی اقدامات امنیتی (**ALC_DVS**) | **نام عنصر: شناسایی اقدامات امنیتی ۱**<br>**شماره مؤلفه: (ALC_DVS.1.1C)**<br>**شرح مؤلفه:**<br>مستندات توسعه امنیت باید همه‌ی اقدامات فیزیکی، رویه‌ای، پرسنلی و دیگر اقدامات امنیتی لازم را برای محافظت از محرمانگی و یکپارچگی طراحی و پیاده‌سازی محصول در محیط توسعه‌ای آن توصیح دهد. |
| **مؤلفه‌های اقدامات ارزیاب** | |
| **نام خانواده** | **عنصر امنیتی** |
| شناسایی اقدامات امنیتی (**ALC_DVS**) | **نام عنصر: شناسایی اقدامات امنیتی ۱**<br>**شماره مؤلفه: (ALC_DVS.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |
| | **نام عنصر: شناسایی اقدامات امنیتی ۱** |

| نام خانواده | عنصر امنیتی |
| --- | --- |
| | **شماره مؤلفه: (ALC_DVS.1.2E)**<br><br>**شرح مؤلفه:**<br><br>ارزیاب باید تأیید کند که اقدامات امنیتی به کار گرفته می‌شوند. |

**مدل چرخه حیات تعریف شده توسط توسعه‌دهنده (ALC_LCD.1)**

**وابستگی:** بدون وابستگی

| **مؤلفه‌های اقدامات توسعه دهنده** | |
| --- | --- |
| **نام خانواده** | **عنصر امنیتی** |
| مدل چرخه حیات تعریف شده توسط توسعه‌دهنده (ALC_LCD) | **نام عنصر: مدل چرخه حیات تعریف شده توسط توسعه‌دهنده ۱**<br><br>**شماره مؤلفه: (ALC_LCD.1.1D)**<br><br>**شرح مؤلفه:**<br><br>توسعه‌دهنده باید مدل چرخه حیات را ایجاد کند تا در توسعه و نگهداری از محصول مورد استفاده قرار گیرد. |

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: مدل چرخه حیات تعریف شده توسط توسعه‌دهنده ۲**<br>**شماره مؤلفه: (ALC_LCD.1.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید مستندات تعریف چرخه حیات را ارائه دهد. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| مدل چرخه حیات تعریف شده توسط توسعه‌دهنده (ALC_LCD) | **نام عنصر: مدل چرخه حیات تعریف شده توسط توسعه‌دهنده ۱**<br>**شماره مؤلفه: (ALC_LCD.1.1C)**<br>**شرح مؤلفه:**<br>مستندات تعریف چرخه حیات باید مدل مورد استفاده برای توسعه و حفظ محصول را توصیف کند. |
| | **نام عنصر: مدل چرخه حیات تعریف شده توسط توسعه‌دهنده ۲**<br>**شماره مؤلفه: (ALC_LCD.1.2C)**<br>**شرح مؤلفه:**<br>مدل چرخه حیات باید کنترل لازم بر روی توسعه و نگهداری از محصول را فراهم آورد. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| مدل چرخه حیات تعریف شده توسط توسعه‌دهنده (ALC_LCD) | **نام عنصر: مدل چرخه حیات تعریف شده توسط توسعه‌دهنده ۱**<br>**شماره مؤلفه: (ALC_LCD.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

### ۷-۴-۵- ابزار توسعه‌ی‌خوب تعریف شده (ALC_TAT.1)

**وابستگی:** **ADV_IMP.1** بازنمایی پیاده‌سازی توابع هدف امنیتی (**TSF**)

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| ابزار توسعه‌ی‌خوب تعریف شده (**ALC_TAT**) | **نام عنصر: ابزار توسعه‌ی‌خوب تعریف شده ۱**<br>**شماره مؤلفه: (ALC_TAT.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید مستندات شناسایی کننده‌ی هر ابزار توسعه، که برای محصول استفاده می‌شود را فراهم آورد. |

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: ابزار توسعه‌ی‌خوب تعریف شده ۲**<br>**شماره مؤلفه: (ALC_TAT.1.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید گزینه‌های وابسته به پیاده‌سازی انتخاب شده‌ی هر ابزار توسعه را مستند کرده و ارائه دهد. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| ابزار توسعه‌ی‌خوب تعریف شده **(ALC_TAT)** | **نام عنصر: ابزار توسعه‌ی‌خوب تعریف شده ۱**<br>**شماره مؤلفه: (ALC_TAT.1.1C)**<br>**شرح مؤلفه:**<br>هر ابزار توسعه مورد استفاده در پیاده‌سازی، باید به خوبی تعریف شود. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: ابزار توسعه‌ی‌خوب تعریف شده ۲**<br>**شماره مؤلفه: (ALC_TAT.1.2C)**<br>**شرح مؤلفه:**<br>مستندات هر یک از ابزارهای توسعه، باید معنای تمام جملات و همچنین شرایط و دستورات مورد استفاده در پیاده‌سازی را بدون ابهام تعریف کند. |
| | **نام عنصر: ابزار توسعه‌ی‌خوب تعریف شده ۳**<br>**شماره مؤلفه: (ALC_TAT.1.3C)**<br>**شرح مؤلفه:**<br>مستندات هر یک از ابزارهای توسعه، باید معنای تمام گزینه‌های وابسته به پیاده‌سازی را بدون ابهام تعریف کند. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| ابزار توسعه‌ی-خوب تعریف شده (**ALC_TAT**) | **نام عنصر: ابزار توسعه‌ی‌خوب تعریف شده ۱**<br>**شماره مؤلفه: (ALC_TAT.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

**۷-۵- کلاس آزمون (ATE)**

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

**۷-۵-۱-تحلیل پوشش (ATE_COV.2)**

**وابستگی:**

ADV_FSP.2 مشخصات کارکردی اعمال کننده‌ی امنیت

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| تحلیل پوشش (**ATE_COV**) | **نام عنصر: تحلیل پوشش ۱**<br>**شماره مؤلفه: (ATE_COV.2.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید تحلیلی از پوشش آزمون ارائه دهد. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| تحلیل پوشش (**ATE_COV**) | **نام عنصر: تحلیل پوشش ۱**<br>**شماره مؤلفه: (ATE_COV.2.1C)**<br>**شرح مؤلفه:**<br>تحلیل پوشش آزمون، باید تناظر بین آزمون‌ها در مستندات آزمون و TSFIهای مشخصات کارکردی را نشان دهد. |
| | **نام عنصر: تحلیل پوشش ۲**<br>**شماره مؤلفه: (ATE_COV.2.2C)**<br>**شرح مؤلفه:**<br>تحلیل پوشش آزمون، باید نشان دهد که همه‌ی TSFIها در مشخصات کارکردی مورد آزمون قرار گرفته‌اند. |
| **مؤلفه‌های اقدامات ارزیاب** | |

| نام خانواده | عنصر امنیتی |
| --- | --- |
| تحلیل پوشش (ATE_COV) | **نام عنصر: تحلیل پوشش ۱**<br>**شماره مؤلفه: (ATE_COV.2.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

**۷-۵-۲- آزمون: پیمانه‌های اعمال کننده امنیت (ATE_DPT.2)**

**وابستگی:**

ADV_ARC.1، توصیف معماری امنیت

ADV_TDSS.3، طراحی پیمانه‌ای پایه‌ای

ATE_FUN.1، آزمون کارکردی

| مؤلفه‌های اقدامات توسعه دهنده | |
| --- | --- |
| **نام خانواده** | **عنصر امنیتی** |

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| آزمون: پیمانه‌های اعمال کننده امنیت (**ATE_DPT**) | **نام عنصر: آزمون: پیمانه‌های اعمال کننده امنیت ۱**<br>**شماره مؤلفه: (ATE_DPT.2.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید تحلیلی از عمق آزمون ارائه دهد. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| آزمون: پیمانه‌های اعمال کننده امنیت (**ATE_DPT**) | **نام عنصر: آزمون: پیمانه‌های اعمال کننده امنیت ۱**<br>**شماره مؤلفه: (ATE_DPT.2.1C)**<br>**شرح مؤلفه:**<br>تحلیل عمق آزمون باید تناظر بین آزمون‌ها در مستندات آزمون و زیر سیستم‌های توابع هدف امنیتی (TSF) و پیمانه‌های اعمال کننده‌ی الزامات کارکرد امنیت در طراحی محصول را نشان دهد. |

| مؤلفه‌های محتوایی | |
|---|---|
| نام خانواده | عنصر امنیتی |
| | **نام عنصر: آزمون: پیمانه‌های اعمال کننده امنیت ۲**<br><br>**شماره مؤلفه: (ATE_DPT.2.2C)**<br><br>**شرح مؤلفه:**<br><br>تحلیل عمق آزمون باید تمام زیر سیستم‌های توابع هدف امنیتی (TSF) را در طراحی محصول نشان دهد. |
| | **نام عنصر: آزمون: پیمانه‌های اعمال کننده امنیت ۳**<br><br>**شماره مؤلفه: (ATE_DPT.2.3C)**<br><br>**شرح مؤلفه:**<br><br>تحلیل عمق آزمون باید نشان دهد که پیمانه‌های اعمال کننده‌ی الزامات کارکرد امنیت در طراحی محصول مورد آزمون قرار گرفته‌اند. |

| مؤلفه‌های اقدامات ارزیاب | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| آزمون: پیمانه های اعمال کننده امنیت (**ATE_DPT**) | **نام عنصر: آزمون: پیمانه‌های اعمال کننده امنیت ۱**<br>**شماره مؤلفه: (ATE_DPT.2.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

### ۷-۵-۳- آزمون کارکردی (ATE_FUN.1)

**وابستگی: ATE_COV.1** شواهد پوشش

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| آزمون کارکردی (**ATE_FUN**) | **نام عنصر: آزمون کارکردی ۱**<br>**شماره مؤلفه: (ATE_FUN.1.1D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید توابع هدف امنیتی (TSF) را مورد آزمون قرار دهد و نتایج را مستند کند. |

| مؤلفه‌های اقدامات توسعه دهنده | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: آزمون کارکردی ۲**<br>**شماره مؤلفه: (ATE_FUN.1.2D)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید مستندات آزمون را ارائه دهد. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| آزمون کارکردی **(ATE_FUN)** | **نام عنصر: آزمون کارکردی ۱**<br>**شماره مؤلفه: (ATE_FUN.1.1C)**<br>**شرح مؤلفه:**<br>مستندات آزمون باید طرح آزمون، نتایج مورد انتظار آزمون و نتایج واقعی آزمون را در بر بگیرد. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: آزمون کارکردی ۲**<br>**شماره مؤلفه: (ATE_FUN.1.2C)**<br>**شرح مؤلفه:**<br>طرح آزمون باید آزمون‌هایی را که اجرا شده است شناسایی کرده و سناریوهایی برای اجرای هر آزمون ارائه دهد. این سناریوها باید هر گونه وابستگی ترتیبی در نتایج آزمون‌های دیگر را در بر گیرد. |
| | **نام عنصر: آزمون کارکردی ۳**<br>**شماره مؤلفه: (ATE_FUN.1.3C)**<br>**شرح مؤلفه:**<br>نتایج مورد انتظار آزمون باید خروجی پیش‌بینی شده‌ی اجرای موفق آزمون‌ها را نشان دهد. |

| مؤلفه‌های محتوایی | |
|---|---|
| **نام خانواده** | **عنصر امنیتی** |
| | **نام عنصر: آزمون کارکردی ۱**<br>**شماره مؤلفه: (ATE_FUN.1.4C)**<br>**شرح مؤلفه:**<br>نتایج آزمون واقعی باید با نتایج مورد انتظار آزمون‌ها سازگار باشد. |

**مؤلفه‌های اقدامات ارزیاب**

| شماره الزام | نام خانواده | عنصر امنیتی |
|---|---|---|
| ۱ | آزمون کارکردی (ATE_FUN) | **نام عنصر: آزمون کارکردی ۱**<br>**شماره مؤلفه: (ATE_FUN.1.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |

**۷-۵-۴- آزمون مستقل -نمونه (ATE_IND.2)**

**وابستگی:**

ADV_FSP.2، مشخصات کارکردی جرا کننده‌ی امنیت

AGD_OPE.1، راهنمای کاربری

AGD_PRE.1، راهنمای آماده‌سازی

ATE_COV.1، شواهد پوشش

ATE_FUN.1، آزمون کارکردی

**مؤلفه‌های اقدامات توسعه دهنده**

| شماره الزام | نام خانواده | عنصر امنیتی |
|---|---|---|
| ۱ | آزمون مستقل –نمونه (**ATE_IND**) | **نام عنصر: آزمون مستقل –نمونه ۲**<br>**شماره مؤلفه: (ATE_IND.2.1D)** |

**شرح مؤلفه:**

توسعه‌دهنده باید آزمونی برای محصول تعریف کند.

**مؤلفه‌های محتوایی**

| شماره الزام | نام خانواده | عنصر امنیتی |
|---|---|---|

**مؤلفه‌های محتوایی**

| شماره الزام | نام خانواده | عنصر امنیتی |
|---|---|---|
| ۱ | آزمون مستقل –نمونه (**ATE_IND**) | **نام عنصر: آزمون مستقل –نمونه ۲**<br>**شماره مؤلفه: (ATE_IND.2.1C)**<br>**شرح مؤلفه:**<br>محصول باید مناسب برای آزمون باشد. |
| ۲ | | **نام عنصر: آزمون مستقل –نمونه ۲**<br>**شماره مؤلفه: (ATE_IND.2.2C)**<br>**شرح مؤلفه:**<br>توسعه‌دهنده باید مجموعه‌ای معادل از منابع استفاده شده در آزمون کارکردی توابع هدف امنیتی (TSF) توسعه دهنده را ارائه دهد. |

**مؤلفه‌های اقدامات ارزیاب**

| شماره الزام | نام خانواده | عنصر امنیتی |
|---|---|---|
| ۱ | آزمون مستقل –نمونه (**ATE_IND**) | **نام عنصر: آزمون مستقل –نمونه ۲**<br>**شماره مؤلفه: (ATE_IND.2.1E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد. |
| ۲ | | **نام عنصر: آزمون مستقل –نمونه ۲**<br>**شماره مؤلفه: (ATE_IND.2.2E)**<br>**شرح مؤلفه:**<br>ارزیاب باید نمونه‌ای از آزمون‌ها را در مستندات آزمون اجرا کند تا نتایج آزمون توسعه دهنده را تأیید کند. |
| ۳ | | **نام عنصر: آزمون مستقل –نمونه ۲**<br>**شماره مؤلفه: (ATE_IND.2.3E)** |

**مؤلفه‌های اقدامات ارزیاب**

**شماره الزام نام خانواده عنصر امنیتی**

**شرح مؤلفه:**

ارزیاب باید زیرمجموعه‌ای از توابع هدف امنیتی (TSF) را مورد آزمون قرار دهد تا این موضوع را تایید کند که توابع هدف امنیتی (TSF) به نحوی کار می‌کند که مشخص شده است.

## ۷-۶- کلاس تحلیل آسیب‌پذیری (AVA)

### ۷-۶-۱- تحلیل آسیب‌پذیری روشمند (AVA_VAN.4)

**وابستگی:**

ADV_ARC.1، توصیف معماری امنیتی

ADV_FSP.4، مشخصات کارکردی کامل

ADV_TDS.3، طراحی پیمانه‌ای پایه‌ای

ADV_IMP.1، بازنمایی پیاده‌سازی توابع هدف امنیتی (TSF)

AGD_OPE.1، راهنمای کاربری

AGD_PRE.1، راهنمای آماده‌سازی

ATE_DPT.1، آزمون: طراحی پایه

**مؤلفه‌های اقدامات توسعه دهنده**

| شماره الزام | نام خانواده | عنصر امنیتی |
| --- | --- | --- |
| ۱ | تحلیل آسیب‌پذیری روشمند (AVA_VAN) | **نام عنصر: تحلیل آسیب‌پذیری روشمند ۴**<br>**شماره مؤلفه: (AVA_VAN.4.1D)** |

**شرح مؤلفه:**

توسعه دهنده باید محصول را برای آزمون ارائه دهد.

**مؤلفه‌های محتوایی**

| شماره الزام | نام خانواده | عنصر امنیتی |
| --- | --- | --- |

**مؤلفه‌های محتوایی**

| شماره الزام | نام خانواده |
| --- | --- |
| ۱ | تحلیل آسیب‌پذیری روشمند (AVA_VAN) |

**عنصر امنیتی**

**نام عنصر: تحلیل آسیب‌پذیری روشمند ۴**

**شماره مؤلفه: (AVA_VAN.4.1C)**

**شرح مؤلفه:**

محصول باید برای آزمون مناسب باشد.

**مؤلفه‌های اقدامات ارزیاب**

| شماره الزام | نام خانواده |
| --- | --- |
| ۱ | تحلیل آسیب‌پذیری روشمند (AVA_VAN) |

**عنصر امنیتی**

**نام عنصر: تحلیل آسیب‌پذیری روشمند ۴**

**شماره مؤلفه: (AVA_VAN.4.1E)**

**شرح مؤلفه:**

ارزیاب باید تایید کند که اطلاعات ارائه شده همه الزامات برای محتوا و ارائه شواهد را برآورده می‌سازد.

**مؤلفه‌های اقدامات ارزیاب**

| شماره الزام | نام خانواده | عنصر امنیتی |
| --- | --- | --- |
| ۲ | | **نام عنصر: تحلیل آسیب‌پذیری روشمند ۴**<br>**شماره مؤلفه: (AVA_VAN.4.2E)**<br>**شرح مؤلفه:**<br>ارزیاب باید جستجویی در منابع دامنه‌ی عمومی برای شناسایی آسیب‌پذیری بالقوه در محصول داشته باشد. |
| ۳ | | **نام عنصر: تحلیل آسیب‌پذیری روشمند ۴**<br>**شماره مؤلفه: (AVA_VAN.4.3E)**<br>**شرح مؤلفه:**<br>ارزیاب باید تحلیل آسیب‌پذیری روشمند و مستقلی از محصول با استفاده از مستندات راهنما، مشخصات عملکردی، طراحی محصول، توصیف معماری امنیتی و بازنمایی پیاده‌سازی را جهت شناسایی آسیب‌پذیری‌های بالقوه در محصول انجام دهد. |
| ۴ | | **نام عنصر: تحلیل آسیب‌پذیری روشمند ۴** |

**مؤلفه‌های اقدامات ارزیاب**

**شماره الزام** **نام خانواده** **عنصر امنیتی**

**شماره مؤلفه: (AVA_VAN.4.4E)**

**شرح مؤلفه:**

ارزیاب باید آزمون نفوذ را بر اساس آسیب‌پذیری بالقوه شناسایی شده اجرا کند تا تعیین کند که محصول نسبت به حملات انجام شده متوسط مهاجم با پتانسیل حمله متوسط، مقاوم است.

## ۸- منطق الزامات امنیتی

منطق الزامات امنیتی نشان می‌دهد که الزامات امنیتی فناوری اطلاعات شرح داده شده برای برآوردن اهداف امنیتی مناسب هستند و در نتیجه، برای مورد توجه قرار دادن مسائل امنیتی مناسب هستند.

### ۸-۱- منطق الزامات کارکرد امنیتی

منطق الزامات کارکرد امنیتی محصول موارد زیر را نشان می‌دهد:

- هر هدف امنیتی محصول حداقل یک الزام تابع امنیتی محصول دارد که به آن ردگیری می‌شود.
- هر الزام کارکرد امنیتیی محصول حداقل به یک هدف امنیتی محصول بر می‌گردد.
- **Error! Reference source not found.**، نگاشتی بین اهداف امنیتی و الزامات کارکرد امنیتی ارائه می‌دهد.

**جدول ۱۴- خلاصه‌ای از نگاشت بین اهداف امنیتی و الزامات کارکرد امنیت**

| اهداف امنیتی / الزامات کارکرد امنیت | اهداف امنیتی محصول | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | O.EAC | O.BAC | O.Handling_Info_Leakage | O.Access_Control | O.Replay Prevention | O.Deleting_Residua_Info | O.Secure State | O.Certificate Verification | O.Secure_Messaging | O.Session Termination | O.Security_Mechanism_Application_Procedures | O.Management |
| FCS_CKM.1 | × | × | | | | | | | | | | |
| FCS_CKM.1 | | × | | | × | | | | | | | |
| FCS_CKM.2(2) | × | | | | | | | | | | | |
| FCS_CKM.4 | | | | | | × | | | | | | |
| FCS_COP.1(1) | | × | | | | | | | × | | | |
| FCS_COP.1(2) | | × | | | | | | | × | | | |
| FCS_COP.1(3) | × | × | | | | | | | | | | |
| FCS_COP.1(4) | × | | | | | | | × | | | | |
| FDP_ACC.1 | | | | × | | | | | | | | |
| FDP_ACF.1 | × | × | | × | | | | | | | × | × |
| FDP_RIP.1 | | | | | × | × | | | | | | |
| FDP_UCT.1 | | | | | × | | | | × | | | |
| FDP_UIT.1 | | | | | × | | | | × | | | |
| FIA_AFL.1 | × | × | | × | | | | | | × | × | |
| FIA_UAU.1(1) | | × | | × | | | | | | × | | |
| FIA_UAU.1(2) | × | | | × | | | | | | × | × | |
| FIA_UAU.4 | × | × | | | × | | | | | | | |
| FIA_UAU.5 | × | × | | × | | | | | | | × | |
| FIA_UID.1 | × | × | | | | | | | | | | |
| FMT_MOF.1 | | | | × | | | | | | | | × |
| FMT_MSA.1 | | | | × | | | | | × | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FMT_MSA.3 | | | | | | | | × | | | × |
| FMT_MTD.1(1) | | | | | | | | × | | | × |
| FMT_MTD.1(2) | | | | | | | | | × | | |
| FMT_MTD.3 | × | | | | | × | | | | × | |
| FMT_SMF.1 | | | | | × | | | | | | × |
| FMT_SMR.1 | | | | | | | | | | | × |
| FPR_UNO.1 | | | | | | | | | | | |
| FPT_FLS.1 | | | | | | | × | | | | |
| FPT_ITI.1 | | | | | | | | | × | × | |
| FPT_TST.1 | | | | | | | × | | | | |

**۸-۱-۱- تولید کلید رمزنگاری (ساز و کار اشتقاق کلید) (FCS_CKM.1)**

این مؤلفه نیاز به تولید کلید احراز هویت کنترل دسترسی پایه (BAC)، کلیدهای نشست کنترل دسترسی پایه (BAC) و کنترل دسترسی توسعه یافته (EAC) ۱۱۲ بیتی مطابق با الگوریتم تولید کلید رمزنگاری مشخص شده در سند سازمان بین‌المللی هواپیمایی غیر نظامی (ICAO) دارد. از این طریق، کلید احراز هویت کنترل دسترسی پایه (BAC) جهت استفاده در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) تولید شده و کلید نشست کنترل دسترسی پایه (BAC) یا کنترل دسترسی توسعه یافته (EAC) برای استفاده در پیام‌رسانی پیام امن تولید شده است. بنابر این، این مؤلفه اهداف امنیتی O.BAC و O.EAC را برآورده می‌سازد.

**۸-۱-۲-توزیع کلید رمزنگاری (توزیع نقطه‌ی آغاز تصادفی (seed) تابع اشتقاق کلید (KDF) برای تولید کلید نشست کنترل دسترسی پایه (BAC)) (FCS_CKM.2 (1))**

این مؤلفه روشی برای توزیع نقطه‌ی آغاز تصادفی (seed) ساز و کار اشتقاق کلید تعریف می‌کند که در تولید کلید نشست کنترل دسترسی پایه (BAC) برای سامانه بازرسی ضروری است (ISO/IEC 1170-2، ۶ ساز و کار برقراری کلید).

روش توزیع تعریف شده در این مؤلفه، هدف امنیتی O.Replay_Prevention را برآورده می‌سازد که این هدف امنیتی از اعداد تصادفی استفاده می‌کند و همچنین O.BAC را برآورده می‌سازد که این هدف امنیتی را قادر به تولید کلید نشست کنترل دسترسی پایه (FCS_CKM.1(BAC از طریق تولید نقطه‌ی آغاز تصادفی(seed)تابع اشتقاق کلید (KDF)می‌کند.

**۸-۱-۳- توزیع کلید رمزنگاری (توزیع نقطه‌ی آغاز تصادفی (seed) تابع اشتقاق کلید (KDF)برای تولید کلید نشست کنترل دسترسی توسعه یافته (EAC))(FCS_CKM.2 (2))**

این مؤلفه روشی برای توزیع نقطه‌ی آغاز تصادفی (seed) ساز و کار اشتقاق کلید تعریف می‌کند که در تولید کلید نشست کنترل دسترسی توسعه یافته (EAC) برای سامانه بازرسی ضروری است (پروتکل توزیع کلید دیفی – هلمن (DH) یا منحنی بیضوی دیفی– هلمن (ECDH)در PKCS#3، ANSI X9.42 ، ISO/IEC 15946-3).

روش توزیع تعریف شده در این مؤلفه، هدف امنیتی O.EAC را برآورده می‌سازد که این هدف امنیتی را قادر به تولید کلید نشست کنترل دسترسیتوسعه یافته (FCS_CKM.1(EAC از طریق تولید نقطه‌ی آغاز تصادفی(seed)تابع اشتقاق کلید (KDF)می‌کند.

**۸-۱-۴-تخریب کلید رمزنگاری (FCS_CKM.4)**

این مؤلفه اطمینان حاصل می‌کند که نویسنده‌ی هدف امنیتی روشی را برای تخریب امن کلید تولید شده توسط ساز و کار اشتقاق کلید FCS_CKM.1 تعریف می‌کند.

این مؤلفه هدف امنیتی O.Deleting_Residua_Info را برآورده می‌کند که این هدف امنیتی روش تخریب کلید تولید شده توسط توابع هدف امنیتی (TSF) و باقیمانده در حافظه موقت را با استفاده از روش تعریف شده توسط نویسنده هدف امنیتی ارائه می‌دهد.

**۸-۱-۵-عملیات رمزنگاری (عملیات رمزنگاری کلید متقارن) ((FCS_COP.1 (1)**

این مؤلفه، عملیات رمزنگاری استاندارد رمزگذاری داده سه گانه (TDES) مورد استفاده در احراز هویت سامانه بازرسی را تعریف می‌کند، که از کنترل دسترسی پایه (BAC) پشتیبانی می‌کند یا از افشای داده کاربر انتقال یافته جلوگیری می‌کند.

عملیات رمزنگاری تعریف شده در این مؤلفه هدف امنیتی O.Secure_Messaging را برآورده می‌سازد که این هدف امنیتی از محرمانگی داده کاربر انتقال یافته ما بین محصول و سامانه بازرسی از طریق استفاده از الگوریتم رمزنگاری اطمینان حاصل می‌کند.

عملیات رمزنگاری تعریف شده در این مؤلفه هدف امنیتی O.BAC را برآورده می‌ساز که این هدف امنیتی در پیاده‌سازی احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) ضروری است.

**۸-۱-۶-عملیات رمزنگاری (کد احراز هویت پیام (MAC)) ((FCS_COP.1 (2)**

این مؤلفه، کد احراز هویت پیام (MAC) جزئی مورد استفاده برای احراز هویت سامانه بازرسی را تعریف می‌کند، که از کنترل دسترسی پایه (BAC) پشتیبانی می‌کند یا تغییرات در داده کاربر انتقال یافته را تشخیص می‌دهد.

عملیات کد احراز هویت پیام (MAC) تعریف شده در این مؤلفه هدف امنیتی O.Secure_Messaging را برآورده می‌سازد که این هدف امنیتی از یکپارچگی در روش ارائه شده برای تشخیص تغییر داده کاربر انتقال یافته ما بین محصول و سامانه بازرسی اطمینان حاصل می‌کند.

عملیات کد احراز هویت پیام (MAC) تعریف شده در این مؤلفه هدف امنیتی O.BAC را برآورده می‌سازد که این هدف امنیتی در پیاده‌سازی احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) ضروری است.

**۸-۱-۷- عملیات رمزنگاری (تابع چکیده‌ساز) ((FCS_COP.1 (3)**

این مؤلفه، تابع چکیده‌ساز SHA-1 ضروری در پیاده‌سازی تابع اشتقاق کلید (KDF) مطابق FCS_CKM.1 را تعریف می‌کند.

تابع چکیده‌ساز تعریف شده در این مؤلفه، هدف امنیتی O.BAC و O.EAC را برآورده می‌سازد که این اهدا امنیتی تابع اشتقاق کلید (KDF) را قادر به تولید کلید نشست کنترل دسترسی پایه (BAC) و کنترل دسترسی توسعه یافته (EAC) می‌کند.

**۸-۱-۸- عملیات رمزنگاری (درستی‌سنجی امضای دیجیتال برای درستی‌سنجی گواهی‌ها) ((4) FCS_COP.1)**

این مؤلفه روش درستی‌سنجی امضای دیجیتال ضروری در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) را تعریف می‌کند.

روش درستی‌سنجی امضای دیجیتال تعریف شده در این مؤلفه هدف امنیتی O.Certificate_Verification را برآورده می‌سازد که این هدف امنیتی گواهی پیوند CVCS، گواهی تأیید کننده سند (DV) و سامانه بازرسی (IS) ارائه شده توسط سامانه بازرسی به محصول را مورد بررسی قرار می‌دهد. همچنین، این مؤلفه هدف امنیتی O.EAC را برآورده می‌سازد که روش درستی‌سنجی امضای دیجیتالی مورد نیاز در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) را به منظور بررسی حق دسترسی به داده زیست‌سنجی دارنده‌گذرنامه الکترونیک ارائه می‌دهد.

**۸-۱-۹-کنترل دسترسی زیر مجموعه (FDP_ACC.1)**

این مؤلفه فهرستی از موجودیت‌های فعال، غیر فعال و عملیات را به منظور تصمیم‌گیری در مورد دامنه‌ی کنترل برای خط‌مشی‌های کنترل دسترسی گذرنامه الکترونیک تعریف می‌کند.

خط‌مشی‌های کنترل دسترسی به گذرنامه الکترونیک تعریف شده در این مؤلفه، هدف امنیتی O.Access_Control را برآورده می‌سازد که این هدف امنیتی عامل شخصی‌سازی، موجودیت‌های فعال سامانه بازرسی کنترل دسترسی پایه (BAC) و سامانه بازرسی کنترل دسترسی توسعه یافته (EIS)، داده شخصی، داده زیست‌سنجیدارنده گذرنامه الکترونیک و داده احراز هویت دارنده گذرنامه الکترونیک بکار و غیره را به عنوان موجودیت‌های غیر فعال و روابط آن‌ها را به عنوان عملیات تعریف می‌کند.

**۸-۱-۱۰- مشخصه‌های امنیتی مبتنی بر کنترل دسترسی (FDP_ACF.1)**

به منظور اجرای خط‌مشی‌های کنترل دسترسی به گذرنامه الکترونیک، این مؤلفه مشخصه‌های امنیتی موجودیت‌های فعال و موجودیت‌های‌غیر فعال تعریف شده در FDP_ACC.1 را تعریف می‌کند و قواعد کنترل دسترسیگذرنامه الکترونیک را مشخص می‌کند.

مشخصه‌های امنیتی و قواعد کنترل دسترسی‌گذرنامه الکترونیک تعریف شده در این مؤلفه اهداف امنیتی O.Management و O.Acess_Control را برآورده می‌سازد که تنها عامل شخصی‌سازی مجاز با عامل شخصی‌سازی صادر کننده مجوز می‌توانند توابع مدیریتی را اجرا کنند.

همچنین، این مؤلفه اهداف امنیتی O.BAC، O.EAC و O.Aceess_Control را برآورده می‌سازد چرا که حق خواندن داده شخصی گذرنامه الکترونیک و داده احراز هویت دارنده‌گذرنامه الکترونیک و غیره تنها به موجودیت‌های فعال دارنده مجوز کنترل دسترسی پایه (BAC) داده می‌شود و حق خواندن داده زیست‌سنجی دارنده‌گذرنامه الکترونیک تنها به موجویت‌های فعال دارنده مجوز کنترل دسترسی توسعه‌یافته (EAC) داده می‌شود.

قوانین رد صریح FDP_ACF.1.4 تعریف شده در این مؤلفه هدف امنیتی O.Security_Machanism_Application_Procedures را برآورده می‌سازد چرا که ترتیب کاربرد ساز و کارهای امنیتی به گونه‌ای تضمین شده است، که هنگام نقض ترتیب دستورالعمل‌های انتقالی مشخص شده در بخش ۲،۱ روش‌های اجرایی بازرسی مشخصات کنترل دسترسی توسعه‌یافته (EAC)، دسترسی توسط سامانه بازرسی انکار می‌شود.

**۸-۱-۱۱- حفاظت از اطلاعات باقیمانده‌ی زیر مجموعه (FDP_RIP.1)**

این مؤلفه اطمینان حاصل می‌کند که هنگامی که توابع هدف امنیتی (TSF) منابع حافظه را برای کلید احراز هویت کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی توسعه‌یافته (EAC) و اعداد تصادفی تخصیص بدهد یا ندهد، اطلاعات قبلی گنجانده نمی‌شود.

این مؤلفه هدف امنیتی O.Deleting_Residua_Info را برآورده می‌سازد به گونه‌ای که این هدف اطمسنان حاصل می‌کند که هنگام تخریب کلیدهای احراز هویت کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی پایه (BAC)، کلید نشست کنترل دسترسی توسعه‌یافته (EAC) طبق روش تعریف شده در FCS_CKM.4، اطلاعات قبلی این کلیدها در دسترس نیست. همچنین این مؤلفه با اطمینان از این موضوع که اطلاعات قبلی اعداد تصادفی مورد استفاده برای

احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC)، کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) و تولید کلید نشست در دسترس نیستهدف امنیتی O.Replay_Prevention را برآورده می‌سازد.

**۸-۱-۱۲- محرمانگی تبادل داده پایه‌ای (FDP_UCT.1)**

این مؤلفه، هنگام انتقال موجودیت‌های غیر فعال مانند داده شخصی و داده زیست‌سنجی دارنده‌گذرنامه الکترونیک درون دامنه‌ی خط‌مشی‌های کنترل دسترسی گذرنامه الکترونیک روشی برای محافظت از افشای اطلاعات تعریف می‌کند.

این مؤلفه، پیام‌رسانی امن کنترل دسترسی پایه (BAC) یا کنترل دسترسی توسعه‌یافته (EAC) را با اجرای عملیات رمزنگاری برای داده شخصی دارنده‌گذرنامه الکترونیک و غیره انتقال یافته بین محصول و سامانه بازرسی با کلید رمزگذاری نشست کنترل دسترسی پایه (BAC)، یا داده زیست‌سنجی دارنده‌گذرنامه الکترونیک و غیره انتقال یافته بین محصول و سامانه بازرسی با کلید رمزگذاری نشست کنترل دسترسی توسعه‌یافته (EAC) برقرار می‌کند. بنابراین این مؤلفه هدف امنیتی O.Secure_Messaging را برآورده می‌سازد که از محرمانگی داده کاربر اطمینان حاصل می‌کند.

این مؤلفه هدف امنیتی O.Replay_Prevention را با حصول اطمینان از این موضوع برآورده می‌سازد که کلید رمزگذاری نشست کنترل دسترسی پایه (BAC) هنگام برقراری پیام‌رسانی امن کنترل دسترسی پایه (BAC) به عنوان کلید احراز هویت کنترل دسترسی پایه (BAC) مورد استفاده قرار نگرفته است.

**۸-۱-۱۳- یکپارچگی تبادل داده (FDP_UIT.1)**

این مؤلفه، هنگام انتقال موجودیت‌های غیر فعال مانند داده شخصی و داده زیست‌سنجی دارنده‌گذرنامه الکترونیک درون دامنه‌ی خط‌مشی‌های کنترل دسترسی گذرنامه الکترونیک روشی برای محافظت در برابر تغییر، حذف، اصلاح و استفاده مجدد اطلاعات تعریف می‌کند.

این مؤلفه، پیام‌رسانی امن کنترل دسترسی پایه (BAC) یا کنترل دسترسی توسعه‌یافته (EAC) را با اجرای عملیات رمزنگاری برای داده شخصی دارنده‌گذرنامه الکترونیک و غیره انتقال یافته بین محصول و سامانه بازرسی با کلید کد احراز هویت پیام (MAC) نشست کنترل دسترسی پایه (BAC)، یا داده

زیست‌سنجی دارنده‌گذرنامه الکترونیک و غیره انتقال یافته بین محصول و سامانه بازرسی با کلید کد احراز هویت پیام (MAC) نشست کنترل دسترسی توسعه‌یافته (EAC) برقرار می‌کند. بنابراین این مؤلفه هدف امنیتی O.Secure_Messaging را برآورده می‌سازد که از یکپارچگی داده کاربر اطمینان حاصل می‌کند.

این مؤلفه هدف امنیتی O.Replay_Prevention را با حصول اطمینان از این موضوع برآورده می‌سازد که کلید کد احراز هویت پیام (MAC) نشست کنترل دسترسی پایه (BAC) هنگام برقراری پیام‌رسانی امن کنترل دسترسی پایه (BAC) به عنوان کلید احراز هویت کنترل دسترسی پایه (BAC) مورد استفاده قرار نگرفته است.

**۸-۱-۱۴- ساماندهی خرابی احراز هویت (FIA_AFL.1)**

اگر تعداد شکست تلاش‌های احراز هویت از حد تعریف شده توسط نویسنده‌ی هدف امنیتی فراتر رود، این مؤلفه آن را تشخیص داده و نیاز به خاتمه بخشیدن به نشست کاربر است.

این مؤلفه هدف امنیتی O.Session_Termination را برآورده می‌سازد به طوریکه چنانچه تعداد شکست تلاش‌های احراز هویت احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) فراتر رفت، نشست خاتمه می‌یابد. علاوه بر آن، این مؤلفه هدف امنیتی O.Security_Mechanism_Application_Procedures، را با ناتوان کردن موجودیت‌های بیرونی غیر مجاز برای حرکت به فاز بعدی روش‌های اجرایی بازرسی برآورده می‌سازد به طوری که چنانچه احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) با شکست روبرو شود، به نشست پایان می‌بخشد.

علاوه بر این، این مؤلفه اهداف امنیتی O.EAC و O.Access_Control را برآورده می‌سازد چرا که با شکست احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) یا کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) اینگونه در نظر گرفته می‌شود که حق دسترسی‌ای به داده کاربر وجود ندارد دسترسی به داده کاربر با پایان بخشیدن به نشست، انکار می‌شود.

**۸-۱-۱۵- زمان‌بندی احرازهویت (احراز هویت دو طرفه‌یکنترل دسترسی پایه (BAC)) ((1) FIA_UAU.1)**

این مؤلفه تابعی برای کاربر تعریف می‌کند که باید قبل از احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) اجرا شود، و احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) را برای کاربر اجرا می‌کند.

در این مؤلفه به منظور توانمند کردن سامانه بازرسی شناسایی شده در FIA_UID.1، جهت اجرای تابع بازرسی جهت پشتیبانی از ساز و کار کنترل دسترسی پایه (BAC) و برای خواندن داده شخصی دارنده‌گذرنامه الکترونیک احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) اجرا شده است. این مؤلفه اهداف امنیتی O.Session Termination، O.BAC و O.Access_Control را برآورده می‌سازد به طوری که چنانچه احراز هویت با شکست مواجه شود شناسایی توسط FIA_AFL.1 را ممکن می‌سازد و در صورتی که احراز هویت با موفقیت انجام شود، حق خواندن داده شخصی دارنده‌گذرنامه الکترونیک داده می‌شود.

**۸-۱-۱۶- زمان‌بندی احراز هویت (کنترل دسترسی توسعه یافته–احرازهویت پایانه (EAC-TA)) ((2) FIA_UAU.1)**

این مؤلفه توابعی را برای کاربر تعریف می‌کند که باید قبل از کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) اجرا شود و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) را برای کاربر اجرا می‌کند.

در این مؤلفه تنها سامانه بازرسی‌ای که احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) در FIA_UAU.1(1) را با موفقیت پشت سر گذاشته است می‌تواند EAC_CA را اجرا کرده و داده کاربر (به جز داده زیست‌سنجی دارنده‌گذرنامه الکترونیک) را بخواند. برای خواندن داده زیست‌سنجی دارنده‌گذرنامه‌الکترونیک، کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) باید اجرا شود. این مؤلفه اهداف امنیتی O.Session_Termination، O.Security_Mechanism_Application_Procedures، O.EAC و O.Access_Control را برآورده می‌سازد به طوری که در صورت شکست احراز هویت شناسایی توسط FIA_AFL.1 را ممکن می‌سازد و در صورتی که احراز هویت با موفقیت انجام شود، حق خواندن داده شخصی دارنده‌گذرنامه الکترونیک داده می‌شود.

**۸-۱-۱۷- ساز و کارهای احراز هویت تک کاربردی (FIA_UAU.4)**

این مؤلفه مستلزم این است که اطلاعات مرتبط با احراز هویت در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) توسط توابع هدف امنیتی (TSF) به سامانه بازرسی ارسال شود و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) بدون مجدداً تکرار نشود.

این مؤلفه اهداف امنیتی O.Replay_Prevention، O.BAC و O.EAC را برآورده می‌سازد به گونه‌ای که توابع هدف امنیتی (TSF) احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) را اجرا می‌کند. این کار با تولید اعداد تصادفی مختلف مورد استفاده در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) در هر نشست و انتقال آن‌ها به سامانه بازرسی انجام می‌شود.

**۸-۱-۱۸- ساز و کارهای احراز هویت چندگانه (FIA_UAU.5)**

این مرلفه ساز و کارهای احراز هویت چندگانه و قوانین استفاده ازساز و کارهای احراز هویت را با توجه به نوع داده کاربری که در دسترس سامانه بازرسی خواهد بود تعریف می‌کند.

این مؤلفه اهداف امنیتی O.Security_Mechanism_Application_Procedures، O.Access_Control، O.BAC و O.EAC را برآورده می‌سازد چنانکه سامانه بازرسی، مجوز احراز هویت کنترل دسترسی پایه (BAC) را با موفقیت در احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) و مجوز کنترل دسترسی توسعه‌یافته (EAC) را با موفقیت در در کنترل دسترسی توسعه یافته - احراز هویت تراشه (EAC-CA)، کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) و درستی‌سنجی گواهی بعد از احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) طبق قوانین کاربرد ساز و کار احراز هویت به دست می‌آورد.

**۸-۱-۱۹- زمان‌بندی شناسایی (FIA_UID.1)**

این مؤلفه مستلزم برقراری کانال ارتباطی مبتنی بر پروتکل انتقال کارت مدار مجتمع (IC) بدون تماس (ISO/IEC 1443-4) است، به گونه‌ای توابع برای کاربر قبل از شناسایی و جهت شناسایی کاربر اجرا شوند.

این مؤلفه اهداف امنیتی O.BAC و O.EAC را برآورده می‌سازد به گونه‌ای که چنانچه یک موجودیت بیرونی برای برقراری کانال ارتباطی درخواست استفاده از برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) را داشته باشد، موجودیت بیرونی توسط سامانه بازرسی مورد شناسایی قرار می‌گیرد.

**۸-۱-۲۰- مدیریت رفتار توابع امنیتی (FMT_MOF.1)**

این مؤلفه تعریف می‌کند که توانایی غیر فعال کردن تابع نوشتن تنها به عامل شخصی‌سازی در فاز شخصی‌سازی داده می‌شود.

این مؤلفه اهداف امنیتی O.Management و O.Access_Control، را با غیرفعال کردن تابع نوشتن عامل شخصی‌سازی در فاز شخصی‌سازی برآورده می‌سازد به گونه‌ای که محصول در فاز استفاده عملیاتی نتواند هیچ داده‌ای را ثبت کند.

**۸-۱-۲۱- مدیریت مشخصه‌های امنیتی (FMT_MSA.1)**

این عنصر مستلزم محدود کردن توانایی مقدار دهی اولیه ویژگی‌های امنیتی کاربر تنها برای توابع هدف امنیتی (TSF) است که به عنوان اقدامی است که باید هنگامی اتخاذ گردد که توابع هدف امنیتی (TSF) تغییر داده توابع هدف امنیتی (TSF) انتقال یافته در FPT_IT.1 را تشخیص دهد.

این مؤلفه اهداف امنیتی O.Secure_Messaging و O.Access_Control را برآوده می‌سازد به گونه‌ای که از یکپارچگی اطمینان یافته و دسترسی به داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) مسدود می‌شود، این کار باید با تنظیم مجدد مشخصه‌های امنیتی داده شده‌ی قبلی عامل شخصی‌سازی یا سامانه بازرسی انجام می‌شود که به عنوان اقدامی است که باید زمانی اتخاذ شود کهتوابع هدف امنیتی (TSF) تغییری درداده توابع هدف امنیتی (TSF) انتقال یافته را تشخیص دهد.

**۸-۱-۲۲- مقداردهی اولیه مشخصه‌ی ایستا (FMT_MSA.3)**

این مؤلفه مستلزم این است که عامل شخصی‌سازی جهت محدود کردن مقادیر پیش‌فرض برای مشخصه‌های امنیتی در هنگام ایجاد یک موجودیت غیر فعال، مقادیر اولیه را تعیین کند.

این مؤلفه اهداف امنیتی O.Management و O.Access_Control را برآورده می‌سازد به طوری که تنها عامل شخصی‌سازی مجاز داده کاربر را جهت اجرای خط‌مشی‌های کنترل دسترسی در فاز شخصی‌سازی تولید می‌کند و مقادیر اولیه را جهت محدود کردن مشخصه‌های امنیتی داده تعیین می‌کند.

**۸-۱-۲۳- مدیریت داده‌توابع هدف امنیتی (TSF) (اطلاعات درستی‌سنجی گواهی) ((1) FMT_MTD.1)**

این مؤلفه نوشتن اطلاعات درستی‌سنجی گواهی ضروی برای کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) در حافظه‌ی امن را منحصر به عامل شخصی‌سازی در فاز شخصی می‌کند.

این مؤلفه اهداف امنیتی O.Managment و O.Access_Control را برآورده می‌سازد. این کار با توانمند ساختن تنها عامل شخصی‌سازی مجاز جهت داشتن توانایی نوشتن داده توابع هدف امنیتی (TSF) مثل کلید خصوصی احراز هویت تراشه‌ی کنترل دسترسی توسعه یافته (EAC)، تاریخ جاری، گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) وغیره در حافظه امن فاز شخصی سازی صورت می‌پذیرد.

**۸-۱-۲۴- مدیریت داده‌توابع هدف امنیتی (TSF) (مقداردهی اولیه شمارنده‌ی دنباله‌ی ارسال (SSC)) ((2) FMT_MTD.1)**

این مؤلفه مستلزم خاتمه بخشیدن پیام‌رسانی امن کنترل دسترسی پایه (BAC)، قبل از برقراری پیام‌رسانی امن کنترل دسترسی توسعه یافته (EAC) است.

این مؤلفه هدف امنیتی O.Security_Mechanism_Application_Procedures را با مقداردهی اولیه صفر، برای شمارنده‌ی دنباله‌ی ارسال (SSC) به منظور خاتمه بخشیدن به پیام‌رسانی امن کنترل دسترسی پایه (BAC) بعد از تولید کلید نشست کنترل دسترسی توسعه یافته (EAC) و ایجاد پیام‌رسانی امن کنترل دسترسی توسعه یافته (EAC) بکار می‌رود.

### ۸-۱-۲۵- داده‌توابع هدف امنیتی (TSF) امن (FMT_MTD.3)

این مؤلفه مستلزم این است که تنها به مقادیر امن به عنوان داده‌توابع هدف امنیتی (TSF) اجازه دهد تا از اعداد تصادفی امن اطمینان یابد و اطمینان حاصل کند که تاریخ اعتبار گواهی‌های استفاده شده در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) منقضی نشده است.

این مؤلفه هدف امنیتی O.Replay_Prevention را برآورده می‌سازد چرا که هنگامی که توابع هدف امنیتی (TSF) کلید نشست تولید می‌کنند تنها اعداد تصادفی امن مورد استفاده قرار گرفته‌اند تا از حمله‌ی تکرار مجدد جلوگیری شود.

همچنین، توابع هدف امنیتی (TSF)، گواهی پیوند مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) ارائه شده توسط سامانه بازرسی را با گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) ذخیره شده در محصول مقایسه می‌کند. این مقایسه برای درستی‌سنجی گواهی سامانه بازرسی (IS) استفاده شده در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) است. اگر گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) نیاز به بروز رسانی داشته باشد، توابع هدف امنیتی (TSF) به صورت داخلی گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، تاریخ‌های فعلی و EF.CVCA را به روز رسانی می‌کند، بنابراین داده‌توابع هدف امنیتی (TSF) را به عنوان مقادیر امن نگهداری می‌کند. این مؤلفه اهداف امنیتی O.Certificate_Verification و O.EAC را برآورده می‌سازند چرا که با بررسی گواهی تأیید کننده سند (DV) و گواهی سامانه بازرسی (IS) با گواهی مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA) امن، کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) می‌تواند با موفقیت اجرا شود.

### ۸-۱-۲۶- مشخصات توابع مدیریتی (FMT_SMF.1)

این مؤلفه ابزاری برای مدیریت داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) در فاز شخصی‌سازی فراهم می‌آورد.

این مؤلفه هدف امنیتی O.Management را برآورده می‌سازد به گونه‌ای که تابع نوشتن داده کاربر و داده‌توابع هدف امنیتی (TSF) را در فاز شخصی‌سازی تعریف می‌کند.

همچنین این مؤلفه هدف امنیتی O.Certificate_Verification را برآورده می‌سازد به طوری که این مؤلفه تابعی برایتوابع هدف امنیتی (TSF) جهت به روز رسانی گواهی مرجع صلاحیت‌دار تأییدکننده گواهیکشور(CVCA)، کلید درستی‌سنجی امضای دیجیتال مرجع صلاحیت‌دار تأییدکننده گواهی کشور(CVCA)، تاریخ‌های فعلی و غیره در فاز استفاده عملیاتی معرفی می‌کند.

**۸-۱-۲۷- نقش‌های امنیتی (FMT_SMR.1)**

این مؤلفه نقش عامل شخصی‌سازی را جهت مدیریتداده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) تعریف می‌کند.

این مؤلفه هدف امنیتی O.Managment را برآورده می‌سازد به گونه‌ای که نقش عامل شخصی‌سازی‌ای که تابع نوشتن داده کاربر و داده‌توابع هدف امنیتی (TSF) را در فاز شخصی‌سازی اجرا می‌کند، تعریف می‌کند.

**۸-۱-۲۸- غیر قابل رویت بودن (FPR_UNO.1)**

این مؤلفه اطمینان حاصل می‌کند که موجودیت‌های خارجی قادر به مشاهده‌ی داده مرتبط با رمزنگاری مثل کلید احراز هویت کنترل دسترسی پایه(BAC)، کلید نشست کنترل دسترسی پایه (BAC)،کلید نشست کنترل دسترسی توسعه یافته (EAC) و کلید خصوصی احراز هویت تراشه‌ی کنترل دسترسی توسعه یافته (EAC) هنگام اجرای عملیات رمزنگاری توسط توابع هدف امنیتی (TSF) نیستند.

این مؤلفه هدف امنیتی O.Handing_Info_Leakage را برآورده می‌سازد، به گونه‌ای که اطمینان می‌یابد که موجودیت‌های خارجی نمی‌توانند هیچ داده مرتبط با رمزنگاری را با بهره‌برداری از پدیده‌های فیزیکی (تغییر جریان، ولتاژ، الکترومغناطیس و غیره) بیابند که هنگامی رخ می‌دهد که توابع هدف امنیتی (TSF) عملیات رمزنگاری استاندارد رمزگذاری داده سه گانه (TDES)، کد احراز هویت پیام (MAC) و درستی‌سنجی امضای دیجیتال و غیره را اجرا می‌کنند.

**۸-۱-۲۹- خرابی با حفظ حالت امن (FPT_FLS.1)**

این مؤلفه مستلزم حفظ یک حالت امن در زمانی است که انواع خرابی‌ها مانند خرابی شناسایی شده از خودآزمایی و شرایط غیر عادی در تراشه‌ی مدار مجتمع (IC) و غیره رخ می‌دهد.

این مؤلفه هدف امنیتی O.Self-protection را برآورده می‌سازد، به گونه‌ای که یک حالت امن را حفظ می‌کند تا از بد عمل کردن توابع هدف امنیتی (TSF) هنگام تشخیص تغییر در یکپارچگی داده‌توابع هدف امنیتی (TSF) یا توابع هدف امنیتی (TSF) از خود آزمایی TPT_TST.1 یا تشخیص شرایط غیر عادی عملکرد توسط تراشه‌ی مدار مجتمع (IC) جلوگیری کند.

**۸-۱-۳۰- آشکارسازی تغییر توسط توابع هدف امنیتی (TSF) به صورت درونی (FPT_ITI.1)**

این مؤلفه مستلزم تشخیص تغییر در داده انتقال یافته‌ی توابع هدف امنیتی (TSF) و تعریف اقدامی که باید هنگام تشخیص تغییر اتخاذ شود است.

این مؤلفه اهداف امنیتی O.Secure_Messaging و O.Session_Termination را برآورده می‌سازد. این کار با تشخیص تغییر داده توابع هدف امنیتی (TSF) انتقال یافته در فاز استفاده عملیاتی و با اجرای اقداماتی مانند پایان دادن به کانال‌های ارتباطی مربوطه، حذف کلید نشست مرتبط و مدیریت اقدامات مشخص شده در FMT_MSA.1 و غیره صورت می‌گیرد که هنگام تشخیص تغییر باید اتخاذ گردد.

**۸-۱-۳۱- آزمون توابع هدف امنیتی (TSF) (FPT_TST.1)**

این مؤلفه مستلزم خود آزمایی برای تشخیص از دست دادن توابع هدف امنیتی (TSF) و داده‌توابع هدف امنیتی (TSF) با خرابی‌های مختلف (مد خرابی غیر منتظره، فقدان طراحی تراشه‌ی مدار مجتمع (IC)، صدمه عمدی به توابع هدف امنیتی (TSF) و غیره) است.

این مؤلفه هدف امنیتی O.Self-protection را برآورده می‌سازد. این کار با اجرای خود آزمایی تحت شرایط تعریف شده توسط نویسنده‌ی هدف امنیتی، و در نتیجه نشان دادن عملکرد صحیح توابع هدف امنیتی (TSF) انجام می‌شود. همچنین، این مؤلفه هدف امنیتی O.Self-protection را با بررسی یکپارچگی

قسمت‌های داده‌ای توابع هدف امنیتی (TSF) تعریف شده توسط نویسنده‌ی هدف امنیتی و توابع هدف امنیتی (TSF) ذخیره شده در محصول، و در نتیجه تشخیص از دست دادن داده‌توابع هدف امنیتی (TSF) برآورده می‌سازد.

### ۸-۲- منطق الزامات تضمین امنیت

سطح تضمینارزیابی[۳۸] (EAL) این پرفایل حفاظتی با در نظر گرفتن ارزش دارایی‌های محافظت شده توسط محصول و سطح تهدیدات و غیره EAL4+ (ADV_IMP.2, ATE_DPT.2, AVA_VAN.4) انتخاب شده است.

EAL4، به توسعه‌دهنده اجازه‌ی بدست آوردن حداکثر اطمینان از مهندسی امنیت قطعی بر اساس شیوه‌های توسعه‌ی تجاری درست را می‌دهد، که هر چند دقیق است، نیازی به دانش، مهارت‌ها و دیگر منابع قابل توجه متخصصان ندارد. EAL4 بالاترین سطح عملی ممکن از نظر اقتصادی برای مقاوم‌سازی یک خط تولید موجود است.

بنابراین EAL4 در شرایطی عملی است که توسعه‌دهندگان یا کاربران خواستار سطح بالای امنیت تضمین شده‌ی مستقل در هدف‌های ارزیابی کالاهای مرسوم بوده و آماده‌ی تحمل هزینه‌های افزوده‌ی مهندسی خاص امنیت هستند.

این پرفایل حفاظتی تا اندازه‌ای مؤلفه‌های تضمینی را که بالاتر از EAL4 باشند را انتخاب کرده است. منطق تکمیلی با مؤلفه‌های تضمین به شرح زیر است.

**۸-۲-۱-نگاشت کامل از بازنمایی پیاده‌سازی توابع هدف امنیتی (TSF)،ATE_DPT.2 آزمون: پیمانه‌های اعمال کننده امنیت، AVA_VLA.4 تحلیل آسیب پذیری روشمند (ADV_IMP.2)**

[۳۸] Evaluation Assurance Level

محصول، سیستم عامل و برنامه کاربردی (App) به کار گرفته شده در تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) است. بنابراین محصول از دیدگاه تابع عملیات رمزنگاری و امنیت فیزیکی تا حد زیادی به تراشه‌ی مدار مجتمع (IC) وابسته است. برای اطمینان از امنیت تراشه‌ی سند مسافرتی قابل خواندن توسط ماشین (MRTD) اطمینان‌پذیری و عملیات امن نه تنها محصول، بلکه حتی تراشه‌ی مدار مجتمع (IC) باید تأیید شده باشد.

محصول با استفاده از مشخصات پیاده‌سازی استاندارد در دسترس عموم توسعه یافته است. بنابراین، دستیابی به اطلاعات مرتبط با طراحی و عملکرد محصول آسان است. همچنین، محصول، با محض اینکه در محیط بازی مورد استفاده قرار گیرد به آسانی قابل دستیابی است و ردیابی حمله دشوار است. هر چند، از آنجا که تراشه‌ی مدار مجتمع (IC) در دامنه‌ی محصول گنجانده نشده است، نیازی به فهم ساختار سخت‌افزاری و تجهیزات تخصصی پیشرفته و غیره نیست. بنابراین، با در نظر گرفتن منابع، انگیزه و مهارت، محصول باید با مهاجمان دارای پتانسیل حمله‌ی متوسط مقابله کند. EAL4 شامل AVA_VL.3 است که در مقابل حملات پایه‌ای و پیشرفته مقاوم است. AVA_VLA.4 برای نیاز به اجرای تحلیل آسیب‌پذیری نظام‌مند و مقاومت در برابر مهاجمان دارای پتانسیل حمله‌ی متوسط افزوده شده است. با این حال، همچنان احتمال حمله مستقیم به تراشه‌ی مدار مجتمع (IC) توسط عامل تهدید دارای پتانسیل حمله‌ی بالا وجود دارد و ارزیابی و درستی‌سنجی برای این تراشه ممکن است به سازنده‌ی تراشه‌ی مدار مجتمع (IC) اختصاص یابد.

اصلاح نقض حتی اگر نقض پس از صدور گذرنامه و بارگذاری شده بر روی تراشه‌ی مدار مجتمع (IC) رخ داده باشد، دشوار است و ممکن است مورد بهره‌برداری توسط عامل تهدید قرار گیرد. بنابراین ADV_IMP.2 به منظور تحلیل کامل افزوده شده است تا بررسی کند که آیا توابع هدف امنیتی (TSF) به درستی پیاده‌سازی شده است و کد معیوبی وجود ندارند، و ATE_DPT.2 برای آزمون پیمانه‌ی اعمال کننده‌ی امنیت افزوده شده است.

### ۸-۳- منطق وابستگی

#### ۸-۳-۱- وابستگی الزامات کارکرد امنیت محصول

**Error! Reference source not found.**، وابستگی مؤلفه‌های کارکردی محصول را نشان می‌دهد.

**جدول ۱۵- وابستگی عناصر عملیاتی محصول**

| شماره | عناصر عملیاتی | وابستگی | شماره مرجع |
|---|---|---|---|
| ۱ | FCS_CKM.1 | [FCS_CKM.2 or FCS_COP.1]<br>FCS.CKM.4 | ۲و۳<br>۴ |
| ۲ | FCS_CKM.2(1) | [FDP_ITC.1 or FDP_ITC.2 or CS_CKM.1]<br>FMT_CKM.4 | ۱<br>۴ |
| ۳ | FCS_CKM.2(2) | [FDP_ITC.1 or FDP_ITC.2 or CS_CKM.1]<br>FMT_CKM.4 | ۱<br>۴ |
| ۴ | FCS_CKM.4 | [FDP_ITC.1 or FDP_ITC.2 or<br>FCS_CKM.1] | ۱ |
| ۵ | FCS_COP.1(1) | [FDP_ITC.1 or FDP_ITC.2 or CS_CKM.1]<br>FCS_CKM.4 | ۱<br>۴ |
| ۶ | FCS_COP.1(2) | [FDP_ITC.1 or FDP_ITC.2 or CS_CKM.1]<br>FCS_CKM.4 | ۱<br>۴ |
| ۷ | FCS_COP.1(3) | [FDP_ITC.1 or FDP_ITC.2 or CS_CKM.1]<br>FCS_CKM.4 | ۱<br>۴ |
| ۸ | FCS_COP.1(4) | [FDP_ITC.1 or FDP_ITC.2 or CS_CKM.1]<br>FCS_CKM.4 | ۱<br>۴ |
| ۹ | FDP_ACC.1 | FDP_ACF.1 | ۱۰ |
| ۱۰ | FDP_ACF.1 | FDP_ACC.1<br>FMT_MSA.3 | ۹<br>۲۲ |
| ۱۱ | FDP_RIP.1 | | |
| ۱۲ | FDP_UCT.1 | [FPT_ITC.1 or FPT_TRP.1]<br>[FDP_ACC.1 or FDP_IFC.1] | ۹ |
| ۱۳ | FDP_UIT.1 | [FDP_ACC.1 or FDP_IFC.1]<br>[FTP_ITC.1 or FTP_TRP.1] | ۹ |

| | | | |
|---|---|---|---|
| ۱۴ | FIA_AFL.1 | FIA_UAU.1 | ۱۶-۱۵ |
| ۱۵ | FIA_UAU.1(1) | FIA_UID.1 | ۱۹ |
| ۱۶ | FIA_UAU.1(2) | FIA_UAU.1(1) | ۱۵ |
| ۱۷ | FIA_UAU.4 | | |
| ۱۸ | FIA_UAU.5 | | |
| ۱۹ | FIA_UID.1 | | |
| ۲۰ | FMT_MOF.1 | FMT_SMF.1<br>FMT_SMR.1 | ۲۶<br>۲۷ |
| ۲۱ | FMT_MSA.1 | [FDP_ACC.1 or FDP_IFC.1]<br>FMT_SMF.1<br>FMT_SMR.1 | ۹<br>۲۶<br>۲۷ |
| ۲۲ | FMT_MSA.3 | FMT_MSA.1<br>FMT_SMR.1 | ۲۱<br>۲۷ |
| ۲۳ | FMT_MTD.1(1) | FMT_SMF.1<br>FMT_SMR.1 | ۲۶<br>۲۷ |
| ۲۴ | FMT_MTD.1(2) | FMT_SMF.1<br>FMT_SMR.1 | ۲۶<br>۲۷ |
| ۲۵ | FMT_MTD.3 | FMT_MTD.1 | ۲۳ |
| ۲۶ | FMT_SMF.1 | | |
| ۲۷ | FMT_SMR.1 | FIA_UID.1 | ۱۹ |
| ۲۸ | FPR_UNO.1 | | |
| ۲۹ | FPT_FLS.1 | | |
| ۳۰ | FPT_ITI.1 | | |

| | | | |
|---|---|---|---|
| ۳۱ | FPT_TST.1 | | |

FDP_UCT.1و FDP_UIT.1 با FTP_ITC.1 یا FTP_TRP.1 وابستگی دارند، ولی این وابستگی در این پرفایل حفاظتی گنجانده نشده است. FDP_UCT و FDP_UIT.1 نیاز به پیام‌رسانی امن بین سامانه بازرسی و محصول دارد. از آنجا که پیام‌رسانی امن بین سامانه بازرسی و محصول کانال منحصر به فردی است، نیازی نیست به صورت منطقی از دیگر کانال‌های ارتباطی جدا شود. بنابراین، بنابراین در این پرفایل حفاظتی الزامات، FTP_ITC.1 تعریف نشده است.

FIA_UAU.1 (2) باید وابستگی‌ای با FIA_UID.1 داشته باشد ولی وابستگی به دلیل عملیات پالایش به FIA_UAU.1 (1) تغییر کرده است. از آنجا که کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) بعد از احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) اجرا می‌شود، FIA_UAU.1(2) وابسته به FIA_UAU.1(1) است و FIA_UAU.1(1) به FIA_UID.1. بنابراین،وابستگی به صورت غیر مستقیم برآورده شده است.

### ۸-۳-۲- وابستگی الزامات تضمین امنیت محصول

وابستگی EAL4 در معیار مشترک در حال حاضر برآوده شده است. بنابراین، این منطق حذف شده است. در جدول ۱۶، وابستگی‌های الزامات تضمین امنیت افزوده شده نشان داده شده است.

ADV_IMP.2 با ALC_CMC.5 وابستگی دارد، اما ADV_IMP.2 برای ایجاد امکان تحلیل بر روی تمام بازنمایی پیاده‌سازی افزوده شده است تا بررسی کند که آیا توابع هدف امنیتی (TSF) با دقت پیاده‌سازی شده است و هیچ کد معیوبی وجود ندارد. و ADV_IMP.2، به این پرفایل حفاظتی افزوده نشده است، چرا که CM در سطح ALC_CMC.5 که اقدامات خودکاری برای تعیین این موضوع که آیا تغییرات در اقلام پیکربندی بر دیگر اقلام پیکربندی تأثیر دارد یا خیر ضرورتاً مورد نیاز تشخیص داده نشده است.

AVA_VLA.4 دارای وابستگی با ADV_IMP.1 و ATE_DPT.1 است. این وابستگی با ADV_IMP.2 و ATE_DPT.2 در ارتباط‌های سلسله مراتبی با ADV_IMP.1 و ATE_DPT.1 برآورده شده است.

**جدول ۱۶- وابستگی عناصر تضمین**

| شماره | مؤلفه‌ی تضمین | وابستگی | شماره مرجع |
|---|---|---|---|
| ۱ | ADV_IMP.2 | ADV_TDS.3<br>ALC_TAT.1<br>ALC_CMC.5 | EAL4<br>EAL4<br>هیچ |
| ۲ | ATE_DPT.2 | ADV_ARC.1<br>ADV_TDS.3<br>ATE_FUN.1 | EAL4<br>EAL4<br>EAL4 |
| ۳ | AVA_VAN.4 | ADV_ARC.1<br>ADV_FSP.4<br>ADV_TDS.3<br>ADV_IMP.1<br>AGD_OPE.1<br>AGD_PRE.1<br>ATE_DPT.1 | EAL4<br>EAL4<br>EAL4<br>1<br>EAL4<br>EAL4<br>2 |

### ۸-۴- منطق پشتیبانی دو طرفه و سازگاری داخلی

این منطق نشان می‌دهد که الزامات امنیتی محصول پشتیبانی دو طرفه و سازگاری داخلی‌ای دارند.

در بخش ۶-۳-۳-۱- وابستگی الزامات کارکرد امنیتی محصول و در بخش ۶-۳-۳-۲- وابستگی الزامات تضمین امنیت محصول معرفی شده‌اند. در این دو بخش وابستگی به عنوان یک واسطه حمایتی در میان الزامات امنیتی مورد تحلیل قرار گرفته است که این وابستگی به دیگر الزامات امنیتی به دلیل ناکافی بودن یک الزام امنیتی به منظور دستیابی به یک هدف امنیتی ضروری است. در مواردی که وابستگی برآورده نشده باشد، منطق افزوده‌ای ارائه شده است.

همچنین، اگرچه هیچ وابستگی در میان الزامات کارکرد امنیتی وجود ندارد، الزامات کارکرد امنیتی در واسطه با عملیات توابع هدف امنیتی (TSF) که در ادامه تشریح خواهد شد، به صورت دو طرفه حمایت کننده و به صورت داخلی سازگارند.

در فاز شخصی، عامل شخصی‌سازی داده برنامه‌ی کاربردی سند مسافرتی قابل خواندن توسط ماشین (MRTD) ((FMT_MTD.1(1)، FMT_MSA.3) را ثبت کرده و تابع نوشتن را غیر فعال می‌کند به گونه‌ای که هنگامی که محصول به فاز استفاده عملیاتی (FMT_MOF.1، FMT_SMF.1) تحویل داده می‌شود توسط موجودیت‌های بیرونی مورد تغییر قرار نمی‌گیرد. نقش عامل شخصی‌سازی که به عنوان نقش امنیتی (FMT_SMR.1) تعریف شده است، تحت کنترل خط‌مشی‌های کنترل دسترسی گذرنامه الکترونیک (FDP_ACC.1، FDP_ACF.1) است.

توابع هدف امنیتی (TSF)، پس از شناسایی سامانه بازرسی (FIA_UID.1)، احراز هویت دو طرفه‌ی کنترل دسترسی پایه (BAC) ((1) FIA_UAU.1) و کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA) ((2) FIA_UAU.1) را طبق قوانین کاربرد ساز و کار احراز هویت (FIA_UAU.5) اجرا می‌کند. چنانچه سامانه بازرسی در احراز هویت با شکست مواجه شود، نشست خاتمه می‌یابد (FIA_AFL.1). اعداد تصادفی باید به گونه‌ای مورد استفاده قرار گیرند که از استفاده مجدد از داده مرتبط با احراز هویت مورد استفاده در احراز هویت جلوگیری شود (FIA_UAU.4). به منظور حصول اطمینان از اعداد تصادفی امن و گواهی‌های امن استفاده شده در کنترل دسترسی توسعه یافته – احراز هویت پایانه (EAC-TA)، گواهی‌ها باید مورد بررسی و به روزرسانی قرار گیرند (FMT_MTD.3). بنابراین، این الزامات امنیتی به صورت دو طرفه حمایت کننده و به صورت داخلی سازگارند.

توابع هدف امنیتی (TSF) باید شمارنده‌ی دنباله‌ی ارسال (SSC) را با مقدار صفر مقداردهی اولیه کند ((2) FMT_MTD.1) تا هنگامی که پیام‌رسانی امن کنترل دسترسی پایه (BAC) (FDP_UCT.1 و FDP_UIT.1) برقرار شده به منظور حفاظت از داده کاربر انتقال یافته خاتمه می‌یابد پایان کانال را نشان دهد. بنابراین، این الزامات امنیتی به صورت دو طرفه حمایت کننده و به صورت داخلی سازگارند.

توابع هدف امنیتی (TSF) باید اطمینان حاصل کند که پدیده‌های فیزیکی مانند جریان، ولتاژ و امواج الکترومغناطیسی و غیره که هنگام انجام عملیات رمزنگاری، ((1) FCS_COP.1، (2)FCS_COP.1، (4)FCS_COP.1) اتفاق می‌افتند مورد بهره‌برداری عوامل (FPR_UNO.1) قرار نمی‌گیرند. داده مربوط به رمزنگاری که در حافظه موقت ایجاد شده‌اند، باید پس از عملیات رمزنگاری تخریب شوند تا از استفاده مجدد جلوگیری شود (FCS_CKM.4، FDP_RIP.1). بنابراین، این الزامات امنیتی به صورت دو طرفه حمایت کننده و به صورت داخلی سازگارند.

در صورتی که تغییر داده انتقال یافته‌ی توابع هدف امنیتی (TSF) شناسایی شد، توابع هدف امنیتی (TSF) باید نشست را خاتمه دهد (FPT_ITI.1) و حق دسترسی سامانه بازرسی را مجدداً تنظیم نماید (FMT_MSA.1). بنابراین، این الزامات امنیتی به صورت دو طرفه حمایت کننده و به صورت داخلی سازگارند.

توابع هدف امنیتی (TSF) باید خود آزمایی‌ای را تحت شرایط تصمیم گرفته شده توسط نویسنده هدف امنیتی اجرا کند (FPT_TST.1). در صورت تشخیص خرابی، محصول باید حالت امن را حفظ کند (FPT_FLS.1). بنابراین، این الزامات امنیتی به صورت دو طرفه حمایت کننده و به صورت داخلی سازگارند.

## پیوست ۱ نمادها و اختصارات آن‌ها

| نماد | معادل انگلیسی | معادل فارسی |
|---|---|---|
| AA | Active Authentication | احرازهویت فعال |
| BAC | Basic Access Control | کنترل دسترسی پایه |
| BIS | BAC Inspection System | سامانه بازرسی کنترل دسترسی پایه (BAC) |
| CA | Chip Authentication | احراز هویت تراشه |
| CC | Common Criteria | معیار مشترک |
| CCMB | Common Criteria Maintenance Board | هئیت نگهداشت معیار مشترک |
| CCRA | Common Criteria Recognition Arrangement | توافقنامه‌ی به رسمیت شناختن معیار مشترک |
| COS | Card Operating System | سیستم عامل کارت |
| CSCA | Country Signing Certification Authority | مرجع صلاحیت دار امضا کننده گواهی کشور |
| CVCA | Country Verifying Certification Authority | مرجع صلاحیت‌دار تأییدکننده گواهی کشور |
| DES | Data Encryption Standard | استاندارد رمزگذاری داده |
| DF | Dedicated File | فایل تخصیص یافته |
| DG | Data Group | گروه داده |
| DH | Diffie Hellman | دیفی - هلمن |
| DPA | Differential Power Analysis | تحلیل تفاضلی نیرو |
| DS | Document Signer | امضا کننده‌ی سند |
| DV | Document Verifier | تایید کننده سند |
| EAC | Extended Access Control | کنترل دسترسی توسعه یافته |
| EAC-CA | EAC Chip Authentication | کنترل دسترسی توسعه یافته - احراز هویت تراشه |

| | | |
|---|---|---|
| EAC-TA | EAC-terminalAuthentication | کنترل دسترسی توسعه یافته – احراز هویت پایانه |
| EAL | Evaluation Assurance Level | سطح تضمین ارزیابی |
| ECDH | Elliptic Curve Diffie Hellman | منحنی بیضوی دیفی- هلمن |
| EEPROM | Electrically Erasable Programmable Read Only Memory | حافظه‌ی فقط خواندنی قابل پاک کردن و قابل برنامه‌نویسی به صورت الکترونیکی |
| EF | Elementary File | فایل ابتدایی |
| EIS | EAC Inspection System | سامانه بازرسی کنترل دسترسی توسعه یافته (EAC) |
| IC | Integrated Circuit | مدار مجتمع |
| ICAO | International Civil Aviation Organization | سازمان بین‌المللی هواپیمایی غیر نظامی |
| IS | Inspection System | سامانه بازرسی |
| ISO | International Organization for Standardization | سازمان بین‌المللی استاندارد |
| IT | Information Technology | فناوری اطلاعات |
| KDF | Key Derivation Function | تابع اشتقاق کلید |
| KDM | Key Derivation Mechanism | ساز و کار اشتقاق کلید |
| LDS | Logical Data Structure | ساختار داده منطقی |
| MAC | Message Authentication Code | کد احراز هویت پیام |
| MF | Master File | فایل اصلی |
| MRTD | Machine Readable Travel Document | سند مسافرتی قابل خواندن توسط ماشین |
| MRZ | Machine Readable Zone | ناحیه قابل خواندن توسط ماشین |
| PA | Passive Authentication | احراز هویت غیر فعال |
| PKI | Public Key Infrastructure | زیرساخت کلید عمومی |
| PP | Protection Profile | پرفایل حفاظتی |
| RAM | Random Access Memory | حافظه‌ی دستیابی تصادفی |

| | | |
|---|---|---|
| RF | Radio Frequency | فرکانس رادیویی |
| ROM | Read Only Memory | حفظه فقط خواندنی |
| SFP | Security Function Policy | خط مشی کارکرد امنیتی |
| SOD | Security Object of Document | سند موجودیت غیر فعال امنیتی |
| SPA | simple power analysis | تحلیل نیروی ساده |
| ST | Security Target | هدف امنیتی |
| TA | Terminal Authentication | احراز هویت پایانه |
| TDES | Triple-DES | استاندارد رمزگذاری داده سه گانه |
| TOE | Target of Evaluation | محصول |
| TSF | TOE Security Functions | توابع هدف امنیتی |

## پیوست ۲ مراجع


[1] Doc 9303 “Machine Readable Travel Documents” Part 1 “Machine Readable Passports” Volume 2 “Specification for Electronically Enabled Passports with Biometri Identification Capability” Sixth Edition, International Civil Aviation Organization(ICAO), 2006. 8

[2] Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, TR- 03110, Bundesamt für Sicherheit in der Information stechnik(BSI), 2008. 2

[3] Common Criteria Protection Profile, Machine Readable Travel Document with ICAO Application, Basic Access Control, Bundesamt für Sicherheit in der Informationstechnik(BSI), 2005. 8

[4] Common Criteria Protection Profile, Machine Readable Travel Document with ICAO Application, Extended Access Control, Bundesamt für Sicherheit in der Informationstechnik(BSI), 2006. 9

[5] Common Criteria for Information Technology Security Evaluation, Version 3.1r3, CCMB, 2009. 7

[6] Common Methodology for Information Technology Security Evaluation, Version 3.1r3, CCMB, 2009. 7

[7] Smart Card Open Platform Protection Profile V2.1, IT Security Certification Center, 2010.6

[8] Supporting Document Mandatory Technical Document, Application of Attack Potential to Smartcards, Version 2.1, CCDB, 2006. 4

[9] Supporting Document Mandatory Technical Document, The Application of CC to Integrated Circuits, Version 2.0, CCDB, 2006. 4

[10] ISO/IEC 7816-4:2005, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange

[11] ISO/IEC 7816-8:2004, Identification cards – Integrated circuit cards – Part 8: Commands for security operations

[12] ISO/IEC 7816-9:2004, Identification cards – Integrated circuit cards – Part 9: Commands for card management

[13] ISO/IEC 14443-4:2001, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol

[14] ISO/IEC 9798-2:1999, Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms

[15] ISO/IEC 11770-2:1996, Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques

[16] ISO/IEC 10116:2006, Information technology – Security techniques – Modes of operation for an n-bit block cipher

[17] ISO/IEC 18033-3:2005, Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers

[18] ISO/IEC 10118-3:2004, Information technology – Security techniques – Hash-functions - Part 3: Dedicated hash-functions

[19] ISO/IEC 9797-1:1999, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block Cipher

[20] ISO/IEC 15946-3:2002, Information technology - Security techniques – Cryptographic techniques based on elliptic curves - Part 3: Key Establishment

[21] ISO/IEC 15946-2:2002, Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital Signatures.