به نام خدا

پروفایل حفاظتی افزاره ایجاد امضای امن- قسمت ۲: افزاره با تولید کلید

بهمن ۹۵

نسخه ۱,۱

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 ارائه‌شده‌اند، در محصول خود فراهم کنند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد.

در این سند الزامات امنیتی پروفایل حفاظتی افزاره ایجاد امضای امن[۱] که ممکن است کلیدهای امضا را به صورت داخلی تولید کند، تبیین می‌شود: «افزاره ایجاد امضای امن با تولید کلید، (SSCD with key generation)».

این پروفایل حفاظتی، الزامات امنیتی اصلی برای افزاره امن تولید کلید امضا[۲] (داده ایجاد امضا،[۳] (SCD)) و نیز برای ایجاد امضای الکترونیکی با کلیدهای تولیدشده را بیان می‌کند. افزاره‌ای که با این پروفایل حفاظتی ارزیابی می‌شود و در محیط‌های تعیین‌شده استفاده می‌شود می‌تواند برای ایجاد هر نوع امضای دیجیتالی قابل‌اعتماد باشد. این پروفایل حفاظتی برای هر افزاره‌ای که به‌منظور ایجاد امضای دیجیتالی پیکربندی‌شده است، می‌تواند به کار گرفته شود. به‌طور خاص این پروفایل حفاظتی، صلاحیت محصول به‌عنوان افزاره‌ای برای ایجاد امضای الکترونیکی پیشرفته همان‌گونه که در دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا[۴] توضیح داده‌شده است را نیز تعیین می‌کند.

---

[۱] Secure Signature Creation Device (SSCD)

[۲] SSCD ای که می‌تواند SCD/SVD مربوط به خود را ایجاد کند، به عنوان SSCD نوع ۳ شناخته می‌شود که از نوع ۱ و ۲ آن متمایز می‌باشد. پروفایل حفاظتی برای SSCD نوع ۲ در " پروفایل حفاظتی افزاره ایجاد امضای امن: افزاره با ورود کلید" می‌باشد.

[۳] Signature Creation Data

[۴] دستورالعمل 1999/93/ec پارلمان اروپا و شورای ۱۳ دسامبر ۱۹۹۹ مربوط به "چارچوب عمومی برای امضای الکترونیک" [1]، می‌باشد.

بعد از آنکه افزاره ایجاد امضای امن (SSCD)، کلید امضا را تولید کرد، کلید عمومی متناظر (داده درستی‌سنجی امضا،[۱] (SVD)) به‌عنوان ورودی برنامه کاربردی تولید گواهی[۲] (CGA) ارائه می‌شود. الزامات امنیتی برای صدور داده درستی‌سنجی امضا در پروفایل حفاظتی («پروفایل حفاظتی برای افزاره ایجاد امضای امن- قسمت ۳: افزاره‌ای با تولید کلید و کانال قابل‌اعتماد بین افزاره ایجاد امضای امن و برنامه کاربردی تولید گواهی») مشخص‌شده است که در این سند در مورد آن بحث نشده است.

سطح تضمین این پروفایل حفاظتی، سطح تضمین ارزیابی ۴[۳] (EAL4) تکمیل شده با تحلیل آسیب‌پذیری روشمند هوشمند است.

۲- فرهنگ اصطلاحات

برای این استاندارد اروپایی اصطلاحات زیر تعریف می‌شود:

۲-۱- مراجع قانونگذاری

این استاندارد اروپایی، منعکس‌کننده الزامات دستورالعمل اروپایی در شرایط فنی پروفایل حفاظتی می‌باشد. اصطلاحات زیر در متن برای ارجاع به دستورالعمل استفاده می‌شود:

- **دستورالعمل**

دستورالعمل 1999/93/ec پارلمان اروپا و شورای ۱۳ دسامبر ۱۹۹۹ مربوط به «چارچوب عمومی برای امضای الکترونیک» است [1].

تبصره ۱: ارجاع این سند به فصل یا پاراگراف خاص این دستورالعمل به این صورت می‌باشد: (دستورالعمل: n.m).

[۱] Signature Verification Data

[۲] Certificate Generation Application

[۳] Evaluation Assurance Level

- **پیوست**

یکی از پیوست‌ها، پیوست ۱ ، پیوست ۲ یا پیوست ۳ دستورالعمل.

۲-۲- اصطلاحات ارزیابی امنیت

- **استاندارد ارزیابی معیار مشترک[۱] (CC)**

استاندارد ارزیابی معیار مشترک برای ارزیابی امنیت فناوری‌های اطلاعات است و مجموعه‌ای از معیارها و روش‌های اجرایی برای ارزیابی ویژگی‌های امنیتی یک محصول.

تبصره: برای جزئیات بیشتر در مورد مشخصه‌های معیار مشترک به مراجع مراجعه شود.

- **سطح تضمین ارزیابی[۲] (EAL)**

مجموعه‌ای از الزامات تضمین برای یک محصول، فرایندهای ساخت آن و ارزیابی امنیتی که توسط معیار مشترک مشخص شده‌است و از قسمت سوم از سندهای سه‌گانه «استاندارد ارزیابی معیار مشترک» برگرفته شده است و نشان‌دهنده سطح امنیتی محصول می‌باشد. سطوح تضمین از سطح ۱ تا سطح ۷ می‌باشند.

- **پروفایل حفاظتی[۳] (PP)**

[۱] Common Criteria

[۲] Evaluation Assurance Level

[۳] Protection Profile

سندی است که الزامات امنیتی کلاسی از محصولات را مشخص می‌کند که از نظر ساختار و محتوا با قوانین تعریف شده توسط معیار مشترک تطابق دارد.

- **هدف امنیتی[۱] (ST)**

سندی است که الزامات امنیتی را برای محصولات خاصی مشخص می‌کند که از نظر ساختار و محتوا با قوانین تعریف شده توسط معیار مشترک مطابقت دارد که این قوانین ممکن است بر اساس یک یا چند پروفایل حافظتی دیگری باشد.

- **هدف ارزیابی[۲] (TOE)**

مرجع انتزاعی در یک سند مانند پروفایل حفاظتی، برای یک محصول خاص که الزامات امنیتی خاصی را برآورده می‌سازد.

- **توابع امنیتی هدف ارزیابی[۳] (TSF)**

توابع پیاده‌سازی شده توسط محصول برای برآورده ساختن الزامات تعیین‌شده برای آن در یک پروفایل حفاظتی یا هدف امنیتی.

۳-۲- اصطلاحات فنی

- **مدیر سیستم[۴]**

کاربری که مقداردهی اولیه محصول، شخصی‌سازی محصول و یا کارکردهای اجرایی محصول را انجام می‌دهد.

---

[۱] Security Target

[۲] Target of Evaluation

[۳] TOE Security Functions

[۴] Administrator

- **امضای الکترونیکی پیشرفته**[۱]

امضای دیجیتالی که الزامات خاصی از دستورالعمل مرتبط را برطرف می‌سازد (دستورالعمل: ۲,۲).

تبصره: بر اساس دستورالعمل، امضای دیجیتالی در صورتی به‌عنوان امضای الکترونیکی واجد شرایط است، که:

- به شکل منحصر به فرد به صاحب‌امضای مربوطه پیوند داده شود.
- قادر به شناسایی صاحب‌امضا باشد.
- با استفاده از ابزارهایی ایجاد شده‌باشد که صاحب‌امضا می‌تواند تحت کنترل انحصاری خود داشته باشد.
- به‌گونه‌ای به داده‌های مرتبط پیوند داده شده باشد که هر تغییر بعدی در داده‌ها قابل تشخیص باشد.

- **داده احرازهویت**[۲]

اطلاعات استفاده‌شده برای بررسی و تایید هویت ادعا شده از سوی یک کاربر.

- **گواهی**[۳]

امضای دیجیتالی مورد استفاده به‌عنوان گواهی الکترونیکی که یک داده درستی‌سنجی امضا (SVD) را به فرد پیوند داده و هویت آن فرد را به عنوان یک امضاکننده مجاز تأیید می‌کند (دستورالعمل: ۲,۹).

- **اطلاعات گواهی**[۱]

[۱] Advanced electronic signature

[۲] Authentication data

[۳] Certificate

اطلاعات مرتبط با یک زوج داده درستی سنجی امضا / داده ایجاد امضا (SCD/SVD) که ممکن است در یک افزاره ایجاد امضای امن ذخیره شده باشد.

تبصره: اطلاعات گواهی می‌تواند شامل موارد زیر باشد:

- گواهی کلید عمومی امضاکننده یا
- یک یا چند مقدار چکیده‌ساز[۲] پیام گواهی کلید عمومی امضاکننده به همراه شناسه تابع چکیده‌ساز که برای محاسبه مقادیر چکیده پیام از آن استفاده شده است.

اطلاعات گواهی ممکن است با اطلاعات لازم برای مجوز دادن به کاربر جهت تمایز بین چند گواهی، ترکیب شود.

- **برنامه‌کاربردی تولید گواهی (CGA)**[۳]

---

[۱] Certificate information

[۲] hash

[۳] Certificate generation application

مجموعه‌ای از اجزای برنامه‌کاربردی که داده درستی سنجی امضا (SVD) را از افزاره ایجاد امضای امن (SSCD) دریافت می‌کند تا با به دست آوردن داده‌ای که باید در گواهی گنجانده شود، گواهی تولید کرده و امضای دیجیتالی را از گواهی ایجاد کند.

- **تامین‌کننده خدمات صدور گواهی[۱] (CSP)**

موجودیتی که گواهی را صادر می‌کند یا خدمات مرتبط با امضاهای الکترونیک را ارائه می‌دهد (دستورالعمل: ۲,۱۱).

- **داده‌ای که باید امضا شوند[۲] (DTBS)**

تمام داده‌های الکترونیکی که باید امضا شوند از جمله پیام کاربر و خصیصه‌های امضا.

- **داده‌ای که باید امضا شوند یا بازنمایی منحصر به فرد متعلق به آن[۳] (DTBS/R)**

داده‌هایی که به عنوان ورودی در عملیات ایجاد امضای یکتا، توسط افزاره ایجاد امضای امن دریافت شده‌است.

تبصره: داده‌ای که باید امضا شوند یا بازنمایی منحصر به فرد متعلق به آن شامل:

- مقدار چکیده‌پیام داده‌ای که بایستی امضا شود (DTBS)، یا
- مقدار چکیده‌پیام میانی[۴] قسمت اولیه داده‌ای که باید امضا شود (DTBS) که با قسمت باقیمانده از داده‌ای که باید امضا شود (DTBS) تکمیل شده است، یا
- خود داده‌ای که باید امضا شود (DTBS).

[۱] Certification Service Provider

[۲] Data to be signed

[۳] Data to be signed or its unique representation

[۴] intermediate

- **کاربر مجاز**[۱]

کاربر افزاره ایجاد امضای امن که مالکیت آن را از یک تأمین‌کننده خدمات تدارک افزاره ایجاد امضای امن (SSCD) دریافت کرده است و کسی است که می‌تواند به عنوان صاحب‌امضا توسط افزاره ایجاد امضای امن (SSCD) احراز اصالت شود.

- **مرجع توصیه شده**[۲]

نهاد سازمانی که توسط یک کشور عضو اتحادیه اروپا به‌عنوان مسئول اعطای مجوز رسمی[۳] و نظارت بر فرایند ارزیابی محصولات منطبق بر این استاندارد و تعیین‌کننده الگوریتم‌ها و پارامترهای الگوریتم قابل قبول، تعیین شده است.

- **گواهی واجد شرایط**

گواهی کلید عمومی که الزامات موجود در پیوست ۱ را برآورده کرده و توسط تامین‌کننده خدمات صدور گواهی (CSP) ارائه می‌شود که الزامات موجود در پیوست ۲ دستورالعمل را برآورده می‌کند (دستورالعمل: ۲,۱۰).

- **امضای الکترونیکی واجد شرایط**

امضای الکترونیکی پیشرفته که با یک کلید گواهی‌شده با یک گواهی واجد شرایط توسط افزاره ایجاد امضای امن (SSCD) ایجاد شده‌است (دستورالعمل: ۵,۱).

- **داده احرازهویت مرجع**[۱] **(RAD)**

[۱] Legitimate user

[۲] Notified body

[۳] accreditation

داده‌ای که به‌صورت ماندگار توسط محصول جهت احرازهویت یک کاربر به‌عنوان کاربر مجاز برای ایفای یک نقش خاص ذخیره شده است.

- **افزاره ایجاد امضای امن[۲] (SSCD)**

افزاره شخصی‌شده‌ای که الزامات موجود در پیوست ۳ را با ارزیابی شدن بر اساس اهداف امنیتی مطابق با یک هدف امنیتی منطبق بر این پروفایل حفاظتی برآورده می‌سازد (دستورالعمل: ۲,۵ و ۲,۶).

- **صاحب‌امضا[۳]**

کاربر مجاز یک افزاره ایجاد امضای امن (SSCD) که در گواهی درستی‌سنجی امضا به آن مرتبط شده است و کسی است که توسط افزاره ایجاد امضای امن (SSCD) برای اجرای کارکردها و توابع ایجاد امضا مجاز شده است (دستورالعمل: ۲,۳).

- **مشخصه‌های امضا[۱]**

---

[۱] Reference Authentication data

[2] Secure signature creation device

[3] Signatory

اطلاعات افزوده‌ای که همراه با پیام کاربر امضا می‌شود.

- **برنامه‌کاربردی ایجاد امضا[۲] (SCA)**

برنامه‌کاربردی که با یک واسط کاربری، افزاره ایجاد امضای امن (SSCD) را با هدف ایجاد امضای الکترونیک تکمیل می‌کند.

تبصره: برنامه‌کاربردی ایجاد امضا نرم‌افزاری است که شامل مجموعه‌ای از اجزای کاربردی پیکربندی‌شده برای موارد زیر است:

- ارائه داده‌ای که باید امضا شود (DTBS) جهت بازنگری توسط صاحب‌امضا،
- گرفتن تصمیم توسط صاحب‌امضا قبل از فرایند امضا،
- اگر صاحب‌امضا با داده و یا فعالیت بدون‌ابهام مشخصی نیت خود را برای امضا نشان دهد، داده‌ای که باید امضا شود یا بازنمایی منحصر به فرد متعلق به آن (DTBS/R) را به محصول می‌فرستد.

---

[۱] Signature attributes

[2] Signature creation application

- پردازش امضای الکترونیک تولید شده توسط افزاره ایجاد امضای امن (SSCD) به‌گونه‌ای مناسب از جمله با پیوست به داده‌ای که باید امضا شود (DTBS).

- **داده ایجاد امضا[1] (SCD)**

کلید رمزنگاری خصوصی که جهت ایجاد امضای الکترونیکی تحت کنترل انحصاری توسط صاحب‌امضا در افزاره ایجاد امضای امن (SSCD) ذخیره شده است (دستورالعمل: ۲,۴).

- **سامانه ایجاد امضا[2] (SCS)**

سامانه کاملی شامل برنامه‌کاربردی ایجاد امضا (SCA) و افزاره ایجاد امضای امن (SSCD) که امضای الکترونیکی ایجاد می‌کند.

- **داده درستی‌سنجی امضا[3] (SVD)**

کلید رمزنگاری عمومی که می‌تواند برای بررسی امضای الکترونیکی استفاده شود (دستورالعمل: ۲,۷).

- **خدمات تدارک افزاره ایجاد امضای امن[4]**

خدمات انجام شده برای آماده‌سازی و ارائه یک افزاره ایجاد امضای امن (SSCD) برای امضاکننده و پشتیبانی از صاحب‌امضا با صدور گواهی کلیدهای تولید شده و کارکردها و توابع اجرایی افزاره ایجاد امضای امن (SSCD).

[1] Signature creation data
[2] Signature Creation System
[3] Signature verification data
[4] SSCD provisioning service

- **کاربر**

موجودیت (کاربر انسانی یا موجودیت بیرونی فناوری اطلاعات) که بیرون از محصول قرار گرفته و با محصول تعامل دارد.

- **پیام کاربر**

داده‌ای که به عنوان ورودی صحیح برای امضا توسط صاحب‌امضا تعیین شده است.

- **داده درستی‌سنجی احرازهویت[۱] (VAD)**

داده‌ای که به عنوان ورودی جهت احرازهویت با شناخت یا با داده به دست آمده از مشخصه‌های زیست‌سنجی کاربر برای افزاره ایجاد امضای امن (SSCD) فراهم شده است.

۳- شرح محصول

۳-۱- محصول

محصول ترکیبی از سخت‌افزار و نرم‌افزار پیکربندی شده برای ورود، استفاده و مدیریت امن داده ایجاد امضا (SCD) است. افزاره ایجاد امضای امن از داده ایجاد امضا (SCD) در تمام طول چرخه حیاتش که با ورود جهت استفاده در یک فرایند ایجاد داده تنها توسط صاحب‌امضا آغاز می‌شود محافظت می‌کند.

محصول کارکردهای زیر را ارائه می‌دهد:

۱) تولید داده ایجاد امضا (SCD) و به صورت اختیاری، داده درستی‌سنجی امضا (SVD) متناظر[۲]،

۲) صدور داده درستی‌سنجی امضا (SVD) برای صدور گواهی،

[1] Verification authentication data

[۲] correspondent

۳) دریافت و ذخیره اطلاعات گواهی، به صورت اختیاری،

۴) تغییر حالت دادن محصول از یک حالت غیر عملیاتی به یک حالت عملیاتی، و

۵) ایجاد امضاهای دیجیتال برای داده در یک حالت عملیاتی، با مراحل زیر:

الف- انتخاب یک مجموعه از داده ایجاد امضا (SCD) اگر چندین داده ایجاد امضا (SCD) در افزاره ایجاد امضای امن وجود دارد،

ب- دریافت داده‌هایی که باید امضا شوند و یا بازنمایی منحصر به فرد متعلق به آن (DTBS/R)،

پ- احرازهویت صاحب‌امضا و تعیین نیت او از امضا،

ت- به کار بردن یک تابع ایجاد امضای رمزنگاری شده مناسب با استفاده از داده ایجاد امضا (SCD) انتخاب شده برای داده‌هایی که باید امضا شوند و یا بازنمایی منحصر به فرد متعلق به آن (DTBS/R).

محصول ممکن است کارکردهای خود را برای ایجاد امضای الکترونیک منطبق با مشخصه‌های موجود در ETSI TS 101 733 (CAdES) و ETSI TS 101 903 (XAdES) پیاده‌سازی کند. در این صورت هدف ارزیابی ممکن است توابع پشتیبانی بیشتری ازجمله برای پشتیبانی از دریافت و یا اعتبارسنجی مهر زمانی[۱]، ارائه دهد.

محصول همه قابلیت‌های کارکردی امنیتی IT ضروری برای حصول اطمینان از رازمانی داده ایجاد امضا (SCD) و امنیت امضای دیجیتال را در بر می‌گیرد.

محصول برای استفاده صاحب‌امضا به شکل زیر آماده شده است:

۱) تولید حداقل یک زوج داده ایجاد امضا / داده درستی‌سنجی امضا، و

۲) شخصی‌سازی برای صاحب‌امضا با ذخیره در محصول:

الف- داده احرازهویت مرجع (RAD) صاحب‌امضا

ب- اطلاعات گواهی برای حداقل یک داده ایجاد امضا (SCD) در محصول، به صورت اختیاری.

[۱] time stamp

بعد از آماده‌سازی، داده ایجاد امضا (SCD) باید در یک حالت غیرعملیاتی باشد. به محض دریافت محصول صاحب‌امضا باید حالت غیر عملیاتی آن را بررسی کند و حالت داده ایجاد امضا (SCD) را به عملیاتی تغییر دهد.

بعد از آماده‌سازی توصیه می‌شود کاربر قانونی مورد نظر از داده درستی سنجی احزار هویت (VAD) صاحب‌امضا که برای استفاده محصول در امضا کردن مورد نیاز است اطلاع یابد. اگر داده درستی سنجی احزار هویت (VAD) یک کلمه‌عبور یا پین[۱] باشد، ارائه این اطلاعات باید از محرمانگی داده احرازهویت مرجع (RAD) متناظر محافظت کند.

اگر دیگر لزومی به استفاده از یک داده ایجاد امضا (SCD) وجود ندارد، محصول آن داده ایجاد امضا (SCD) را غیرفعال خواهد کرد. به طور مثال با پاک کردن آن از حافظه.

۲-۳- عملکرد هدف ارزیابی

همان‌طور که در **Error! Reference source not found.** خلاصه شده است، این بخش مروری از کارکرد هدف ارزیابی در محیط عملیاتی مجزا را ارائه می‌دهد.

۱-۲-۳-محیط امضا

جایی که محصول با امضا کننده برای امضای داده با برنامه‌کاربردی ایجاد امضا (SCA) تعامل می‌کند. امضای داده بعد از اصالت‌سنجی امضا کننده به عنوان صاحب آن امضا صورت می‌گیرد. برنامه‌کاربری ایجاد امضا (SCA)، داده‌ای که باید امضا شود (DTBS) و یا بازنمایی منحصر به فرد متعلق به آن (DTBS/R) را به عنوان ورودی‌ای برای کارکرد ایجاد امضای محصول فراهم کرده و امضای دیجیتال حاصل[۱] را به دست می‌آورد.

[۱] PIN

۲-۲-۳- محیط آماده‌سازی

جایی است که محصول جهت بدست آوردن گواهی برای داده درستی‌سنجی امضای (SVD) متناظر با داده ایجاد امضا (SCD) که محصول تولید کرده است از طریق برنامه کاربردی تولید گواهی (CGA) با تامین‌کننده خدمات صدور گواهی تعامل می‌کند. محیط مقداردهی اولیه بیشتر برای شخصی‌سازی محصول با مقادیر اولیه داده احرازهویت مرجع (RAD) با محصول تعامل می‌کند.

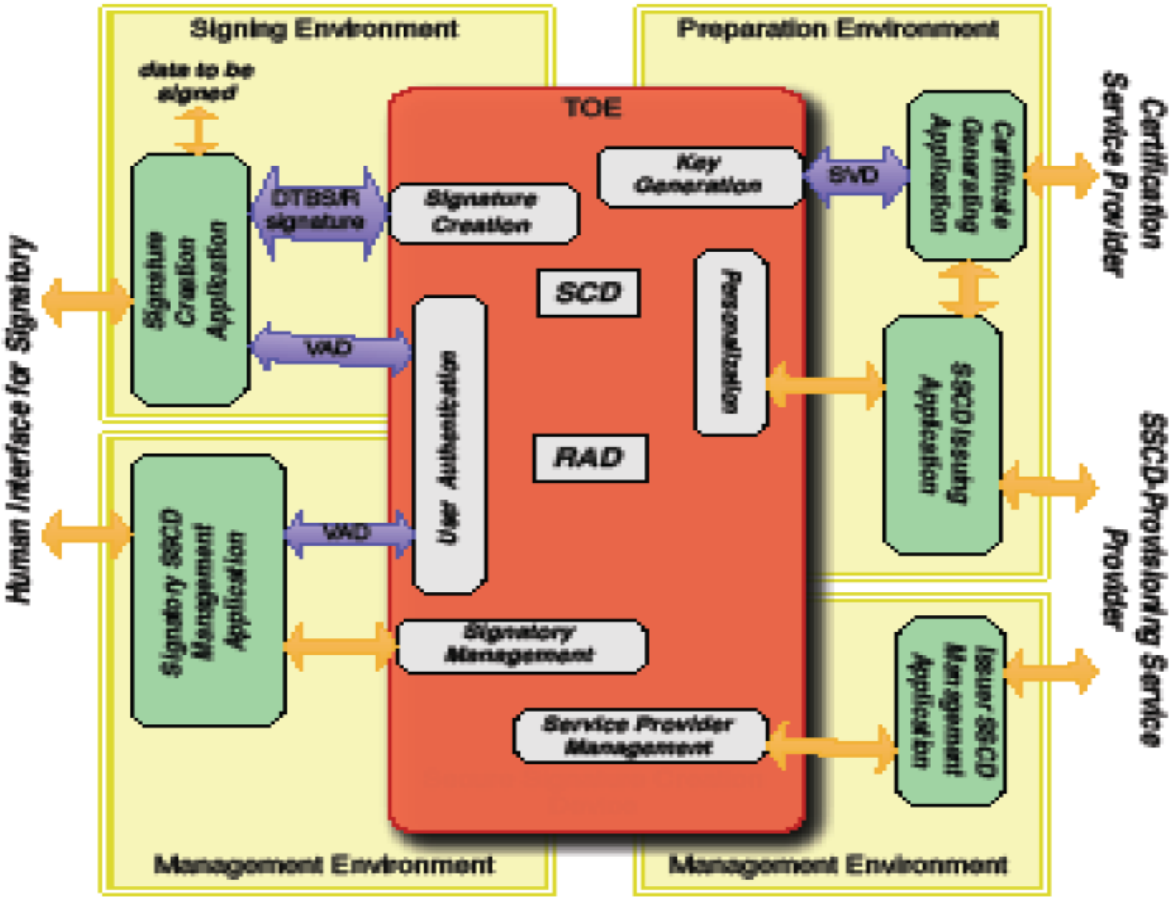
۲-۲-۳- محیط‌های مدیریتی

جایی است که محصول با کاربر و یا تأمین‌کننده خدمات تدارک افزاره ایجاد امضای امن برای انجام عملیات مدیریتی تعامل دارد به طور مثال، برای تنظیم مجدد یک داده احرازهویت مرجع (RAD) مسدود شده برای صاحب‌امضا. یک افزاره منحصر به فرد، به طور مثال پایانه کارت هوشمند، ممکن است محیط امن مورد نیاز برای مدیریت و امضا کردن را فراهم آورد.

---

[۱] در سطح کارکردی محض، SSCD امضای دیجیتالی را تولید می‌کند؛ برای پیاده‌سازی SSCD، با توجه به الزامات موجود در این پروفایل حفاظتی و گواهی کلید ایجاد شده همانگونه که در پیوست ۱ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا توضیح داده شده است، نتیجه فرایند امضا می‌تواند برای ایجاد امضای الکترونیکی واجد شرایط استفاده شود.

محیط امضا، محیط مدیریتی و محیط آماده‌سازی هر سه امن هستند و از داده‌های تبادل شده توسط محصول حفاظت می‌کنند.



شکل ۱- کارکردهای اصولی افزاره ایجاد امضای امن و محیط‌های عملیاتی

محصول، داده ایجاد امضا (SCD) و داده احرازهویت مرجع (RAD) را ذخیره می‌کند. محصول ممکن است چندین نمونه از داده ایجاد امضا (SCD) را ذخیره کند. در این صورت، محصول تابعی برای شناسایی هر داده ایجاد امضا (SCD) فراهم می‌کند و برنامه‌کاربردی ایجاد امضا (SCA) رابطی برای امضا کننده فراهم می‌آورد تا یک داده ایجاد امضا (SCD) را برای استفاده در تابع ایجاد امضای افزاره ایجاد امضای امن (SSCD) انتخاب کند. محصول از محرمانگی و یکپارچگی داده ایجاد امضا (SCD) محافظت کرده و استفاده از آن را محدود به ایجاد امضا توسط صاحب‌امضای خودش می‌کند. همان‌گونه که در پیوست ۱ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا تعریف شده است امضای دیجیتال ایجاد شده توسط محصول یک امضای الکترونیکی واجد شرایط است اگر گواهی داده درستی‌سنجی امضا (SVD) یک گواهی واجد شرایط باشد. تعیین حالت گواهی به عنوان واجد شرایط فراتر از دامنه کاربرد این استاندارد است.

برنامه کاربردی ایجاد امضا باید از یکپارچگی ورودی‌هایی که برای تابع ایجاد امضای محصول فراهم می‌آورد حفاظت می‌کند به طوریکه با داده‌های کاربر مجاز برای امضا توسط صاحب‌امضا سازگار باشد. به جز مواردی که به صورت تلویحی برای محصول شناخته شده باشد، برنامه‌کاربردی ایجاد امضا (SCA) نوع ورودی امضایی که فراهم می‌کند (به عنوان مثال بازنمایی منحصر به فرد متعلق به داده‌ای که باید امضا شود (DTBS/R)) را نشان می‌دهد و هر گونه مقادیر چکیده‌پیام مورد نیاز را محاسبه می‌کند. محصول ممکن است بازنمایی منحصر به فرد متعلق به داده‌ای که باید امضا شود (DTBS/R) را با پارامترهای امضایی که ذخیره نموده تکمیل کند و سپس یک مقدار چکیده‌پیام را روی ورودی مورد نیاز توسط نوع ورودی و الگوریتم رمزنگاری استفاده شده محاسبه کند.

محصول، داده احرازهویت مرجع (RAD) صاحب‌امضا را برای احراز اصالت یک کاربر به عنوان صاحب‌امضا ذخیره می‌کند. داده احرازهویت مرجع (RAD) یک کلمه‌عبور (به طور مثال پین[1])، یک الگوی زیست‌سنجی و یا ترکیبی از این‌ها است. محصول از محرمانگی و یکپارچگی داده احرازهویت مرجع (RAD)

[1] PIN

محافظت می‌کند. محصول ممکن است رابط کاربری‌ای برای دریافت مستقیم داده درستی‌سنجی احرازهویت (VAD) از کاربر فراهم کند، یا اینکه داده درستی‌سنجی احرازهویت (VAD) را از برنامه کاربردی ایجاد امضا (SCA) دریافت کند. چنانچه برنامه کاربردی ایجاد امضا به کار رود، که خواستار دریافت یک داده درستی‌سنجی احرازهویت (VAD) از کاربر است، چنانچه برنامه است، باید از محرمانگی و یکپارچگی این داده محافظت کند.

یک تأمین کننده خدمت صدور گواهی و یک تأمین کننده خدمات تدارک افزاره ایجاد امضای امن (SSCD) در محیط آماده‌سازی امن با محصول تعامل می‌کند تا هرگونه تابع آماده‌سازی مورد نیاز محصول را قبل از کنترلِ محصول داده شده به کاربر قانونی اجرا کند. این توابع ممکن است شامل موارد زیر باشد:

- مقدار دهی اولیه به داده احرازهویت مرجع (RAD)،
- تولید یک زوج کلید،
- ذخیره‌سازی اطلاعات شخصی کاربر قانونی.

نمونه بارزی از افزاره ایجاد امضای امن (SSCD) یک کارت هوشمند است. در این حالت، یک پایانه کارت هوشمند ممکن است به نحوی گسترش یابد که محیط امن مورد نیاز برای رسیدگی به درخواست برای اعطای مجوز به صاحب‌امضا را فراهم آورد. یک امضا را می‌توان از یک سند آماده شده توسط مؤلفه‌ای از برنامه کاربردی ایجاد امضای در حال اجرا بر روی کامپیوتر شخصیِ متصل به پایانه کارت به دست آورد. برنامه کاربردی ایجاد امضا، بعد از ارائه سند به کاربر و پس از کسب پین اعطای مجوز، تابع ایجاد امضای دیجیتال کارت هوشمند را از طریق پایانه آغاز می‌کند.

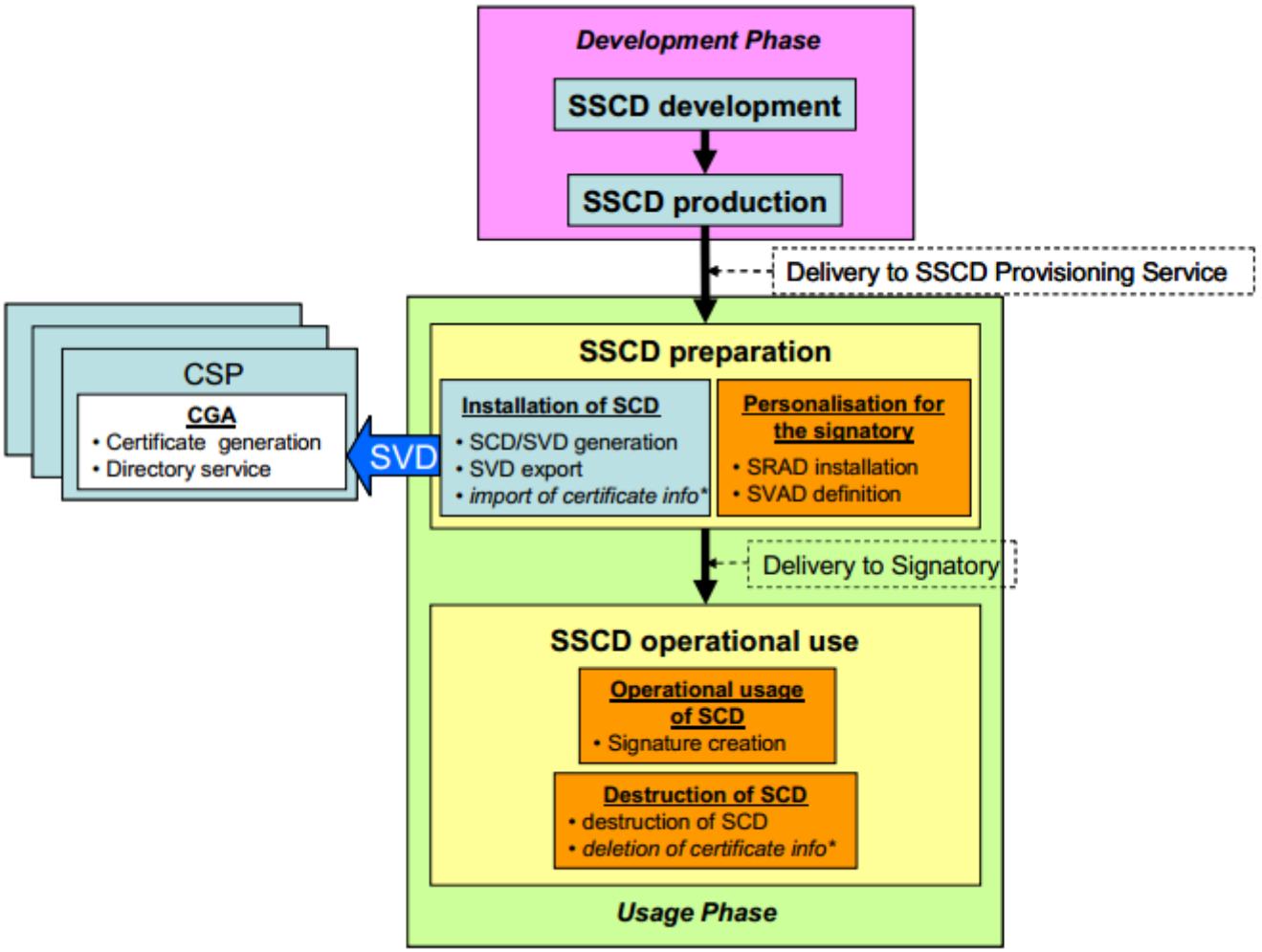
۳-۳- چرخه حیات هدف ارزیابی

چرخه حیات هدف ارزیابی در **Error! Reference source not found.** مراحل توسعه، تولید، آماده‌سازی و استفاده عملیاتی را مشخص و متمایز می‌کند. توسعه و تولید هدف ارزیابی (به قسمت ۱ معیارمشترک پاراگراف ۱۳۹ مراجعه شود) با یکدیگر فاز توسعه هدف ارزیابی را تشکیل می‌دهند. فاز توسعه، مطابق با

کلاس چرخه حیات تضمین[۱] (ALC) موضوع ارزیابی معیار مشترک می‌باشد. فاز توسعه با تحویل هدف ارزیابی به ارائه‌دهنده خدمات تدارک افزاره ایجاد امضای امن، پایان می‌پذیرد. یکپارچگی کارکردی هدف ارزیابی باید در تحویل آن به ارائه‌دهنده خدمات تدارک افزاره ایجاد امضای امن، حفظ شود.

فاز استفاده عملیاتی هدف ارزیابی زمانی آغاز می‌شود که صاحب‌امضا، عملیات هدف ارزیابی را به‌منظور استفاده در عملیات امضا اجرا می‌کند. فعال‌سازی هدف ارزیابی برای امضا حداقل به یک کلید ذخیره شده در حافظه آن نیاز دارد. چرخه حیات هدف ارزیابی زمانی پایان می‌یابد که تمام کلیدهای ذخیره شده در آن به‌طور دائم غیرقابل استفاده باشند. ارائه یک کلید غیرقابل استفاده در افزاره ایجاد امضای امن ممکن است حذف هرگونه اطلاعات گواهی متناظر را شامل شود.

[۱] assurance lifecycle class



شکل ۲- چرخه حیات هدف ارزیابی

۱-۳-۳- گام آماده‌سازی

ارائه‌دهنده خدمات تدارک افزاره ایجاد امضای امن که محصول را از یک سازنده پذیرفته است، هدف ارزیابی جهت استفاده و تحویل آن به کاربر قانونی آماده می‌کند. فاز آماده‌سازی زمانی پایان می‌پذیرد که کاربر قانونی هدف ارزیابی، با دریافت محصول از ارائه‌دهنده خدمات تدارک افزاره ایجاد امضای امن در صورت داشتن داده ایجاد امضا (SCD) آن را برای استفاده در امضا فعال می‌کند. در طول آماده‌سازی هدف ارزیابی، همان‌گونه که در بالا نیز توضیح داده شد، ارائه‌دهنده خدمات تدارک افزاره ایجاد امضای امن، وظایف زیر را انجام می‌دهد:

- به دست آوردن اطلاعات موردنیاز از گیرنده موردنظر افزاره که برای آماده‌سازی فرایند و شناسایی به‌عنوان کاربر قانونی هدف ارزیابی،
- تولید پین[۱] و یا به دست آوردن نمونه‌های زیست‌سنجی از کاربر قانونی، ذخیره این داده‌ها به‌عنوان داده احرازهویت مرجع (RAD) در هدف ارزیابی و آماده‌سازی اطلاعات در مورد داده درستی‌سنجی احرازهویت (VAD) برای تحویل به کاربر قانونی.
- تولید گواهی برای حداقل یک داده ایجاد امضا (SCD) با:

أ) هدف ارزیابی تولید کننده یک زوج داده ایجاد امضا / داده درستی‌سنجی امضا و اخذ گواهی برای داده درستی‌سنجی امضا (SVD) صادر شده از هدف ارزیابی، یا

ب) مقداردهی اولیه توابع امنیتی در هدف ارزیابی برای صدور محافظت‌شده داده درستی‌سنجی امضا (SVD) و اخذ گواهی برای داده درستی‌سنجی امضا (SVD) بعد از دریافت درخواست محافظت‌شده از هدف ارزیابی،

- ارائه اطلاعات گواهی به افزاره ایجاد امضای امن (SSCD)، به‌صورت اختیاری،
- تحویل هدف ارزیابی و اطلاعات داده درستی‌سنجی احرازهویت (VAD) مربوطه به کاربر قانونی.

---

[۱] پین

همان‌طور که در این پروفایل حفاظتی توضیح داده‌شده است، وظیفه صدور گواهی داده درستی‌سنجی امضا (SVD) (سومین وظیفه مطرح‌شده در بالا) ارائه‌دهنده خدمات تدارک افزاره ایجاد امضای امن، ممکن است از فرایند تولید کلید متمرکز شده و پیش صدور، با حداقل یک کلید تولیدشده و تأییدشده، قبل از تحویل به کاربر قانونی پشتیبانی کند. یا اینکه، علاوه بر این ممکن است، این وظیفه تولید کلید را توسط صاحب‌امضا بعد از تحویل و بیرون از محیط آماده‌سازی امن، پشتیبانی کند. هدف ارزیابی ممکن است از هر دو فرایند تولید کلید پشتیبانی کند، به‌عنوان‌مثال اولین کلید متمرکز تولیدشده و کلیدهای اضافی توسط صاحب‌امضا در گام استفاده عملیاتی تولید شود.

حداقل داده‌های موردنیاز برای افزودن به داده درستی‌سنجی امضا (SVD) (پیوست ۲ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا) شامل موارد زیر می‌باشد:

- داده درستی‌سنجی امضا (SVD)
- نام صاحب‌امضا

أ) نام قانونی

ب) نام مستعار به همراه نشانه‌ای به نام حقیقی.

داده‌های موجود در گواهی ممکن است در طی شخصی‌سازی در افزاره ایجاد امضای امن ذخیره شود.

قبل از مقداردهی امضای گواهی واقعی، برنامه‌کاربردی تولید گواهی، صحت داده درستی‌سنجی امضا (SVD) دریافت شده از هدف ارزیابی را از طریق موارد زیر بررسی می‌کند:

- تعیین فرستنده به‌عنوان افزاره ایجاد امضای امن (SSCD) اصلی،
- تعیین یکپارچگی داده درستی‌سنجی امضا (SVD) که توسط افزاره ایجاد امضای امن (SSCD) مبدأ فرستاده‌شده است.
- تعیین اینکه افزاره ایجاد امضای امن (SSCD) مبدأ برای کاربر قانونی، شخصی‌سازی شده است.
- تعیین تناظر میان داده ایجاد امضا (SCD) و داده درستی‌سنجی امضا (SVD)، و

- اثبات این موضوع که الگوریتم امضا و اندازه کلید داده درستی‌سنجی امضا (SVD) برای نوع گواهی مورد تأیید و مناسب می‌باشد.

اثبات تناظر میان داده ایجاد امضا (SCD) ذخیره شده در هدف ارزیابی و داده درستی‌سنجی امضا (SVD) ممکن است در سازوکارهای اعمال‌شده توسط برنامه کاربردی تولید گواهی (CGA) به صورت ضمنی آمده باشد. به‌صورت اختیاری، هدف ارزیابی ممکن است از تابعی پشتیبانی کند که به‌وضوح تناظر بین داده‌های ایجاد امضا (SCD) که ذخیره می‌کند و داده درستی‌سنجی امضا (SVD) تحقق بخشیده شده توسط صدور گواهی توسط خود را اثبات می‌کند. چنین تابعی ممکن است به‌صورت ضمنی در تابع صدور داده درستی‌سنجی امضا (SVD) اعمال شود و ممکن است در محیط آماده‌سازی بدون موافقت آشکار صاحب‌امضا، فراخوانی شود[1]. الزامات امنیتی برای حفاظت از تابع صدور داده درستی‌سنجی امضا (SVD) و داده صدور گواهی اگر داده درستی‌سنجی امضا (SVD) توسط صاحب‌امضا تولید شود و سپس از افزاره ایجاد امضای امن (SSCD) به برنامه کاربردی تولید گواهی (CGA) صادر شود، در یک پروفایل حفاظتی جداگانه توضیح داده‌شده است (بخش مقدمه را ببینید).

قبل از تولید گواهی، ارائه‌دهنده خدمات صدور گواهی باید هویت صاحب‌امضا که در درخواست گواهی به‌عنوان کاربر قانونی هدف ارزیابی مشخص‌شده است را اثبات کند.

۲-۳-۳- گام استفاده عملیاتی

در این گام از چرخه حیات، صاحب‌امضا می‌تواند از هدف ارزیابی برای ایجاد امضای الکترونیکی پیشرفته استفاده کند.

[1] صدور گواهی داده درستی‌سنجی امضا (SVD) توسط خود، به گونه‌ای مؤثر امضای دیجیتالی را با داده ایجاد امضا (SCD) متناظر محاسبه می‌کند. عملیات امضا به کنترل انحصاری صریح صاحب‌امضا نیاز دارد، این حالت خاص، در صورتیکه پشتیبانی شود، استثنائی را برای این قانون ایجاد می‌کند که، قبل از اینکه به صاحب‌امضا تحویل داده شود، چنین کنترلی آشکارا غیرممکن باشد.

صاحب‌امضا همچنین می‌تواند با افزاره ایجاد امضای امن (SSCD) جهت انجام وظایف مدیریتی تعامل کند، به‌عنوان‌مثال تنظیم مجدد مقدار داده احرازهویت مرجع (RAD) یا استفاده از شمارشگر درصورتی‌که کلمه‌عبور یا پین[۱] در داده‌های مرجع ازدست‌رفته یا مسدود شده باشد. چنین وظایف مدیریتی به محیط امن نیاز دارد.

صاحب‌امضا می‌تواند یک داده ایجاد امضا (SCD) را در محصول ارائه دهد که به طور دائم قابل استفاده نباشد. ارائه آخرین داده ایجاد امضا (SCD) در محصول که به طور دائم غیر قابل استفاده باشد حیات محصول به عنوان افزاره ایجاد امضای امن (SSCD) را پایان می‌بخشد.

محصول ممکن است از توابع تولید کلیدهای امضای اضافی پشتیبانی کند. اگر محصول این کارکردها را پشتیبانی کند از کارکردهای بیشتری برای کسب امن گواهی برای کلیدهای جدید پشتیبانی خواهد کرد. برای یک کلید اضافی ممکن است صاحب‌امضا اجازه انتخاب نوع گواهی (واجد شرایط و یا فاقد شرایط) را برای به دست آوردن داده درستی‌سنجی امضا (SVD) از کلید جدید داشته باشد. همچنین ممکن است صاحب‌امضا اجازه داشته باشد برخی از داده‌ها را هنگام درخواست گواهی انتخاب کند به عنوان مثال استفاده از اسم مستعار به جای نام قانونی در گواهی[۲]. چنانچه شرایط کسب یک گواهی واجد شرایط برآورده شود، کلید جدید نیز برای ایجاد امضاهای الکترونیک پیشرفته قابل استفاده است. توابع اختیاری محصول برای تولید کلید اضافی و گواهی ممکن است نیازمند توابع امنیتی اضافی در محصول و تعامل با تأمین کننده خدمات تدارک افزاره ایجاد امضای امن (SSCD) در یک محیط امن باشد.

۴- مسائل امنیتی

۴-۱- دارایی‌ها، کاربران و عوامل تهدید

[۱] PIN

[۲] درخواست گواهی در این حالت شامل نام صاحب‌امضا به عنوان درخواست کننده خواهد بود به طوری که به عنوان مثال این درخواست ممکن است توسط داده ایجاد امضای موجود صاحب‌امضا، امضا شود.

معیار مشترک، دارایی‌ها را به عنوان موجودیت‌هایی تعریف می‌کند که مالکِ محصول، احتمالاً به آن مقداری می‌دهد. اصطلاح «دارایی» برای توصیف تهدیدات در محیط عملیاتی محصول استفاده می‌شود.

۱-۱-۴- دارایی‌ها و موجودیت‌های غیرفعال

۱.داده ایجاد امضا (SCD): کلید خصوصی‌ای است که برای انجام عملیات امضای الکترونیک مورد استفاده است. محرمانگی، یکپارچگی و کنترل انحصاری صاحب‌امضا بر روی استفاده از داده ایجاد امضا (SCD) بایستی محفوظ باشد.

۲.داده درستی‌سنجی امضا (SVD): کلید عمومی پیوند داده شده به داده ایجاد امضا (SCD) است که برای انجام درستی‌سنجی امضای دیجیتال مورد استفاده قرار می‌گیرد. یکپارچگی داده درستی‌سنجی امضا (SVD) هنگام صدورش باید حفظ گردد.

۳.داده‌ای که باید امضا شود (DTBS) یا بازنمایی منحصربه‌فرد متعلق به آن (DTBS/R): مجموعه‌ای از داده‌ها و یا بازنمایی‌های آن است، که صاحب‌امضا قصد امضای آن‌ها را دارد. یکپارچگی آن‌ها و غیر قابل‌جعل بودن پیوند با صاحب‌امضا که توسط امضای الکترونیکی ارائه شده است، بایستی حفظ شود.

۲-۱-۴- کاربران و موجودیت‌های فعال در حال اقدام برای کاربران

۱.کاربر: کاربر نهاییِ محصول که می‌تواند به عنوان مدیر سیستم یا صاحب‌امضا شناخته شود. در محصول موجودیت فعال کاربر[۱] ممکن است به عنوان موجودیت فعال مدیر سیستم[۲] در نقش مدیر سیستم[۳] و یا به عنوان موجودیت فعال صاحب‌امضا[۴] در نقش صاحب‌امضا[۵] ایفای نقش کند.

---

[۱] S.User

[۲] S.Admin

[۳] R.Admin

[۴] S.Sigy

[۵] R.Sigy

۲.مدیر سیستم: کاربری است که مسئول انجام مقداردهی اولیه محصول، شخصی‌سازی محصول و یا دیگر کارکردهای اجرایی محصول می‌باشد. در محصول موجودیت فعال مدیر سیستم برای این کاربر بعد از احرازهویت موفقیت‌آمیز به عنوان مدیر سیستم در حال ایفای نقشِ مدیر سیستم است.

۳.صاحب‌امضا: کاربری است که محصول را دارد و از آن از طرف خود یا از طرف شخص حقیقی یا حقوقی یا موجودیتی که نمایندگی آن را بر عهده دارد استفاده می‌کند. موجودیت فعال صاحب‌امضا برای این کاربر بعد از احرازهویت موفقیت‌آمیز به عنوان صاحب‌امضا نقش صاحب‌امضا را ایفا می‌کند.

۳-۱-۴-عوامل تهدید

۱.مهاجم: انسان یا فرایندی که از طرف آن‌هایی که بیرون از محصول قرار دارند در حال فعالیت است. هدف اصلی مهاجم دستیابی به داده ایجاد امضا (SCD) یا جعل امضای الکترونیک است. مهاجم پتانسیل بالایی برای حمله دارد و از هیچ رازی آگاه نیست.

۴-۲- تهدیدات

تهدیدات	توضیحات
T.SCD_Divulg	مهاجم بیرون از محصول، داده ایجاد امضا (SCD) را ذخیره و یا از آن نسخه‌برداری می‌کند. مهاجم می‌تواند داده ایجاد امضا (SCD) را در طول تولید، انبارش و استفاده برای ایجاد امضا در محصول، به دست آورد.
T.SCD_Derive	مهاجم، داده ایجاد امضا (SCD) را از داده‌های شناخته شده عمومی مانند داده درستی‌سنجی امضا (SVD) متناظر با داده ایجاد امضا (SCD) یا امضای ایجاد شده به وسیله داده ایجاد امضا (SCD) یا هر داده دیگری که به خارج از محصول صادر شده است، استخراج می‌کند که عامل تهدیدی در مقابل محرمانگی داده ایجاد امضا (SCD) است.
T.Hack_phys	مهاجم برای بهره‌برداری از آسیب‌پذیری‌ها به صورت فیزیکی با محصول تعامل برقرار می‌کند که منتج به خطرات امنیتی عمدی می‌شود. این تهدید در برابر داده ایجاد امضا (SCD)، داده درستی‌سنجی امضا (SVD) و داده‌ای که باید امضا شود (DTBS) عمل می‌کند.
T.SVD_Forgery	مهاجم داده درستی‌سنجی امضا (SVD) جعل شده را به برنامه کاربردی تولید گواهی (CGA) ارائه می‌دهد. این امر منجر به از دست رفتن یکپارچگی داده درستی‌سنجی امضا (SVD) در گواهی صاحب‌امضا می‌شود.
T.SigF_Misuse	مهاجم از تابع ایجاد امضای محصول سوءاستفاده می‌کند تا داده ایجاد امضا (SCD) را برای داده‌ای ایجاد کند که صاحب‌امضا، تصمیم به امضای آن را ندارد. محصول سوژه‌ای برای حملات عمدی متخصصانی است که با دانش پیشرفته از اصول و مفاهیم امنیتی به کار گرفته شده در محصول دارای پتانسیل حمله بالایی می‌باشند.
T.DTBS_Forgery	مهاجم داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) ارسال شده توسط برنامه کاربردی ایجاد امضا (SCA) را تغییر می‌دهد. بنابراین داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) که توسط محصول برای امضا استفاده می‌شود با داده‌ای که باید امضا شود (DTBS) و صاحب‌امضا قصد امضای آن را دارد، مطابقت ندارد.
T.Sig_Forgery	بدون استفاده از داده‌ه ایجاد امضا (SCD) داده مرتبط با امضای دیجیتالی را جعل کرده و درستی‌سنجی امضای دیجیتال توسط داده درستی‌سنجی امضا (SVD) جعل را تشخیص نمی‌دهد. امضای تولید شده توسط محصول سوژه‌ای برای حملات عمدی متخصصانی است که با دانش پیشرفته از اصول و مفاهیم امنیتی به کار رفته در محصول دارای پتانسیل بالایی برای حمله می‌باشند.

۴-۳- خط‌مشی‌های امنیت سازمانی

خط‌مشی‌ها	توضیحات
P.CSP_QCert	تامین‌کننده خدمات صدور گواهی (CSP) از یک برنامه کاربردی تولید گواهی (CGA) قابل‌اعتماد برای تولید گواهی واجد شرایط یا غیر واجد شرایط برای داده درستی‌سنجی امضا (SVD) تولید شده توسط افزاره ایجاد امضای امن (SSCD) استفاده می‌کند (مراجعه شود به: دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا ، ماده ۲ بند ۹ و پیوست ۱). گواهی حداقل شامل نام صاحب‌امضا و داده درستی‌سنجی امضا (SVD) متناظر با داده ایجاد امضا (SCD) پیاده‌سازی شده در محصول تحت کنترل انحصاری صاحب‌امضا می‌باشد. تامین‌کننده خدمات صدور گواهی (CSP) تضمین می‌کند که استفاده از محصول به عنوان افزاره ایجاد امضای امن (SSCD) با امضاهایی که از طریق گواهی یا هرگونه اطلاعات قابل‌دسترس عموم مشهود است.
P.QSign	صاحب‌امضا از سامانه ایجاد امضا برای امضای داده با یک امضای الکترونیکی پیشرفته استفاده می‌کند (دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا: ماده ۱، بند ۲)، که اگر بر اساس گواهی واجد شرایط معتبر باشد یک امضای الکترونیکی واجد شرایط خواهد بود (طبق دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا پیوست ۱). داده‌ای که باید امضا شود (DTBS) به صاحب‌امضا ارائه می‌شود و به عنوان داده‌ای که باید امضا شود یا بازنمایی منحصر به فرد متعلق به آن (DTBS/R) توسط برنامه کاربردی ایجاد امضا (SCA) به افزاره ایجاد امضای امن (SSCD) ارسال می‌شود. افزاره ایجاد امضای امن (SSCD) امضای دیجیتالی ایجاد شده با یک داده ایجاد امضا (SCD) پیاده‌سازی‌شده در افزاره ایجاد امضای امن (SSCD) ایجاد می‌کند که صاحب‌امضا آن را تحت کنترل انحصاری خود حفظ می‌کند و به روشی به داده‌ای که باید امضا شود یا بازنمایی منحصر به فرد متعلق به آن (DTBS/R) پیوند داده می‌شود که هر تغییر بعدی در داده قابل تشخیص است.
P.Sigy_SSCD	محصول الزامات لازم برای افزاره ایجاد امضای امن (SSCD) که در پیوست ۳ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا بیان شده است را برآورده می‌کند [۱]. این امر حاکی از این است که داده ایجاد امضا (SCD) برای ایجاد امضای دیجیتالی تحت کنترل انحصاری صاحب‌امضا استفاده شده است و داده ایجاد امضا (SCD) عملاً تنها یکبار می‌تواند اتفاق بیفتد.

P.Sig_Non-Repud	چرخه حیات افزاره ایجاد امضای امن (SSCD)، داده ایجاد امضا (SCD) و داده درستی‌سنجی امضا (SVD) باید به روشی پیاده‌سازی شوند که اگر امضا به صورت موفقیت آمیزی با داده درستی‌سنجی امضا (SVD) موجود در گواهی باطل نشده‌اش تأیید شد صاحب‌امضا قادر به انکار داشتن داده امضا شده نباشد.

۴-۴- مفروضات

مفروضات	توضیحات
A.CGA	برنامه‌کاربردی تولید گواهی (CGA) از اصالت‌سنجی نام و یا اسم مستعار صاحب‌امضا و داده درستی‌سنجی امضا (SVD) در گواهی (واجد شرایط) توسط امضای الکترونیکی پیشرفته تامین‌کننده خدمات صدور گواهی (CSP) محافظت می‌کند.
A.SCA	صاحب‌امضا تنها از یک برنامه‌کاربردی ایجاد امضا (SCA) قابل‌اعتماد استفاده می‌کند. برنامه‌کاربردی ایجاد امضا (SCA) از داده‌هایی که صاحب‌امضا می‌خواهد امضا نماید داده‌ای که باید امضا شود یا بازنمایی منحصر به فرد متعلق به آن (DTBS/R) را به شکل مناسبی برای امضا کردن توسط محصول تولید و ارسال می‌کند.

۵- اهداف امنیتی

۵-۱- کلیات

این بخش اهداف امنیتی محصول و محیط آن را شناسایی و معرفی می‌کند. اهداف امنیتی مقاصد بیان شده را منعکس کرده و با تهدیدهای شناسایی شده مقابله کرده و همچنین مفروضات و خط‌مشی‌های امنیت سازمانی تعیین‌شده را برآورده می‌سازد.

۵-۲- اهداف امنیتی برای محصول

هدف امنیتی	توضیحات

A OT.Lifecycle_Security CGA	محصول باید نقص‌ها را در طول مقداردهی اولیه، شخصی‌سازی و کاربری عملیاتی تشخیص دهد. محصول باید قابلیت کارکردی تخریب امن داده ایجاد امضا (SCD) را فراهم آورد. **نکته کاربردی ۱**: محصول ممکن است بیش از یک مجموعه داده ایجاد امضا (SCD) را دربرداشته باشد. هیچ نیازی به تخریب داده ایجاد امضا (SCD) در موارد تولید مجدد داده ایجاد امضا (SCD) نیست. صاحب‌امضا باید به عنوان مثال بعد از منقضی‌شدن گواهی (واجد شرایط) برای داده درستی‌سنجی امضا (SVD) متناظر قادر به تخریب داده ایجاد امضا (SCD) ذخیره شده در افزاره امن ایجاد امضا (SSCD) باشد.
OT.SCD/SVD_Gen	هدف ارزیابی ویژگی‌های امنیتی‌ای ارائه دهد تا اطمینان حاصل کند که تنها کاربران مجاز تولید داده ایجاد امضا (SCD) و داده درستی‌سنجی امضا(SVD) را فراخوانی می‌کنند.
OT.SCD_unique	هدف ارزیابی باید از مناسب بودن کیفیت رمزنگاری زوج کلید داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) برای امضای الکترونیکی واجد شرایط یا پیشرفته استفاده می‌شود، اطمینان حاصل کند. داده ایجاد امضا (SCD) استفاده‌شده برای تولید امضا، در عمل تنها یک‌بار رخ می‌دهد و از داده درستی‌سنجی امضا (SVD) قابل‌بازسازی نمی‌باشد. در این زمینه «در عمل یک‌بار رخ می‌دهد» بدین معنا است که احتمال یکسان بودن داده‌های ایجاد امضا (SCD) ناچیز است.
OT.SCD_SVD_Corresp	هدف ارزیابی باید از تناظر میان داده درستی‌سنجی امضا (SVD) و داده ایجاد امضا (SCD) تولیدشده با محصول اطمینان حاصل کند. این شامل مرجع بدون ابهام از زوج کلید داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) ایجادشده برای صدور داده درستی‌سنجی امضا (SVD) و در هنگام ایجاد امضای دیجیتالی توسط داده ایجاد امضا (SCD) می‌باشد.
OT.SCD_Secrecy	رازمانی[۱] داده ایجاد امضا (SCD) (استفاده شده برای ایجاد امضا) بایستی به صورت قابل قبولی در مقابل حملات با پتانسیل بالای حمله بیمه شود. **نکته کاربردی ۲**: محصول باید محرمانگی داده ایجاد امضا (SCD) را در هر زمانی به خصوص در طول تولید داده ایجاد امضا (SCD)، عملیات امضای داده ایجاد امضا (SCD)، انبارش و تخریب امن حفظ کند

۱ Secrecy

OT.Sig_Secure	محصول باید امضاهای دیجیتالی را تولید کند که بدون دانستن داده ایجاد امضا (SCD) از طریق تکنیک‌های رمزنگاری قوی، قابل جعل کردن نباشد. داده ایجاد امضا (SCD) نباید با استفاده از امضاهای دیجیتال یا هر داده دیگر صادرشده از محصول قابل بازسازی باشد. امضاهای دیجیتالی باید در مقابل این حملات مقاوم باشند، حتی اگر با پتانسیل بالایی برای حمله اجرا می‌شوند.
OT.Sigy_SigF	محصول باید تابع ایجاد امضای دیجیتالی را تنها برای صاحب‌امضای قانونی فراهم آورده و از داده ایجاد امضا (SCD) در برابر استفاده دیگران محافظت کند. محصول باید در برابر حملات با پتانسیل بالای حمله مقاوم باشد.
OT.DTBS_Integrity_TOE	محصول نباید داده‌ای که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن (DTBS/R) را تغییر دهد، این هدف در تضاد با فرایند ایجاد امضایی نیست که در آن محصول تابع چکیده‌سازی را روی داده‌ای که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن (DTBS/R) به کار می‌برد که آن را برای الگوریتم ایجاد امضا آماده می‌سازد.
OT.EMSEC_Design	محصول باید به روشی طراحی و ساخته شود که تولید برون‌تابی‌های[1] معلوم را در محدوده‌های مشخص کنترل کند.
OT.Tamper_ID	محصول باید ویژگی‌های سامانه‌ای را ارائه دهد که دست‌کاری فیزیکی مؤلفه‌هایش را تشخیص داده و از آن ویژگی‌ها برای محدود کردن رخنه‌های امنیتی استفاده کند.
OT.Tamper_Resistance	محصول باید در مقابل دست‌کاری‌های فیزیکی افزاره‌ها و مؤلفه‌های سامانه مشخص، جلوگیری یا مقاومت کند.

۳-۵-اهداف امنیتی برای محیط عملیاتی

هدف امنیتی محیط عملیاتی	توضیحات
OE.SVD_Auth	محیط عملیاتی باید از یکپارچگی داده درستی‌سنجی امضا (SVD) صادر شده توسط محصول به برنامه‌کاربردی تولید گواهی (CGA) اطمینان حاصل کند. برنامه‌کاربردی تولید گواهی (CGA)، تناظر بین داده ایجاد امضا (SCD) در افزاره ایجاد امضای امن (SSCD) صاحب‌امضا و داده درستی‌سنجی امضا (SVD) در ورودی ارائه شده برای تابع تولید گواهی تامین‌کننده خدمات صدور گواهی (CSP) را بررسی می‌کند.

[1] physical-emanation

OE.CGA_QCert	برنامه‌کاربردی تولید گواهی (CGA) یک گواهی واجد شرایط شامل موارد زیر را تولید کند: الف- نام صاحب‌امضای کنترل‌کننده محصول، ب- داده درستی‌سنجی امضا (SVD) منطبق بر داده ایجاد امضای (SCD) ذخیره شده در محصول تحت کنترل انحصاری صاحب‌امضا، ج- امضای پیشرفته تامین‌کننده خدمات صدور گواهی (CSP). برنامه‌کاربردی تولید گواهی (CGA) باید تصدیق کند که داده ایجاد امضا (SCD) متناظر با داده درستی‌سنجی امضا (SVD) در افزاره ایجاد امضای امن (SSCD) ذخیره شده است.
OE.SSCD_prov_Service	خدمات تدارک افزاره ایجاد امضای امن (SSCD) افزاره‌های موثقی را به کار می‌برد که محصول‌ای که باید برای کاربر قانونی به عنوان صاحب‌امضا آماده شود را شخصی‌سازی کرده و محصول را به عنوان افزاره ایجاد امضای امضای امن (SSCD) به صاحب‌امضا تحویل می‌دهد.
OE.HID_VAD	اگر یک افزاره خارجی رابط انسانی (HID) برای احرازهویت کاربر فراهم آورد، این افزاره باید از محرمانگی و یکپارچگی داده درستی‌سنجی احرازهویت (VAD) به گونه‌ای اطمینان حاصل کند که مورد نیاز روش احرازهویت استفاده‌شده از ورود از طریق رابط انسانی‌اش تا ورود از طریق رابط محصول می‌باشد.
OE.DTBS_Intend	صاحب‌امضا باید از برنامه‌کاربردی ایجاد امضا (SCA) قابل‌اعتمادی استفاده کند که: الف-داده‌ای که باید امضا شود یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) را از داده‌ای تولید می‌کند که به عنوان داده‌ای که باید امضا شود (DTBS) ارائه شده و صاحب‌امضا آن را برای امضا در نظر گرفته است به شکلی که برای امضا کردن توسط محصول مناسب است. ب- داده‌ای که باید امضا شود یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) را به محصول می‌فرستد و درستی‌سنجی یکپارچگی داده‌ای که باید امضا شود یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) توسط محصول را فعال می‌سازد. ج- امضای تولید شده توسط محصول را به داده‌ها پیوست می‌کند و یا آن را به شکل جداگانه‌ای ارائه می‌دهد.
OE.DTBS_Protect	محیط عملیاتی باید اطمینان حاصل کند که داده‌ای که باید امضا شود یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) در گذر بین برنامه‌کاربردی ایجاد امضا (SCA) و محصول تغییر نخواهد کرد.

OE.Signatory	صاحب‌امضا بررسی می‌کند که داده ایجاد امضا (SCD) ذخیره شده در افزاره ایجاد امضای امن (SSCD) که از خدمات تدارک افزاره ایجاد امضای امن (SSCD) دریافت شده است، در حالت غیر عملیاتی قرار دارد. صاحب‌امضا باید محرمانگی داده درستی‌سنجی احرازهویت (VAD) خود را حفظ کند.

۴-۵- منطق اهداف امنیتی

۱-۴-۵- پوشش اهداف امنیتی

جدول ۱ نگاشت تعریف مسأله امنیتی به اهداف امنیتی

	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp	OE.CGA_QCert	OE.SVD_Auth	OE.Dev_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory
T.SCD_Divulg					×															
T.SCD_Derive		×				×														
T.Hack_Phys					×				×	×	×									
T.SVD_Forgery				×											×					
T.SigF_Misuse	×						×	×									×	×	×	×
T.DTBS_Forgery								×										×	×	
T.Sig_Forgery			×			×								×						
P.CSP_QCert	×			×										×						
P.QSign						×	×							×				×		
P.Sigy_SSCD	×	×	×		×	×	×	×	×		×					×				
P.Sig_Non-Repud	×		×	×	×	×	×	×	×	×	×	×	×	×	×	×		×	×	×
A.CGA														×	×					
A.SCA																		×		

۲-۴-۵- اهداف امنیتی

۱-۲-۴-۵- مقابله با تهدیدات با اهداف امنیتی

تهدیدات اهداف امنیتی	توضیحات

T.SCD_Divulg تهدید ذخیره‌سازی، نسخه‌برداری و انتشار داده ایجاد امضا	همانگونه که در بند (۱۸) دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا آمده است تهدیدات را در برابر اعتبار قانونی امضای الکترونیک به علت انبارش و نسخه‌برداری از داده ایجاد امضا (SCD) بیرون از محصول مورد توجه قرار می‌دهد[۱]. این تهدید با هدف امنیتی برای محصول – رازمانی داده ایجاد امضا (OT.SCD_Secrecy) مورد مقابله قرار می‌گیرد، که از رازمانی داده ایجاد امضا (SCD) در طول استفاده توسط محصول برای ایجاد امضا، اطمینان حاصل می‌کند.
T.SCD_Derive تهدید استخراج داده ایجاد امضا	این تهدید با حمله‌هایی روی داده ایجاد امضا (SCD) سروکار دارد که از طریق داده عمومی شناخته‌شده که داده درستی‌سنجی امضا (SVD) و امضاهای ایجاد شده با داده ایجاد امضا (SCD) هستند و توسط محصول تولید شده‌اند صورت می‌گیرند. هدف امنیتی برای محصول - تولید داده ایجاد امضا / داده درستی‌سنجی امضا (OT.SCD/SVD_Gen) با پیاده‌سازی تولید امن رمزنگاری‌شده زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SVD/SCD) با این تهدید مقابله می‌کند. هدف امنیتی برای محصول - امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure)، از امضاهای الکترونیک امن رمزنگاری‌شده اطمینان حاصل می‌کند.
T.Hack_Phys تهدید بهره‌برداری از آسیب‌پذیری‌های فیزیکی	این تهدید با حملات فیزیکی‌ای سر وکار دارد که از آسیب‌پذیری‌های فیزیکی محصول بهره‌برداری می‌کند. هدف امنیتی برای محصول - رازمانی داده ایجاد امضا (OT.SCD_Secrecy) از رازمانی داده ایجاد امضا (SCD) را محافظت می‌کند. هدف امنیتی برای محصول - فراهم آوردن امنیت برون‌تابی‌های فیزیکی (OT.EMSEC_Design) با حملات فیزیکی از طریق رابط‌های محصول و مشاهده برون‌تابی‌های محصول مقابله می‌کند. هدف امنیتی برای محصول آشکارسازی دست‌کاری (OT.Tamper_ID) و هدف امنیتی برای محصول مقاومت در برابر دست‌کاری (OT.Tamper_Resistance) با شناسایی و مقاومت در برابر حملات دستکاری با تهدید بهره‌بردای از آسیب‌پذیری‌های فیزیکی (T.Hack_Phys) مقابله می‌کنند.

T.SVD_Forgery تهدید جعل داده درستی‌سنجی امضا	این تهدید با جعل داده درستی‌سنجی امضا (SVD) صادر شده توسط محصول به برنامه‌کاربردی تولید گواهی (CGA) برای تولید گواهی سر و کار دارد. تهدید جعل داده درستی‌سنجی امضا (T.SVD_Forgery) مورد توجه هدف امنیتی برای محیط عملیاتی - تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا (OE.SCD_SVD_Corresp) قرار دارد که از تناظر میان داده درستی‌سنجی امضا (SVD) و داده ایجاد امضا (SCD) و مرجع بدون ابهام زوج داده ایجاد امضا / داده درستی‌سنی امضا (SVD/SCD) برای صدور داده درستی‌سنجی امضا (SVD) و ایجاد امضا با داده ایجاد امضا (SCD) اطمینان حاصل می‌کند، و همچنین مورد توجه هدف امنیتی برای محیط عملیاتی - اصالت‌سنجی داده درستی‌سنجی امضا (OE.SVD_Auth) است که از یکپارچگی داده درستی‌سنجی امضا (SVD) صادر شده توسط محصول به برنامه‌کاربردی تولید گواهی (CGA) اطمینان حاصل می‌کند.

T.SigF_Misuse تهدید سوءاستفاده از تابع ایجاد امضای محصول	این تهدید، سوءاستفاده از تابع ایجاد امضای محصول را برای ایجاد موجودیت غیرفعال داده امضاشده (SDO) توسط دیگران به جای صاحب‌امضا برای ایجاد امضای دیجیتال بر روی داده‌ای که صاحب‌امضا تصمیم به امضایش را نداشته مورد توجه قرار می‌دهد که در دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا [۱]، پیوست ۳، پاراگراف ۱، بند C، نیاز است. هدف امنیتی برای محصول - امنیت چرخه‌حیات (OT.Lifecycle_Security) به محصول برای تشخیص نقص‌ها در طول مقداردهی اولیه، شخصی‌سازی و کاربری عملیاتی نیاز دارد که شامل تخریب امن داده ایجاد امضایی (SCD) است که صاحب‌امضا قصد تخریب آن را دارد. هدف امنیتی تابع ایجاد امضا تنها برای صاحب‌امضای قانونی (OT.Sigy_SigF) اطمینان حاصل می‌کند که محصول تابع ایجاد امضا را تنها برای صاحب‌امضای قانونی ارائه می‌دهد. هدف امنیتی برای محیط عملیاتی - ارسال داده‌های درنظر گرفته شده برای امضا توسط برنامه کاربردی تولید امضا (OE.DTBS_Intend) اطمینان حاصل می‌کند که برنامه‌کاربردی ایجاد امضا (SCA)، داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) را تنها برای داده‌ای که صاحب‌امضا قصد امضای آن‌ها را دارد، می‌فرستد و هدف امنیتی برای محیط عملیاتی - محافظت از داده‌های در نظر گرفته شده برای امضا توسط برنامه کاربردی ایجاد امضا (OE.DTBS_Protect) با دستکاری داده‌ای که باید امضا شود (DTBS) در طول انتقال بر روی کانال بین برنامه‌کاربردی ایجاد امضا (SCA) و محصول مقابله می‌کند. هدف امنیتی برای محصول - یکپارچگی داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) درون محصول (OT.DTBS_Integrity_TOE) از تغییر داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) در درون محصول محافظت می‌کند. اگر برنامه‌کاربردی ایجاد امضا (SCA) رابط انسانی را برای احرازهویت کاربر فراهم کند، هدف امنیتی برای محیط عملیاتی - محافظت از داده درستی‌سنجی احرازهویت (OE.HID_VAD) به گونه‌ای محرمانگی و یکپارچگی داده درستی‌سنجی احرازهویت (VAD) را فراهم می‌آورد که مورد نیاز روش احرازهویت به کار گرفته شده است. همچنین هدف امنیتی برای محیط عملیاتی - التزام امنیتی صاحب‌امضا (OE.Signatory) اطمینان حاصل می‌کند که صاحب‌امضا بررسی کند که داده ایجاد امضا (SCD) ذخیره شده در افزاره ایجاد امضای امن (SSCD) هنگامی از خدمات تدارک افزاره ایجاد امضای امن (SSCD) دریافت می‌شود در حالت غیر عملیاتی قرار دارد، یعنی داده ایجاد امضا نمی‌تواند قبل از کنترل انحصاری افزاره ایجاد امضای امن (SSCD) توسط صاحب‌امضا استفاده شده باشد. این هدف امنیتی همچنین این اطمینان را حاصل می‌کند که صاحب‌امضا SVAD خود را به صورت محرمانه حفظ می‌کند.

T.DTBS_Forgery تهدید جعل داده‌ای که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن	این تهدید، تهدید برخاسته از تغییرات ایجاد شده در داده فرستاده شده به عنوان ورودی برای تابع ایجاد امضای محصول است که داده‌ای که باید امضا شود (DTBS) و امضایی که صاحب‌امضا قصد امضای آن را داشته است را به شکلی که برای صاحب‌امضا ارائه شده بازنمایی نکرده است. محیط فناوری اطلاعات محصول تهدید جعل داده‌ای که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن (T.DTBS_Forgery) را با مفاهیم زیر مورد توجه قرار می‌دهد: - هدف امنیتی برای محیط عملیاتی - ارسال داده‌های درنظر گرفته شده برای امضا توسط برنامه کاربردی تولید امضا (OE.DTBS_Intend) که اطمینان حاصل می‌کند که برنامه‌کاربردی ایجاد امضا (SCA) قابل‌اعتماد داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) را از داده‌ای تولید می‌کند که به‌عنوان داده‌ای که باید امضا شود (DTBS) ارائه شده است و صاحب‌امضا قصد امضای آن را به شکل مناسبی برای امضا توسط محصول داشته‌است. - هدف امنیتی برای محیط عملیاتی - محافظت از داده‌های در نظر گرفته شده برای امضا توسط برنامه کاربردی ایجاد امضا (OE.DTBS_Protect) اطمینان حاصل می‌کند که داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) در طول انتقال بین برنامه‌کاربردی ایجاد امضا (SCA) و محصول قابل تغییر نیست. محصول با این عامل تهدید با استفاده از هدف امنیتی برای محصول - یکپارچگی داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) درون محصول (OT.DTBS_Integrity_TOE) و با حصول اطمینان از یکپارچگی داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) در درون محصول مقابله می‌کند.

T.Sig_Forgery تهدید جعل امضای الکترونیکی	این تهدید با جعل غیرقابل تشخیص امضای دیجیتالی سر و کار دارد. هدف امنیتی برای محصول - امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure)، هدف امنیتی برای محیط عملیاتی - یکتایی داده ایجاد امضا (OE.SCD_Unique) و هدف امنیتی برای محیط عملیاتی - تولید گواهی‌های واجد شرایط (OE.CGA_Qcert)، به طور کلی این عوامل تهدید را مورد توجه قرار می‌دهند. هدف امنیتی برای محصول - امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure) با استفاده از تکنیک‌های قوی رمزنگاری این اطمینان را حاصل می‌کند که داده امضا شده و امضای دیجیتالی به‌گونه‌ای امن به یکدیگر پیوند داده شده‌اند. هدف امنیتی برای محیط عملیاتی - یکتایی داده ایجاد امضا (OE.SCD_Unique) اطمینان حاصل می‌کند که یک داده ایجاد امضا (SCD) بیشتر از یکبار نمی‌تواند تولید شود و داده درستی‌سنجی امضا (SVD) متناظر هم نمی‌تواند به طور تصادفی در گواهی دیگری وجود داشته باشد. هدف امنیتی برای محیط عملیاتی - تولید گواهی‌های واجد شرایط (OE.CGA_Qcert) از جعل گواهی برای داده درستی‌سنجی امضا (SVD) متناظر جلوگیری می‌کند، که می‌تواند منجر به تصمیم درستی‌سنجی نادرست شود که مربوط به یک امضای جعلی است.

۲-۲-۴-۵- اجرای خط‌مشی‌های امنیتی سازمانی با اهداف امنیتی

خط‌مش‌های سازمانی	توضیحات
P.CSP_QCert خط‌مشی تولید گواهی‌های واجد شرایط توسط تامین‌کننده خدمات صدور گواهی	این خط‌مشی امنیت سازمانی تعیین می‌کند که تامین‌کننده خدمات صدور گواهی (CSP) گواهی واجد شرایط یا غیر واجد شرایطی را تولید می‌کند، که صاحب‌امضا و داده درستی‌سنجی امضا (SVD) پیاده‌سازی‌شده در افزاره ایجاد امضا امن (SSCD) تحت کنترل انحصاری این صاحب‌امضا را به یکدیگر پیوند می‌دهد. خط‌مشی گواهی واجد شرایط (P.CSP_QCert) مورد توجه موارد زیر است: - هدف امنیتی برای محصول - امنیت چرخه‌حیات (OT.Lifecycle_Security) که برای شناسایی نقص‌های موجود در طول مقداردهی اولیه، شخصی‌سازی و کاربری عملیاتی به محصول نیاز دارد، - هدف امنیتی برای محصول - تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا (OE.SCD_SVD_Corresp) که برای حصول اطمینان از تناظر بین داده درستی‌سنجی امضا (SVD) و داده ایجاد امضا (SCD) در طول تولید آن‌ها به محصول نیاز دارد، هدف امنیتی برای محیط عملیاتی - تولید گواهی‌های واجد شرایط (OE.CGA_Qcert) برای تولید گواهی‌های واجد شرایط یا غیر واجد شرایط، که به برنامه‌کاربردی تولید گواهی (CGA) نیاز دارد تا تصدیق نماید که داده درستی‌سنجی امضا (SVD) با داده ایجاد امضا (SCD) پیاده‌سازی‌شده در محصول که تحت کنترل انحصاری صاحب‌امضا می‌باشد مطابقت دارد.
P.QSign خط‌مشی امضای الکترونیکی واجد شرایط	این خط‌مشی این امکان را فراهم می‌آورد که محصول و برنامه‌کاربردی ایجاد امضا (SCA) برای امضای داده با یک امضای الکترونیکی پیشرفته داده به کار رود که اگر بر اساس گواهی معتبر واجد شرایط باشد یک امضای الکترونیکی واجد شرایط خواهد بود. هدف امنیتی برای محصول - تابع ایجاد امضا تنها برای صاحب‌امضای قانونی (OT.Sigy_SigF) از کنترل انحصاری صاحب‌امضا روی داده ایجاد امضا (SCD) با الزام محصول به ارائه تابع ایجاد امضا تنها برای صاحب‌امضا قانونی و محافظت از داده ایجاد امضا

	(SCD) در مقابل استفاده دیگران اطمینان حاصل می‌کند. هدف امنیتی برای محصول - امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure) این اطمینان را حاصل می‌کند که محصول امضاهای دیجیتالی را ایجاد کند که بدون دانستن داده ایجاد امضا (SCD) از طریق تکنیک‌های رمزنگاری قوی قابل‌جعل نیستند. هدف امنیتی برای محیط عملیاتی - تولید گواهی‌های واجد شرایط (OE.CGA_Qcert) الزامات گواهی الکترونیکی واجد شرایط یا غیر واجد شرایط را مورد توجه قرار می‌دهد که مبنایی برای امضای الکترونیکی ایجاد می‌کنند. هدف امنیتی برای محیط عملیاتی - ارسال داده‌های درنظر گرفته شده برای امضا توسط برنامه کاربردی تولید امضا (OE.DTBS_Intend) این اطمینان را می‌دهد که برنامه‌کاربردی ایجاد امضا (SCA) تنها داده‌ای که باید امضا شود (DTBS) را به محصول ارائه می‌دهد که صاحب‌امضا قصد امضای آن‌ها را دارد.
P.QSign خط‌مشی امضای الکترونیکی واجد شرایط	این خط‌مشی این امکان را فراهم می‌آورد که محصول و برنامه‌کاربردی ایجاد امضا (SCA) برای امضای داده با یک امضای الکترونیکی پیشرفته داده به کار رود که اگر بر اساس گواهی معتبر واجد شرایط باشد یک امضای الکترونیکی واجد شرایط خواهد بود. هدف امنیتی برای محصول - تابع ایجاد امضا تنها برای صاحب‌امضای قانونی (OT.Sigy_SigF) از کنترل انحصاری صاحب‌امضا روی داده ایجاد امضا (SCD) با الزام محصول به ارائه تابع ایجاد امضا تنها برای صاحب‌امضا قانونی و محافظت از داده ایجاد امضا (SCD) در مقابل استفاده دیگران اطمینان حاصل می‌کند. هدف امنیتی برای محصول - امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure) این اطمینان را حاصل می‌کند که محصول امضاهای دیجیتالی را ایجاد کند که بدون دانستن داده ایجاد امضا (SCD) از طریق تکنیک‌های رمزنگاری قوی قابل‌جعل نیستند. هدف امنیتی برای محیط عملیاتی - تولید گواهی‌های واجد شرایط (OE.CGA_Qcert) الزامات گواهی الکترونیکی واجد شرایط یا غیر واجد شرایط را مورد توجه قرار می‌دهد که مبنایی برای امضای الکترونیکی ایجاد می‌کنند. هدف امنیتی برای محیط عملیاتی - ارسال داده‌های درنظر گرفته شده برای امضا توسط برنامه کاربردی تولید امضا (OE.DTBS_Intend) این اطمینان را می‌دهد که برنامه‌کاربردی ایجاد امضا (SCA) تنها داده‌ای که باید امضا شود (DTBS) را به محصول

	ارائه می‌دهد که صاحب‌امضا قصد امضای آن‌ها را دارد.
P.Sigy_SSCD خط‌مشی محصول به عنوان افزاره ایجاد امضای امن	این خط‌مشی مستلزم آن است که محصول الزامات پیوست ۲ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا را برآورده سازد [۱]. این اطمینان از طرق زیر حاصل می‌شود: - هدف امنیتی برای محصول - یکتایی داده ایجاد امضا (OT.SCD_Unique) پاراگراف (a) ۱ پیوست ۳ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا [۱] را با الزاماتی برآورده می‌سازد که داده ایجاد امضا (SCD) مورد استفاده برای ایجاد امضا، عملاً فقط یکبار بتواند رخ دهد. - هدف امنیتی برای محصول - یکتایی داده ایجاد امضا (OT.SCD_Unique)، هدف امنیتی برای محصول - امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure) و هدف امنیتی برای محصول - رازمانی داده ایجاد امضا (OT.SCD_Secrecy) پاراگراف ۱(a) پیوست ۳ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا [۱] را با الزاماتی برای حصول اطمینان از رازمانی داده ایجاد امضا (SCD) برآورده می‌سازد. هدف امنیتی برای محصول - فراهم آوردن امنیت برون‌تابی‌های فیزیکی (OT.EMSEC_Design) و هدف امنیتی برای محصول - مقاومت در برابر دست‌کاری (OT.Tamper_Resistance) اهداف مشخص برای اطمینان از رازمانی داده ایجاد امضا (SCD) در برابر حملات مشخص را مدنظر قرار می‌دهد. - هدف امنیتی برای محصول – را زمانی داده ایجاد امضا (OT.SCD_Secrecy) و هدف امنیتی برای محصول - امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure) پاراگراف (b) ۱پیوست ۳ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا [۱] را با الزاماتی برآورده می‌سازد که اطمینان حاصل می‌کند که داده ایجاد امضا (SCD) نمی‌تواند از داده درستی‌سنجی امضا (SVD)، امضای دیجیتالی یا هر داده دیگر صادر شده به بیرون از محصول به دست آید. - هدف امنیتی برای محصول - تابع ایجاد امضا تنها برای

	صاحب‌امضای قانونی (OT.Sigy_SigF) پاراگراف (c) ۱پیوست ۳ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا [۱] را با الزاماتی برآورده می‌سازد که اطمینان حاصل می‌کند محصول تابع تولید امضا را تنها به صاحب‌امضای قانونی ارائه می‌دهد و از داده ایجاد امضا (SCD) در برابر استفاده دیگران محافظت می‌کند.
P.Sig_Non-Repud خط‌مشی انکارناپذیری امضا	این خط‌مشی با انکار داده امضا شده توسط صاحب‌امضا سروکار دارد، هر چند امضای الکترونیکی توسط داده درستی‌سنجی امضا (SVD) موجود در گواهی معتبر در زمان ایجاد امضا، به‌گونه‌ای موفق مورد تایید قرار گرفته باشد. این خط‌مشی با ترکیبی از اهداف امنیتی برای محصول و محیط عملیاتی‌اش، پیاده‌سازی شده است که از جنبه‌های کنترل انحصاری صاحب‌امضا و مسئولیت‌پذیری برای امضای دیجیتالی ایجاد شده توسط محصول اطمینان حاصل می‌کند. هدف امنیتی برای محیط عملیاتی - افزاره ایجاد امضای امن موثق ارائه شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.SSCD_prov_Service) این اطمینان را می‌دهد که صاحب‌امضا از نسخه‌ای موثق از محصول معتبر استفاده کند، که برای صاحب‌امضا مقداردهی اولیه و شخصی‌سازی شده است. هدف امنیتی برای محیط عملیاتی - تولید گواهی‌های واجد شرایط (OE.CGA_Qcert) اطمینان حاصل می‌کند که گواهی اجازه شناسایی صاحب‌امضا و سپس پیوند داده درستی‌سنجی امضا (SVD) صاحب‌امضا را بدهد. هدف امنیتی برای محیط عملیاتی - اصالت‌سنجی داده درستی‌سنجی امضا (OE.SVD_Auth) و هدف امنیتی برای محیط عملیاتی - تولید گواهی‌های واجد شرایط (OE.CGA_Qcert) نیازمند محیطی هستند تا از اصالت‌سنجی داده درستی‌سنجی امضا (SVD) صادر شده توسط محصول و استفاده‌شده تحت کنترل انحصاری صاحب‌امضا اطمینان حاصل کنند. هدف امنیتی برای محصول - تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا (OT.SCD_SVD_Corresp) تضمین می‌کند که داده درستی‌سنجی امضا (SVD) صادر شده توسط محصول با داده ایجاد امضا (SCD) پیاده‌سازی‌شده در محصول تناظر داشته باشد.

	هدف امنیتی برای محصول - یکتایی داده ایجاد امضا (OT.SCD_Unique) این امکان را فراهم می‌آورد که داده ایجاد امضا (SCD) صاحب‌امضا عملاً فقط یکبار اتفاق بیفتد. هدف امنیتی برای محیط عملیاتی - التزام امنیتی صاحب‌امضا (OE.Signatory) از این موضوع اطمینان حاصل می‌کند که صاحب‌امضا بررسی می‌کند که آیا داده ایجاد امضا (SCD) ذخیره‌شده در افزاره ایجاد امضای امن (SSCD) که از خدمات تدارک افزاره ایجاد امضای امن (SSCD) دریافت شده است در حالت غیر عملیاتی است یا خیر (یعنی داده ایجاد امضا (SCD) نمی‌تواند قبل از آن که صاحب‌امضا کنترل انحصاری بر روی افزاره ایجاد امضای امن (SSCD) داشته باشد، مورد استفاده قرار بگیرد). هدف امنیتی برای محصول - تابع ایجاد امضا تنها برای صاحب‌امضای قانونی (OT.Sigy_SigF) این امکان را فراهم می‌کند که تنها صاحب‌امضا امکان استفاده از محصول برای ایجاد امضا را داشته باشد. هدف امنیتی برای محیط عملیاتی - التزام امنیتی صاحب‌امضا (OE.Signatory) از این موضوع اطمینان حاصل می‌کند که صاحب‌امضا محرمانگی SAVD خود را حفظ می‌کند. هدف امنیتی برای محیط عملیاتی - ارسال داده‌های درنظر گرفته شده برای امضا توسط برنامه کاربردی تولید امضا (OE.DTBS_Intend)، هدف امنیتی برای محیط عملیاتی - محافظت از داده‌های در نظر گرفته شده برای امضا توسط برنامه کاربردی ایجاد امضا (OE.DTBS_Protect) و هدف امنیتی برای محصول – یکپارچگی داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) درون محصول (OT.DTBS_Integrity_TOE)، این اطمینان را می‌دهد که محصول امضاهای دیجیتالی را فقط برای داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) تولید کند که صاحب‌امضا تصمیم به امضا به عنوان داده‌ای که باید امضا شود (DTBS) را داشته است. تکنیک‌های رمزنگاریِ قوی مورد نیاز هدف امنیتی برای محصول - امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure) اطمینان حاصل می‌کند که تنها این داده ایجاد امضا (SCD) ممکن است امضای دیجیتالی معتبری ایجاد کند که بتواند به طور موفقیت‌آمیزی با داده درستی‌سنجی امضا (SVD) متناظر مورد استفاده برای درستی‌سنجی امضا

	تأیید شود. هدف امنیتی برای محصول - امنیت چرخه حیات (OT.Lifecycle_Security)، هدف امنیتی برای محصول – را زمانی داده ایجاد امضا (OT.SCD_Secrecy)، هدف امنیتی برای محصول - فراهم آوردن امنیت برون‌تابی‌های فیزیکی (OT.EMSEC_Design)، هدف امنیتی برای محصول - آشکارسازی دست‌کاری (OT.Tamper_ID) و هدف امنیتی برای محصول - مقاومت در برابر دست‌کاری (OT.Tamper_Resistance) از داده ایجاد امضا (SCD) در مقابل هرگونه خطر کشف رمز محافظت می‌کند.

۳-۲-۴-۵- مفروضات و کفایت اهداف امنیتی

مفروضات اهداف امنیتی	توضیحات
A.SCA فرض برنامه‌کاربردی ایجاد امضای قابل اعتماد	این فرض قابل‌اعتماد بودن برنامه‌کاربردی ایجاد امضا (SCA) را با توجه به تولید داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) تعیین می‌کند. این موضوع، مورد توجه هدف امنیتی برای محیط عملیاتی - ارسال داده‌های درنظر گرفته شده برای امضا توسط برنامه کاربردی تولید امضا (OE.DTBS_Intend) قرار دارد که این اطمینان را می‌دهد که برنامه‌کاربردی ایجاد امضا (SCA)، داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) را از داده‌ای تولید می‌کند که به عنوان داده‌ای که باید امضا شود (DTBS) به صاحب‌امضا ارائه شده است و صاحب‌امضا قصد امضای آن را به شکل مناسب برای امضا توسط محصول دارد.
A.CGA فرض برنامه‌کاربردی تولید گواهی قابل اعتماد	این فرض محافظت از اصالت‌سنجیِ نام صاحب‌امضا و داده درستی‌سنجی امضا (SVD) موجود در گواهی واجد شرایط توسط امضای پیشرفته تامین‌کننده خدمات صدور گواهی (CSP) را به وسیله برنامه‌کاربردی تولید گواهی (CGA) تعیین می‌کند. این موضوع مورد توجه هدف امنیتی برای محیط عملیاتی - تولید گواهی‌های واجد شرایط (OE.CGA_Qcert) قرار دارد، که از تولید گواهی واجد شرایط اطمینان حاصل می‌کند. همچنین هدف امنیتی برای محیط عملیاتی - اصالت‌سنجی داده درستی‌سنجی امضا (OE.SVD_Auth) که از محافظت از یکپارچگی و درستی‌سنجی تناظر بین داده درستی‌سنجی امضا (SVD) و داده ایجاد امضا (SCD) پیاده‌سازی شده توسط افزاره ایجاد امضای امن (SSCD) صاحب‌امضا اطمینان حاصل می‌کند.

۶- الزامات کارکرد امنیتی

۱-۶- قراردادها

معیار مشترک اجازه می‌دهد عملیات متعددی بر روی الزامات کارکردی اجرا شوند. پالایش، انتخاب، اختصاص و تکرار در این پروفایل حفاظتی استفاده شده‌است.

"عملیات پالایش" برای افزودن جزئیات به یک الزام استفاده می‌شود در نتیجه محدودیت‌های بیشتر برای یک الزام مورد استفاده قرار گرفته است. پالایش الزامات امنیتی (۱) با واژه "پالایش" به شکل **پر رنگ** نشان داده شده است و واژگان اضافه شده و یا تغییر یافته نوشته **پر رنگی** هستند، یا (۲) در متن به عنوان نوشته **پر رنگ** گنجانده شده و با زیرنویسی مشخص شده است. در مواردی که کلمات از یک الزام معیار مشترک حذف شده باشد، پیوست جداگانه‌ای کلماتی که حذف شده است را نشان می‌دهد.

"عملیات انتخاب" برای انتخاب یک یا تعداد بیشتری از گزینه‌های ارائه شده توسط معیار مشترک در بیان الزامات استفاده می‌شود. انتخابی که در این استاندارد اروپایی انجام می‌شود، در متن زیرخط‌داری مشخص شده و متن اصلی این مؤلفه در زیرنویس ارائه می‌شود. انتخاب‌هایی که باید توسط نویسنده هدف امنیتی انجام شود در براکتی با نشانی ظاهر می‌شود که نشان‌دهنده این است یک انتخاب انجام شده، [انتخاب:]، و با حروف مورب نشان داده می‌شود.

"عملیات اختصاص"، برای اختصاص مقدار مشخص به یک پارامتر نامشخص استفاده می‌شود مانند طول یک کلمه‌عبور. اختصاصی که در این استاندارد اروپایی استفاده می‌شود، به‌صورت متن زیرخط‌داری مشخص شده و متن اصلی این مؤلفه در زیرنویس آورده می‌شود. اختصاص صورت گرفته توسط نویسنده هدف امنیتی با براکتی با نشانی ظاهر می‌شود که نشان‌دهنده این است یک اختصاص انجام شده، [اختصاص:]، و با حروف مورب نشان داده شده است.

"عملیات تکرار" زمانی استفاده می‌شود که یک مؤلفه با عملیات مختلف تکرار می‌شود. تکرار با یک اسلش "/" نشان داده می‌شود و نشانگر تکرار بعد از شناسه مؤلفه آورده می‌شود.

جدول ۱- الزامات کارکرد امنیتی

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**مدیریت کلید رمزنگاری ۱ (احرازهویت)**	FCS_CKM.1.1
۲	**مدیریت کلید رمزنگاری ۶**	FCS_CKM_EXT.4.1
۳	**عملیات رمزنگاری ۱ (۱)**	FCS_COP.1.1(1)

شماره الزام	نام الزام	تطابق الزام با استاندارد
۴	عملیات رمزنگاری ۱ (۲)	FCS_COP.1.1(2)
۵	تولید بیت تصادفی ۱	FCS_RBG_EXT.۱,۱
۶	تولید بیت تصادفی ۲	FCS_RBG_EXT.۱,۲
۷	کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا ۱	FDP_ACC.1.1/SCD/SVD_Generation_SFP
۸	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا ۱	FDP_ACF.1.1/SCD/SVD_Generation_SFP
۹	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا ۲	FDP_ACF.1.2/SCD/SVD_Generation_SFP
۱۰	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا ۳	FDP_ACF.1.3/SCD/SVD_Generation_SFP
۱۱	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا ۴	FDP_ACF.1.4/SCD/SVD_Generation_SFP
۱۲	کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا ۱	FDP_ACC.1.1/SVD_Transfer_SFP
۱۳	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا ۱	FDP_ACF.1.1/SVD_Transfer_SFP
۱۴	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا ۲	FDP_ACF.1.2/SVD_Transfer_SFP
۱۵	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا ۳	FDP_ACF.1.3/SVD_Transfer_SFP
۱۶	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا ۴	FDP_ACF.1.4/SVD_Transfer_SFP
۱۷	کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی ایجاد امضا ۱	FDP_ACC.1.1/Signature_creation_SFP
۱۸	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی	FDP_ACF.1.1/Signature_creation_SFP

شماره الزام	نام الزام	تطابق الزام با استاندارد
	کارکرد امنیتی ایجاد امضا ۱	
۱۹	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی ایجاد امضا ۲**	FDP_ACF.1.2/Signature_creation_SFP
۲۰	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی ایجاد امضا ۳**	FDP_ACF.1.3/Signature_creation_SFP
۲۱	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی ایجاد امضا ۴**	FDP_ACF.1.4/Signature_creation_SFP
۲۲	**حفاظت از اطلاعات باقیمانده زیرمجموعه ۱**	FDP_RIP.1.1
۲۳	**نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / ماندگاری ۱**	FDP_SDI.2.1/Persistent
۲۴	**نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / ماندگاری ۲**	FDP_SDI.2.2/Persistent
۲۵	**نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / داده‌ای که باید امضا شود ۱**	FDP_SDI.2.1/DTBS
۲۶	**نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / داده‌ای که باید امضا شود ۲**	FDP_SDI.2.2/DTBS
۲۷	**زمانبندی شناسایی ۱**	FIA_UID.1.1
۲۸	**زمانبندی شناسایی ۲**	FIA_UID.1.2
۲۹	**زمانبندی احرازهویت ۱**	FIA_UAU.1.1
۳۰	**زمانبندی احرازهویت ۲**	FIA_UAU.1.2
۳۱	**ساماندهی شکست در احرازهویت ۱**	FIA_AFL.1.1
۳۲	**ساماندهی شکست در احرازهویت ۲**	FIA_AFL.1.2
۳۳	**نقش‌های امنیتی ۱**	FMT_SMR.1.1
۳۴	**نقش‌های امنیتی ۲**	FMT_SMR.1.2
۳۵	**مشخصات کارکردهای مدیریت امنیت ۱**	FMT_SMF.1.1
۳۶	**مدیریت رفتار توابع امنیتی ۱**	FMT_MOF.1.1
۳۷	**مدیریت مشخصه‌های امنیتی / مدیر سیستم ۱**	FMT_MSA.1.1/Admin
۳۸	**مدیریت مشخصه‌های امنیتی / صاحب‌امضا ۱**	FMT_MSA.1.1/Signatory
۳۹	**مشخصه‌های امنیتی امن ۱**	FMT_MSA.2.1
۴۰	**مقداردهی اولیه مشخصه ایستا ۱**	FMT_MSA.3.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۴۱	**مقداردهی اولیه مشخصه ایستا ۲**	FMT_MSA.3.2
۴۲	**ارث‌بری مقادیر مشخصه‌های امنیتی ۱**	FMT_MSA.4.1
۴۳	**مدیریت داده امنیتی / مدیر سیستم ۱**	FMT_MTD.1.1/Admin
۴۴	**مدیریت داده امنیتی / صاحب‌امضا ۱**	FMT_MTD.1.1/Signatory
۴۵	**برون‌تابی هدف ارزیابی ۱**	FPT_EMS.1.1
۴۶	**برون‌تابی هدف ارزیابی ۲**	FPT_EMS.1.2
۴۷	**حفظ حالت امن در صورت شکست ۱**	FPT_FLS.1.1
۴۸	**آشکارسازی انفعالی حمله فیزیکی ۱**	FPT_PHP.1.1
۴۹	**آشکارسازی انفعالی حمله فیزیکی ۲**	FPT_PHP.1.2
۵۰	**مقاومت در مقابل حمله فیزیکی ۱**	FPT_PHP.3.1
۵۱	**آزمون محصول ۱**	FPT_TST.1.1
۵۲	**آزمون محصول ۲**	FPT_TST.1.2
۵۳	**آزمون محصول ۳**	FPT_TST.1.3

۲-۶- کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱	**مدیریت کلید رمزنگاری ۱ (برای احرازهویت)**

محصول باید کلیدهای رمزنگاری نامتقارن جهت استفاده در احرازهویت را مطابق با الگوریتم‌های تولیدکلید رمزنگاری زیر [انتخاب:

- FIPS PUB 186-4، *" استاندارد امضای دیجیتال (DSS) " ، پیوست b.3 برای طرح RSA*
- *FIPS PUB 186-4، " استاندارد امضای دیجیتال (DSS) " ، پیوست b.3 برای طرح ECDSA و پیاده‌سازی " منحنی‌های NIST" P-256، P-384 و [انتخاب: P-521، هیچ منحنی دیگر]*

تولید نمایند همچنین اندازه‌ی کلید رمزنگاری باید معادل یا بزرگتر از قدرت یک کلید متقارن ۱۱۲ بیتی باشد.

نکته کاربردی۱:

استحکام کلید تولیدشده ۲۰۴۸ بیتی RSA و DSA باید معادل، یا بیشتر از، یک کلید متقارن ۱۱۲ بیتی باشد. برای کسب اطلاعات در مورد قدرت معادل کلید، رجوع کنید به گزارش ویژه NIST 800-57 با عنوان «توصیه‌هایی برای

مدیریت کلید».	
۲	**مدیریت کلید رمزنگاری ۶**

محصول باید تمامی کلیدهای رمزنگاری و پارامترهای امنیتی حساس را که دیگر نیازی به آن‌ها نیست و به طور دائمی به طور سخت افزاری مورد حفاظت قرار نمی‌گیرند، مطابق یکی از روش‌های زیر تخریب کند:
[انتخاب:

- با پاک کردن کلید رمزگذاری کلید (KEK) که کلید هدف با آن رمز شده است.
- در مورد حافظه های فرار ، تخریب باید [انتخاب:
  - با بازنویسی مستقیم اطلاعات دیگر روی حافظه انجام شود [انتخاب:
    - یک الگوی شبه تصادفی با استفاده از RBG محصول (همان‌طور که FCS_RBG_EXT.1 در تعیین شد)،
    - بیت های صفر
    - بیت های یک
    - مقدار یک کلید جدید
    - [اختصاص: مقداری که شامل یک داده حساس امنیتی نباشد.]
  - قطع برق حافظه
  - نابود کردن ارجاع به کلید و بلافاصله بعد از آن درخواست بازیافت حافظه
- برای حافظه‌های غیر فرار که دارای رابطی است که به پلت‌فرم زمینه فرمان می‌دهد که مشخص کننده کلید را پاک کند یا به طور منطقی اشاره می‌کند به محل ذخیره سازی کلید و بازنویسی یکباره یا چندباره را به صورت زیر انجام می‌دهد:
  - یک الگوی شبه تصادفی با استفاده از RBG تابع امنیتی محصول (همان‌طور که FCS_RBG_EXT.1 در تعیین شد)،
  - بیت های صفر
  - بیت های یک
  - مقدار یک کلید جدید
  - [اختصاص: مقداری که شامل یک داده حساس امنیتی نباشد.]

نکته کاربردی۲ :

رابط ذکر شده در الزام می‌تواند فرم‌های مختلفی بگیرد. مرسوم‌ترین آنها یک API به هسته سیستم عامل است. سطوح مختلفی از انتزاع ممکن است قابل مشاهده باشد. برای مثال در یک پیاده‌سازی برنامه مورد نظر ممکن است به جزئیات فایل سیستم دسترسی داشته باشد و قادر به آدرس‌دهی منطقی به بخش‌های خاص از حافظه باشد. در پیاده سازی‌های دیگر، برنامه دسترسی محدودی به یک منبع دارد و صرفا می‌تواند از پلتفرم درخواست کند که آن منبع را پاک کند. سطح جزئیاتی که محصول به آن دسترسی دارد در بخش TSS از ST بیان شده است.

۳	**عملیات رمزنگاری ۱ (۱)(برای امضای دیجیتال)**

محصول، باید خدمات رمزنگاری امضا را مطابق با الگوریتم‌های زیر انجام دهد:

[انتخاب:

- الگوریتم امضای دیجیتال مبتنی بر RSA (rDSA) با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با استاندارد FIPS PUB 186-4 ، «استاندارد امضای دیجیتال»
- الگوریتم امضای دیجیتال مبتنی بر خم های بیضوی (ECDSA) با کلید ۲۵۶ بیتی یا بیشتر مطابق با استاندارد FIPS PUB 186-4، «استاندارد امضای دیجیتال» با منحنی‌های استاندارد P-256، P-384 و [انتخاب: P-521 ، نه سایر منحنی‌ها] (هم‌چنان‌که در FIPS PUB 186-4، «استاندارد امضای دیجیتال» تعریف شده‌است) را پیاده‌سازی کند.

  الگوریتم امضای دیجیتال (DSA) با طول کلید (پیمانه) ۲۰۴۸ بیتی یا بیشتر که مطابق استاندارد FIPS 186-4 باشد.

نکته کاربردی ۳:

سند هدف امنیتی باید مشخص کند که آیا محصول، به تنهایی یا در ترکیب با محیط عملیاتی الگوریتم‌ها را اجرا می‌کند. برای هر یک از پلت‌فرم‌های محصول تحت پشتیبانی، نیاز به مدارکی است که نشان دهد این پلت‌فرم قادر است الزامات را از جانب محصول برآورده سازد. نویسنده محصول باید الگوریتمی را برای پیاده‌سازی انتخاب کند تا کار امضای دیجیتال را انجام دهد؛ اگر بیش از یک الگوریتم در دسترس باشد، این الزام (و الزام مربوط به تولید کلید) باید تکرار شوند تا کارکرد آن تعیین شود. در مورد الگوریتم انتخابی، نویسنده هدف امنیتی باید اختصاص/انتخاب‌های مناسبی اتخاذ کند تا پارامترهای الگوریتم پیاده‌سازی شده، تعیین شوند. در مورد الگوهای رمزگذاری خم‌های بیضوی، اندازه کلید اشاره به لگاریتم پایه ۲ نقطه پایه دارد. به عنوان رویکرد ارجح در امضاهای دیجیتال، ECDSA برای کاربردهای آتی از این پروفایل، الزامی است.

۴	**عملیات رمزنگاری ۱(۲)(درهم‌سازی رمزنگاری)**

محصول باید [خدمات درهم‌سازی رمزنگاری] را مطابق با یک الگوریتم رمزنگاری مشخص [انتخاب: *SHA-256, SHA-*

384, SHA-512] و اندازه‌ی خلاصه پیام[۱][انتخاب: *۱۶۰، ۲۵۶، ۳۸۴ و ۵۱۲ بیت*] که مطابق با استاندارد FIPS 180-4، «استاندارد درهم‌ساز امن» باشد، انجام دهد. **نکته کاربردی ۴:** انتخاب الگوریتم درهم‌سازی باید متناسب با اندازه خلاصه پیام باشد. برای کاربردهای مربوط به تولید امضای دیجیتال الگوریتم SHA-1 نا امن شناخته می‌شود. ولی برای سایر کاربردها قابل استفاده است.

۵	**تولید بیت تصادفی ۱**

[انتخاب: محصول، محیط محصول] باید تمام خدمات تولید بیت تصادفی را مطابق با [انتخاب: یکی از: *استاندارد NIST 800-90A با استفاده از الگوریتم* [انتخاب: *Hash_DRBG (هرکدام)، HMAC_DRBG(هرکدام)، CTR_DRBG (AES)*]، *پیوست سه استاندارد FIPS Pub 140-2؛ ضمیمه ۲,۴ از استاندارد X9.31 با استفاده از الگوریتم AES*] انجام بدهند که توسط یک منبع آنتروپی ورودی اولیه داده می‌شوند، آنتروپی از [انتخاب: یکی یا هر دو : *منبع نویز مبتنی بر نرم‌افزار، نویز مبتنی بر سخت‌افزار*] محاسبه می‌گردد.

نکته کاربردی ۵:

در اولین انتخاب این الزام، نویسنده هدف امنیتی باید استانداردی را که مطابق با خدمات RBG است، انتخاب کند.(یا NIST 800-90 یا پیوست سه استاندارد FIPS.)

استاندارد SP 800-90 در برگیرنده‌ی چهار روش متفاوت برای تولید اعداد تصادفی می‌باشد که هرکدام از این روش‌ها به اصول اولیه رمزنگاری (توابع درهم‌ساز/رمز) بستگی دارند. نویسنده هدف امنیتی تابع مورد استفاده برای تولید عدد تصادفی را در این الزام انتخاب خواهد نمود(اگر 800-90 انتخاب شده باشد) همچنین اصول اولیه رمزنگاری استفاده شده را با اضافه نمودن الزام یا در بخش خلاصه امنیتی محصول لحاظ می‌نماید.

درحالی‌که هر کدام از توابع درهم‌ساز تعریف‌شده(SHA-1, SHA-224,SHA-256, SHA-384, SHA-512) برای Hash_DRBG یا HMAC_DRBG مجاز هستند، برای CT_DRBG تنها پیاده‌سازی‌های مبتنی بر AES مجازند.

برای Dual_EC_DRBG هر یک از منحنی‌های تعریف شده در استاندارد SP 800-90 مجاز هستند، نویسنده هدف امنیتی باید در سند هدف امنیتی منحنی و الگوریتم درهم‌ساز استفاده شده را لحاظ نماید.

در دومین انتخاب این الزام، نویسنده هدف امنیتی مشخص می‌نماید که منبع آنتروپی مبتنی بر نرم‌افزار است یا سخت‌افزار یا هردو.

اگر چند منبع آنتروپی وجود داشته باشد، نویسنده هدف امنیتی باید به طور دقیق منبع هر آنتروپی را مشخص نماید که مبتنی بر سخت‌افزار یا نرم‌افزار است. به طور کلی اولویت با منابع نویز مبتنی بر سخت‌افزار است.

[۱] Message Digest Sizes

توجه داشته باشید که در پیوست سه استاندارد FIPS 140-2، در حال حاضر تنها روش شرح داده شده در توصیه‌ی NIST، تولید کننده عدد تصادفی مبتنی بر پیوست سه از ANSI X9.31 با استفاده از سه کلید سه‌تایی الگوریتم‌های DES و AES [۱] معتبر می‌باشند.

در صورتی که طول کلید استفاده شده در پیاده‌سازی AES با طول کلید استفاده شده در رمزنگاری داده متفاوت باشد، آنگاه باید الزام عملیات رمزنگاری(رمزنگاری-رمزگشایی داده)[۲] را برای منعکس کردن طول کلید متفاوت، دو بار تکرار نمود.

	تولید بیت تصادفی۲

تابع تولید بیت تصادفی قطعی باید توسط منبع آنتروپی تغذیه شود که آنتروپی را از [انتخاب: منبع نویز مبتنی بر نرم افزار، منبع نویز مبتنی بر سخت افزار] با حداقل [انتخاب: *۱۲۸، ۲۵۶ بیت*] آنتروپی تأمین می‌نماید که این مقدار دست‌کم با بزرگ‌ترین طول بیت کلیدها و پارامترهای احراز هویتی که تولید خواهد نمود، برابر است.

نکته کاربردی ۶:

در این الزام، نویسنده هدف امنیتی حداقل تعداد بیت‌های آنتروپی را که برای مقدار اولیه داده به تابع تولید بیت تصادفی استفاده شده است، را انتخاب می‌نماید.

۳-۶- کلاس حفاظت از داده‌های کاربری (FDP)

مشخصه‌های امنیتی و وضعیت مرتبط با موجودیت‌های فعال و غیرفعال در جدول زیر نمایش داده‌شده است.

جدول ۲- موجودیت‌های فعال و مشخصه‌های امنیتی برای کنترل دسترسی

موجودیت فعال یا غیرفعال مرتبط با مشخصه‌های امنیتی	نوع مشخصه‌های امنیتی	مقادیر مشخصه‌های امنیتی
موجودیت فعال کاربر	نقش[۳]	نقش مدیر سیستم: موجودیت فعال کاربر که به‌عنوان موجودیت فعال مدیر سیستم عمل می‌کند. نقش صاحب‌امضا: موجودیت فعال کاربر که به‌عنوان موجودیت فعال

[۱] ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms

[۲] FCS_COP.1.1(1)

[۳] Role

		صاحب‌امضا عمل می‌کند.
موجودیت فعال کاربر	مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا	مجاز، غیرمجاز
داده ایجاد امضا	عملیات داده‌های ایجاد امضا	بله، خیر
داده ایجاد امضا	شناسه داده‌های ایجاد امضا	مقادیر دلخواه
داده اعتبارسنجی امضا	این پروفایل حفاظتی مشخصه امنیتی برای داده درستی‌سنجی امضا تعریف نمی‌کند.	این پروفایل حفاظتی مشخصه امنیتی برای داده درستی‌سنجی امضا تعریف نمی‌کند.

نکته کاربردی ۷: نویسنده پروفایل حفاظتی یا هدف امنیتی ممکن است موجودیت‌های غیرفعال و یا مشخصه‌های امنیتی اضافی تعریف کنند.

شماره الزام	نام الزام
۷	کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی تولید داده ایجاد امضا / داده درستی‌سنجی امضا ۱
وراثت از هیچ مؤلفه دیگری ندارد. وابستگی: مشخصه‌های امنیتی مبتنی بر کنترل دسترسی محصول باید خط‌مشی کارکرد امنیتی تولید داده ایجاد امضا / داده درستی‌سنجی امضا[۱] را روی موارد زیر اعمال کند: (۱) موجودیت‌های فعال: موجودیت فعال کاربر (۲) موجودیت‌های غیرفعال: داده ایجاد امضا، داده درستی‌سنجی امضا عملیات: تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا[۲]	
۸	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید داده ایجاد امضا / داده درستی‌سنجی امضا ۱

[۱] [اختصاص: *خط‌مشی کارکرد امنیتی کنترل دسترسی*]

[۲] [اختصاص: *فهرستی از موجودیت‌های فعال، غیرفعال و عملیات میان موجودیت‌های فعال و غیرفعال تحت پوشش خط‌مشی کارکرد امنیتی*]

وراثت از هیچ مؤلفه دیگر ندارد. وابستگی: کنترل دسترسی زیرمجموعه[۱] مقداردهی اولیه مشخصه ایستا محصول باید خط‌مشی کارکرد امنیتی تولید داده ایجاد امضا / داده درستی‌سنجی امضا[۲] را روی موجودیت‌های غیرفعال بر اساس موارد زیر اعمال کند: موجودیت فعال کاربر به مشخصه امنیتی "مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا"[۳] پیوند داده شده است.	
۹	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید داده ایجاد امضا / داده درستی‌سنجی امضا ۲
محصول باید قوانین زیر را اجرا کند تا تعیین کند که عملیات میان موجودیت‌های فعال کنترل‌شده و موجودیت‌های غیرفعال کنترل‌شده، مجاز است: موجودیت فعال کاربر که با مشخصه امنیتی "مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا" به‌عنوان "مجاز" تنظیم شده است، اجازه دارد زوج داده ایجاد امضا / داده درستی‌سنجی امضا را تولید کند[۴].	
۱۰	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید داده ایجاد امضا / داده درستی‌سنجی امضا ۳
محصول باید به‌صراحت دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را براساس قوانین افزوده زیر مجاز کند: هیچ‌چیز[۵]	
۱۱	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید داده ایجاد امضا / داده درستی‌سنجی امضا ۴
محصول باید به‌صراحت دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را بر اساس قوانین افزوده زیر انکار کند: موجودیت فعال کاربر که با مشخصه امنیتی «مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا» به‌عنوان	

[۱] FDP_ACC.1

[۲] [اختصاص: *خط‌مشی کارکرد امنیتی کنترل دسترسی*]

[۳] [اختصاص: *فهرستی از موجودیت‌های فعال و غیرفعال تحت کنترل خط‌مشی کارکرد امنیتی تعیین شده و برای هر کدام، مشخصه‌های امنیتی مربوط به خط‌مشی کارکرد امنیتی یا مشخصه‌های امنیتی مربوط به خط‌مشی کارکرد امنیتی از گروه نامبرده شده*]

[۴] [اختصاص: *قوانین حاکم بر دسترسی به موجودیت‌های فعال و غیرفعال کنترل شده با استفاده از عملیات کنترل شده روی موجودیت‌های غیرفعال کنترل شده*]

[۵] [اختصاص: *قوانین مبتنی بر مشخصه‌های امنیتی که به صراحت اجازه دسترسی موجودیت‌های فعال به غیرفعال را می‌دهد*]

«غیرمجاز» تنظیم شده است، اجازه ندارد زوج داده ایجاد امضا / داده درستی‌سنجی امضا را تولید کند[۱].	
۱۲	کنترل دسترسی زیرمجموعه / خط‌مشی کنترل دسترسی انتقال داده درستی‌سنجی امضا ۱
وراثت از هیچ مؤلفه دیگر ندارد. وابستگی: کنترل دسترسی بر اساس مشخصه‌های امنیتی محصول باید خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا[۲] را بر روی موارد زیر اعمال نماید : (۱) موجودیت‌های فعال: موجودیت فعال کاربر (۲) موجودیت‌های غیرفعال: داده درستی‌سنجی امضا عملیات: صدور[۳]	
۱۳	کنترل دسترسی بر اساس مشخصه‌های امنیتی / خط‌مشی کنترل دسترسی انتقال داده درستی‌سنجی امضا ۱
وراثت از هیچ مؤلفه دیگر ندارد. وابستگی: کنترل دسترسی زیرمجموعه مقداردهی اولیه مشخصه ایستا محصول باید خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا[۴] را به موجودیت‌های غیرفعال بر اساس موارد زیر اعمال کند: (۱) موجودیت فعال کاربر به نقش مشخصه امنیتی مرتبط شده است، داده درستی‌سنجی امضا[۵]	
۱۴	کنترل دسترسی بر اساس مشخصه‌های امنیتی / خط‌مشی کنترل دسترسی انتقال داده درستی‌سنجی امضا ۲
محصول باید قوانین زیر را اجرا کند تا مجاز بودن عملیات میان موجودیت‌های غیرفعال کنترل‌شده و موجودیت‌های فعال کنترل‌شده، را تعیین نماید: [انتخاب: *نقش مدیر سیستم، نقش صاحب‌امضا*] برای صدور داده	

[۱] [اختصاص: *قوانین مبتنی بر مشخصه‌های امنیتی که به صراحت اجازه دسترسی موجودیت‌های فعال به غیرفعال را رد می‌کند*]

[۲] [اختصاص: *خط‌مشی کارکرد امنیتی کنترل دسترسی*]

[۳] [اختصاص: *فهرستی از موجودیت‌های فعال، غیرفعال و عملیات میان موجودیت‌های فعال و غیرفعال خط‌مشی کارکرد امنیتی*]

[۴] [اختصاص: *خط‌مشی کارکرد امنیتی کنترل دسترسی*]

[۵] [اختصاص: *فهرستی از موجودیت‌های فعال و غیرفعال تحت کنترل خط‌مشی کارکرد امنیتی تعیین شده و برای هر کدام، مشخصه‌های امنیتی مربوط به خط‌مشی کارکرد امنیتی یا مشخصه‌های امنیتی مربوط به خط‌مشی کارکرد امنیتی از گروه نامبرده شده*]

درستی‌سنجی امضا اجازه داده شده است[۱].	
۱۵	کنترل دسترسی بر اساس مشخصه‌های امنیتی / خط‌مشی کنترل دسترسی انتقال داده درستی‌سنجی امضا ۳
محصول باید به صراحت دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را بر اساس قوانین افزوده پیرو مجاز کند: هیچ‌چیز[۲]	
۱۶	کنترل دسترسی بر اساس مشخصه‌های امنیتی / خط‌مشی کنترل دسترسی انتقال داده درستی‌سنجی امضا ۴
محصول باید به صراحت دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را بر اساس قوانین افزوده زیر انکار کند: هیچ‌چیز[۳]	

نکته کاربردی ۸: نویسنده هدف امنیت باید عملیات موجود در الزام کارکرد امنیتی مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا ۱ را بر اساس قوانین کنترل دسترسی ارائه‌شده توسط هدف ارزیابی برای صدور داده درستی‌سنجی امضا اجرا کند. قوانین کنترل دسترسی ممکن است همان‌گونه که در مثال‌های زیر نشان داده‌شده است به چرخه حیات هدف ارزیابی وابسته باشد.

- مدیر سیستم مجاز است زوج کلید داده ایجاد امضا / داده درستی‌سنجی امضا مطابق با مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا را تولید کرده و داده درستی‌سنجی امضا را قبل از اینکه نقش صاحب‌امضا (RAD) ایجاد شود صادر نماید. این کار اجازه شناسایی نمونه خاصی از هدف ارزیابی را به‌وسیله داده درستی‌سنجی امضا می‌دهد.

- مدیر سیستم مجاز به تولید زوج کلید داده ایجاد امضا / داده درستی‌سنجی امضا مطابق با الزام کارکرد امنیتی مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا می‌باشد و تنها صاحب‌امضا مجاز به صدور داده درستی‌سنجی امضا به برنامه‌کاربردی تولید گواهی است. این کار اجازه تعیین این موضوع را می‌دهد که آیا صاحب‌امضا بر روی مقداردهی اولیه هدف ارزیابی و گواهی که ممکن است تولید شود، کنترل دارد یا نه.

- صاحب‌امضا مجاز به تولید زوج کلید داده ایجاد امضا / داده درستی‌سنجی امضا مطابق با الزام کارکرد

[۱] [اختصاص: *قوانین حاکم بر دسترسی میان موجودیت‌های فعال کنترل شده و موجودیت‌های غیرفعال کنترل شده با استفاده از عملیات کنترل شده روی موجودیت‌های غیرفعال کنترل شده*]

[۲] [اختصاص: *قوانین مبتنی بر مشخصه‌های امنیتی که به صراحت اجازه دسترسی موجودیت‌های فعال به غیرفعال را می‌دهد*]

[۳] [اختصاص: *قوانین مبتنی بر مشخصه‌های امنیتی که به صراحت اجازه دسترسی موجودیت‌های فعال به غیرفعال را رد می‌کند*]

امنیتی مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا و و صدور داده درستی‌سنجی امضا به برنامه‌کاربردی تولید گواهی برای استفاده در گواهی است.

در این پروفایل حفاظتی نیازی نیست که هدف ارزیابی از یکپارچگی و اصالت‌سنجی کلید عمومی داده درستی‌سنجی امضا صادرشده محافظت کند اما چنین حفاظتی توسط محیط عملیاتی موردنیاز است. اگر محیط عملیاتی اقدامات امنیتی مناسبی را برای برنامه‌کاربردی تولید گواهی ارائه ندهد تا از اصالت‌سنجی کلید عمومی مطمئن شود، هدف ارزیابی باید توابع امنیتی اضافی را پیاده‌سازی نماید تا از صدور کلیدهای عمومی با یکپارچگی و احراز هویت مبدأ داده‌ها، اطمینان یابد. «پروفایل حفاظتی افزاره ایجاد امضای امن- قسمت ۳: افزاره‌ای با تولید کلید و کانال قابل‌اعتماد بین افزاره ایجاد امضای امن و برنامه‌کاربردی تولید گواهی» را ببینید تا الزامات اضافی به‌منظور استفاده یک افزاره ایجاد امضای امن را در محیطی که نمی‌تواند چنین حفاظتی را ایجاد کند ملاحظه کنید.

۱۷	کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی ایجاد امضا ۱
وراثت از هیچ مؤلفه دیگر ندارد. وابستگی: کنترل دسترسی بر اساس مشخصه‌های امنیتی محصول باید خط‌مشی کارکرد امنیتی ایجاد امضا[۱] را روی موارد زیر اعمال نماید: (۱) موجودیت‌های فعال: موجودیت فعال کاربر (۲) موجودیت‌های غیرفعال: داده‌هایی که باید امضا شوند یا بازنمایی منحصربه‌فرد متعلق به آن، داده ایجاد امضا (۳) عملیات: ایجاد امضا[۲]	
۱۸	کنترل دسترسی بر اساس مشخصه‌های امنیتی / خط‌مشی کارکرد امنیتی ایجاد امضا ۱
وراثت: از هیچ مؤلفه دیگر ندارد. وابستگی: کنترل دسترسی زیرمجموعه مقداردهی اولیه مشخصه ایستا محصول باید خط‌مشی کارکرد امنیتی ایجاد امضا[۳] را روی موجودیت‌های غیرفعال بر اساس موارد زیر اعمال نماید: (۱) موجودیت فعال کاربر که با مشخصه امنیتی "نقش" مرتبط شده است و (۲) داده‌های ایجاد امضا با مشخصه امنیتی "داده‌های ایجاد امضا عملیاتی"[۴]	
۱۹	کنترل دسترسی بر اساس مشخصه‌های امنیتی / خط‌مشی کارکرد امنیتی ایجاد امضا ۲

[۱] [اختصاص: *خط‌مشی کارکرد امنیتی کنترل دسترسی*]

[۲] [اختصاص: *فهرستی از موجودیت‌های فعال، غیرفعال و عملیات میان موجودیت‌های فعال و غیرفعال خط‌مشی کارکرد امنیتی*]

[۳] [اختصاص: *خط‌مشی کارکرد امنیتی کنترل دسترسی*]

[۴] [اختصاص: *فهرستی از موجودیت‌های فعال و غیرفعال تحت کنترل خط‌مشی کارکرد امنیتی تعیین شده و برای هر کدام، مشخصه‌های امنیتی مربوط به خط‌مشی کارکرد امنیتی یا مشخصه‌های امنیتی مربوط به خط‌مشی کارکرد امنیتی از گروه نامبرده شده*]

محصول باید قوانین زیر را برای مجاز بودن عملیات در میان موجودیت‌های غیرفعال کنترل‌شده و موجودیت‌های فعال کنترل‌شده، اعمال نماید: نقش صاحب‌امضا برای ایجاد امضای دیجیتال برای داده‌هایی که باید امضا شوند یا بازنمایی منحصربه‌فرد متعلق به آن با داده‌های ایجاد امضایی مجاز است که مشخصه امنیتی "داده ایجاد امضا عملیاتی" آن، "بله" تنظیم شده باشد[۱].	
۲۰	کنترل دسترسی بر اساس مشخصه‌های امنیتی / خط‌مشی کارکرد امنیتی ایجاد امضا ۳
محصول باید به صراحت دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را بر اساس قوانین افزوده زیر مجاز کند: هیچ‌چیز[۲]	
۲۱	کنترل دسترسی بر اساس مشخصه‌های امنیتی / خط‌مشی کارکرد امنیتی ایجاد امضا ۴
محصول باید به صراحت دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را بر اساس قوانین افزوده زیر انکار کند: موجودیت فعال کاربر مجاز به ایجاد امضای دیجیتال برای داده‌هایی که باید امضا شوند یا بازنمایی منحصربه‌فرد آن‌ها با داده ایجاد امضایی نیست که مشخصه امنیتی «داده ایجاد امضا عملیاتی» آن، «خیر» تنظیم شده‌باشد[۳].	
۲۲	حفاظت از اطلاعات باقیمانده زیرمجموعه ۱
محصول باید اطمینان حاصل کند که هرگونه محتوای اطلاعات قبلی از یک منبع به هنگام عدم تخصیص منبع از[۴] موجودیت‌های غیرفعالی که در ادامه می‌آید، از دسترس خارج شده است: داده ایجاد امضا[۵] داده‌های زیر که به‌صورت ماندگار توسط هدف ارزیابی ذخیره می‌شود، مشخصه داده کاربر را "کنترل یکپارچگی داده‌های ذخیره‌شده پایدار" را دارد: ۱. داده ایجاد امضا ۲. داده درستی‌سنجی امضا (درصورتی‌که به‌صورت ماندگار توسط هدف ارزیابی ذخیره شده باشد). داده‌ای که باید امضا شوند یا بازنمایی منحصربه‌فرد متعلق به آن که به‌صورت موقت توسط هدف ارزیابی ذخیره	

[۱] [اختصاص: *قوانین حاکم بر دسترسی میان موجودیت‌های فعال کنترل شده و موجودیت‌های غیرفعال کنترل شده با استفاده از عملیات کنترل شده روی موجودیت‌های غیرفعال کنترل شده*]

[۲] [اختصاص: *قوانین مبتنی بر مشخصه‌های امنیتی که به صراحت اجازه دسترسی موجودیت‌های فعال به غیرفعال را می‌دهد*]

[۳] [اختصاص: *قوانین مبتنی بر مشخصه‌های امنیتی که به صراحت اجازه دسترسی موجودیت‌های فعال به غیرفعال را رد می‌کند*]

[۴] [اختصاص: *تخصیص منابع به، عدم تخصیص منابع از*]

[۵] [اختصاص: *فهرستی از موجودیت‌های غیرفعال*]

شده‌است، مشخصه داده کاربر " داده ذخیره‌شده کنترل‌شده از نظر یکپارچگی" را دارد.	
۲۳	نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / ماندگاری ۱
وراثت: از نظارت بر یکپارچگی داده ذخیره‌شده۱ وابستگی: ندارد محصول باید بر روی داده‌های کاربر که در مجموعه‌ای تحت کنترل محصول ذخیره‌شده است، نظارت کند تا خطاهای یکپارچگی[۲] را بر روی تمام موجودیت‌های غیرفعال بر اساس مشخصاتی که در ادامه می‌آید تشخیص دهد: داده ذخیره‌شده کنترل‌شده از نظر یکپارچگی[۳]	
۲۴	نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / ماندگاری ۲
در صورت آشکارسازی خطای یکپارچگی داده، محصول باید اقدامات زیر را انجام دهد: (۱) استفاده از داده‌های تغییر یافته را منع کند. (۲) موجودیت فعال صاحب‌امضا را از خطای یکپارچگی مطلع کند.[۴]	
۲۵	نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / داده‌ای که باید امضا شود ۱
وراثت: از نظارت بر یکپارچگی داده ذخیره‌شده وابستگی: ندارد محصول باید بر روی داده‌های کاربر که در مجموعه‌ای تحت کنترل محصول ذخیره‌شده‌است، نظارت کند تا خطاهای یکپارچگی[۵] را بر روی تمام موجودیت‌های غیرفعال بر اساس مشخصاتی که در ادامه می‌آید تشخیص دهد: داده ذخیره‌شده کنترل‌شده از نظر یکپارچگی[۶]	
۲۶	نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / داده‌ای که باید امضا شود ۲
در صورت تشخیص خطای یکپارچگی داده، محصول باید اقدامات زیر را انجام دهد: (۱) استفاده از داده‌های تغییر یافته را منع کند. (۲) موجودیت فعال صاحب‌امضا را از خطای یکپارچگی مطلع کند.[۷] **نکته کاربردی** ۹: یکپارچگی داده امنیتی مانند داده احرازهویت مرجع باید حفظ شود تا از اثربخشی احرازهویت کاربر اطمینان حاصل شود. این حفاظت، جنبه خاصی از معماری امنیتی است (به الزامات تضمین امنیت طراحی	

[۱] FDP_SDI.1

[۲] [اختصاص: *خطاهای یکپارچگی*]

[۳] [اختصاص: *مشخصات داده‌های کاربر*]

[۴] [اختصاص: *اقدامی که باید انجام شود*]

[۵] [اختصاص: *خطاهای یکپارچگی*]

[۶] [اختصاص:*مشخصات داده‌های کاربر*]

[۷] [اختصاص:*اقدامی که باید انجام شود*]

معماری با جداسازی دامنه‌ها و بدون قابلیت دور زدن[۱] رجوع شود).

۴-۶- کلاس شناسایی و احرازهویت

۲۷	زمانبندی شناسایی ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد محصول باید به کاربر پیش از شناسایی شدن، اجازه‌ی اقدامات زیر را بدهد: (۱) خودآزمائی بر اساس آزمون توابع هدف امنیتی (۲) [اختصاص: فهرستی از اقدامات اضافه‌ای که محصول واسطه آن هستند][۲]	
۲۸	زمانبندی شناسایی ۲
محصول باید پیش از اجازه‌ی هر اقدامی به کاربر، او را به‌طور موفقیت‌آمیز شناسایی کند. **نکته کاربردی ۱۰**: نویسنده هدف امنیتی باید عملیات ازدست‌رفته در الزام کارکرد امنیتی زمانبندی شناسایی ۱را انجام دهد. فهرست اقدامات اضافه‌ای که محصول واسطه آنند ممکن است خالی باشد (به‌عنوان‌مثال، اختصاص "هیچ‌چیز") یا شامل اقداماتی باشد که محصول واسطه آن هستند مانند برقراری یک مسیر قابل‌اعتماد بین کاربرانی که در حال استفاده از رابط انسانی[۳] (کاربری) یک افزاره بیرونی هستند. هدف ارزیابی ممکن است به‌طور پیش‌فرض یا با انتخاب نقش و داده احرازهویت مرجع در برابر احرازهویتی که صورت خواهد گرفت، کاربر را شناسایی کند. شناسایی به‌طور پیش‌فرض، معمولا به چرخه‌حیات هدف ارزیابی پیوند داده می‌شود به‌عنوان‌مثال هدف ارزیابی ممکن است قبل از اینکه داده احرازهویت مرجع صاحب‌امضا ایجاد شود به‌طور پیش‌فرض مدیر سیستم را شناسایی کند، و اگر داده احرازهویت مرجع صاحب‌امضا وجود داشته باشد صاحب‌امضا را شناسایی کند. در مورد کارت‌های هوشمند چند کاربردی (به‌عبارت‌دیگر کارت‌های هوشمندی که کاربردی بیش از کاربرد ایجاد امضا را ارائه می‌دهند)، کاربر با انتخاب فایل راهنمای فایل‌ها و مسیرها[۴] برنامه‌کاربردی امضا، خود را به‌عنوان صاحب‌امضا شناسایی کرده و بنابراین احرازهویت پین بر اساس پین صاحب‌امضا انجام خواهد شد. کاربر ممکن است با انتخاب کلید احرازهویت، خود را به‌عنوان مدیر سیستم شناسایی کرده و بنابراین احرازهویت با احراز اصالت بیرونی یا احرازهویت افزاره دو طرفه انجام خواهد شد.	
۲۹	زمانبندی احرازهویت ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: زمانبندی شناسایی	

[۱] ADV_ARC.1

[۲] [اختصاص: *فهرستی از اقدامات انجام شده به واسطه توابع امنیتی محصول*]

[۳] HI

[۴] directory

محصول باید قبل از احراز هویت کاربر اجازه‌ی اقدامات زیر را بدهد: (۱) انجام خودآزمائی مطابق آزمون توابع هدف امنیتی (۲) شناسایی کاربر به‌وسیله محصول موردنیاز توسط الزام کارکرد امنیتی زمانبندی شناسایی (۳) [اختصاص: *فهرستی از اقدامات اضافی که محصول واسطه آن هستند*][۱]	
۳۰	زمانبندی احرازهویت ۲
محصول باید مستلزم آن باشد که قبل از اینکه به هر اقدام دیگری که محصول واسطه آن هستند در طرف کاربر انجام شود، هر کاربری با موفقیت احرازهویت شود. **نکته کاربردی ۱۱:** نویسنده هدف امنیتی باید عملیات ازدست‌رفته در زمانبندی احرازهویت ۱ را انجام دهد. فهرست اقدامات افزوده‌ای که محصول واسطه آن هستند ممکن است خالی باشد (به‌عنوان‌مثال، اختصاص"هیچ‌چیز") یا شامل اقداماتی باشد که محصول واسطه آن هستند مانند برقراری یک مسیر قابل‌اعتماد بین کاربرانی که در حال استفاده از افزاره رابط انسانی (کاربری) یک افزاره بیرونی هستند.	
۳۱	ساماندهی شکست در احرازهویت ۱
وراثت: از هیچ مؤلفه دیگری ندارد. وابستگی: زمانبندی احرازهویت محصول باید زمانی که [اختصاص: *عدد صحیح مثبت*] عدد صحیح مثبت قابل تنظیم توسط مدیر سیستم به همراه [اختصاص: *گستره‌ای از مقادیر قابل قبول*] تلاش‌های احرازهویت ناموفق مربوط به تلاش‌های احرازهویت شکست‌خورده متوالی[۲] اتفاق می‌افتد را تشخیص دهد.	
۳۲	ساماندهی شکست در احرازهویت ۲
محصول زمانی که با تعداد تعریف شده از تلاش‌های احرازهویت ناموفق مواجه شد[۳]، باید داده احرازهویت مرجع را مسدود کند[۴]. **نکته کاربردی ۱۲:** نویسنده هدف امنیت باید عملیات ازدست‌رفته در الزام کارکرد امنیتی ساماندهی شکست در احراز هویت ۱ را انجام دهد. اختصاص باید با سازوکار احرازهویت پیاده‌سازی‌شده سازگار بوده و در برابر حملات با پتانسیل حمله بالا، مقاوم باشد.	

۵-۶- کلاس مدیریت امنیت

[۱] اختصاص: *فهرستی ازاقدامات انجام شده به واسطه توابع امنیتی محصول*]
[۲] [اختصاص: *فهرستی از رویدادهای احرازهویت*]
[۳] [انتخاب: *برآورده ساختن، پیشی گرفتن*]
[۴] [اختصاص: *فهرستی از اقدامات*]

۳۳	نقش‌های امنیتی ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: زمانبندی شناسایی محصول باید نقش‌های مدیر سیستم و صاحب‌امضا[۱] را حفظ کند.	
۳۴	نقش‌های امنیتی ۲
محصول باید بتواند کاربران را به نقش‌هایشان مرتبط کند.	
۳۵	مشخصات کارکردهای مدیریت امنیت ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد محصول باید بتواند کارکردهای مدیریتی زیر را اجرا کنند: (۱) ایجاد و تغییر داده احرازهویت مرجع، (۲) فعال کردن تابع ایجاد امضا، (۳) تغییر مشخصه‌های امنیتی مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا، داده ایجاد امضا عملیاتی، (۴) تغییر مقدار پیش‌فرض مشخصه امنیتی شناسه داده ایجاد امضا، (۵) [اختصاص: *فهرستی از دیگر کارکردهای مدیریت امنیت که باید توسط محصول ارائه شود*][۲]. **نکته کاربردی**: نویسنده هدف امنیتی باید عملیات ازدست‌رفته در الزام کارکرد امنیتی مشخصات کارکردهای مدیریت امنیت ۱ را انجام دهد. فهرست دیگر کارکردهای مدیریت امنیتی که باید توسط محصول انجام شود، ممکن است خالی باشد (به‌عبارت‌دیگر: اختصاص«هیچ‌چیز»)	
۳۶	مدیریت رفتار توابع امنیتی ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: نقش‌های امنیتی مشخصات کارکردهای مدیریت امنیت	

[۱] [اختصاص: *نقش‌های مجاز شناسایی‌شده*]

[۲] [اختصاص: *فهرستی از کارکردهای مدیریت امنیت که توسط توابع امنیتی محصول ارائه شده‌است*]

محصول باید امکان فعال‌سازی[۱] کارکردهای تابع ایجاد امضا[۲] را به نقش صاحب‌امضا[۳] محدود کند.	
۳۷	مدیریت مشخصه‌های امنیتی / مدیر سیستم ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: [کنترل دسترسی زیرمجموعه یا کنترل جریان اطلاعات زیرمجموعه[۴] نقش‌های امنیتی مشخصات کارکردهای مدیریت امنیت	
محصولباید خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا [۵] را اعمال کند تا امکان تغییر [اختصاص: *عملیات دیگر*][۶] مشخصه‌های امنیتی مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا[۷] را به نقش مدیر سیستم[۸] محدود کند.	
۳۸	مدیریت مشخصه‌های امنیتی / صاحب‌امضا ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: [کنترل دسترسی زیرمجموعه یا کنترل جریان اطلاعات زیرمجموعه] نقش‌های امنیتی مشخصات کارکردهای مدیریت امنیت	
محصولباید خط‌مشی کارکرد امنیتی ایجاد امضا[۹] را اعمال نماید تا امکان تغییر[۱۰] مشخصه‌های امنیتی داده‌های ایجاد امضا عملیاتی[۱۱] را به نقش صاحب‌امضا[۱۲] محدود کند.	
۳۹	مشخصه‌های امنیتی امن ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: [کنترل دسترسی زیرمجموعه یا کنترل جریان اطلاعات زیرمجموعه] نقش‌های امنیتی	

[۱] [انتخاب: *تعیین رفتار، غیرفعال کردن، فعال کردن، تغییر رفتار*]
[۲] [اختصاص: *فهرستی از کارکردها*]
[۳] [اختصاص: *نقش‌های مجاز مشخص‌شده*]
[۴] FDP_IFC.1
[۵] [اختصاص: *خط‌مشی(های) کارکرد امنیتی کنترل دسترسی، خط‌مشی(های) کارکرد امنیتی کنترل جریان اطلاعات*]
[۶] [انتخاب: *تغییر-پیش‌فرض، پرس و جو، تغییر، حذف، [اختصاص:دیگر عملیات]*]
[۷] [اختصاص: *فهرستی از مشخصه‌های امنیتی*]
[۸] [اختصاص: *نقش‌های مجاز مشخص‌شده*]
[۹] [اختصاص: *خط‌مشی(های) کارکرد امنیتی کنترل دسترسی، خط‌مشی(های) کارکرد امنیتی کنترل جریان اطلاعات]*
[۱۰] *[انتخاب: تغییر-پیش‌فرض، پرس و جو، تغییر، حذف، [اختصاص:دیگر عملیات]]*
[۱۱] [اختصاص: *فهرستی از مشخصه‌های امنیتی*]
[۱۲] [اختصاص: *نقش‌های مجاز مشخص‌شده*]

مشخصات کارکردهای مدیریت امنیت محصولباید اطمینان یابد که تنها مقادیر امن برای مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا و داده ایجاد امضا عملیاتی[۱] پذیرفته شده‌اند. **نکته کاربردی ۱۳:** نویسنده هدف امنیتی باید تعریف کند که کدام یک از مقادیر مشخصه‌های امنیتی مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا برای هدف ارزیابی و چرخه حیات هدف ارزیابی مورد نظر امن هستند به‌عبارت‌دیگر اگر هدف ارزیابی از تولید زوج‌های داده ایجاد امضا / داده درستی‌سنجی امضا توسط صاحب‌امضا و کانال قابل‌اعتماد برای صدور داده درستی‌سنجی امضا به برنامه‌کاربردی تولید گواهی پشتیبانی کند، پس موجودیت فعال صاحب‌امضا ممکن است "بله" را به مشخصه امنیتی مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا اختصاص بدهد یا ممکن است این کار را انجام ندهد. اگر هدف ارزیابی از تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا در فاز آماده‌سازی در محیط امن پشتیبانی کند تنها محصولباید "بله" را به ویژگی امنیتی مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا مربوط به موجودیت فعال مدیر سیستم اختصاص داده و "خیر" را به این ویژگی مربوط به موجودیت فعال صاحب‌امضا اختصاص دهد.	
مقداردهی اولیه مشخصه ایستا ۱	**۴۰**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: مدیریت مشخصه‌های امنیتی[۲] نقش‌های امنیتی محصولباید خط‌مشی کارکرد امنیتی تولید داده ایجاد امضا / داده درستی‌سنجی امضا، خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا و خط‌مشی کارکرد امنیتی ایجاد امضا[۳] را به‌منظور ارائه مقادیر پیش‌فرض محدودکننده[۴] برای مشخصه‌های امنیتی اعمال کند که جهت اجرای خط‌مشی کارکرد امنیتی استفاده شده است.	
مقداردهی اولیه مشخصه ایستا ۲	**۴۱**
محصول باید به نقش مدیر سیستم[۵] اجازه دهد تا هنگامی‌که یک موجودیت غیرفعال یا اطلاعات ایجاد می‌شود مقادیر اولیه جایگزینی را برای ابطال مقادیر پیش‌فرض مشخص کند.	
ارث‌بری مقادیر مشخصه‌های امنیتی ۱	**۴۲**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: کنترل دسترسی زیرمجموعه یا	

[۱] [انتخاب: *فهرستی از مشخصه‌های امنیتی*]

[۲] FMT_MSA.1

[۳] [اختصاص: *خط‌مشی(های) کارکرد امنیتی کنترل دسترسی، خط‌مشی(های) کارکرد امنیتی کنترل جریان اطلاعات*]

[۴] [انتخاب: *انتخاب یکی از: محدود، مجاز، [اختصاص: دیگر ویژگی‌ها]*]

[۵] [اختصاص: *نقش‌های مجاز مشخص‌شده*]

کنترل جریان اطلاعات زیرمجموعه

محصولباید از قوانین زیر برای تنظیم مقادیر مشخصه‌های امنیتی استفاده کند:

۱) اگر موجودیت فعال مدیر سیستم زوج داده ایجاد امضا / داده درستی‌سنجی امضا را بدون احرازهویت موجودیت فعال صاحب‌امضا با موفقیت تولید کند، مشخصه امنیتی "داده ایجاد امضای عملیاتی" از داده ایجاد امضا باید به‌عنوان یک عملیات یکتا، "خیر" تنظیم گردد.

۲) اگر موجودیت فعال صاحب‌امضا زوج داده ایجاد امضا / داده درستی‌سنجی امضا را با موفقیت تولید کند، مشخصه امنیتی " داده ایجاد امضای عملیاتی" از داده ایجاد امضا باید به‌عنوان یک عملیات یکتا، "بله" تنظیم شود.[۱]

نکته کاربردی ۱۴: ممکن است هدف ارزیابی از تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا توسط صاحب‌امضا به تنهایی پشتیبانی نکند که در این مورد قانون (۲) مرتبط نیست.

۴۳	مدیریت داده‌های امنیتی / مدیر سیستم ۱

وراثت: از هیچ مؤلفه دیگر ندارد

وابستگی: مشخصات کارکردهای مدیریت امنیت

نقش‌های امنیتی

محصول باید امکان ایجاد[۲]داده احرازهویت مرجع[۳] را به نقش مدیر سیستم[۴] محدود کند.

۴۴	مدیریت داده امنیتی / صاحب‌امضا ۱

وراثت: از هیچ مؤلفه دیگر ندارد

وابستگی: مشخصات کارکردهای مدیریت امنیت

نقش‌های امنیتی

محصول باید امکلن تغییر [اختصاص: *سایر عملیات*][۵] داده احرازهویت مرجع[۶] را به نقش صاحب‌امضا[۷] محدود کند.

نکته کاربردی ۱۵: نویسنده هدف امنیتی باید عملیات ازدست‌رفته در الزام کارکردی امنیت مدیریت داده امنیتی ۱ را اجرا کند. اختصاص موارد ازدست‌رفته ممکن است "مسدود نشده" یا "هیچ" باشد.

---

[۱] [اختصاص: *قوانینی برای تنظیم مقادیر مشخصه‌های امنیتی*]

[۲] [انتخاب: *تغییر-پیش‌فرض، پرس و جو، تغییر، حذف، شفاف‌سازی[اختصاص:دیگر عملیات]*]

[۳] [اختصاص: *فهرستی از داده‌های امنیتی*]

[۴] [اختصاص: *نقش‌های مجاز مشخص‌شده*]

[۵] [انتخاب: *تغییر-پیش‌فرض، پرس و جو، تغییر، حذف، شفاف‌سازی[اختصاص: دیگر عملیات]*]

[۶] [اختصاص: *فهرستی از داده‌های امنیتی*]

[۷] [اختصاص: *نقش‌های مشخص مجاز*]

۶-۶- کلاس حفاظت از توابع هدف امنیتی

۴۵	حفظ حالت امن در صورت شکست ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد محصول باید زمانی که انواع شکست‌های زیر رخ می‌دهد، حالت امن را حفظ کند. (۱) خودآزمائی مطابق شکست‌های خودآزمائی توابع هدف امنیتی[۱] (۲) [اختصاص: *فهرستی از انواع شکست‌ها در توابع هدف امنیتی*][۲] **نکته کاربردی ۱۶**: نویسنده هدف امنیتی باید اختصاص‌های ازدست‌رفته در الزام کارکرد امنیتی حفظ حالت امن در صورت شکست اجرا کند. اختصاص (۱) شکست‌هایی را که توسط خودآزمائی شکست خورده تشخیص داده‌شده و نیاز به اقدامات مناسب برای جلوگیری از تخلف امنیتی را مورد رسیدگی قرار می‌دهد. زمانی که هدف ارزیابی در حالت امن قرار دارد، محصول نباید هیچگونه عملیات رمزنگاری را انجام دهد و تمام رابط‌های خروجی داده باید توسط محصول مهار شوند.	
۴۶	آشکارسازی انفعالی حمله فیزیکی ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد محصول باید آشکارسازی بدون ابهامی از دستکاری‌های فیزیکی ارائه دهد که ممکن است محصول را در معرض خطر قرار دهند.	
۴۷	آشکارسازی انفعالی حمله فیزیکی ۲
محصول باید قابلیتی را ارائه دهد که تعیین کند آیا دست‌کاری فیزیکی با افزاره‌های محصول یا اجزای محصول اتفاق افتاده است یا خیر.	
۴۸	مقاومت در مقابل حمله فیزیکی ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد محصول باید با پاسخگویی خودکار مانند الزامات کارکرد امنیتی‌ای که همیشه به کار گرفته می‌شوند مانع [اختصاص: *سناریوهای دست‌کاری فیزیکی*] در [اختصاص: *فهرستی از افزاره‌ها یا اجزای توابع هدف امنیتی*] شوند. **نکته کاربردی ۱۷:** هدف ارزیابی اقدامات مناسبی را به‌طور مداوم برای مقابله با دستکاری‌های فیزیکی اجرا خواهد کرد که ممکن است داده ایجاد امضا را در معرض خطر قرار دهد. "پاسخگویی خودکار" در الزام کارکرد امنیتی	

[۱] FPT TST

[۲] [اختصاص: *فهرستی از انواع شکست‌ها در توابع امنیتی محصول*]

مقاومت در مقابل حمله فیزیکی ۱ بدان معنی است که (۱) فرض شده است که ممکن است در هر زمانی یک حمله وجود داشته‌باشد و (۲) اقدامات مقابله‌ای در هر زمانی ارائه‌شده‌اند. به واسطه ماهیت این حملات، هدف ارزیابی می‌تواند بدون هیچ ابزاری حملات را در تمام اجزای خود تشخیص دهد (به عنوان مثال محصول خراب شده است). اما دستکاری‌های فیزیکی نباید اطلاعاتی از داده ایجاد امضا را فاش کند، به‌عنوان‌مثال هدف ارزیابی ممکن است در حالت خاموشِ به‌طور فیزیکی دست‌کاری شود (مانند کارت هوشمند) که به محصول اجازه نوشتن مجدد داده ایجاد امضا را نمی‌دهد اما منجر به تخریب فیزیکی حافظه و تمام اطلاعات موجود در آن درباره داده ایجاد امضا می‌شود. در صورت دست‌کاری فیزیکی، محصول ممکن است توابع در نظر گرفته شده برای تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا یا ایجاد امضا را ارائه ندهد اما با مسدود کردن این توابع از محرمانگی داده ایجاد امضا اطمینان حاصل کند. الزام کارکرد امنیتی آشکارسازی انفعالی حمله فیزیکی مستلزم آن است که محصول به دستکاری‌های فیزیکی به‌گونه‌ای واکنش نشان دهد که صاحب‌امضا بتواند تشخیص دهد که هدف ارزیابی به‌طور فیزیکی دست‌کاری شده است یا نه. به‌عنوان‌مثال، محصول ممکن است پیغام مناسبی را در هنگام راه‌اندازی نشان دهد یا مستندات راهنما یک شکست در هنگام راه‌اندازی هدف ارزیابی را به‌عنوان نشانه‌ای از دست‌کاری فیزیکی توصیف کنند.
۴۹ آزمون محصول ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد محصول باید مجموعه‌ای از خودآزمائی‌ها را اجرا کند [انتخاب: *در طول راه‌اندازی اولیه، به‌صورت دوره‌ای در حین عملیات عادی، به هنگام درخواست کاربر مجاز، تحت شرایطی [اختصاص: شرایطی که تحت آن خودآزمائی باید صورت گیرد]*] تا عملکرد صحیح توابع هدف امنیتی[۱] را نشان دهد.
۵۰ آزمون محصول ۲
محصول باید این قابلیت را برای کاربران مجاز فراهم آورند تا بتوانند یکپارچگی داده امنیتی[۲] را بررسی کنند.
۵۱ آزمون محصول ۳
محصول باید این قابلیت را برای کاربران مجاز فراهم آورند تا بتوانند یکپارچگی توابع هدف امنیتی[۳] را بررسی کنند. **نکته کاربردی ۱۸:** نویسنده هدف امنیتی باید عملیات موجود در الزام کارکرد امنیتی آزمون محصول ۱ را اجرا کند. الزام کارکرد امنیتی آزمون محصول تنها خودآزمائی محصول را مورد توجه قرار می‌دهد. اگر محصول متکی بر مشخصه‌های امنیتی بستره سخت‌افزاری قسمتی از هدف ارزیابی باشد، نویسنده هدف امنیتی باید الزام کارکرد

[۱] [انتخاب: *[اختصاص: قسمت‌هایی ازمحصول]، محصول*]

[۲] [انتخاب: *[اختصاص: قسمت‌هایی از داده‌های امنیتی]، داده‌های امنیتی*]

[۳] [انتخاب: *[اختصاص: قسمت‌هایی از محصول]، محصول*]

امنیتی آزمودن موجودیت‌های بیرونی[۱] را بگنجاند که به محصول برای آزمودن این ویژگی‌ها برای عملکرد صحیح محصول وابسته نیاز دارد.

خانواده برون‌تابی محصول

خانواده افزوده برون‌تابی محصول[۲] از کلاس حفاظت از محصول (FPT) در اینجا برای توصیف الزامات کارکرد امنیتی محصول اصلی تعریف شده است. محصول باید از داده ایجاد امضا و دیگر داده‌های محرمانه در مقابل حملاتی که برپایه پدیده‌های فیزیکی و قابل‌مشاهده بیرونی محصول رخ می‌دهند محافظت کند. برای نمونه از چنین حملاتی می‌توان به، ارزیابی تابش الکترومغناطیسی محصول، تحلیل ساده نیرو[۳] (SPA)، تحلیل تفاضلی نیرو[۴] حملات زمانبندی شده، برون‌تابی امواج رادیویی و غیره اشاره کرد. این خانواده الزامات کارکردی را برای محدود کردن برون‌تابی‌های معلوم ارائه می‌دهد. خانواده برون‌تابی محصول متعلق به کلاس حفاظت از محصول می‌باشد، که کلاسی برای حفاظت از محصول است. خانواده‌های دیگر موجود در کلاس حفاظت از محصول برون‌تابی محصول را پوشش نمی‌دهند.

- **رفتار خانواده برون‌تابی محصول:**

این خانواده الزامات لازم برای کاهش برون‌تابی‌های معلوم را تعریف می‌کند.

- **سطح‌بندی مؤلفه:**

برون‌تابی محصول دو جزء اصلی دارد:

۱. محدود کردن تابش امواج (FPT_EMS.1.1) مستلزم آن است که تابش امواج معلومی منتشر نشوند که دسترسی به داده‌های محصول یا داده‌های کاربر را میسر سازد.

محصول نباید [اختصاص: *انواع تابش امواج*] را بیش از [اختصاص: *محدود مشخص شده*] منتشر سازد که دسترسی به [اختصاص: *فهرستی از انواع داده‌ی امنیتی*] و [اختصاص: *فهرستی از انواع داده‌ی کاربر*] را ممکن می‌سازد.

۲. رابط برون‌تابی (FPT_EMS.1.2) مستلزم آن است که برون‌تابی‌ها رابطی را منتشر نکنند که دسترسی به داده‌های محصول یا داده‌های کاربر را میسر سازد.

محصول باید اطمینان حاصل کنند که [اختصاص: *انواع کاربران*] قادر به استفاده از رابط‌هایی که در ادامه آمده‌اند [اختصاص: *انواع اتصالات*] برای دسترسی به [اختصاص: *فهرستی از انواع داده امنیتی*] و [اختصاص: *فهرستی از داده‌های کاربر*] نیستند.

- **اقدامات مدیریتی برون‌تابی محصول**

[۱] FPT_TEE.1

[۲] FPT_EMS

[۳] Simple Power Analysis

[۴] Differential Power Analysis

هیچگونه فعالیت مدیریتی پیش‌بینی نشده‌است.

- **اقدامات ممیزی برون‌تابی محصول**

اگر در پروفایل حفاظتی یا هدف امنیتی استفاده‌کننده از الزام کارکرد امنیتی برون‌تابی محصول تولید داده ممیزی امنیتی[۱] گنجانده شود، اقدامی که قابل ممیزی باشد وجود ندارد.

[۱] FAU_GEN

۵۲	برون‌تابی محصول ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد هدف ارزیابی نباید [اختصاص: انواع *تابش‌های امواج*[۱]] را بیش از [اختصاص: *محدوده مشخص*] ساطع کند که توانایی دسترسی به داده احرازهویت مرجع[۲] و داده ایجاد امضا[۳] را میسر می‌کند.	
۵۳	برون‌تابی محصول ۲
محصول باید اطمینان حاصل کند [اختصاص: انواع کاربران] قادر به استفاده از رابط‌ها [اختصاص: انواع اتصالات] به‌منظور دسترسی به داده احرازهویت مرجع[۴] و داده ایجاد امضا[۵] نیستند. **نکته کاربردی ۱۹:** محصول باید از حملات علیه داده ایجاد امضا و دیگر داده‌های محرمانه که مبتنی بر پدیده‌ها و آثار فیزیکی قابل‌مشاهده بیرونی هدف ارزیابی می‌باشند، جلوگیری کند. چنین حملاتی ممکن است در رابط‌های هدف ارزیابی قابل مشاهده باشد یا ممکن است از عملیات درونی هدف ارزیابی نشأت بگیرد یا ممکن است از مهاجمی نشأت بگیرد که محیط فیزیکی که هدف ارزیابی در آن عمل می‌کند را تغییر می‌دهد. مجموعه آثار فیزیکی قابل اندازه‌گیری تحت تأثیر تکنولوژی به‌کار رفته در پیاده‌سازی هدف ارزیابی قرار دارد. مثال‌هایی از این آثار قابل‌اندازه‌گیری، تغییر در مصرف نیرو، زمان‌بندی انتقال حالات درونی، تشعشعات الکترومغناطیس ناشی از عملیات درونی، تابش امواج رادیویی می‌باشد. با توجه به اینکه ماهیت تکنولوژی‌هایی که ممکن است باعث چنین برون‌تابی‌هایی شوند ناهمگن است، ارزیابی در برابر حملات پیشرفته کاربردپذیر در تکنولوژی‌های به‌کارگرفته شده در هدف ارزیابی، فرض شده‌است. مثال‌هایی از این حملات می‌تواند شامل این موارد باشد البته محدود به این موارد نیستند: ارزیابی تشعشعات الکترومغناطیس هدف ارزیابی، تحلیل ساده نیرو[۶] (SPA)، تحلیل تفاضلی نیرو[۷] (DPA)، حملات زمان‌بندی شده و غیره.	

۷- الزامات تضمین امنیت هدف ارزیابی

جدول ۲ الزامات تضمین: سطح تضمین ارزیابی ۴ تکمیل‌شده با تحلیل آسیب‌پذیری روش‌مند هوشمند

[۱] emissions

[۲] [اختصاص: *فهرستی از انواع داده‌های امنیتی*]

[۳] [اختصاص: *فهرستی از انواع داده‌های کاربر*]

[۴] [اختصاص: *فهرستی از انواع داده‌های امنیتی*]

[۵] [اختصاص: *فهرستی از انواع داده‌های کاربر*]

[۶] Simple Power Analysis

[۷] Differential Power Analysis

نام کلاس	نام الزام	توضیحات
Development ADV	ADV_ARC.1	طراحی معماری با جداسازی دامنه‌ها و بدون قابلیت دور
	ADV_FSP.4	مشخصات کارکرد کامل
	ADV_IMP.1	پیاده‌سازی بازنمایی توابع هدف امنیتی
	ADV_TDS.3	طراحی پیمانه‌ای پایه
Guidance Documents AGD	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests ATE	ATE_COV.2	تحلیل پوشش‌دهی
	ATE_DPT.1	آزمون طراحی پایه
	ATE_FUN.1	آزمون کارکردی
	ATE_IND.2	آزمون مستقل- نمونه
Vulnerability Assessment AVA	AVA_VAN.5	تحلیل آسیب‌پذیری روش‌مند پیشرفته
Life cycle Support ALC	ALC_CMC.4	پشتیبانی تولید، روش‌های اجرایی پذیرش و
	ALC_CMS.4	پوشش پیکربندی محصول
	ALC_DEL.1	روش‌های اجرایی تحویل
	ALC_DVS.1	شناسایی اقدامات امنیتی
	ALC_LCD.1	مدل چرخه حیات تعریف‌شده توسعه‌دهنده
	ALC_TAT.1	ابزارهای توسعه‌ی خوب تعریف شده
Security Target evaluation ASE	ASE_CCL.1	ادعاهای انطباق
	ASE_ECD.1	تعریف مؤلفه‌های توسعه‌یافته
	ASE_INT.1	معرفی هدف امنیتی
	ASE_OBJ.2	اهداف امنیتی
	ASE_REQ.2	الزامات امنیتی مشتق شده
	ASE_SPD.1	تعریف مسئله امنیتی
	ASE_TSS.1	خلاصه مشخصه هدف ارزیابی

۸- منطق

۸-۱- توجیه الزامات امنیتی

۱-۱-۸- پوشش‌دهی الزامات امنیتی

جدول ۳ الزامات کارکردی جهت نگاشت اهداف امنیتی هدف ارزیابی

اهداف امنیتی محصول / الزامات کارکردی	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.1	×		×	×	×						
FCS_CKM.4	×				×						
FCS_COP.1	×					×					
FDP_ACC.1/SCD/SVD_Generation_SFP	×	×									
FDP_ACC.1/SVD_Transfer_SFP	×										
FDP_ACC.1/Signature_Creation-SFP	×						×				
FDP_AFC.1/SCD/SVD_Generation_SFP	×	×									
FDP_AFC.1/SVD_Transfer_SFP	×										
FDP_AFC.1/Signature_Creation_SFP	×						×				
FDP_RIP.1					×		×				
FDP_SDI.2/Persistent				×	×	×					
FDP_SDI.2/DTBS							×	×			
FIA_AFL.1							×				
FIA_UAU.1		×					×				
FIA_UID.1		×					×				
FMT_MOF.1	×						×				
FMT_MSA.1/Admin	×	×									
FMT_MSA.1/Signatory	×						×				
FMT_MSA.2	×	×					×				
FMT_MSA.3	×	×					×				
FMT_MSA.4	×	×					×				
FMT_MTD.1/Admin	×						×				
FMT_MTD.1/Signatory	×						×				
FMT_SMR.1	×						×				
FMT_SMF.1	×						×				

اهداف امنیتی محصول / الزامات کارکردی	OT.Lifecycle_Security	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FPT_EMSEC.1					×				×		
FPT_FLS.1					×						
FPT_PHP.1										×	
FPT_PHP.3					×						×
FPT_TST.1	×				×	×					

۲-۱-۸-کفایت الزامات امنیتی هدف ارزیابی

هدف امنیتی محصول	شرح
OT.Lifecycle_Security	این هدف توسط الزام کارکرد امنیتی تولید کلید رمزنگاری جهت تولید داده ایجاد امضا / داده درستی‌سنجی امضا، الزام کارکرد امنیتی عملیات رمزنگاری جهت کاربری داده ایجاد امضا و الزام کارکرد امنیتی تخریب کلید رمزنگاری جهت تخریب داده‌های ایجاد امضا ارائه شده است که از چرخه حیات امن رمزنگاری‌شده داده ایجاد امضا اطمینان حاصل می‌کند. تولید داده ایجاد امضا / داده درستی‌سنجی امضا توسط محصول مطابق با الزام کارکرد امنیتی کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا و الزام کارکرد امنیتی مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا کنترل می‌شود. انتقال داده درستی‌سنجی امضا برای تولید گواهی توسط محصول مطابق با الزام کارکرد امنیتی کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا و الزام کارکرد امنیتی مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا کنترل می‌شود. کاربری داده ایجاد امضا با الزامات کارکرد امنیتی کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی ایجاد امضا، مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی ایجاد امضا تضمین می‌شود که مطابق الزامات کارکرد امنیتی مدیریت رفتار توابع امنیتی، مدیریت مشخصه‌های امنیتی / مدیر سیستم، مدیریت مشخصه‌های امنیتی / صاحب‌امضا، مشخصه‌های امنیتی امن، مقداردهی اولیه مشخصه ایستا، ارث‌بری مقادیر مشخصه‌های امنیتی، مدیریت داده امنیتی / مدیر سیستم، مدیریت داده امنیتی / صاحب‌امضا، مشخصات کارکردهای مدیریت امنیت و نقش‌های امنیتی مبتنی بر مشخصه‌های امنیتی مدیریت محصول امن می‌باشد. کارکرد آزمون الزام کارکرد امنیتی آزمودن محصول تشخیص شکست در طول چرخه‌حیات را برعهده دارد.
OT.SCD/SVD_Gen	این هدف تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا که به احرازهویت مناسب کاربر نیاز دارد را مورد توجه قرار می‌دهد. محصول مشخص‌شده توسط الزامات کارکرد امنیتی زمانبندی شناسایی و زمانبندی احرازهویت، شناسائی کاربر

	و احرازهویت او را قبل از دسترسی به توابع مجاز فراهم می‌کند. الزام کارکرد امنیتی کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا و مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا، کنترل دسترسی را برای تولید داده ایجاد امضا / داده درستی‌سنجی امضا ارائه می‌دهد. مشخصه‌های امنیتی کاربر احرازهویت شده با الزامات کارکرد امنیتی مدیریت مشخصه‌های امنیتی / مدیر سیستم، مشخصه‌های امنیتی امن و مقداردهی اولیه مشخصه ایستا برای مقداردهی اولیه مشخصه‌های ایستا فراهم می‌شود. الزام کارکرد امنیتی ارث‌بری مقادیر مشخصه‌های امنیتی قوانینی را برای وراثت مشخصه امنیتی " داده ایجاد امضا عملیاتی" از داده‌های ایجاد امضا تعریف می‌کند. هدف امنیتی برای محصول - منحصربه‌فردبودن داده ایجاد امضا (OT.SCD_Unique) الزامات داده ایجاد امضا یکتای کاربردی را که با الگوریتم رمزنگاری مشخص‌شده در الزام کارکرد امنیتی تولید کلید رمزنگاری فراهم می‌شود به‌گونه‌ای پیاده‌سازی می‌کند که در پاراگراف ۱(a) پیوست ۳ آمده است.
OT.SCD_SVD_Corresp	این هدف این موضوع را مورد رسیدگی قرار می‌دهد که آیا داده درستی‌سنجی امضا با داده ایجاد امضای پیاده‌سازی‌شده توسط هدف ارزیابی مطابقت دارد یا خیر. این هدف به‌وسیله الگوریتم مشخص‌شده توسط الزام کارکرد امنیتی تولید کلید رمزنگاری برای تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا متناظر، تامین می‌شود. توابع امنیتی مشخص‌شده توسط الزام کارد امنیتی نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / ماندگاری تضمین می‌کند که کلیدها تغییر نکرده‌اند، بنابراین تناظر حفظ شده‌است. علاوه‌براین، شناسه داده‌های ایجاد امضا به محیط اجازه می‌دهد تا داده‌های ایجاد امضا را شناسایی کند و آن را به داده درستی‌سنجی امضا مناسب پیوند دهد. کارکردهای مدیریتی مشخص‌شده توسط الزامات کارکرد امنیتی، مشخصات کارکردهای مدیریت امنیت و ارث‌بری مقادیر مشخصه‌های امنیتی به نقش مدیر سیستم اجازه می‌دهد تا مقادیر پیش‌فرض مشخصه امنیتی شناسه داده‌های ایجاد امضا را تغییر دهد.
OT.SCD_Secrecy	این هدف با توابع امنیتی مشخص‌شده توسط الزامات کاکرد امنیتی زیر تامین می‌شود. الزام کارکرد امنیتی تولید کلید رمزنگاری این اطمینان را می‌دهد که از الگوریتم‌های رمزنگاری امن برای تولید داده ایجاد امضا / داده درستی‌سنجی امضا

	استفاده می‌شود. کیفیت رمزنگاری زوج داده ایجاد امضا / داده درستی‌سنجی امضا باید از افشای داده‌های ایجاد امضا توسط حملات رمزنگاری که از داده درستی‌سنجی امضا به عمومیت شناخته‌شده استفاده می‌کند، جلوگیری کند. توابع امنیتی مشخص شده توسط الزامات کارکرد امنیتی حفاظت از اطلاعات باقیمانده زیر مجموعه و تخریب کلید رمزنگاری تضمین می‌کنند که اطلاعات باقیمانده روی داده ایجاد امضا بعد از استفاده از داده ایجاد امضا برای ایجاد امضا از بین خواهند رفت و تخریب داده ایجاد امضا هیچ اطلاعات باقیمانده‌ای بر جای نخواهد گذاشت. تابع امنیتی مشخص شده توسط الزام کارکرد امنیتی نظارت بر یکپارچگی داده‌های ذخیره شده و اقدامی برای آن / ماندگاری تضمین می‌کند که هیچ داده حیاتی‌ای به گونه‌ای تغییر نیابد که بتواند کارایی توابع امنیتی را تغییر دهد و یا اطلاعات داده ایجاد امضا را فاش کند. الزام کارکرد امنیتی آزمودن محصول شرایط کار کردن محصول را می‌آزماید و الزام کارکرد امنیتی حفظ حالت امن در صورت شکست، حالت امن را زمانی که یکپارچگی نقص شده‌است تضمین می‌کند و بنابراین این اطمینان را می‌دهد که توابع امنیتی مشخص‌شده، عملیاتی هستند. نمونه‌ای که در آن شرایط خطای تهدیدآمیز با الزام کارکرد امنیتی حفظ حالت امن در صورت شکست پاسخ داده می‌شود، تزریق خطا برای تحلیل خطای تفاضلی[۱] (DFA) می‌باشد. الزامات کارکرد امنیتی برون‌تابی محصول ۱ و مقاومت در مقابل حمله فیزیکی به ویژگی‌های امنیتی بیشتری برای حصول اطمینان از محرمانگی داده ایجاد امضا نیاز دارد.
OT.Sig_Secure	این هدف که توسط الگوریتم رمزنگاری مشخص‌شده توسط الزام کارکردی عملیات رمزنگاری فراهم می‌شود و قدرت رمزنگاری الگوریتم‌های امضا را تضمین می‌کند. الزام کارکرد امنیتی نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / ماندگاری مربوط به یکپارچگی داده ایجاد امضای پیاده‌سازی توسط هدف ارزیابی می‌باشد و الزام کارکرد امنیتی آزمون محصول این اطمینان را می‌دهد که خودآزمائی برای تضمین ایجاد امضای صحیح صورت گرفته‌است.
OT.Sigy_SigF	این هدف با الزام کارکرد امنیتی‌ای برای شناسایی احرازهویت و کنترل دسترسی تامین شده‌است. الزامات کارکرد امنیتی زمانبندی احرازهویت و زمانبندی شناسایی تضمین می‌کنند

[۱] Differential Fault Analysis

	که هیچ تابع ایجاد امضایی نمی‌تواند قبل از اینکه صاحب‌امضا شناسایی و احرازهویت شود، فراخوانی گردد. توابع امنیتی توصیف شده توسط الزامات کارکرد امنیتی مدیریت داده امنیتی / مدیر سیستم و مدیریت داده امنیتی / صاحب‌امضا توابع احرازهویت را مدیریت می‌کنند. الزام کارکرد امنیتی ساماندهی شکست در احرازهویت در برابر تعدادی از حملات ازجمله استخراج رمزنگاری اطلاعات باقیمانده، حملات جستجوی فراگیر[۱] در مقابل احرازهویت محافظت می‌کند. تابع امنیتی توصیف شده توسط الزام کارکرد امنیتی نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / داده‌ای که باید امضا شود، یکپارچگی DTBS ذخیره‌شده را تضمین می‌کند و الزام کارکرد امنیتی حفاظت از اطلاعات باقیمانده زیرمجموعه مانع از سوءاستفاده از هرگونه منابع حاوی داده‌های ایجاد امضا بعد از تخصیص مجدد می‌شود (به‌عنوان‌مثال بعد از فرایند ایجاد امضا). توابع امنیتی مشخص‌شده توسط الزامات کارکرد امنیتی کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی ایجاد امضا و مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی ایجاد امضا، کنترل دسترسی را بر اساس مشخصه‌های امنیتی مدیریت شده طبق الزامات کارکرد امنیتی مدیریت داده امنیتی / صاحب‌امضا، مدیریت مشخصه‌های امنیتی / صاحب‌امضا، مشخصه‌های امنیتی امن، مقداردهی اولیه مشخصه ایستا و ارث‌بری مقادیر مشخصه‌های امنیتی ارائه می‌دهد. الزامات کارکرد امنیتی، مشخصات کارکردهای مدیریت امنیت و نقش‌های امنیتی این کارکردها و نقش‌های مدیریتی را فهرست می‌کنند. این الزامات این اطمینان را حاصل می‌کند که فرایند امضا به صاحب‌امضا محدود شود. الزام کارکرد امنیتی مدیریت رفتار توابع امنیتی توانایی فعال‌سازی تابع ایجاد امضا را به صاحب‌امضا محدود می‌کند. الزام کارکرد امنیتی مدیریت مشخصه‌های امنیتی / صاحب‌امضا توانایی تغییر مشخصه‌های امنیتی عملیات داده‌های ایجاد امضا را به صاحب‌امضا محدود می‌کند.
OT.DTBS_Integrity_TOE	این هدف تضمین می‌کند که داده‌هایی که باید امضا شوند یا بازنمایی منحصربه‌فرد متعلق به آن‌ها توسط هدف ارزیابی تغییر نمی‌کند. توابع یکپارچگی مشخص‌شده توسط الزام کارکرد امنیتی نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / داده‌ای که باید امضا شود مستلزم آن است که داده‌هایی که باید امضا شوند یا بازنمایی منحصربه‌فرد متعلق به آن‌ها توسط هدف ارزیابی تغییر داده نشود.

[۱] Brute force

OT.EMSEC_Design	این هدف این موضوع را پوشش می‌دهد که هیچ‌گونه اطلاعات قابل‌فهمی به بیرون ساتع نشود. این هدف با الزام کارکرد امنیتی برون‌تابی هدف ارزیابی ۱ تامین می‌شود.
OT.Tamper_ID	این هدف با الزام کارکرد امنیتی آشکارسازی انفعالی حمله فیزیکی از طریق آشکارسازی انفعالی حملات فیزیکی، تامین می‌شود.
OT.Tamper_Resistance	این هدف با الزام کارکرد امنیتی مقاومت در مقابل حمله فیزیکی برای مقابله با حملات فیزیکی تامین می‌شود.

۲-۸- برآوردن وابستگی‌های الزامات امنیتی

جدول زیر مروری بر چگونگی رفع وابستگی‌های الزامات کارکرد امنیتی و توجیه اینکه چرا برخی از وابستگی‌ها، مطلوب نیستند، دارد.

جدول ۴ وابستگی‌های الزامات کارکردی

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM_EXT.4
FCS_CKM_EXT.4	[FDP_ITC.1 or FDP_ITC.2 or	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM_EXT.4
FDP_ACC.1/SCD/SVD_Generation_SFP	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation_SFP
FDP_ACC.1/Signature_Creation_SFP	FDP_ACF.1	FDP_ACF.1/Signature_Creation_SFP
FDP_ACC.1/SVD_Transfer_SFP	FDP_ACF.1	FDP_ACF.1/SVD_Transfer_SFP
FDP_ACF.1/SCD/SVD_Generation_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation_SFP FMT_MSA.3
FDP_ACF.1/Signature_Creation_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation_SFP, FMT_MSA.3
FDP_ACF.1/SVD_Transfer_SFP	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer_SFP, FMT_MSA.3

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
FDR_RIP.1	بدون وابستگی	n/a
FDP_SDI.2/Persistent	بدون وابستگی	n/a
FDP_SDI.2/DTBS	بدون وابستگی	n/a
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	بدون وابستگی	n/a
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD/SVD_Generation_SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature_Creation_SFP, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1/SCD/SVD_Generation_SFP, FDP_ACC.1/Signature_Creation_SFP, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1
FMT_MSA.4	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1/SCD/SVD_Generation_SFP, FDP_ACC.1/ Signature_Creation_SFP
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	بدون وابستگی	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_EMS.1	بدون وابستگی	n/a
FPT_FLS.1	بدون وابستگی	n/a
FPT_PHP.1	بدون وابستگی	n/a

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
FPT_PHP.3	بدون وابستگی	n/a
FPT_TST.1	بدون وابستگی	n/a

۳-۸- منطق برای سطح تضمین ارزیابی ۴ تکمیل‌شده

سطح تضمین برای این پروفایل حفاظتی سطح تضمین ارزیابی ۴ تکمیل‌شده می‌باشد. سطح تضمین ارزیابی ۴ به توسعه‌دهنده اجازه دستیابی به سطح بسیار قابل قبولی از تضمین را می‌دهد بدون آنکه نیاز به فرایندها و اقدامات بسیار تخصصی باشد. این را می‌توان به عنوان بالاترین سطح قابل کاربرد برای یک خط تولید موجود بدون هزینه و پیچیدگی اضافی در نظر گرفت. به این ترتیب، سطح تضمین ارزیابی ۴ برای محصولات تجاری‌ای مناسب است که برای تعدیل کارکردهای امنیتی بالا قابل اجراء باشند. محصول توصیف شده در این پروفایل حفاظتی دقیقاً چنین محصولی است. تکمیل شدن نتیجه انتخابِ مورد زیر است:

"تحلیل آسیب‌پذیری روشمند پیشرفته (AVA_VAN.5)"

محصول برای کارکرد در سامانه‌های متنوع ایجاد امضا برای امضاهای الکترونیک (واجد شرایط) در نظر گرفته شده است. به واسطه ماهیت کاربرد در نظر گرفته‌شده برای آن، به عنوان مثال ممکن است محصول برای کاربران انتشار یابد و ممکن است مستقیماً تحت کنترل مدیران سیستم آموزش دیده و تخصصی نباشد. در نتیجه، ضروری است راهنمایی‌های گمراه کننده، غیر منطقی و متضاد در مدارک راهنما وجود نداشته باشد، و روش‌های اجرایی امن برای همه مدهای عملیاتی مورد توجه قرار بگیرد. حالات ناامن باید به آسانی قابل تشخیص باشند.

باید نشان داده شود که محصول در برابر حملات نفوذی بسیار مقاوم است تا اهداف امنیتی برای محصول رازمانی داده ایجاد امضا، تابع ایجاد امضا تنها برای صاحب‌امضای قانونی و امنیت رمزنگاری امضای دیجیتال را برآورده سازد.

عنصر تحلیل آسیب‌پذیری روشمند هوشمند وابستگی‌های زیر را دارد:

ADV_ARC.1 طراحی معماری با جداسازی دامنه‌ها و بدون قابلیت دور زدن

ADV_FSP.4 مشخصات کارکردی کامل

ADV_IMP.1 پیاده‌سازی بازنمایی توابع هدف امنیتی

ADV_TDS.3 طراحی پیمانه‌ای پایه

AGD_OPE.1 راهنمای کاربر عملیاتی

AGD_PRE.1 روش‌های اجرایی آماده‌سازی

ATE_DPT.1 آزمون: طراحی پایه

تمام این وابستگی‌ها در بسته تضمین سطح تضمین ارزیابی ۴ وجود دارد یا اضافه شده است.

پیوست ۱ نمادها و اختصارات آن‌ها

نماد	معادل انگلیسی	معادل فارسی
CC	Common Criteria	معیار مشترک
CGA	Certification generation application	برنامه کاربردی تولید گواهی
CSP	Certification Service Provider	تامین‌کننده خدمات صدور گواهی
DTBS	Data to be signed	داده‌ای که باید امضا شوند
DTBS/R	Data to be signed or its unique representation	داده‌ای که باید امضا شوند یا بازنمایی منحصربه‌فرد متعلق به آن
EAL	Evaluation Assurance Level	سطح تضمین ارزیابی
HID	Human Interface Device	افزاره رابط انسانی (کاربری)
IT	Information Technology	فناوری اطلاعات
OE	Operational Environment	محیط عملیاتی
OSP	Organizational Security Policy	خط‌مشی امنیتی سازمانی
RAD	Reference Authentication data	داده احرازهویت مرجع
PP	Protection Profile	پروفایل حفاظتی
RAD	Reference authentication data	داده‌های احراز اصالت مرجع
SAR	Security Assurance Requirement	الزام تضمین امنیتی
SCA	Signature creation application	برنامه کاربردی ایجاد امضا
SCD	Signature creation data	داده ایجاد امضا
SCS	Signature creation system	سامانه ایجاد امضا
SDO	Signed data object	موجودیت غیرفعال داده امضاشده
SFP	Security Function Policy	خط‌مشی کارکرد امنیتی
SFR	Security Functional Requirement	الزام کارکرد امنیتی
SSCD	Secure signature creation device	افزاره ایجاد امضای امن
ST	Security Target	هدف امنیتی
SVD	Signature verification data	داده درستی‌سنجی امضا
TOE	Target of Evaluation	محصول
TSF	TOE Security Functionality	توابع هدف امنیتی
TSS	TOE Summary Specification	خلاصه مشخصه محصول
VAD	Verification authentication data	داده درستی‌سنجی احرازهویت

منابع و مراجع

[1] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, CCMB-2009-07-001, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 3, CCMB-2009-07-002, July 2009

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 3, CCMB-2009-07-003, July 2009

[5] Protection Profile Secure Signature-Creation Device Type 3, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0006-2002T, also short SSVG-PPs or CWA14169

[6] ETSI Technical Specification 101 733: CMS Advanced Electronic Signatures (CAdES), V.1.7.4, 2008-07

[7] ETSI Technical Specification 101903: XML Advanced Electronic Signatures (XAdES), V.1.3.2, 2006-03