به نام خدا

پروفایل حفاظتی افزاره ایجاد امضای امن

قسمت ۴: الحاقی برای افزاره با تولید کلید و کانال قابل‌اعتماد با برنامه‌کاربردی تولید گواهی

اریبهشت ۹۵

نسخه ۱,۰

فهرست

۱- مقدمه

این سند که در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک توسط مرکز مدیریت راهبردی افتا و سازمان فناوری اطلاعات ایران تهیه و نهایی شده است، برای بیان الزامات کارکرد امنیتی هر محصول لازم است. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی را که در این سند برای برآورده کردن الزامات ارائه شده‌اند، در محصول 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 به‌صورت داخلی تولید کرده و کلید عمومی را به روش حفاظت‌شده‌ای صادر کند، تبیین می‌شود: "افزاره ایجاد امضای امن با تولید کلید و ارتباط قابل‌اعتماد با برنامه‌کاربردی تولید گواهی[۲] (SSCD KG TCCGA)".

این پروفایل حفاظتی در مورد افزاره ایجاد امضای امن با تولید کلید و ارتباط قابل‌اعتماد با برنامه‌کاربردی تولید گواهی است و الزامات امنیتی را برای افزاره ایجاد امضای امنی تعریف می‌کند که داده ایجاد امضا،[۳] (SCD) را تولید کرده و امضاهای الکترونیک پیشرفته ایجاد می‌کند. همان‌گونه که در افزاره ایجاد امضای امن برای تولید کلید[۴] اصلی شرح داده شده است اگر این امر مبتنی بر گواهی‌های واجد شرایط معتبر باشد امضاهای الکترونیکی تولیدشده نیز واجد شرایط خواهند بود [۷]. محصول این پروفایل حفاظتی همچنین از احراز هویت آن به‌عنوان افزاره ایجاد امضای امن پشتیبانی می‌کند، این کار با استفاده از برنامه‌کاربردی تولید گواهی (CGA) ارائه‌دهنده خدمات صدور گواهی[۵] (CSP) و ارتباط قابل‌اعتماد با این برنامه‌کاربردی تولید گواهی (CGA) برای حفاظت از داده درستی‌سنجی

---

[۱] Secure Signature Creation Device (SSCD)

[۲] Certificate Generation Application (CGA)

[۳] Signature Creation Data

[۴] PP SSCD KG

[۵] Certification Service Provider (CSP)

امضای[۶] (SVD) تولید و صادرشده توسط محصول و واردشده توسط برنامه‌کاربردی تولید گواهی (CGA) صورت می‌پذیرد. این ویژگی‌های امنیتی، چرخه حیات تغییریافته محصول را امکان‌پذیر می‌سازد. این پروفایل حفاظتی با افزاره ایجاد امضای امن اصلی مطابقت دارد [۷].

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[۷] توضیح داده‌شده است را نیز تعیین می‌کند.

سطح اطمینان این پروفایل حفاظتی، سطح تضمین ارزیابی ۴[۸] (EAL4) تکمیل‌شده با تحلیل آسیب‌پذیری روشمند هوشمند می‌باشد.

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:

---

[۶] Signature Verification Data (SVD)

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

[۸] Evaluation Assurance Level

- **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).

- **پیوست**

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

۲-۲- اصطلاحات ارزیابی امنیت

- **استاندارد ارزیابی معیار مشترک[۹] (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[۱۰] (EAL)**

[۹] Common Criteria

[۱۰] Evaluation Assurance Level

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[۱۱] (PP)**

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[۱۲] (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[۱۳] (TOE)**

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

- **توابع امنیتی هدف ارزیابی[۱۴] (TSF)**

---

[۱۱] Protection Profile

[۱۲] Security Target

[۱۳] Target of Evaluation

[۱۴] TOE Security Functions

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

۲-۳- اصطلاحات فنی

- **مدیر سیستم**[۱۵]

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

- **امضای الکترونیکی پیشرفته**[۱۶]

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**[۱۷]

---

[۱۵] Administrator

[۱۶] Advanced electronic signature

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

- **گواهی**[۱۸]

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**[۱۹]

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:

---

[۱۷] Authentication data

[۱۸] Certificate

[۱۹] Certificate information

- گواهی کلید عمومی امضاکننده یا
- یک یا چند مقدار چکیده‌ساز[۲۰] 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)**[۲۱]

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**[۲۲] **(CSP)**

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

- **داده‌ای که باید امضا شوند**[۲۳] **(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**[۲۴] **(DTBS/R)**

---

[۲۰] hash

[۲۱] Certificate generation application

[۲۲] Certification Service Provider

[۲۳] Data to be signed

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[۲۵] 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).

- **کاربر مجاز**[۲۶]

---

[۲۴] Data to be signed or its unique representation

[۲۵] intermediate

[۲۶] Legitimate user

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**[۲۷]

نهاد سازمانی که توسط یک کشور عضو اتحادیه اروپا به‌عنوان مسئول اعطای مجوز رسمی۲۸ 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**[۲۹] **(RAD)**

---

[۲۷] Notified body

[۲۸] accreditation

[۲۹] Reference Authentication data

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[۳۰] (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[۳۱]**

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[۳۲]**

اطلاعات افزوده‌ای که همراه با پیام کاربر امضا می‌شود.

- **برنامه‌کاربردی ایجاد امضا[۳۳] (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:

---

30 Secure signature creation device

31 Signatory

۳۲ Signature attributes

33 Signature creation application

- 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.
- 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[۳۴] (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[۳۵] (SCS)**

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

- **داده درستی‌سنجی امضا[۳۶] (SVD)**

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

---

[34] Signature creation data
[35] Signature Creation System
[36] Signature verification data

- **خدمات تدارک افزاره ایجاد امضای امن**[۳۷]

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).

- **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**[۳۸] **(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

[37] SSCD provisioning service
[38] Verification authentication data

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 طول چرخه حیاتش که با ورود جهت استفاده در یک فرایند ایجاد داده تنها توسط صاحب‌امضا آغاز می‌شود محافظت می‌کند.

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 کارکردهای زیر را ارائه می‌دهد:

۱) تولید داده ایجاد امضا (SCD) و به صورت اختیاری، داده درستی‌سنجی امضا (SVD) متناظر[۳۹]،

۲) صدور داده درستی‌سنجی امضا (SVD) به برنامه‌کاربردی تولید گواهی (CGA) برای صدور گواهی از طریق یک کانال قابل‌اعتماد،

۳) اثبات هویت به‌عنوان افزاره ایجاد امضای امن برای موجودیت‌های بیرونی،

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

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

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

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

ب. احراز هویت صاحب‌امضا و تعیین نیت او از امضا،

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

د. 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).

[۳۹] correspondent

محصول ممکن است کارکردهای خود را برای ایجاد امضای الکترونیک منطبق با مشخصه‌های موجود در ETSI TS 101 733 (CAdES)، ETSI TS 101 903 (XAdES) و ETSI TS 101 903 (PAdES) پیاده‌سازی کند.

محصول برای استفاده صاحب‌امضا به شکل زیر آماده شده است:

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

۲) شخصی‌سازی برای صاحب‌امضا با ذخیره در محصول:

أ. داده احراز هویت مرجع[۴۰] (RAD) صاحب‌امضا

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

بعد از آماده‌سازی، داده ایجاد امضا (SCD) باید در یک حالت غیر عملیاتی 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[۴۱] باشد انتظار می‌رود ابزارهای ارائه این اطلاعات از محرمانگی و یکپارچگی داده احراز هویت مرجع (RAD) متناظر محافظت کنند.

اگر دیگر لزومی به استفاده از یک داده ایجاد امضا (SCD) وجود ندارد، بایستی آن داده ایجاد امضا (SCD) و همچنین اطلاعات گواهی مرتبط، در صورت وجود از بین بروند (به طور مثال با پاک کردن آن از حافظه).

۳-۲- عملکرد محصول

[۴۰] Reference Authentication Data (RAD)

[۴۱] PIN

این بخش مرور کلی در مورد کارکرد محصول در محیط‌های عملیاتی مجزا را ارائه می‌دهد:

۳-۲-۱-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 برنامه‌کاربردی تولید گواهی (CGA) با تامین‌کننده خدمات صدور گواهی تعامل می‌کند. محصول، داده درستی‌سنجی امضا (SVD) را از طریق یک کانال قابل‌اعتماد صادر می‌کند که به برنامه‌کاربردی تولید گواهی (CGA) اجازه بررسی اصالت‌سنجی داده درستی‌سنجی امضا (SVD) را می‌دهد. محیط مقداردهی اولیه بیشتر برای شخصی‌سازی محصول با مقادیر اولیه داده احراز هویت مرجع (RAD) با محصول تعامل می‌کند.

۳-۲-۲- محیط امضا

جایی که محصول با امضا کننده برای امضای داده با برنامه‌کاربردی ایجاد امضا[۴۲] (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 نتایج امضای الکترونیک[۴۳] حاصل را به دست می‌آورد.

۳-۲-۳- محیط‌های مدیریتی

[۴۲] Signature Creation Application (SCA)

[۴۳] در یک سطح کارکردی ناب، افزاره ایجاد امضای امن امضای الکترونیک ایجاد می‌کند؛ برای پیاده‌سازی افزاره ایجاد امضای امن برای برآوردن الزامات این نمایه حفاظتی و با کلید گواهی تولید شده همانگونه که در، پیوست ۱ دستورالعمل مشخص شده است نتایج فرایند امضا می‌تواند برای ایجاد یک امضای الکترونیک واجد شرایط مورد استفاده قرار گیرد.

جایی است که محصول با کاربر و یا تأمین کننده خدمات تدارک افزاره ایجاد امضای امن برای انجام عملیات مدیریتی تعامل دارد به طور مثال، برای تنظیم مجدد یک داده احراز هویت 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 به فراهم آورد.

محیط امضا، محیط مدیریتی و محیط آماده‌سازی هر سه امن هستند و از داده‌های تبادل شده توسط محصول حفاظت می‌کنند. شکل ۴ در قسمت ۱ این استاندارد محیط عملیاتی را نشان می‌دهد [۶].

محصول، داده ایجاد امضا (SCD) و داده احراز هویت 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.

محصول، داده ایجاد امضا و داده احراز هویت مرجع را ذخیره می‌کند. محصول ممکن است چندین نمونه از داده ایجاد امضا را ذخیره کند. در این حالت محصول تابعی برای شناسایی هر داده ایجاد امضا فراهم می‌کند و برنامه‌کاربردی ایجاد امضا[۴۴] (SCA) می‌تواند رابطی برای امضا کننده فراهم آورد تا یک داده ایجاد امضا را برای استفاده در تابع ایجاد امضای افزاره ایجاد امضای امن بکار گیرد. محصول از محرمانگی و یکپارچگی داده ایجاد امضا محافظت کرده و استفاده از آن را محدود به ایجاد امضا توسط صاحب‌امضای می‌کند. بر طبق آنچه در دستورالعمل تعریف شده است، امضای الکترونیکی ایجادشده توسط محصول یک امضای

[۴۴] Signature Creation Application (SCA)

الکترونیکی معتبر خواهد بود اگر گواهی داده درستی‌سنجی امضا یک گواهی واجد شرایط و معتبر باشد. تعیین حالت واجد شرایط بودن گواهی فراتر از هدف و دامنه کاربرد این استاندارد است.

فرض می‌شود که برنامه‌کاربردی ایجاد امضا 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 احراز هویت مرجع (RAD) صاحب‌امضا را برای احراز اصالت یک کاربر به عنوان صاحب‌امضا ذخیره می‌کند. داده احراز هویت مرجع (RAD) یک کلمه‌عبور (به طور مثال پین[۴۵])، یک الگوی زیست‌سنجی و یا ترکیبی از این‌ها است. محصول از محرمانگی و یکپارچگی داده احراز هویت مرجع (RAD) محافظت می‌کند. محصول ممکن است رابط کاربری برای دریافت مستقیم داده درستی‌سنجی احراز هویت (VAD) از کاربر فراهم کند، یا اینکه داده درستی‌سنجی احراز هویت (VAD) را از برنامه‌کاربردی ایجاد امضا (SCA) دریافت کند. چنانچه برنامه‌کاربردی ایجاد امضا به کار رود، که یک داده درستی‌سنجی احراز هویت (VAD) را از کاربر دریافت و یا درخواست می‌کند، فرض بر آنست که محرمانگی و یکپارچگی این داده حفظ می‌شود.

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 احراز هویت مرجع (RAD)،
- تولید یک زوج کلید،

[45] PIN

- ذخیره‌سازی اطلاعات شخصی کاربر قانونی.

محصول و برنامه‌کاربردی تولید گواهی (CGA) به منظور محافظت از یکپارچگی و اصالت‌سنجی داده درستی‌سنجی امضا (SVD) صادر شده از محصول از طریق یک کانال قابل‌اعتماد ارتباط برقرار می‌کنند.

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 برنامه‌کاربردی ایجاد امضای در حال اجرا بر روی کامپیوتر شخصیِ متصل به پایانه کارت به دست آورد. برنامه‌کاربردی ایجاد امضا، بعد از ارائه سند به کاربر و پس از کسب پین اعطای مجوز، تابع ایجاد امضای الکترونیک کارت هوشمند را از طریق پایانه آغاز می‌کند.

۳-۳- چرخه حیات محصول

چرخه حیات محصول همان چیزی است که در بخش ۴,۳,۳ سند پروفایل حفاظتی افزاره ایجاد امضای امن – تولید کلید[۴۶] تعریف شده است [۷]، به‌استثنای موارد زیر:

- در مرحله آماده‌سازی از فاز کاربری، تأمین کننده خدمات تدارک افزاره ایجاد امضای امن (SSCD)، توابع امنیتی را در محصول مقداردهی می‌کند تا شناسایی به‌عنوان افزاره ایجاد امضای امن (SSCD)، اثبات هویت افزاره ایجاد امضای امن (SSCD) برای موجودیت‌های بیرونی، و صدور حفاظت‌شده داده درستی‌سنجی امضا (SVD) امکان‌پذیر باشد.
- در مرحله آماده‌سازی فاز کاربری، تأمین کننده خدمات تدارک افزاره ایجاد امضای امن (SSCD)، هویت محصول به‌عنوان افزاره ایجاد امضای امن (SSCD) و هویت کاربر قانونی به‌عنوان متقاضی بالقوه برای گواهی‌های داده درستی‌سنجی امضا (SVD) تولیدشده توسط محصول را به هم پیوند می‌دهد.

---

[۴۶] PP SSCD KG

- در فاز کاربری، تولید SCD/SVD توسط محصول و صدور داده درستی‌سنجی امضا (SVD) از محصول ممکن است در مرحله آماده‌سازی و یا در مرحله استفاده عملیاتی رخ دهد، سپس محصول کانال قابل‌اعتمادی برای برنامه‌کاربردی تولید گواهی (CGA) فراهم می‌آورد که از یکپارچگی داده درستی‌سنجی امضا (SVD) محافظت می‌کند.
- در فاز کاربری، قبل از تولید گواهی که شامل داده درستی‌سنجی امضا (SVD) صادره از محصول می‌باشد، برنامه‌کاربردی تولید گواهی (CGA) همچنین این موارد را تعیین می‌کند: (۱) هویت محصول به‌عنوان افزاره ایجاد امضای امن (SSCD)، (۲) افزاره ایجاد امضای امن (SSCD) مبدأ که برای متقاضی گواهی به‌عنوان کاربر قانونی شخصی‌سازی شده است، و (۳) مطابقت بین داده ایجاد امضا (SCD) ذخیره‌شده در افزاره ایجاد امضای امن (SSCD) و داده درستی‌سنجی امضا (SVD) دریافت شده.

۴- مسائل امنیتی

۴-۱- دارایی‌ها، کاربران و عوامل تهدید

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. دارایی‌های این پروفایل حفاظتی همان‌هایی هستند که در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید[۴۷] تعریف شده است [۷].

۴-۱-۱- دارایی‌ها و موجودیت‌های غیرفعال

[۴۷] PP SSCD KG

۱.داده ایجاد امضا (SCD): کلید خصوصی 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 الکترونیک 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 غیرقابل‌جعل بودن پیوند با صاحب‌امضا که توسط امضای الکترونیکی ارائه شده است، بایستی حفظ شود.

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

۱.کاربر: کاربر نهاییِ محصول که می‌تواند به عنوان مدیر سیستم یا صاحب‌امضا شناخته شود. موجودیت فعال کاربر[۴۸] ممکن است به عنوان موجودیت فعال مدیر سیستم[۴۹] در نقش مدیر سیستم[۵۰] و یا به عنوان موجودیت فعال صاحب‌امضا[۵۱] در نقش صاحب‌امضا[۵۲] ایفای نقش کند.

۲.مدیر سیستم: کاربری است که مسئول انجام مقداردهی اولیه محصول، شخصی‌سازی محصول و یا دیگر کارکردهای اجرایی محصول می‌باشد. موجودیت فعال مدیر سیستم برای این کاربر بعد از احراز هویتِ 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 احراز هویت موفقیت‌آمیز به عنوان صاحب‌امضا نقش صاحب‌امضا را ایفا می‌کند.

---

[۴۸] S.User

[۴۹] S.Admin

[۵۰] R.Admin

[۵۱] S.Sigy

[۵۲] R.Sigy

۴-۱-۳-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

این پروفایل حفاظتی همه تهدیدات پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید را دارا می‌باشد[۷]:

تهدید ذخیره‌سازی، نسخه‌برداری و انتشار داده ایجاد امضا (T.SCD_Divulg)، تهدید استخراج داده ایجاد امضا (T.SCD_Derive)، تهدید حملات فیزیکی از طریق رابط‌های محصول (T.Hack_phys)، تهدید جعل داده درستی‌سنجی امضا (T.SVD_Forgery)، تهدید سوءاستفاده از تابع ایجاد امضای محصول (T.SigF_Misuse)، تهدید جعل داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) (T.DTBS_Forgery)، تهدید جعل امضای دیجیتالی (T.Sig_Forgery).

این پروفایل حفاظتی تهدیدات اضافه دیگری را تعریف نکرده است.

۴-۳-خط‌مشی‌های امنیت سازمانی

این پروفایل حفاظتی شامل همه خط‌مشی‌های امنیت سازمانی موجود در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید می‌باشد[۷]:

خط‌مشی گواهی واجد شرایط (P.CSP_QCert)، خط‌مشی امضای الکترونیک واجد شرایط (P.QSign)، خط‌مشی محصول به عنوان افزاره ایجاد امضای امن (P.Sigy_SSCD)، خط‌مشی انکارناپذیری امضا (P.Sig_Non-Repud).

این پروفایل حفاظتی خط‌مشی امنیت سازمانی بیشتری تعریف نمی‌کند.

۴-۴- مفروضات

این پروفایل حفاظتی شامل همه مفروضات موجود در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید می‌باشد[۷]:

فرض برنامه‌کاربردی تولید گواهی قابل‌اعتماد (A.CGA)، فرض برنامه‌کاربردی ایجاد امضای قابل‌اعتماد (A.SCA).

این پروفایل حفاظتی مفروضات بیشتری درباره محیط عملیاتی تعریف نمی‌کند.

۵- اهداف امنیتی

۵-۱- کلیات

این بخش اهداف امنیتی هدف ارزیابی 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

۵-۲-۱-ارتباط با پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید

این پروفایل حفاظتی همه اهداف امنیتی تعریف شده برای محصول در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید را در بر می‌گیرد، این اهداف امنیتی شامل موارد زیر می‌باشند [۷]:

هدف امنیتی امنیت چرخه‌حیات (OT.Lifecycle_Security)، هدف امنیتی تولید داده ایجاد امضا / داده درستی‌سنجی امضا (OT.SCD/SVD_Gen)، هدف امنیتی یکتایی داده ایجاد امضا (OT.SCD_unique)، هدف امنیتی تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا (OT.SCD_SVD_Corresp)، هدف امنیتی رازمانی داده ایجاد امضا (OT.SCD_Secrecy)، هدف امنیتی امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure)، هدف امنیتی تابع ایجاد امضا تنها برای صاحب‌امضای قانونی (OT.Sigy_SigF)، هدف امنیتی یکپارچگی داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) درون محصول (OT.DTBS_Integrity_TOE)، هدف امنیتی فراهم آوردن امنیت برون‌تابی‌های فیزیکی (OT.EMSEC_Design)، هدف امنیتی آشکارسازی دست‌کاری (OT.Tamper_ID)، هدف امنیتی مقاومت در برابر دست‌کاری (OT.Tamper_Resistance).

این پروفایل حفاظتی اهداف امنیتی افزوده زیر را برای محصول توصیف می‌کند:

تهدیدات	توضیحات
OT.TOE_SSCD_Auth اثبات احرازهویت به‌عنوان افزاره ایجاد امضای امن	محصول باید داده‌های منحصربه‌فرد هویت و احراز هویت به‌عنوان افزاره ایجاد امضای امن (SSCD) را حفظ کند و سازوکارهای امنیتی‌ای برای شناسایی و احراز هویت خود به‌عنوان افزاره ایجاد امضای امن (SSCD) فراهم آورد.
OT.TOE_TC_SVD_Exp کانال قابل‌اعتماد محصول برای صدور داده درستی‌سنجی امضا	محصول باید کانال قابل‌اعتمادی برای برنامه‌کاربردی تولید گواهی (CGA) فراهم آورد تا از یکپارچگی داده درستی‌سنجی امضا (SVD) صادرشده برای برنامه‌کاربردی تولید گواهی (CGA) محافظت کند. محصول باید برنامه‌کاربردی تولید گواهی (CGA) را قادر به تشخیص تغییر داده درستی‌سنجی امضا (SVD) صادرشده توسط محصول کند.

۵-۳- اهداف امنیتی برای محیط عملیاتی

۵-۳-۱-ارتباط با پروفایل حفاظتی افزاره ایجاد امضای امن – تولید کلید

این پروفایل حفاظتی همه اهداف امنیتی تعریف شده برای محصول در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید را در بر می‌گیرد، این اهداف امنیتی شامل موارد زیر می‌باشند [۷]:

هدف امنیتی اصالت‌سنجی داده درستی‌سنجی امضا (OE.SVD_Auth)، هدف امنیتی تولید گواهی‌های واجد شرایط (OE.CGA_Qcert)، هدف امنیتی محافظت از داده درستی‌سنجی احرازهویت (OE.HID_VAD)، هدف امنیتی ارسال داده‌های درنظر گرفته شده برای امضا توسط برنامه‌کاربردی تولید امضا (OE.DTBS_Intend)، هدف امنیتی محافظت از داده‌های در نظر گرفته شده برای امضا توسط برنامه‌کاربردی ایجاد امضا (OE.DTBS_Protect) و هدف امنیتی التزام امنیتی صاحب‌امضا (OE.Signatory).

این پروفایل حفاظتی هدف امنیتی برای محیط عملیاتی – افزاره ایجاد امضای امن موثق ارائه‌شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.Dev_Prov_Service) را جایگزین هدف امنیتی افزاره ایجاد امضای امن موثق ارائه شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.SSCD_prov_Service) در پروفایل اصلی کرده و اهداف امنیتی برای محیط عملیاتی پیش راه‌اندازی محصول برای احرازهویت افزاره ایجاد امضای امن (OE.CGA_SSCD_Auth) و کانال قابل‌اعتماد برنامه‌کاربردی تولید گواهی برای ورود داده درستی‌سنجی امضا (OE.CGA_TC_SVD_Imp) را افزوده تا روش‌های بیشتری جهت استفاده به‌عنوان تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVC) بعد از تحویل به صاحب‌امضا و بیرون از محیط آماده‌سازی امن را مورد توجه قرار دهد.

هدف امنیتی محیط عملیاتی	توضیحات

OE.Dev_Prov_Service افزاره ایجاد امضای امن موثق ارائه‌شده توسط خدمات تدارک افزاره ایجاد امضای امن	خدمات تدارک افزاره ایجاد امضای امن (SSCD) افزاره‌های موثقی را به کار می‌برد که محصول را پیاده‌سازی کرده، محصول را برای اثبات به‌عنوان افزاره ایجاد امضای امن (SSCD) به موجودیت‌های بیرونی آماده می‌کرده، محصول را برای کاربران قانونی به‌عنوان صاحب‌امضا شخصی‌سازی کرده، هویت محصول به‌عنوان افزاره ایجاد امضای امن (SSCD) را به هویت کاربران قانونی پیوند داده و محصول را به صاحب‌امضا تحویل می‌دهد. باید توجه داشت که این اهداف جایگزین هدف امنیتی افزاره ایجاد امضای امن موثق ارائه شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.SSCD_prov_Service) از پروفایل حفاظتی اصلی می‌شوند که ممکن است، همان‌گونه که هست، در مقایسه با هدف امنیتی افزاره ایجاد امضای امن موثق ارائه‌شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.Dev_Prov_Service) هیچ الزامات اضافه‌ای برای محیط عملیاتی نداشته باشد (هدف امنیتی افزاره ایجاد امضای امن موثق ارائه‌شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.Dev_Prov_Service) زیرمجموعه‌ای از هدف امنیتی افزاره ایجاد امضای امن موثق ارائه شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.SSCD_prov_Service) است).
OE.CGA_SSCD_Auth پیش‌راه‌اندازی محصول برای احرازهویت افزاره ایجاد امضای امن	تامین‌کننده خدمات صدور گواهی (CSP) باید با ابزارهایی از برنامه‌کاربردی تولید گواهی (CGA) بررسی کند که آیا افزاره ارائه‌شده برای کاربرد گواهی (واجد شرایط) هویت منحصربه‌فردی به‌عنوان افزاره ایجاد امضای امن (SSCD) نگه‌داری می‌کند که این هویت به‌طور موفقیت‌آمیزی به‌عنوان افزاره ایجاد امضای امن (SSCD) برای برنامه‌کاربردی تولید گواهی (CGA) اثبات شود و آیا این هویت به دارنده قانونی افزاره به‌عنوان متقاضی گواهی، پیوند داده شده است یا خیر.

OE.CGA_TC_SVD_Imp کانال قابل‌اعتماد برنامه‌کاربردی تولید گواهی برای ورود داده درستی‌سنجی امضا	برنامه‌کاربردی تولید گواهی (CGA) باید تغییر در داده درستی‌سنجی امضا (SVD) واردشده از محصول با هویت ادعاشده از افزاره ایجاد امضای امن (SSCD) را تشخیص دهد. توسعه‌دهنده، محصول را با پیش‌راه‌اندازی‌ای برای تحویل به مشتری آماده می‌کند که در فاز توسعه موردتوجه اهداف امنیتی برای محیط عملیاتی قرار نگرفته‌اند (به‌عنوان‌مثال خدمات تدارک افزاره ایجاد امضای امن (SSCD). خدمات تدارک افزاره ایجاد امضای امن (SSCD) مقداردهی اولیه و شخصی‌سازی به‌عنوان محصول را برای کاربر مجاز (به‌عنوان‌مثال صاحب افزاره) انجام می‌دهد. اگر محصول با داده ایجاد امضای امن (SCD) به دارنده افزاره تحویل داده شود، محصول یک افزاره ایجاد امضای امن (SSCD) است. این موقعیت به‌جز مقداردهی اولیه اضافی محصول برای اثبات به‌عنوان افزاره ایجاد امضای امن (SSCD) و کانال قابل‌اعتماد به برنامه‌کاربردی تولید گواهی (CGA)، موردتوجه هدف امنیتی برای محیط عملیاتی افزاره ایجاد امضای امن موثق ارائه شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.SSCD_prov_Service) است. اگر محصول بدون داده ایجاد امضای امن (SCD) به دارنده افزاره تحویل داده شود، محصول تنها بعد از تولید اولین زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) یک افزاره ایجاد امضای امن (SSCD) خواهد بود. ازآنجاکه تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) توسط صاحب‌امضا در مرحله کاربریِ عملیاتی انجام شده است، محصول کارکردهای امنیتی اضافه‌ای را فراهم می‌آورد که موردتوجه هدف امنیتی اثبات احرازهویت به‌عنوان افزاره ایجاد امضای امن (OT.TOE_SSCD_Auth) و هدف امنیتی کانال قابل‌اعتماد محصول برای صدور داده درستی‌سنجی امضا (OT.TOE_TC_SVD_Exp) می‌باشد. اما این کارکرد امنیتی باید توسط خدمات تدارک افزاره ایجاد امضای امن (SSCD) به نحوی مقداردهی شود که در هدف امنیتی برای محیط عملیاتی افزاره ایجاد امضای امن موثق ارائه شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.SSCD_prov_Service) شرح داده شده است. بنابراین این پروفایل حفاظتی، هدف امنیتی برای محیط عملیاتی افزاره ایجاد امضای امن موثق ارائه شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.SSCD_prov_Service) را جایگزین هدف امنیتی افزاره ایجاد امضای امن موثق ارائه شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.SSCD_prov_Service) کرده است تا امکان تولید اولین زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) بعد از تحویل محصول به دارنده افزاره و مقداردهی اولیه موردنیاز کارکرد امنیتی محصول را فراهم نماید. بااین‌وجود، همان‌گونه که در هدف امنیتی پیش‌راه‌اندازی محصول برای احرازهویت افزاره ایجاد امضای امن (OE.CGA_SSCD_Auth) و هدف امنیتی کانال قابل‌اعتماد برنامه‌کاربردی تولید گواهی برای ورود داده درستی‌سنجی امضا (OE.CGA_TC_SVD_Imp) شرح داده شده است، کارکرد امنیتی اضافی بایستی مورداستفاده محیط عملیاتی قرار گیرد. این رویکرد اهداف امنیتی و الزامات محصول را تضعیف نمی‌کند، بلکه بر کارکردهای امنیتی بیشتری از محصول برای روش‌های استفاده بیشتر تأکید می‌کند. بنابراین، با ادعای انطباق پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید با معیار مشترک با در تضاد نیست [۷].

۵-۴- منطق اهداف امنیتی

۵-۴-۱- پیمایش معکوس اهداف امنیتی

جدول زیر نشان می‌دهد که چگونه اهداف امنیتی برای محصول و اهداف امنیتی برای محیط عملیاتی تهدیدات، خط‌مشی‌های امنیت سازمانی و مفروضات را پوشش می‌دهد. توجه داشته باشید که این پروفایل حفاظتی همان تهدیدات، خط‌مشی‌های امنیت سازمانی و مفروضاتی را توصیف می‌کند که برای محصول در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید وجود دارد اما اهداف امنیتی‌ای را برای محصول (اثبات احرازهویت به‌عنوان افزاره ایجاد امضای امن و هدف امنیتی کانال قابل‌اعتماد محصول برای صدور داده درستی‌سنجی امضا) و برای محیط عملیاتی (افزاره ایجاد امضای امن موثق ارائه‌شده توسط خدمات تدارک افزاره ایجاد امضای امن، پیش‌راه‌اندازی محصول برای احرازهویت افزاره ایجاد امضای امن و کانال قابل‌اعتماد برنامه‌کاربردی تولید گواهی برای ورود داده درستی‌سنجی امضا) اضافه می‌کند.

جدول ۱ نگاشت تعریف مسئله 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	OE.CGA_SSCD_Auth	OE.CGA_TC_SVD_Imp
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																		×				

۵-۴-۲- کفایت اهداف امنیتی

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

منطق موجود برای تهدید ذخیره‌سازی، نسخه‌برداری و انتشار داده ایجاد امضا (T.SCD_Divulg)، تهدید استخراج داده ایجاد امضا (T.SCD_Derive)، تهدید بهره‌برداری از آسیب‌پذیری‌های فیزیکی (T.Hack_Phys)، تهدید سوءاستفاده از تابع ایجاد امضای محصول (T.SigF_Misuse)، تهدید جعل داده‌ای که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن (T.DTBS_Forgery)، تهدید جعل امضای الکترونیکی (T.Sig_Forgery) همان منطق موجود در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید است. تنها تهدید جعل داده درستی‌سنجی امضا (T.SVD_Forgery) به شکل زیر توجیه می‌شود:

تهدیدات اهداف امنیتی	توضیحات
T.SVD_Forgery تهدید جعل داده درستی‌سنجی امضا	این تهدید با جعل داده درستی‌سنجی امضا (SVD) داده‌شده توسط محصول به برنامه‌کاربردی تولید گواهی (CGA) برای تولید گواهی سر و کار دارد. تهدید جعل داده درستی‌سنجی امضا (T.SVD_Forgery) مورد توجه موارد زیر است: - هدف امنیتی برای محصول - تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا (OT.SCD_SVD_Corresp) که از تناظر میان داده درستی‌سنجی امضا (SVD) و داده ایجاد امضا (SCD) و مرجع بدون ابهام زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) برای صدور داده درستی‌سنجی امضا (SVD) و ایجاد امضا توسط داده ایجاد امضا (SCD) اطمینان حاصل می‌کند. - هدف امنیتی برای محیط عملیاتی - اصالت‌سنجی داده درستی‌سنجی امضا (OE.SVD_Auth) که از یکپارچگی داده درستی‌سنجی امضا (SVD) صادرشده به برنامه‌کاربردی تولید گواهی (CGA) توسط محصول و از درستی‌سنجی تناظر بین داده ایجاد امضا (SCD) در افزاره ایجاد امضای امن (SSCD) صاحب‌امضا و داده درستی‌سنجی امضا (SVD) در ورودی‌ای که افزاره ایجاد امضای امن (SSCD) برای تابع تولید گواهی تامین‌کننده خدمات صدور گواهی (CSP) اطمینان حاصل می‌کند. - هدف امنیتی برای محصول - کانال قابل‌اعتماد از محصول برای صدور داده درستی‌سنجی امضا (OT.TOE_TC_SVD_Exp) که از این مسئله اطمینان می‌یابد که محصول، داده درستی‌سنجی امضا (SVD) را به شکل وارسی‌پذیری از طریق کانال قابل‌اعتماد برای برنامه‌کاربردی تولید گواهی (CGA) می‌فرستد. - هدف امنیتی برای محیط عملیاتی - کانال قابل‌اعتماد برنامه‌کاربردی تولید گواهی برای ورود داده درستی‌سنجی امضا (OE.CGA_TC_SVD_Imp) که درستی‌سنجی اصالت‌سنجی داده درستی‌سنجی امضا (SVD) با برنامه‌کاربردی تولید گواهی (CGA) را فراهم می‌آورد.

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

منطق موجود برای خط‌مشی امضای الکترونیکی واجد شرایط (P.QSign) همان منطق موجود در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید است. سه خط‌مشی تولید گواهی‌های واجد شرایط توسط تامین‌کننده خدمات صدور گواهی (P.CSP_QCert)، خط‌مشی محصول به عنوان افزاره ایجاد امضای امن (P.Sigy_SSCD) و خط‌مشی انکارناپذیری امضا (P.Sig_Non-Repud) به شکل زیر توجیه می‌شود:

خط‌مشی‌های امنیتی	توضیحات

P.CSP_QCert خط‌مشی تولید گواهی‌های واجد شرایط توسط تامین‌کننده خدمات صدور گواهی	این خط‌مشی امنیت سازمانی همانگونه که در پاراگراف ۱ بند ۵ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا تعریف شده است، این امکان را فراهم می‌آورد که بتوان محصول و برنامه‌کاربردی ایجاد امضا را برای امضای داده با امضاهای الکترونیک واجد شرایط به کار گرفت. قسمت ۱۵ این دستورالعمل برای حصول اطمینان از قابلیت کارکردی امضاهای پیشرفته به افزاره‌های ایجاد امضای امن اشاره می‌کند. هدف امنیتی برای محیط عملیاتی - تولید گواهی‌های واجد شرایط (OE.CGA_Qcert) الزامات امضاهای الکترونیک واجد شرایط (یا پیشرفته) را بر اساس اینکه گواهی‌ها واجد شرایط (و یا غیر واجد شرایط) باشند موردتوجه قرار می‌دهد. طبق هدف امنیتی برای محصول - اثبات احرازهویت به‌عنوان افزاره ایجاد امضای امن (OT.TOE_SSCD_Auth) نسخه‌هایی از محصول، داده‌های هویت و احراز هویت منحصربه‌فردی را به‌عنوان افزاره ایجاد امضای امن نگه می‌دارند و سازوکارهای امنیتی‌ای فراهم می‌آورند که برنامه‌کاربردی تولید گواهی را قادر به شناسایی و احراز هویت محصول به‌عنوان افزاره ایجاد امضای امن می‌کند تا این هویت را به‌عنوان افزاره ایجاد امضای امن برای برنامه‌کاربردی تولید گواهی اثبات کند. هدف امنیتی برای محیط پیش‌راه‌اندازی محصول برای احرازهویت افزاره ایجاد امضای امن (OE.CGA_SSCD_Auth) تضمین می‌کند که تامین‌کننده خدمات[۵۳] دلایلی را موردبررسی قرار می‌دهد که نشان می‌دهد افزاره ارائه‌شده متقاضی یک افزاره ایجاد امضای امن است. هدف امنیتی برای محصول - تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا (OT.SCD_SVD_Corresp) اطمینان حاصل می‌کند که داده درستی‌سنجی امضا (SVD) صادرشده به برنامه‌کاربردی تولید گواهی (CGA) توسط محصول با داده ایجاد امضا (SCD) ذخیره‌شده در محصول و استفاده‌شده توسط صاحب‌امضا، تناظر دارد. هدف امنیتی برای محصول - امنیت چرخه‌حیات (OT.Lifecycle_Security) اطمینان می‌یابد که محصول نقص‌های موجود در طول مقداردهی اولیه، شخصی‌سازی و کاربری عملیاتی را تشخیص دهد.

[۵۳] SP

P.Sigy_SSCD خط‌مشی محصول به عنوان افزاره ایجاد امضای امن	این خط‌مشی مستلزم آن است که محصول الزامات پیوست ۳ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا را برآورده سازد [۱]. هدف امنیتی برای محیط عملیاتی - یکتایی داده ایجاد امضا (OE.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 - رازمانی داده ایجاد امضا (OT.SCD_Secrecy)، هدف امنیتی برای محصول - امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure)، هدف امنیتی برای محصول - فراهم آوردن امنیت برون‌تابی‌های فیزیکی (OT.EMSEC_Design) و هدف امنیتی برای محصول - مقاومت در برابر دست‌کاری (OT.Tamper_Resistance) از رازمانی داده ایجاد امضا اطمینان می‌یابند. هدف امنیتی برای محصول - رازمانی داده ایجاد امضا (OT.SCD_Secrecy) الزامات 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)، امضاهای الکترونیک 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) الزامات 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. 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) الزامات پاراگراف ۲ پیوست ۳ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا [۱] را اینگونه برآورده می‌سازد که محصول نباید داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) را تغییر دهد. کاربری داده ایجاد امضا تحت کنترل انحصاری صاحب‌امضا با الزامات اهداف امنیتی هدف امنیتی برای محصول - امنیت چرخه‌حیات (OT.Lifecycle_Security)، هدف امنیتی تولید داده ایجاد امضا / داده درستی‌سنجی امضا (OT.SCD/SVD_Gen) و هدف امنیتی برای محصول - تابع ایجاد امضا تنها برای صاحب‌امضای قانونی (OT.Sigy_SigF) تضمین می‌شود. هدف امنیتی برای محیط عملیاتی – افزاره ایجاد امضای امن موثق ارائه‌شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.Dev_Prov_Service) اطمینان می‌یابد که کاربر قانونی نمونه‌ای از محصول را به‌عنوان یک محصول احراز اصالت شده، مقداردهی شده و شخصی شده از خدمات تدارک افزاره ایجاد امضای امن در طول روش اجرایی تحویل محصول به دست آورد. چنانچه محصول، داده ایجاد امضای تولیدشده تحت کنترل خدمات تدارک افزاره ایجاد امضای امن را پیاده‌سازی کند، کاربر قانونی محصول را به‌عنوان افزاره ایجاد امضای امن دریافت می‌کند. اگر محصول بدون داده ایجاد امضا به کاربر قانونی تحویل داده شده باشد او در فاز عملیاتی برای گواهی (واجد شرایط) به‌عنوان دارنده افزاره و کاربر قانونی محصول درخواست می‌دهد. تامین‌کننده خدمات صدور گواهی از مشخصه‌های امنیتی محصول (موردتوجه اهداف امنیتی اثبات احرازهویت به‌عنوان افزاره ایجاد امضای امن و کانال قابل‌اعتماد محصول برای صدور داده

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 می‌شود 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 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) با داده ایجاد امضا (SCD) پیاده‌سازی‌شده در محصول مطابقت 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) ذخیره شده 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 (به عبارت دیگر 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). ویژگیِ امنیتی محصول که موردتوجه اهداف امنیتی اثبات احرازهویت به‌عنوان افزاره ایجاد امضای امن و کانال قابل‌اعتماد محصول برای صدور داده درستی‌سنجی امضا است و مورد پشتیبانی هدف امنیتی برای محیط عملیاتی – افزاره ایجاد امضای امن موثق ارائه‌شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.Dev_Prov_Service) است درستی‌سنجی این مسئله را امکان‌پذیر می‌سازد که آیا افزاره ارائه‌شده توسط متقاضی، یک افزاری ایجاد امضای امن موردنیاز هدف امنیتی پیش‌راه‌اندازی محصول برای احرازهویت افزاره ایجاد امضای امن است و آیا داده درستی‌سنجی امضای دریافت‌شده که توسط دارنده افزاره فرستاده‌شده است با داده ایجاد امضا به‌نحوی‌که موردنیاز هدف امنیتی برای محیط عملیاتی - کانال قابل‌اعتماد برنامه‌کاربردی تولید گواهی برای ورود داده درستی‌سنجی امضا (OE.CGA_TC_SVD_Imp) است تناظر دارد یا خیر. 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. به‌عنوان

۵-۴-۲-۳- مفروضات و کفایت اهداف امنیتی

منطق موجود برای مفروضات برنامه‌کاربردی ایجاد امضای قابل اعتماد (A.SCA) و برنامه‌کاربردی تولید گواهی قابل اعتماد(A.CGA) همان منطق موجود در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید است.

۶- الزامات کارکرد امنیتی

۶-۱- قراردادها

معیار مشترک امکان اجرای چندین عملیات روی الزامات کارکردی را فراهم می‌آورد ازجمله: پالایش[۵۴]، انتخاب، اختصاص، و تکرار. هر یک از این عملیات در این پروفایل حفاظتی مورداستفاده قرار گرفته است. عملیاتی که در این پروفایل حفاظتی اجرا نمی‌شوند به‌منظور امکان نمونه‌برداری از پروفایل حفاظتی برای یک هدف امنیتی (ST) شناسایی شده‌اند.

عملیات **پالایش** برای افزودن جزئیات به یک الزام و در نتیجه محدودیت‌های بیشتر یک الزام مورداستفاده قرار گرفته است. پالایش الزامات امنیتی (۱) با واژه "پالایش" به شکل **پررنگ** نشان داده شده است و واژگان اضافه‌شده و یا تغییر یافته نوشته **پررنگی** هستند، یا (۲) در متن به‌عنوان نوشته **پررنگ** گنجانده‌شده و با زیرنویسی مشخص شده است. در مواردی که کلمات از یک الزام معیار مشترک حذف‌شده، پیوست جداگانه‌ای کلماتی که حذف شده است را نشان می‌دهد.

عملیات **انتخاب** برای انتخاب یک یا تعداد بیشتری از گزینه‌های ارائه‌شده توسط معیار مشترک در شرح الزامات مورداستفاده قرار می‌گیرد. انتخابی که در این استاندارد اروپایی صورت گرفته است به شکل نوشته زیرخط‌دار نشان داده شده و متن اصلی از مؤلفه در زیرنویس داده شده است. انتخابی که توسط نویسنده هدف امنیتی ارائه شده است در براکتی با نشانی ظاهر می‌شود که نشان‌دهنده این است یک انتخاب انجام شده، [انتخاب:]، و با *حروف مورب* نشان داده می‌شود.

---

[۵۴] Refinement

عملیات **اختصاص** برای اختصاص مقادیر مشخص به پارامترهای نامشخص مانند طول یک کلمه‌عبور مورداستفاده است. اختصاصی که در این استاندارد اروپایی ایجادشده به شکل نوشته زیرخط‌دار نشان داده شده و متن اصلیِ مؤلفه به‌صورت زیرنویس داده شده است. اختصاصی که توسط نویسنده هدف امنیتی ارائه‌شده در براکتی با نشانی ظاهر می‌شود که نشان‌دهنده این است یک اختصاص انجام شده، [اختصاص:]، و با *حروف مورب* نشان داده شده است.

عملیات **تکرار** موقعی مورداستفاده قرار می‌گیرد که یک مؤلفه با عملیات گوناگونی تکرار شده است. تکرار با نشان دادن یک علامت "/"، و نشانگر تکرار بعد از شناسه مؤلفه مشخص شده است.

این پروفایل حفاظتی به الزامات کارکرد امنیتی زیر نیاز دارد که برخی از این الزامات در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید توضیح داده شده است و تنها موارد اضافی در اینجا توضیح داده می‌شوند [۷]:

جدول ۲ الزامات کارکردی

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**زمانبندی احرازهویت ۱**	FIA_UAU.1.1
۲	**زمانبندی احرازهویت ۲**	FIA_UAU.1.2
۳	**اثبات احراز هویت شناسه ۱**	FIA_API.1.1
۴	**احراز هویت داده با هویت ضامن / داده درستی‌سنجی امضا ۱**	FDP_DAU.2.1/SVD
۵	**احراز هویت داده با هویت ضامن / داده درستی‌سنجی امضا ۲**	FDP_DAU.2.2/SVD

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**زمانبندی احرازهویت ۱**	FIA_UAU.1.1
۲	**زمانبندی احرازهویت ۲**	FIA_UAU.1.2
۳	**اثبات احراز هویت شناسه ۱**	FIA_API.1.1
۶	**کانال درونی قابل‌اعتماد توابع هدف امنیتی / داده درستی‌سنجی امضا ۱**	FTP_ITC.1.1/SVD
۷	**کانال درونی قابل‌اعتماد توابع هدف امنیتی / داده درستی‌سنجی امضا ۲**	FTP_ITC.1.2/SVD
۸	**کانال درونی قابل‌اعتماد توابع هدف امنیتی / داده درستی‌سنجی امضا ۳**	FTP_ITC.1.3/SVD

۶-۲- کلاس شناسایی و احراز هویت

شماره الزام	نام الزام
۱	**زمان‌بندی احراز هویت ۱**
وراثت از هیچ مؤلفه دیگر ندارد وابستگی: زمان‌بندی شناسایی این پروفایل حفاظتی عملیات زمان‌بندی احراز هویت را به شکل زیر افزوده است: توابع هدف امنیتی باید اجازه موارد زیر را بدهد: (۱) خودآزمایی منطبق با الزام کارکرد امنیتی آزمون توابع هدف امنیتی، (۲) شناسایی کاربر با استفاده از توابع هدف امنیتی موردنیاز الزام کارکرد امنیتی زمان‌بندی شناسایی، (۳) برقراری یک کانال قابل‌اعتماد بین برنامه‌کاربردی تولید گواهی و محصول با استفاده از توابع هدف امنیتی موردنیاز الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی / داده درستی‌سنجی امضا، (۴) [اختصاص: *فهرستی از اقدامات اضافه‌ای که توابع هدف امنیتی واسطه آن است*][۵۵] قبل از اینکه کاربر احراز هویت شود در سمت کاربر انجام می‌شود.	
۲	**زمان‌بندی احراز هویت ۲**
توابع هدف امنیتی باید مستلزم آن باشد که قبل از اینکه اجازه هرگونه اقدامی که توابع هدف امنیتی واسطه آنند را در سمت کاربر بدهد، هر کاربری به‌طور	

[۵۵] [اختصاص: *فهرستی از اقداماتی که توابع هدف امنیتی واسطه آن است*]

موفقیت‌آمیز شناسایی شود.

نکته کاربردی ۱: نویسنده هدف امنیتی باید عملیات ازدست‌رفته در عنصر ۱ الزام کارکرد امنیتی زمانبندی احراز هویت را انجام دهد. فهرست اقدامات اضافه‌ای که توابع هدف امنیتی واسطه آنند ممکن است خالی باشد (به‌عنوان‌مثال، اختصاص "هیچ‌چیز"). این پروفایل حفاظتی عملیات شماره (۳) در عنصر ۱ زمان‌بندی احراز هویت پروفایل حفاظتی اصلی را با افزودن امکان برقراری یک کانال قابل‌اعتماد برای برنامه‌کاربردی تولید گواهی انجام می‌دهد.

خانواده اثبات احراز هویت شناسه (FIA_API)

برای توصیف الزامات کارکرد امنیتی فناوری اطلاعات محصول، یک خانواده حساس (FIA_API) از کلاس شناسایی و احراز هویت (FIA) در اینجا تعریف شده است. این خانواده الزامات کارکردی برای اثبات هویت ادعاشده برای درستی‌سنجی احراز هویت توسط یک موجودیت بیرونی را شرح می‌دهد. درحالی‌که دیگر خانواده‌های کلاس شناسایی و احراز هویت اعتبارسنجی هویت یک موجودیت بیرونی را موردتوجه قرار می‌دهند.

- رفتار خانواده اثبات احراز هویت شناسه (FIA_API)

این خانواده توابع ارائه‌شده توسط محصول را برای اثبات هویت آن‌ها و برای تأیید شدن توسط یک موجودیت بیرونی در محیط فناوری اطلاعاتی محصول تعریف می‌کند.

- سطح‌بندی مؤلفه

اثبات احراز هویت شناسه (FIA_API.1)

- اثبات احراز هویت شناسه ۱ (FIA_API.1.1)

توابع هدف امنیتی بایستی یک [اختصاص: *سازوکار احراز هویت*] برای اثبات هویت [اختصاص: *کاربر یا نقش مجاز*] فراهم آورند.

- اقدامات مدیریتی

اقدامات زیر می‌تواند برای کارکردهای مدیریتی در کلاس مدیریت امنیت در نظر گرفته شود:

- مدیریت اطلاعات احراز هویت مورداستفاده برای اثبات هویت ادعاشده.

- اقدامات ممیزی

هیچ‌گونه عملیات قابل ممیزی وجود ندارد.

این پروفایل حفاظتی، الزامات کارکرد امنیتی زیر را اضافه کرده است:

شماره الزام	نام الزام
۳	اثبات احراز هویت ۱
وراثت از هیچ مؤلفه دیگر ندارد وابستگی: ندارد توابع هدف امنیتی باید [اختصاص: سازوکار احراز هویت] را برای اثبات هویت افزاره ایجاد امضای امن فراهم آورد. **نکته کاربردی ۲:** نویسنده هدف امنیتی بایستی همه عملیات ازدست‌رفته در عنصر ۱ الزام کارکرد امنیتی اثبات احراز هویت را انجام دهد. از طریق سازوکار احراز هویتی که در اینجا اختصاص داده می‌شود، محصول با استفاده از داده احراز هویت پیاده‌سازی‌شده در طول فاز پیش راه‌اندازی محصول، قادر به احراز هویت خود به‌عنوان افزاره ایجاد امضای امن برای برنامه‌کاربردی تولید گواهی است.	

۶-۳- کلاس حفاظت از داده‌های کاربر

شماره الزام	نام الزام
۴	احراز هویت داده با هویت ضامن / داده درستی‌سنجی امضا ۱
وراثت: از احراز هویت داده پایه وابستگی: زمان‌بندی شناسایی (۱) توابع هدف امنیتی باید قابلیت تولید شواهدی را فراهم آورد که بتواند به‌عنوان ضامنِ اعتبار داده درستی‌سنجی امضا[۵۶] مورداستفاده قرار بگیرد.	
۵	احراز هویت داده با هویت ضامن / داده درستی‌سنجی امضا ۲
توابع هدف امنیتی باید توانایی بررسی درستی یا نادرستی شواهد اعتبارِ اطلاعاتِ نشان داده‌شده و هویتِ کاربری که شواهد را تولید کرده است را برای برنامه‌کاربردی تولید گواهی[۵۷] فراهم آورد.	

۶-۴- کلاس کانال‌ها و یا مسیرهای قابل‌اعتماد

شماره الزام	نام الزام
۶	کانال قابل‌اعتماد درون توابع هدف امنیتی / داده درستی‌سنجی امضا ۱
وراثت از هیچ مؤلفه دیگر ندارد. وابستگی: ندارد	

[۵۶] *[اختصاص: فهرستی از انواع موجودیت‌های غیرفعال یا اطلاعات]*

[۵۷] *[اختصاص: فهرستی از موجودیت‌های فعال]*

توابع هدف امنیتی باید کانال ارتباطی‌ای بین خود و دیگر محصولات فناوری اطلاعاتی قابل‌اعتماد برنامه‌کاربردی تولید گواهی فراهم آورد که به‌طور منطقی از دیگر کانال‌های ارتباطی مجزا است و شناسایی تضمین‌شده‌ای از نقاط انتهایی خود و حفاظت از داده کانال در برابر تغییر و یا افشاء ارائه دهد.	
۷	کانال قابل‌اعتماد درون توابع هدف امنیتی/داده درستی‌سنجی امضا ۲
توابع هدف امنیتی باید به دیگر محصولات فناوری اطلاعات قابل‌اعتماد [۵۸] اجازه آغاز ارتباط از طریق کانال‌های قابل‌اعتماد را بدهد.	
۸	کانال قابل‌اعتماد درون توابع هدف امنیتی / داده درستی‌سنجی امضا ۳
توابع هدف امنیتی و یا برنامه‌کاربردی تولید گواهی باید آغازکننده ارتباط از طریق کانال‌های قابل‌اعتماد برای موارد زیر باشد: (۱) احراز هویت داده‌ها با هویت ضامن مطابق با الزامات کارکرد امنیتی اثبات احراز هویت شناسه و احراز هویت داده با هویت ضامن / داده درستی‌سنجی امضا. (۲) [اختصاص: *فهرستی از توابع موردنیاز دیگر برای یک کانال قابل‌اعتماد*] [۵۹]. **نکته کاربردی ۳:** عنصر الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی / داده درستی‌سنجی امضا به توابع هدف امنیتی برای به اجرا در آوردن کانال قابل‌اعتماد برقرارشده توسط برنامه‌کاربردی تولید گواهی جهت صدور داده درستی‌سنجی امضا به برنامه‌کاربردی تولید گواهی نیاز دارد. نویسنده هدف امنیتی بایستی عملیات ازدست‌رفته در عنصر ۳ الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی / داده درستی‌سنجی امضا را انجام دهد. چنانچه توابع هدف امنیتی استفاده از کانال قابل‌اعتماد را برای دیگر توابع اجرا نکنند، عملیات در عنصر ۳ الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی / داده درستی‌سنجی امضا "هیچ" است. **نکته کاربردی ۴:** اگر نویسنده هدف امنیتی برای پشتیبانی (نه اجرای) یک کانال قابل‌اعتماد برقرارشده توسط برنامه‌کاربردی تولید گواهی جهت صدور داده درستی‌سنجی امضا به برنامه کاربردی تولید گواهی، به توابع هدف امنیتی نیاز داشت، باید از پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید استفاده	

[۵۸] [*انتخاب: توابع هدف امنیتی، دیگر محصولات قابل اعتماد IT*]

[۵۹] [*اختصاص: فهرستی از کارکردهای مورد نیاز که برای یک کانال قابل اعتماد*]

کند و مؤلفه مشابه کانال درونی قابل‌اعتماد توابع هدف امنیتی / داده درستی‌سنجی امضا را با اختصاص "هیچ" در عنصر ۳ الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی / داده درستی‌سنجی امضا بگنجاند.

۶-۵- کلاس حفاظت از توابع امنیتی محصول

خانواده افزوده‌ی برون‌تابی محصول (FPT_EMS) از کلاس محافظت از توابع هدف امنیتی (FPT) در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید تعریف شده است [۷]. این پروفایل حفاظتی از مؤلفه‌ی FPT_EMS.1 طبق چیزی که در [۷] تعریف شده است استفاده می‌کند.

۷- الزامات تضمین امنیتی

جدول ۳ الزامات تضمین: سطح تضمین ارزیابی ۴ تکمیل‌شده با تحلیل آسیب‌پذیری روشمند پیشرفته

نام کلاس	نام الزام	توضیحات
Development ADV	ADV_ARC.1	طراحی معماری با جداسازی دامنه‌ها و بدون قابلیت دور زدن
	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_CMC.4	پشتیبانی تولید، روش‌های اجرایی پذیرش و خودکارسازی

ALC	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

۸-۱-۱- پوشش الزامات امنیتی

جدول زیر نشان می‌دهد که هر هدف امنیتی محصول حداقل با یکی از الزامات کارکرد امنیتی پوشش داده شده است.

جدول ۴ نگاشت الزامات کارکردیِ اهداف امنیتی به محصول

الزامات کارکردی / اهداف امنیتی محصول	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
FCS_CKM.1	×		×	×	×								
FCS_CKM.4	×				×								
FCS_COP.1	×					×							
FDP_ACC.1/SCD/SVD_Generation	×	×											
FDP_ACC.1/SVD_Transfer	×												×
FDP_ACC.1/Signature_Creation	×						×						
FDP_AFC.1/SCD/SVD_Generation	×	×											
FDP_AFC.1/SVD_Transfer	×												×
FDP_AFC.1/Signature_Creation	×						×						
FDP_RIP.1					×		×						
FDP_SDI.2/Persistent				×	×	×							

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	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp
FDP_SDI.2/DTBS							×	×					
FDP_DAU.2/SVD													×
FIA_AFL.1							×						
FIA_UAU.1		×					×					×	
FIA_API.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	×						×						

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	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp
FMT_SMR.1	×						×						
FMT_SMF.1	×						×						
FPT_EMS.1					×				×				
FPT_FLS.1					×								
FPT_PHP.1										×			
FPT_PHP.3					×						×		
FPT_TST.1	×				×	×							
FTP_ITC.1/SVD													×

۸-۱-۲-کفایت الزامات امنیتی محصول

منطق موجود در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید همچنان معتبر است. در بخش کفایت الزامات امنیتی محصول پروفایل حفاظتی افزاره ایجاد امضای امن – تولید کلید توضیح می‌دهد که چگونه الزامات کارکرد امنیتی، اهداف امنیتی امنیت چرخه حیات، تولید داده ایجاد امضا / داده درستی‌سنجی، یکتایی داده ایجاد امضا، تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا، رازمانی داده ایجاد امضا، امنیت رمزنگاری امضای دیجیتال، تابع ایجاد امضا تنها برای

صاحب‌امضای قانونی، یکپارچگی داده‌ای که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن درون محصول، فراهم آوردن امنیت برون‌تابی‌های فیزیکی، آشکارسازی دست‌کاری و مقاومت در برابر دست‌کاری برای محصول را پوشش می‌دهد. توجیه اهداف امنیتی برای هدف امنیتی اثبات احرازهویت به‌عنوان افزاره ایجاد امضای امن و کانال قابل‌اعتماد محصول برای صدور داده درستی‌سنجی امضا در ادامه آورده شده است.

هدف امنیتی محصول	شرح
OT.TOE_SSCD_Auth اثبات احرازهویت به‌عنوان افزاره ایجاد امضای امن	این هدف امنیتی برای ارائه سازوکارهای امنیتی جهت شناسایی و احراز اصالت محصول به‌عنوان افزاره ایجاد امضای امن که مستقیماً توسط الزام کارکرد امنیتی اثبات احراز هویت شناسه تامین شده است، به محصول نیاز دارد. الزام کارکرد امنیتی زمانبندی احراز هویت (علاوه بر پروفایل حفاظتی اصلی افزار ایجاد امضای امن – تولید کلید) اجازه برقراری کانال قابل‌اعتماد را قبل از احراز هویت شدنِ کاربر (انسان) می‌دهد.
OT.TOE_TC_SVD_Exp کانال قابل‌اعتماد محصول برای صدور داده درستی‌سنجی امضا	این هدف امنیتی برای فراهم آوردن کانال قابل‌اعتماد به برنامه‌کاربردی تولید گواهی به محصول نیاز دارد تا از یکپارچگی داده درستی‌سنجی امضای صادرشده به برنامه‌کاربردی تولید گواهی محافظت شود، که مستقیماً با موارد زیر تامین شده است. - انتقال داده درستی‌سنجی امضا برای تولید گواهی مطابق با الزامات کارکرد امنیتی کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی انتقال درستی‌سنجی امضا و مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی انتقال درستی‌سنجی امضا توسط توابع هدف امنیتی کنترل شده است. - الزام کارکرد امنیتی احراز هویت داده با هویت ضامن / داده درستی‌سنجی امضا به محصول نیاز دارد تا برنامه‌کاربردی تولید گواهی بتواند شواهدی از اعتبار داده درستی‌سنجی امضا و هویت کاربری که شواهد را تولید کرده است را بررسی و تایید کند. - الزام کاربرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی / داده درستی‌سنجی امضا، برای ارائه کانال قابل‌اعتماد به برنامه‌کاربردی تولید گواهی به محصول نیاز دارد.

۸-۲- برآوردن وابستگی‌های الزامات امنیتی

جدول ۵ برآوردن وابستگی‌های الزامات کارکردی امنیتی

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	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.4
FDP_ACC.1/SCD/SVD_Generation	FDP_ACF.1	FDP_ACF.1/SCD/SVD_Generation
FDP_ACC.1/Signature_Creation	FDP_ACF.1	FDP_ACF.1/Signature_Creation
FDP_ACC.1/SVD_Transfer	FDP_ACF.1	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SCD/SVD_Generation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SCD/SVD_Generation, FMT_MSA.3
FDP_ACF.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_ACF.1/SVD_Transfer	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SVD_Transfer, FMT_MSA.3

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
FDP_DAU.2/SVD	FIA_UID1.	FIA_UID.1
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
FIA_API.1	بدون وابستگی	N/A
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, 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, 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, FDP_ACC.1/Signature_Creation, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_SMR.1

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
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, FDP_ACC.1/ Signature_Creation
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
FPT_PHP.3	بدون وابستگی	N/A
FPT_TST.1	بدون وابستگی	N/A
FTP_ITC.1/SVD	بدون وابستگی	N/A

جدول ۶ برآوردن وابستگی‌های الزامات تضمین امنیتی

الزامات تضمین	وابستگی‌ها	برآورده شده توسط
بسته سطح تضمین ارزیابی ۴	(وابستگی‌های بسته سطح تضمین ارزیابی ۴ در اینجا دوباره تولید نمی‌شوند)	با ساخت، همه وابستگی‌ها در بسته سطح تضمین ارزیابی معیار مشترک برآورده شده است.
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1 (همه در بسته سطح تضمین ارزیابی ۴ گنجانده شده‌اند.)

۸-۳- توجیه الزامات تضمین امنیت انتخاب‌شده

سطح تضمین برای این پروفایل حفاظتی سطح تضمین ارزیابی ۴ تکمیل شده است. سطح تضمین ارزیابی ۴ به توسعه دهنده 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 با ریسک 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.

پیوست ۱ نمادها و اختصارات آن‌ها

نماد	معادل انگلیسی	معادل فارسی
CC	Common Criteria	معیار مشترک
CEM	Common Evaluation Methodology	متدولوژی ارزیابی مشترک
CGA	Certification generation application	برنامه‌کاربردی 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 واسط انسانی (کاربری)
IT	Information Technology	فناوری اطلاعات
OE	Operational Environment	محیط عملیاتی
OSP	Organizational Security Policy	خط‌مشی امنیتی سازمانی
RAD	Reference Authentication data	داده احراز هویت مرجع
PP	Protection Profile	پروفایل حفاظتی
RAD	Reference authentication data	داده‌های احراز هویت مرجع

SAR	Security Assurance Requirement	الزام تضمین امنیتی
SCA	Signature creation application	برنامه‌کاربردی 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 احراز هویت

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 4, CCMB-2012-09-001, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; Version 3.1, Revision 4, CCMB-2012-09-002, September 2012

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; Version 3.1, Revision 4, CCMB-2012-09-003, September 2012

[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-00062002, also short SSCD-PP or CWA14169

[6] CEN prEN 14169-1:2012, Protection profiles for secure signature creation device — Part 1: Overview

[7] CEN prEN 14169-2:2012, Protection profiles for secure signature creation device — Part 2: Device with key generation

[8] ETSI Technical Specification 101 733, CMS Advanced Electronic Signatures (CAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp

[9] ETSI Technical Specification 101 903, XML Advanced Electronic Signatures (XAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp

[10] ETSI Technical Specification 102 778: PDF Advanced Electronic Signatures (PAdES), the latest version may be downloaded from the ETSI download page http://pda.etsi.org/pda/queryform.asp