به نام خدا

پروفایل حفاظتی افزاره ایجاد امضای امن

قسمت ۶: الحاقی برای افزاره با ورود کلید و ارتباطات مورد اعتماد

برنامه‌کاربردی ایجاد امضا

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] مشخص می‌شود که ممکن است کلیدهای امضاء را وارد کرده و به روش حفاظت شده‌ای با برنامه‌کاربردی ایجاد امضا[۲] ارتباط برقرار نماید: "افزاره ایجاد امضای امن با ورود کلید و ارتباط قابل اعتماد با برنامه‌کاربردی ایجاد امضا (SSCD KI TCCGA)".

این پروفایل حفاظتی در مورد افزاره ایجاد امضای امن با ورود کلید و ارتباط قابل‌اعتماد با برنامه‌کاربردی ایجاد امضا (PP SSCD KI TCSCA) است و الزامات امنیتی را برای افزاره ایجاد امضای امن با ورود کلید تعریف می‌کند که داده ایجاد امضا،[۳] (SCD) را وارد کرده و امضاهای دیجیتالی ایجاد می‌کند که همان‌گونه که در پروفایل حفاظتی اصلی شرح داده شده است می‌تواند برای امضاهای الکترونیک (واجد شرایط یا پیشرفته) به‌کار رود [۷]. همچنین محصول این پروفایل حفاظتی جهت محافظت از داده احراز هویت و داده‌ای که باید امضا شود از ارتباطات قابل‌اعتماد با برنامه‌کاربردی ایجاد امضا پشتیبانی می‌کند. این ویژگی‌های امنیتی، امکان استفاده از محصول در محیط‌های عملیاتی پیشرفته‌تر را فراهم می‌آورد.

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 به‌منظور ایجاد امضای دیجیتالی پیکربندی‌شده می‌تواند به‌کار گرفته شود. به‌طور خاص این پروفایل حفاظتی، صلاحیت

---

[۱] Secure Signature Creation Device (SSCD)

[۲] Signature Creation Application

[۳] Signature Creation Data

محصول به‌عنوان افزاره‌ای برای ایجاد امضای الکترونیکی پیشرفته را همان‌گونه که در دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا[۴] توضیح داده‌شده است نیز تعیین می‌کند.

سطح تضمین این پروفایل حفاظتی، سطح تضمین ارزیابی ۴ (EAL4) [۵] تکمیل شده 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:

- **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.

---

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

[۵] Evaluation Assurance Level

۲-۲- اصطلاحات ارزیابی امنیت

- **استاندارد ارزیابی معیار مشترک[۶] (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[۷] (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[۸] (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.

---

[۶] Common Criteria

[۷] Evaluation Assurance Level

[۸] Protection Profile

- **هدف امنیتی[۹] (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[۱۰] (TOE)**

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

- **توابع امنیتی هدف ارزیابی[۱۱] (TSF)**

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[۱۲]**

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

- **امضای الکترونیکی پیشرفته[۱۳]**

---

[۹] Security Target

[۱۰] Target of Evaluation

[۱۱] TOE Security Functions

[۱۲] Administrator

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**[۱۴]

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

- **گواهی**[۱۵]

---

[۱۳] Advanced electronic signature

[۱۴] Authentication data

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**[۱۶]

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[۱۷] پیام گواهی کلید عمومی امضاکننده به همراه شناسه تابع چکیده‌ساز که برای محاسبه مقادیر چکیده پیام از آن استفاده شده است.

---

[۱۵] Certificate

[۱۶] Certificate information

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

- **برنامه‌کاربردی تولید گواهی (CGA)**[۱۸]

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**[۱۹] **(CSP)**

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

- **داده‌ای که باید امضا شوند**[۲۰] **(DTBS)**

---

[۱۷] hash

[۱۸] Certificate generation application

[۱۹] Certification Service Provider

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[۲۱] (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[۲۲] 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).

---

[۲۰] Data to be signed

[۲۱] Data to be signed or its unique representation

[۲۲] intermediate

- **کاربر مجاز**[۲۳]

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**[۲۴]

نهاد سازمانی که توسط یک کشور عضو اتحادیه اروپا به‌عنوان مسئول اعطای مجوز رسمی[۲۵] 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).

---

[۲۳] Legitimate user

[۲۴] Notified body

[۲۵] accreditation

- **داده احرازهویت مرجع[۲۶] (RAD)**

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[۲۷] (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[۲۸]**

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[۲۹]**

اطلاعات افزوده‌ای که همراه با پیام کاربر امضا می‌شود.

- **برنامه‌کاربردی ایجاد امضا[۳۰] (SCA)**

---

[۲۶] Reference Authentication data

[27] Secure signature creation device

[28] Signatory

[۲۹] Signature attributes

[30] Signature creation application

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.
- 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[۳۱] (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[۳۲] (SCS)**

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

- **داده درستی‌سنجی امضا[۳۳] (SVD)**

[31] Signature creation data
[32] Signature Creation System

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

- **خدمات تدارک افزاره ایجاد امضای امن**[۳۴]

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.

---

[33] Signature verification data
[34] SSCD provisioning service

- **داده درستی‌سنجی احرازهویت[۳۵] (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 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) ورود داده ایجاد امضا (SCD) و به صورت اختیاری، داده درستی‌سنجی امضا (SVD) متناظر[۳۶]،

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 الکترونیک برای داده در یک حالت عملیاتی، با مراحل زیر:

---

[35] Verification authentication data

[۳۶] correspondent

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).

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 102 778 (PAdES) پیاده‌سازی کند.

محصول برای استفاده صاحب‌امضا به شکل زیر آماده شده است:

۱) ورود حداقل یک مجموعه از داده ایجاد امضا (SCD)، و

۲) شخصی‌سازی برای صاحب‌امضا با ذخیره در محصول:

أ. داده احراز هویت مرجع (RAD) صاحب‌امضا

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

بعد از ورود، داده ایجاد امضا (SCD) در یک حالت غیر عملیاتی است. 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[۳۷] 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

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

۳-۲-۱-محیط آماده‌سازی

جایی است که محصول برای ورود داده ایجاد امضا (SCD) از طریق برنامه‌کاربردی تولید داده درستی‌سنجی / داده ایجاد امضا با یک تأمین‌کننده خدمت صدور گواهی (CSP) تعامل می‌کند، همچنین جهت بدست آوردن گواهی برای داده درستی‌سنجی امضای (SVD) متناظر با داده ایجاد امضا (SCD) که تأمین کننده خدمت صدور گواهی (CSP) تولید کرده است با برنامه‌کاربردی تولید گواهی (CGA) تعامل می‌کند. محیط مقداردهی اولیه بیشتر برای شخصی‌سازی محصول با مقادیر اولیه داده احراز هویت مرجع (RAD) با محصول تعامل می‌کند.

۳-۲-۲- محیط امضا

[۳۷] PIN

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 را به دست می‌آورد. محصول و برنامه‌کاربردی ایجاد امضا به‌منظور اطمینان از یکپارچگی داده‌ای که باید امضا شود (DTBS) مربوط به بازنمایی منحصر به فرد متعلق به آن (DTBS/R) از طریق یک کانال قابل‌اعتماد ارتباط برقرار می‌کنند.

۳-۲-۳- 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 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 ۵ در قسمت ۱ [۶] این استاندارد محیط عملیاتی را نشان می‌دهد.

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) واسطی 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.

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 و برنامه‌کاربردی ایجاد امضا به‌منظور حفاظت از یکپارچگی بازنمایی منحصر به فرد متعلق به داده‌ای که باید امضا شود (DTBS/R)، از طریق کانال قابل‌اعتماد ارتباط برقرار می‌کنند.

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[۳۸])، یک الگوی زیست‌سنجی و یا ترکیبی از این‌ها است. محصول از محرمانگی و یکپارچگی داده احراز هویت مرجع (RAD) محافظت می‌کند. محصول ممکن است واسط کاربری‌ای 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 خواستار دریافت یک داده درستی‌سنجی احراز هویت (VAD) از کاربر است، 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:

---

[38] PIN

- مقداردهی اولیه به داده احراز هویت 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 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 دیجیتال کارت هوشمند را از طریق پایانه آغاز می‌کند.

۳-۳- چرخه حیات محصول

چرخه حیات محصول مشابه تعریفی است که در بخش ۴,۳,۳ پروفایل حفاظتی افزاره ایجاد امضای امن - ورود کلید[۳۹] [۷] آمده است.

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 افزاره ایجاد امضای امن – تولید کلید[۴۰] اصلی تعریف شده است [۷].

---

[۳۹] PP SSCD KG

[۴۰] PP SSCD KG

۴-۱-۱- دارایی‌ها و موجودیت‌های غیر فعال

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 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 غیر قابل‌جعل 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[۴۱] ممکن است به عنوان موجودیت فعال مدیر سیستم[۴۲] در نقش مدیر سیستم[۴۳] و یا به عنوان موجودیت فعال صاحب‌امضا[۴۴] در نقش صاحب‌امضا[۴۵] 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.

---

[۴۱] S.User

[۴۲] S.Admin

[۴۳] R.Admin

[۴۴] S.Sigy

[۴۵] R.Sigy

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.

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 – ورود 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 واسط‌های 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 – ورود 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 – ورود کلید می‌باشد[۷]:

فرض برنامه‌کاربردی تولید گواهی قابل‌اعتماد (A.CGA)، فرض برنامه‌کاربردی ایجاد امضای قابل‌اعتماد (A.SCA)، فرض مدیریت امن داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) توسط تامین‌کننده خدمات صدور گواهی (A.CSP).

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 افزاره ایجاد امضای امن – ورود کلید و ارتباطات قابل‌اعتماد با برنامه‌کاربردی ایجاد امضا همه اهداف امنیتی تعریف‌شده برای محصول در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – ورود کلید را در بر می‌گیرد، این اهداف امنیتی شامل موارد زیر می‌باشند [۷]:

هدف امنیتی امنیت چرخه‌حیات (OT.Lifecycle_Security)، هدف امنیتی ورود داده ایجاد امضا مجاز (OT.SCD_Auth_Imp)، 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:

هدف امنیتی	توضیحات

OT.TOE_TC_VAD_Imp کانال قابل‌اعتماد از محصول برای ورود داده درستی‌سنجی احراز هویت	محصول باید کانال قابل‌اعتمادی را برای محافظت از محرمانگی و یکپارچگی داده درستی‌سنجی احراز هویت (VAD) دریافتی از افزاره واسط انسانی (کاربری)[۴۶] (HID) به شکلی ارائه دهد که مورد نیاز روش احراز هویت به کار گرفته می‌باشد. **نکته کاربردی ۱:** این هدف امنیتی برای محصول تا حدودی هدف امنیتی برای محیط عملیاتی - محافظت از داده درستی‌سنجی احراز هویت (OE.HID_VAD) موجود در پروفایل حفاظتی اصلی را پوشش می‌دهد. درحالی‌که هدف امنیتی برای محیط عملیاتی - محافظت از داده درستی‌سنجی احراز هویت (OE.HID_VAD) موجود در پروفایل حفاظتی اصلی برای حفاظت از داده درستی‌سنجی احراز هویت تنها نیاز به محیط عملیاتی دارد این پروفایل حفاظتی برای پیاده‌سازی یک کانال قابل‌اعتماد جهت محافظت از داده درستی‌سنجی احراز هویت (VAD) به افزاره واسط انسانی (HID) و محصول نیاز دارد: افزاره واسط انسانی (HID) داده درستی‌سنجی احراز هویت (VAD) را صادر کرده و مطابق هدف امنیتی برای محیط عملیاتی - کانال قابل‌اعتماد از افزاره واسط انسانی (HID) برای صدور داده درستی‌سنجی احراز هویت (OE.HID_TC_VAD_Exp) یک انتهای کانال قابل‌اعتماد را برقرار می‌کند، محصول، در انتهای دیگر کانال قابل‌اعتماد، مطابق هدف امنیتی برای محصول - کانال قابل‌اعتماد از محصول برای ورود داده درستی‌سنجی احراز هویت (OT.TOE_TC_VAD_Imp) داده درستی‌سنجی احراز هویت (VAD) را وارد می‌کند. بنابراین این پروفایل حفاظتی تا حدودی محافظت از داده درستی‌سنجی احراز هویت (VAD) را از محیط عملیاتی که در هدف امنیتی برای محیط عملیاتی - محافظت از داده درستی‌سنجی احراز هویت (OE.HID_VAD) توصیف شده است مجدداً طبق هدف امنیتی برای محصول - کانال قابل‌اعتماد از محصول برای ورود داده درستی‌سنجی احراز هویت (OT.TOE_TC_VAD_Imp) را به محصول اختصاص می‌دهد و تنها قابلیت‌های کارکردی ضروری را بر عهده افزاره واسط انسانی (HID) می‌گذارد.

[۴۶] Human Interface Device

OT.TOE_TC_DTBS_Imp کانال قابل اعتماد از محصول برای ورود داده‌ای که باید امضا شود	محصول باید کانال قابل‌اعتمادی برای برنامه‌کاربردی ایجاد امضا (SCA) فراهم آورد تا تغییر داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) دریافت شده از برنامه‌کاربردی ایجاد امضا (SCA) را تشخیص دهد. **نکته کاربردی ۲:** این هدف امنیتی برای محصول تا حدودی هدف امنیتی برای محیط عملیاتی - محافظت از داده‌ای که باید امضا شود (OE.DTBS_Protect) موجود در پروفایل حفاظتی اصلی را پوشش می‌دهد. درحالی‌که هدف امنیتی برای محیط عملیاتی - محافظت از داده‌ای که باید امضا شود (OE.DTBS_Protect) موجود در پروفایل حفاظتی اصلی برای حفاظت از داده‌ای که باید امضا شود (DTBS) تنها به محیط عملیاتی نیاز دارد این پروفایل حفاظتی برای پیاده‌سازی یک کانال مورد اعتماد جهت محافظت از داده‌ای که باید امضا شود (DTBS) به برنامه‌کاربردی ایجاد امضا (SCA) و محصول نیازمند است: برنامه‌کاربردی ایجاد امضا (SCA) داده‌ای که باید امضا شود (DTBS) را صادر کرده و یک انتهای کانال قابل‌اعتماد را مطابق با هدف امنیتی برای محیط عملیاتی - کانال قابل اعتماد برنامه‌کاربردی ایجاد امضا (SCA) برای صدور داده‌ای که باید امضا شود (OE.SCA_TC_DTBS_Exp) برقرار می‌کند، محصول طبق هدف امنیتی برای محصول - کانال قابل اعتماد از محصول برای ورود داده‌ای که باید امضا شود (OT.TOE_TC_DTBS_Imp)، داده‌ای که باید امضا شود (DTBS) را در انتهای دیگر کانال قابل‌اعتماد وارد می‌کند؛ بنابراین این پروفایل حفاظتی تا حدودی محافظت از داده‌ای که باید امضا شود (DTBS) را از محیط عملیاتی که در هدف امنیتی برای محیط عملیاتی - محافظت از داده‌ای که باید امضا شود (OE.DTBS_Protect) توصیف شده است مجدداً طبق هدف امنیتی برای محصول - کانال قابل اعتماد از محصول برای ورود داده‌ای که باید امضا شود (OT.TOE_TC_DTBS_Imp) را به محصول اختصاص می‌دهد و تنها قابلیت‌های کارکردی ضروری را بر عهده برنامه‌کاربردی ایجاد امضا (SCA) می‌گذارد.

۵-۳- اهداف امنیتی برای محیط عملیاتی

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

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

هدف امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا مجاز (OE.SCD/SVD_Auth_Gen)، هدف امنیتی رازمانی داده ایجاد امضا (OE.SCD_Secrecy)، هدف امنیتی یکتایی داده ایجاد امضا (OE.SCD_Unique) و هدف امنیتی تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا (OE.SCD_SVD_Corresp)، هدف امنیتی اصالت‌سنجی داده درستی‌سنجی امضا (OE.SVD_Auth)، هدف امنیتی تولید گواهی‌های واجد شرایط (OE.CGA_Qcert)، هدف امنیتی افزاره ایجاد امضای امن موثق ارائه شده توسط خدمات تدارک افزاره ایجاد امضای امن (OE.SSCD_prov_Service)، هدف امنیتی ارسال داده‌های درنظر گرفته شده برای امضا توسط برنامه‌کاربردی تولید امضا (OE.DTBS_Intend) و هدف امنیتی التزام امنیتی صاحب‌امضا (OE.Signatory).

این پروفایل حفاظتی کانال قابل‌اعتماد افزاره واسط انسانی برای صدور داده درستی‌سنجی احراز هویت (OE.HID_TC_VAD_Exp) را جایگزین هدف امنیتی محافظت از داده درستی‌سنجی احرازهویت (OE.HID_VAD) و کانال قابل‌اعتماد برنامه‌کاربردی تولید امضا برای صدور داده‌ای که باید امضا شود را به شکل زیر جایگزین هدف امنیتی محافظت از داده‌های در نظر گرفته شده برای امضا توسط برنامه‌کاربردی ایجاد امضا (OE.DTBS_Protect) در پروفایل اصلی کرده‌است. در ادامه این دو هدف امنیتی تشریح خواهند شد.

هدف امنیتی محیط عملیاتی	توضیحات

OE.HID_TC_VAD_Exp کانال قابل‌اعتماد افزاره واسط انسانی برای صدور داده درستی‌سنجی احراز هویت	افزاره واسط انسانی (HID) واسط انسانی برای احراز هویت کاربر فراهم می‌کند. افزاره واسط انسانی (HID) از محرمانگی و یکپارچگی داده درستی‌سنجی احرازهویت (VAD) مورد نیاز برای روش احراز هویت بکار رفته که شامل صدور به محصول به وسیله یک کانال قابل‌اعتماد است، اطمینان حاصل می‌کند. **نکته کاربردی ۳:** این هدف امنیتی برای محصول تا حدودی هدف امنیتی برای محیط عملیاتی – محافظت از داده درستی‌سنجی احرازهویت (OE.HID_VAD) موجود در پروفایل حفاظتی اصلی را پوشش می‌دهد. درحالی‌که هدف امنیتی برای محیط عملیاتی – محافظت از داده درستی‌سنجی احرازهویت (OE.HID_VAD) موجود در پروفایل حفاظتی اصلی برای حفاظت از داده درستی‌سنجی احراز هویت (VAD) تنها نیاز به محیط عملیاتی دارد این پروفایل حفاظتی برای پیاده‌سازی یک کانال قابل‌اعتماد برای حفاظت از داده درستی‌سنجی احراز هویت (VAD) به افزاره واسط انسانی (HID) و محصول نیازمند است: افزاره واسط انسانی (HID) داده درستی‌سنجی احراز هویت (VAD) را صادر کرده و یک سوی کانال قابل‌اعتماد را بر اساس هدف امنیتی کانال قابل‌اعتماد افزاره واسط انسانی برای صدور داده درستی‌سنجی احراز هویت (OE.HID_TC_VAD_Exp) برقرار می‌کند و محصول، داده درستی‌سنجی احراز هویت (VAD) را در طرف دیگر کانال قابل‌اعتماد مطابق با هدف امنیتی محصول – کانال قابل‌اعتماد محصول برای ورود داده درستی‌سنجی احراز هویت (OT.TOE_TC_VAD_Imp) وارد می‌کند؛ بنابراین این پروفایل حفاظتی تا حدودی محافظت از داده درستی‌سنجی احراز هویت (VAD) را از محیط عملیاتی که در هدف امنیتی برای محیط عملیاتی – محافظت از داده درستی‌سنجی احرازهویت (OE.HID_VAD) توصیف شده است مجدداً طبق هدف امنیتی محصول – کانال قابل‌اعتماد محصول برای ورود داده درستی‌سنجی احراز هویت (OT.TOE_TC_VAD_Imp) را به محصول اختصاص می‌دهد و تنها قابلیت‌های کارکردی ضروری را بر عهده افزاره واسط انسانی (HID) می‌گذارد.

OE.SCA_TC_DTBS_Exp کانال قابل‌اعتماد برنامه‌کاربردی ایجاد امضا برای صدور داده‌ای که باید امضا شود	برنامه‌کاربردی ایجاد امضا (SCA) کانال قابل‌اعتماد موردنیاز محصول برای حفاظت از یکپارچگی داده‌ای که باید امضا شود (DTBS) فراهم می‌آورد و اطمینان حاصل می‌کند که داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) نمی‌تواند به شکل تشخیص داده نشده‌ای در گذر بین برنامه‌کاربردی ایجاد امضا (SCA) و محصول تغییر کند. **نکته کاربردی ۴:** این هدف امنیتی برای محصول تا حدودی هدف امنیتی برای محیط عملیاتی محافظت از داده‌ای که باید امضا شود (OE.DTBS_Protect) موجود در پروفایل حفاظتی اصلی را پوشش می‌دهد. درحالی‌که هدف امنیتی برای محیط عملیاتی محافظت از داده‌ای که باید امضا شود (OE.DTBS_Protect) موجود در پروفایل حفاظتی اصلی برای حفاظت از داده‌ای که باید امضا شود (DTBS) تنها نیاز به محیط عملیاتی دارد این پروفایل حفاظتی برای پیاده‌سازی یک کانال قابل‌اعتماد برای حفاظت از داده‌ای که باید امضا شود (DTBS) به برنامه‌کاربردی ایجاد امضا (SCA) و محصول نیازمند است: برنامه‌کاربردی ایجاد امضا (SCA) داده‌ای که باید امضا شود (DTBS) را صادر کرده و یک سوی کانال قابل‌اعتماد را بر اساس هدف امنیتی برای محیط عملیاتی – کانال قابل‌اعتماد برنامه‌کاربردی ایجاد امضا برای صدور داده‌ای که باید امضا شود (OE.SCA_TC_DTBS_Exp) برقرار می‌کند و محصول، داده‌ای که باید امضا شود (DTBS) را در طرف دیگر کانال قابل‌اعتماد مطابق هدف امنیتی برای محصول – کانال قابل اعتماد برای ورود داده‌ای که باید امضا شود (OT.TOE_TC_DTBS_Imp) را وارد می‌کند؛ بنابراین این پروفایل حفاظتی تا حدودی محافظت از داده‌ای که باید امضا شود (DTBS) را از محیط عملیاتی که در هدف امنیتی برای محیط عملیاتی – محافظت از داده‌ای که باید امضا شود (OE.DTBS_Protect) توصیف شده است مجدداً طبق هدف امنیتی محصول – کانال قابل‌اعتماد محصول برای ورود داده‌ای که باید امضا شود (OT.TOE_TC_DTBS_Imp) را به محصول اختصاص می‌دهد و تنها قابلیت‌های کارکردی ضروری را بر عهده برنامه‌کاربردی ایجاد امضا (SCA) می‌گذارد.

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 مفروضات را که برای محصول در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید وجود دارد با دو استثنای زیر توصیف می‌کند:

هدف امنیتی برای محیط عملیاتی – محافظت از داده درستی‌سنجی احرازهویت (OE.HID_VAD) موجود در پروفایل حفاظتی اصلی را در این پروفایل به دو هدف امنیتی هدف امنیتی برای محیط عملیاتی کانال قابل‌اعتماد افزاره واسط انسانی برای صدور داده درستی‌سنجی احراز هویت (OE.HID_TC_VAD_Exp) و هدف امنیتی برای محصول کانال قابل‌اعتماد از محصول برای ورود داده درستی‌سنجی احراز هویت (OT.TOE_TC_VAD_Imp) تقسیم شده است، به‌عبارت دیگر قسمتی از اهداف امنیتی برای محیط (که در پروفایل حفاظتی اصلی هدف امنیتی برای محیط عملیاتی – محافظت از داده درستی‌سنجی احرازهویت (OE.HID_VAD) نامیده می‌شود) طبق معیار مشترک اجازه داده شده که توسط خود محصول برآورده شود.

هدف امنیتی برای محیط عملیاتی - محافظت از داده‌ای که باید امضا شود (OE.DTBS_Protect) موجود در پروفایل حفاظتی اصلی در این پروفایل حفاظتی به دو هدف امنیتی کانال قابل‌اعتماد برنامه‌کاربردی ایجاد امضا برای صدور داده‌ای که باید امضا شود (OE.SCA_TC_DTBS_Exp) و هدف امنیتی کانال قابل اعتماد از محصول برای ورود داده‌ای که باید امضا شود (OT.TOE_TC_DTBS_Imp) تقسیم شده است، به‌عبارت دیگر قسمتی از هدف امنیتی برای محیط (هدف امنیتی برای محیط عملیاتی - محافظت از داده‌ای که باید امضا شود (OE.DTBS_Protect) از پروفایل حفاظتی اصلی) طبق معیار مشترک اجازه داده شده که توسط خود محصول برآورده شود.

جدول ۱ نگاشت تعریف مسئله امنیتی برای اهداف امنیتی

	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.DTBS_Intend	OE.Signatory	OE.HID_TC_VAD_Exp	OE.SCA_TC_DTBS_Exp
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																				×			
A.CSP													×	×	×	×							

۵-۴-۲- کفایت اهداف امنیتی

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

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

تهدیدات اهداف امنیتی	توضیحات

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[۴۷] (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. ترکیب هدف امنیتی برای محصول - کانال قابل اعتماد از محصول برای ورود داده‌ای که باید امضا شود (OT.TOE_TC_DTBS_Imp) و هدف امنیتی برای محیط عملیاتی کانال قابل‌اعتماد برنامه‌کاربردی ایجاد امضا برای صدور داده‌ای که باید امضا شود (OE.SCA_TC_DTBS_Exp) با دستکاری‌های تشخیص داده نشده در داده‌ای که باید امضا شود در طول انتقال آن از برنامه‌کاربردی ایجاد امضا به 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) واسط انسانی را برای احرازهویت کاربر فراهم کند، هدف امنیتی برای محیط عملیاتی کانال قابل‌اعتماد افزاره واسط انسانی برای صدور داده درستی‌سنجی احراز هویت (OE.HID_TC_VAD_Exp) به افزاره واسط انسانی برای محافظت از محرمانگی و یکپارچگی داده درستی‌سنجی احرازهویت (VAD) نیاز دارد که مورد نیاز روش احرازهویت به کار گرفته شده است. افزاره واسط انسانی و محصول با یک کانال قابل‌اعتماد بین افزاره واسط انسانی و محصول مطابق هدف امنیتی برای محیط عملیاتی کانال قابل‌اعتماد افزاره واسط انسانی برای صدور داده درستی‌سنجی احراز هویت (OE.HID_TC_VAD_Exp) و هدف امنیتی برای محصول کانال قابل‌اعتماد از محصول برای ورود داده درستی‌سنجی احراز هویت (OT.TOE_TC_VAD_Imp) از داده درستی‌سنجی احراز هویت محافظت خواهند کرد. 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 که از خدمات تدارک افزاره ایجاد امضای امن (SSCD) دریافت می‌شود در حالت غیرعملیاتی 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 از محرمانگی داده درستی‌سنجی احراز هویت خود محافظت می‌کند.

[۴۷] Signed data object

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 داده‌ای که باید امضا شود و یا بازنمایی منحصر به فرد متعلق به آن است که به عنوان ورودی برای تابع ایجاد امضای محصول فرستاده شده و داده‌ای که باید امضا شود و یا بازنمایی منحصر به فرد متعلق به آن با داده‌ای که باید امضا شود و صاحب‌امضا قصد امضای آن را داشته است مطابقت ندارد. این تهدید با اهداف امنیتی هدف امنیتی برای محصول - کانال قابل اعتماد از محصول برای ورود داده‌ای که باید امضا شود (OT.TOE_TC_DTBS_Imp) هدف امنیتی برای محیط عملیاتی کانال قابل‌اعتماد برنامه‌کاربردی ایجاد امضا برای صدور داده‌ای که باید امضا شود (OE.SCA_TC_DTBS_Exp) مورد توجه قرار می‌گیرد، که اطمینان حاصل می‌کند داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) از طریق کانال قابل‌اعتمادی فرستاده شده و در انتقال بین برنامه‌کاربردی ایجاد امضا (SCA) و محصول نمی‌تواند به‌شکل غیر قابل تشخیصی تغییر کند. محصول به صورت درونی با این تهدید به وسیله 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) روبرو می‌شود که از یکپارچگی داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) درون محصول اطمینان حاصل می‌کند. همچنین محیط فناوری اطلاعاتی محصول تهدید جعل داده‌ای که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن (T.DTBS_Forgery) را به وسیله هدف امنیتی برای محیط عملیاتی - ارسال داده‌های درنظر گرفته شده برای امضا توسط برنامه کاربردی تولید امضا (OE.DTBS_Intend) مورد رسیدگی قرار می‌دهد 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.

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

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

خط‌مشی‌های امنیتی	توضیحات

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 تولید 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 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) ذخیره‌شده 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 از محرمانگی داده درستی‌سنجی احراز هویت خود محافظت می‌کند. محرمانگی داده درستی‌سنجی احراز هویت در طول انتقال بین افزاره واسط انسانی و محصول مطابق هدف امنیتی برای محیط عملیاتی کانال قابل‌اعتماد افزاره واسط انسانی برای صدور داده درستی‌سنجی احراز هویت (OE.HID_TC_VAD_Exp) و هدف امنیتی برای محصول کانال قابل‌اعتماد از محصول برای ورود داده درستی‌سنجی احراز هویت (OT.TOE_TC_VAD_Imp) محافظت شده است. هدف امنیتی برای محیط عملیاتی - ارسال داده‌های درنظر گرفته شده برای امضا توسط برنامه کاربردی تولید امضا (OE.DTBS_Intend)، 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)، هدف امنیتی برای محیط عملیاتی کانال قابل‌اعتماد برنامه‌کاربردی ایجاد امضا برای صدور داده‌ای که باید امضا شود (OE.SCA_TC_DTBS_Exp) و هدف امنیتی برای محصول - کانال قابل اعتماد از محصول برای ورود داده‌ای که باید امضا شود (OT.TOE_TC_DTBS_Imp) اطمینان حاصل می‌کنند که محصول امضاهای دیجیتالی را فقط برای داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) تولید می‌کند که صاحب‌امضا تصمیم به امضا به عنوان داده‌ای که باید امضا شود (DTBS) را داشته است.

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) و فرض مدیریت امن داده درستی‌سنجی امضا / داده ایجا امضا توسط تامین‌کننده خدمات صدور گواهی (A.CSP) همان منطق موجود در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – ورود کلید است.

۶- الزامات کارکرد امنیتی

۶-۱- قراردادها

معیار مشترک امکان اجرای چندین عملیات روی الزامات کارکردی را فراهم می‌آورد ازجمله: پالایش[۴۸]، 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.

[۴۸] Refinement

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.

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 – ورود کلید توضیح داده شده است و تنها موارد اضافی در اینجا توضیح داده می‌شوند [۷]:

جدول ۲ الزامات کارکرد امنیتی

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**زمان‌بندی احراز هویت ۱**	FIA_UAU.1.1
۲	**زمان‌بندی احراز هویت ۲**	FIA_UAU.1.2
۳	**یکپارچگی تبادل داده / داده‌ای که باید امضا شود ۱**	FDP_UIT.1.1/DTBS
۴	**یکپارچگی تبادل داده / داده‌ای که باید امضا شود ۲**	FDP_UIT.1.2/DTBS
۵	**کانال قابل‌اعتماد درون توابع هدف امنیتی - کانال قابل‌اعتماد افزاره واسط انسانی / داده درستی‌سنجی امضا ۱**	FTP_ITC.1.1/VAD
۶	**کانال قابل‌اعتماد درون توابع هدف امنیتی - کانال قابل‌اعتماد افزاره واسط انسانی / داده درستی‌سنجی امضا ۲**	FTP_ITC.1.2/VAD

شماره الزام	نام الزام	تطابق الزام با استاندارد
۷	**کانال قابل‌اعتماد درون توابع هدف امنیتی - کانال قابل‌اعتماد افزاره واسط انسانی / داده درستی‌سنجی امضا ۳**	FTP_ITC.1.3/VAD
۸	**کانال درونی قابل‌اعتماد توابع هدف امنیتی - برنامه‌کاربردی ایجاد امضا / داده‌ای که باید امضا شود ۱**	FTP_ITC.1.1/DTBS
۹	**کانال درونی قابل‌اعتماد توابع هدف امنیتی - برنامه‌کاربردی ایجاد امضا / داده‌ای که باید امضا شود ۲**	FTP_ITC.1.2/DTBS
۱۰	**کانال درونی قابل‌اعتماد توابع هدف امنیتی - برنامه‌کاربردی ایجاد امضا / داده‌ای که باید امضا شود ۳**	FTP_ITC.1.3/DTBS

۶-۲- کلاس شناسایی و احرازهویت

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 افزاره واسط انسانی و محصول با استفاده از توابع هدف امنیتی موردنیاز الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی / کانال قابل اعتماد افزاره واسط انسانی،	

(۴) [اختصاص: *فهرستی از اقدامات اضافه‌ای که توابع هدف امنیتی واسطه آن است*][۴۹]

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 موفقیت‌آمیز شناسایی شود.

نکته کاربردی ۵: 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 به افزاره واسط انسانی انجام می‌دهد.

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

۶-۳- کلاس حفاظت از داده‌های کاربر

شماره الزام	نام الزام
۳	**یکپارچگی تبادل داده / داده‌ای که باید امضا شود ۱**
وراثت از هیچ مؤلفه دیگر ندارد وابستگی: [کنترل دسترسی زیرمجموعه[۵۰]، یا کنترل جریان اطلاعات زیرمجموعه[۵۱]] [کانال قابل‌اعتماد درون توابع هدف امنیتی[۵۲]، یا مسیر قابل‌اعتماد[۵۳]] توابع هدف امنیتی باید خط‌مشی کارکرد امنیتی ایجاد امضا[۵۴] را برای دریافت[۵۵] داده کاربر به روش محافظت‌شده از خطاهای تغییر و درج[۵۶] اعمال کنند.	
۴	**یکپارچگی تبادل داده / داده‌ای که باید امضا شود ۲**

[۵۰] FDP_ACC.1

[۵۱] FDP_IFC.1

[۵۲] FTP_ITC.1

[۵۳] FTP_TRP.1

[۵۴] [اختصاص: *خط‌مشی(های) کارکرد امنیتی کنترل دسترسی و یا خط‌مشی(های) کارکرد امنیتی کنترل جریان اطلاعات*]

[۵۵] [انتخاب: *انتقال، دریافت*]

[۵۶] [انتخاب: *تغییر، حذف، درج، بازپخش*]

توابع هدف امنیتی باید قادر به تشخیص اعلام دریافت داده کاربر باشد که چه تغییر و درجی[۵۷] در آن رخ داده است.

۶-۴- کانال‌ها و یا مسیرهای مورد اعتماد

شماره الزام	نام الزام
۵	**کانال قابل‌اعتماد درون توابع هدف امنیتی - کانال قابل‌اعتماد افزاره واسط انسانی / داده درستی‌سنجی امضا ۱**
وراثت از هیچ مؤلفه دیگر ندارد. وابستگی: ندارد توابع هدف امنیتی باید کانال ارتباطی بین خود و دیگر محصولات فناوری اطلاعاتی قابل‌اعتماد افزاره واسط انسانی 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.	
۶	**کانال قابل‌اعتماد درون توابع هدف امنیتی - کانال قابل‌اعتماد افزاره واسط انسانی / داده درستی‌سنجی امضا ۲**
توابع هدف امنیتی باید به دیگر محصولات فناوری اطلاعاتی قابل‌اعتماد از راه دور[۵۸] اجازه آغاز ارتباط از طریق کانال‌های قابل‌اعتماد را بدهد.	
۷	**کانال قابل‌اعتماد درون توابع هدف امنیتی - کانال قابل‌اعتماد افزاره واسط انسانی / داده درستی‌سنجی امضا ۳**
توابع هدف امنیتی و یا افزاره واسط انسانی باید آغازکننده ارتباط از طریق کانال‌های قابل‌اعتماد برای موارد زیر باشد: (۱) احراز هویت داده‌ها با هویت ضامن مطابق با الزامات کارکرد امنیتی زمانبندی احراز هویت،	

[۵۷] [انتخاب: *تغییر، حذف، درج، بازپخش*]

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

(۲) [اختصاص: *فهرستی از توابع موردنیاز دیگر برای یک کانال قابل‌اعتماد*][۵۹].

نکته کاربردی ۶: الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی - کانال قابل‌اعتماد افزاره واسط انسانی / داده درستی‌سنجی امضا برای پشتیبانی از یک کانال قابل‌اعتماد برقرار شده توسط افزاره واسط انسانی جهت ارسال داده درستی‌سنجی امضا، به توابع هدف امنیتی نیاز دارد. نویسنده هدف امنیتی بایستی عملیات ازدست‌رفته در عنصر ۳ الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی - کانال قابل‌اعتماد افزاره واسط انسانی / 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 - کانال قابل‌اعتماد افزاره واسط انسانی / داده درستی‌سنجی امضا "هیچ" است. توجه داشته باشید که داده درستی‌سنجی احراز هویت بسته به روش‌های احراز هویت به‌کار گرفته شده به حفاظت نیاز دارد: داده درستی‌سنجی احراز هویت برای احراز هویت با دانش به حفاظت از محرمانگی نیاز دارد؛ داده درستی‌سنجی احراز هویت برای احراز هویت زیست‌سنجشی ممکن است فقط نیاز به محافظت از یکپارچگی داشته باشد.

۸	**کانال درونی قابل‌اعتماد توابع هدف امنیتی - برنامه‌کاربردی ایجاد امضا / داده‌ای که باید امضا شود ۱**

توابع هدف امنیتی باید کانال ارتباطی بین خود و دیگر محصولات فناوری اطلاعاتی قابل‌اعتماد برنامه‌کاربردی ایجاد امضا 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.

۹	**کانال درونی قابل‌اعتماد توابع هدف امنیتی - برنامه‌کاربردی ایجاد امضا / داده‌ای که باید امضا شود ۲**

توابع هدف امنیتی باید به دیگر محصولات فناوری اطلاعاتی قابل‌اعتماد از راه دور[۶۰] اجازه آغاز ارتباط از طریق کانال‌های قابل‌اعتماد را بدهد.

۱۰	**کانال درونی قابل‌اعتماد توابع هدف امنیتی - برنامه‌کاربردی ایجاد امضا / داده‌ای که باید امضا شود ۳**

توابع هدف امنیتی و یا برنامه‌کاربردی ایجاد امضا باید آغازکننده ارتباط از طریق کانال‌های قابل‌اعتماد برای موارد زیر باشد:

(۱) ایجاد امضا،

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

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

(۲) [اختصاص: *فهرستی از توابع موردنیاز دیگر برای یک کانال قابل‌اعتماد*][۶۱].

نکته کاربردی ۷: الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی - برنامه‌کاربردی ایجاد امضا / داده‌ای که باید امضا شود برای پشتیبانی از یک کانال قابل‌اعتماد برقرار شده توسط برنامه‌کاربردی ایجاد امضا جهت ارسال داده‌ای که باید امضا شود، به توابع هدف امنیتی نیاز دارد. نویسنده هدف امنیتی بایستی عملیات ازدست‌رفته در عنصر ۳ الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی - برنامه‌کاربردی ایجاد امضا / داده‌ای که باید امضا شود 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 - برنامه‌کاربردی ایجاد امضا / داده‌ای که باید امضا شود "تهی" است.

۶-۵- کلاس حفاظت از توابع امنیتی هدف ارزیابی

خانواده افزوده‌ی برون‌تابی محصول (FPT_EMS) از کلاس محافظت از توابع هدف امنیتی (FPT) در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – ورود 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

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

	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 خودکارسازی
	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 هرکدام از اهداف امنیتی برای محصول حداقل توسط یکی از الزامات کارکردی امنیت پوشش داده شده است.

جدول ۴ نگاشت الزامات کارکردی به اهداف امنیتی برای محصول

اهداف هدف امنیتی / الزامات کارکردی	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE _TC_VAD_Imp	OT.TOE _TC_DTBS_Imp
FCS_CKM.4	×		×	×	×						

اهداف هدف امنیتی / الزامات کارکردی	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE _TC_VAD_Imp	OT.TOE _TC_DTBS_Imp
FCS_COP.1	×				×						
FDP_ACC.1/SCD_Import	×	×									
FDP_ACC.1/Signature_Creation	×				×						
FDP_AFC.1/SCD_Import	×	×									
FDP_AFC.1/Signature_Creation	×				×		×				
FDP_ITC.1/SCD	×										
FDP_UCT.1/SCD	×		×								
FDP_RIP.1			×		×		×				
FDP_SDI.2/Persistent			×	×			×				
FDP_SDI.2/DTBS				×	×	×					
FDP_UIT.1/DTBS							×	×			×
FIA_AFL.1					×						
FIA_UAU.1		×			×		×				

اهداف هدف امنیتی / الزامات کارکردی	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE _TC_VAD_Imp	OT.TOE _TC_DTBS_Imp
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_MSA.4	×	×			×		×				
FMT_MTD.1/Admin	×				×		×				
FMT_MTD.1/Signatory	×				×		×				
FMT_SMR.1	×				×		×				
FMT_SMF.1	×				×						

اهداف هدف امنیتی / الزامات کارکردی	OT.Lifecycle_Security	OT.SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE _TC_VAD_Imp	OT.TOE _TC_DTBS_Imp
FPT_EMS.1			×		×		×				
FPT_FLS.1			×								
FPT_PHP.1								×			
FPT_PHP.3			×		×	×			×		
FPT_TST.1	×		×	×							
FTP_ITC.1/SCD	×		×								
FTP_ITC.1/VAD										×	×
FTP_ITC.1/DTBS											

۸-۱-۲-کفایت الزامات امنیتی

منطق موجود در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – ورود کلید همچنان معتبر است. در بخش کفایت الزامات امنیتی محصول پروفایل حفاظتی افزاره ایجاد امضای امن – ورود کلید توضیح می‌دهد که چگونه الزامات کارکرد امنیتی، اهداف امنیتی امنیت چرخه حیات، هدف امنیتی ورود داده ایجاد امضا مجاز، 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 کانال قابل‌اعتماد از محصول برای ورود داده درستی‌سنجی احراز هویت (OT.TOE_TC_VAD_Imp) و هدف امنیتی کانال قابل اعتماد از محصول برای ورود داده‌ای که باید امضا شود (OT.TOE_TC_DTBS_Imp) در ادامه آورده شده است.

هدف امنیتی محصول	شرح
OT.TOE_TC_VAD_Imp کانال قابل‌اعتماد از محصول برای ورود داده درستی‌سنجی احراز هویت	این هدف با الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی - کانال قابل اعتماد افزاره واسط انسانی / داده درستی‌سنجی امضا به منظور فراهم آوردن یک کانال قابل‌اعتماد برای محافظت از داده درستی‌سنجی احراز هویت ارائه شده توسط افزاره واسط انسانی برای محصول تامین شده است.
OT.TOE_TC_DTBS_Imp داده‌ای کانال قابل اعتماد از محصول برای ورود که باید امضا شود	این هدف با الزام کارکرد امنیتی کانال درونی قابل‌اعتماد توابع هدف امنیتی - برنامه‌کاربردی ایجاد امضا / داده‌ای که باید امضا شود، به منظور فراهم آوردن یک کانال قابل‌اعتماد برای محافظت از داده‌ای که باید امضا شود ارائه‌شده توسط برنامه‌کاربردی ایجاد امضا برای محصول و الزام کارکرد امنیتی یکپارچگی تبادل داده / داده‌ای که باید امضا شود تامین شده است که به توابع هدف امنیتی جهت بررسی و تأیید یکپارچگی داده‌ای که باید امضا شود دریافتی نیاز دارد.

۸-۲- برآوردن وابستگی‌های الزامات امنیتی

جدول ۵ برآوردن وابستگی‌های الزامات کارکردی امنیتی

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
FDP_ITC.1/SCD	[FDP_ITC.1 یا FDP_ITC.2 یا FCS_CKM.1]	FCS_CKM.4

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
FDP_ITC.1/SCD, FCS_CKM.4	[FDP_ITC.1 یا FDP_ITC.2 یا FCS_CKM.1], FCS_CKM.4	FCS_COP.1
FDP_ACF.1/SCD_Import	FDP_ACF.1	FDP_ACC.1/SCD_Import
FDP_ACF.1/Signature_Creation	FDP_ACF.1	FDP_ACC.1/Signature_Creation
FDP_ACF.1/SCD_Import, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3	FDP_ACF.1/SCD_Import
FDP_ACF.1/Signature_Creation	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/Signature_Creation, FMT_MSA.3
FDP_ITC.1/SCD	[FDP_ACC.1 یا FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_UCT.1/SCD	[FTP_ITC.1 یا FTP_TRP.1], [FDP_ACC.1 یا FDP_IFC.1]	FPT_ITC.1/SCD, FDP_ACC.1/SCD_Import
FDP_RIP.1	بدون وابستگی	n/a
FDP_SDI.2/Persistent	بدون وابستگی	n/a

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
FDP_SDI.2/DTBS	بدون وابستگی	n/a
FDP_UIT.1/DTBS	[FDP_ACC.1 یا FDP_IFC.1], [FTP_ITC.1 یا FTP_TRP.1]	FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.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 یا FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD_Import, FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Signatory	[FDP_ACC.1 یا 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 یا FDP_IFC.1], FMT_SMR.1, FMT_MSA.1	FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD_Import, FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory

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 یا FDP_IFC.1]	FDP_ACC.1/SCD_Import, 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/SCD	بدون وابستگی	n/a

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
FTP_ITC.1/VAD	بدون وابستگی	n/a
FTP_ITC.1/DTBS	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 سطح تضمین ارزیابی ۴ وجود دارند)

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 آسیب پذیری 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 مدیر سیستمان 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 اصالت 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-0006-2002, 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 14169-3:2012, Protection profiles for secure signature creation device — Part 3: Device with key import

[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