به نام خدا

پروفایل حفاظتی افزاره ایجاد امضای امن-

قسمت ۳: افزاره با ورود کلید

بهمن ماه ۹۵

نسخه ۱,۱

فهرست

۱- مقدمه

این سند که در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک توسط مرکز مدیریت راهبردی افتا و سازمان فناوری اطلاعات ایران تهیه و نهایی شده است، برای بیان الزامات کارکرد امنیتی هر محصول لازم است. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی را که در این سند برای برآورده کردن الزامات 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] با امکان ورود کلیدهای امضا تبیین می‌شود: «افزاره ایجاد امضای امن با ورود کلید (SSCD KI)».

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

هدف از این پروفایل حفاظتی تعیین الزامات کارکرد و تضمین امنیتی تعریف شده در پیوست ۳ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا[۵] برای افزاره‌های ایجاد امضای امن (SSCD) است که محصول[۱] (TOE) که در این سند «محصول» نامیده می‌شود، هستند.

---

[۱] Secure Signature Creation Device (SSCD)

[۲] افزاره ایجاد امضای امنی که SCD/SVD را وارد می‌کند در نسخه‌های قبلی این نمایه حفاظتی (CWA 14169) به عنوان نوع ۲ SSCD تعریف شده است. مفهوم انواع دیگر در این مجموعه از EN ها وجود ندارد. به منظور ارجاع به همان کارکردها، باید به EN14169-3 (به عنوان مثال قسمت ۳) مراجعه شود.

[۳] Signature Creation Data

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

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

این سند الزامات امنیتی اصلی را برای افزاره ایجاد امضای امنی تعریف می‌کند که داده ایجاد امضا (SCD) را وارد می‌کند و امضای الکترونیک پیشرفته ایجاد می‌کند، اگر داده ایجاد امضا بر اساس گواهی‌های معتبر واجد شرایط (معتبر) باشد امضای الکترونیکی واجد شرایط (معتبر) است. تامین‌کننده خدمات صدور گواهی[۲] (CSP) زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) را در یک محیط امن تولید کرده و داده ایجاد امضا (SCD) را برای افزاره ایجاد امضای امن (SSCD) صادر خواهد کرد تا بتواند به امضا کننده‌ای با حداقل یک داده ایجاد امضا (SCD) و اطلاعات گواهی ذخیره‌شده ممکن در افزاره ایجاد امضای امن (SSCD) تحویل داده شود. محصول ممکن است توابع امنیتی اضافه‌ای را به طور مثال برای پشتیبانی حفاظت از یکپارچگی داده وارد شده که باید امضا شود، پیاده‌سازی کند. الزامات امنیتی مرتبط، موضوع این پروفایل حفاظتی اصلی نیستند اما در پروفایل حفاظتی الحاقی «پروفایل حفاظتی افزاره ایجاد امضای امن – قسمت ۶: افزاره با ورود کلید و ارتباط قابل اعتماد با برنامه‌کاربردی ایجاد امضا» آورده شده‌اند.

سطح تضمین این پروفایل حفاظتی، سطح تضمین ارزیابی ۴[۳] (EAL4) 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 می باشد. اصطلاحات زیر در متن برای ارجاع به دستورالعمل استفاده می‌شود:

---

[۱] Target Of Evaluation(در سراسر این سند محصول نامیده می‌شود)

[۲] Certification Service Provider

[۳] 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[۱] (CC)**

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

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

- **سطح تضمین ارزیابی[۲] (EAL)**

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

- **پروفایل حفاظتی[۳] (PP)**

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

- **هدف امنیتی[۱] (ST)**

---

[۱] Common Criteria

[۲] Evaluation Assurance Level

[۳] Protection Profile

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.

- **محصول[۲] (TOE)**

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

- **توابع امنیتی محصول[۳] (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[۴]**

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

- **امضای الکترونیکی پیشرفته[۵]**

---

[۱] Security Target

[۲] Target of Evaluation

[۳] TOE Security Functions

[۴] Administrator

[۵] Advanced electronic signature

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**[۱]

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

- **گواهی**[۲]

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**[۳]

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

---

[۱] Authentication data

[۲] Certificate

[۳] Certificate information

- یک یا چند مقدار چکیده‌ساز[1] 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)**[2]

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**[3] **(CSP)**

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

- **داده‌ای که باید امضا شوند**[4] **(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**[5] **(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[1] قسمت اولیه داده‌ای که باید امضا شود (DTBS) که با قسمت باقیمانده از داده‌ای که باید امضا شود (DTBS) تکمیل شده است، یا

---

[1] hash

[2] Certificate generation application

[3] Certification Service Provider

[4] Data to be signed

[5] Data to be signed or its unique representation

- خود داده‌ای که باید امضا شود (DTBS).

- **کاربر مجاز**[۲]

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**[۳]

نهاد سازمانی که توسط یک کشور عضو اتحادیه اروپا به‌عنوان مسئول اعطای مجوز رسمی[۴] 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).

---

[۱] intermediate

[۲] Legitimate user

[۳] Notified body

[۴] accreditation

- **داده احرازهویت مرجع[1] (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[2] (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[3]**

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[4]**

اطلاعات افزوده‌ای که همراه با پیام کاربر امضا می‌شود.

- **برنامه‌کاربردی ایجاد امضا[5] (SCA)**

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

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

- ارائه داده‌ای که باید امضا شود (DTBS) جهت بازنگری توسط صاحب‌امضا،
- گرفتن تصمیم توسط صاحب‌امضا قبل از فرایند امضا،

---

[1] Reference Authentication data

[2] Secure signature creation device

[3] Signatory

[4] Signature attributes

[5] Signature creation application

- 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[1] (SCD)**

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

- **سامانه ایجاد امضا[2] (SCS)**

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

- **داده درستی‌سنجی امضا[3] (SVD)**

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

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

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

- **کاربر**

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

---

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

- **پیام کاربر**

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

- **داده درستی‌سنجی احرازهویت[1] (VAD)**

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

۳- شرح محصول

۳-۱- عملکرد محصول

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

۳-۱-۱- محیط آماده‌سازی

جایی است که محصول برای ورود داده ایجاد امضا (SCD) از طریق برنامه‌کاربردی تولید داده ایجاد امضا / داده درستی‌سنجی 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. برنامه‌کاربردی تولید داده ایجاد امضا / داده درستی‌سنجی امضا، داده درستی‌سنجی امضای (SVD) را به برنامه‌کاربردی تولید گواهی (CGA) انتقال می‌دهد. محیط مقداردهی اولیه بیشتر برای شخصی‌سازی محصول با مقادیر اولیه داده احراز هویت مرجع (RAD) با محصول تعامل می‌کند.

۳-۲- 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:

[1] Verification authentication data

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

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).

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

[۱] correspondent

احزار هویت (VAD) یک کلمه‌عبور یا پین[1] 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).

۳-۲-۱-محیط امضا

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

۳-۲-۲- محیط‌های مدیریتی

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 ۳ 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) رابطی برای امضا کننده فراهم می‌آورد تا یک داده ایجاد امضا (SCD) را برای استفاده در تابع ایجاد امضای افزاره ایجاد امضای امن (SSCD) بکار گیرد. محصول از محرمانگی و یکپارچگی داده ایجاد امضا (SCD) محافظت کرده و استفاده از آن را محدود به ایجاد امضا توسط صاحب‌امضای خودش می‌کند. امضای دیجیتال ایجاد شده توسط محصول

[1] PIN

ممکن است برای ایجاد یک امضای الکترونیک پیشرفته به گونه‌ای که در ماده ۵,۱ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا تعریف شده مورد استفاده قرار گیرد. 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، 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[1])، 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 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 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:

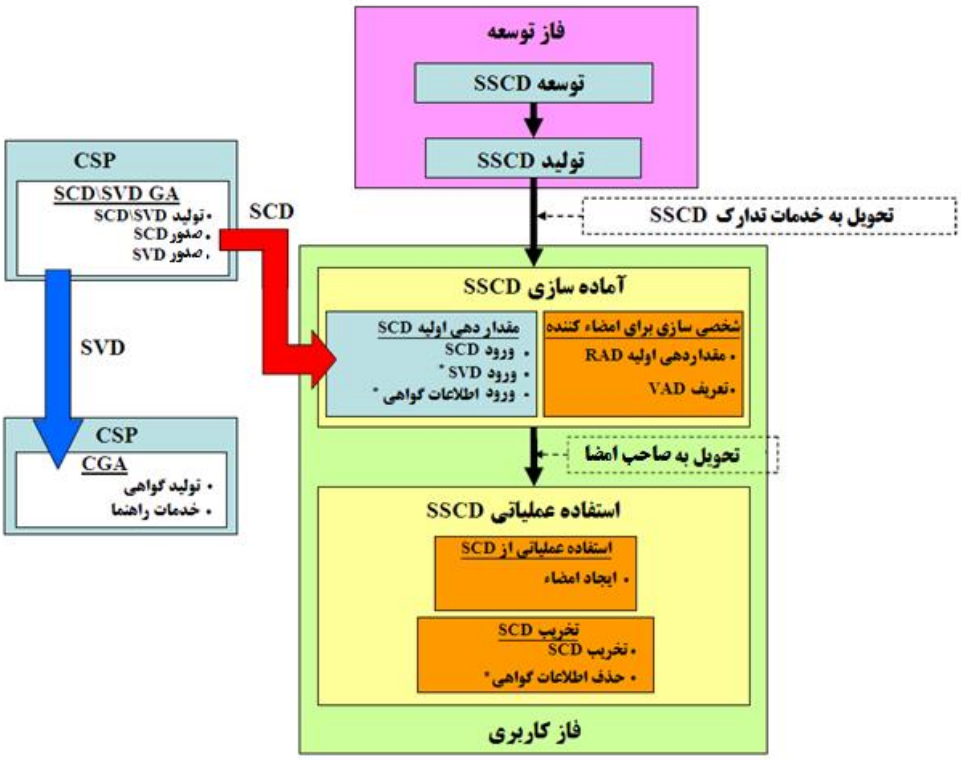
- مقدار دهی اولیه به داده احراز هویت مرجع (RAD)،
- تولید یک زوج کلید،
- ذخیره‌سازی اطلاعات شخصی کاربر مجاز.

[1] PIN

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- چرخه‌حیات محصول

چرخه‌حیات محصول مراحل توسعه، آماده‌سازی و استفاده عملیاتی را متمایز می‌کند. لطفاً توجه داشته باشید که زمانی که این پروفایل حفاظتی توسط دیگر پروفایل‌های حفاظتی ادعا می‌شود تعاریف دیگری از چرخه حیات نیز ممکن است (به طور مثال برای افزاره ایجاد امضای امنی که ارتباط قابل‌اعتمادی با برنامه‌کاربردی ایجاد امضا ارائه می‌دهد).



شکل ۱ نمونه‌ای از چرخه حیات محصول

فاز توسعه شامل توسعه و تولید محصول است. فاز توسعه طبق کلاس چرخه حیات تضمین[1] (ALC) موضوع ارزیابی است. فاز توسعه با تحویل محصول به خدمات تدارک افزاره ایجاد امضای امن (SSCD) پایان می‌یابد.

کاربری عملیاتی محصول شامل مرحله آماده‌سازی و مرحله استفاده عملیاتی است. مرحله استفاده عملیاتی محصول زمانی آغاز می‌شود که صاحب‌امضا داده درستی‌سنجی احراز هویت (VAD) و محصول را به دست آورده باشد. فعال کردن محصول برای امضا کردن، به حداقل یک مجموعه از داده ایجاد امضا (SCD) ذخیره شده در حافظه‌اش نیاز دارد.

شکل ۱ مثالی از چرخه حیات را نشان می‌دهد که در آن یک داده ایجاد امضا (SCD) یا زوج داده ایجاد امضا / داده درستی‌سنجی امضا قبل از تحویل به صاحب‌امضا از خدمات تدارک افزاره ایجاد امضای امن (SSCD) وارد شده‌اند. ممکن است چرخه حیات اجازه ورود داده ایجاد امضا (SCD) یا زوج کلیدهای داده ایجاد امضا / داده درستی‌سنجی امضا را بعد از تحویل به صاحب‌امضا بدهد.

۳-۳-۱- مرحله آماده‌سازی

مرحله آماده‌سازی چرخه حیات محصول شامل پردازش محصول از پذیرش محصول تحویل داده‌شده به مشتری توسط او تا حالت آماده عملیات توسط صاحب‌امضا می‌شود. مشتری‌ای که محصول را از سازنده دریافت می‌کند خدمات تدارک افزاره ایجاد امضای امنی (SSCD) است که افزاره ایجاد امضای امن (SSCD) را آماده کرده و به مشترکان ارائه می‌دهد. آماده‌سازی شامل موارد زیر است:

۱) شخصی‌سازی محصول برای استفاده توسط صاحب‌امضا به طور مثال مقداردهی اولیه داده احراز هویت مرجع (RAD) در محصول و تحویل داده درستی‌سنجی احراز هویت (VAD) به صاحب‌امضا.

۲) مقداردهی اولیه محصول به عنوان مثال، تامین‌کننده خدمات صدور گواهی (CSP) زوج داده ایجاد امضا / داده درستی‌سنجی امضا را به وسیله یک افزاره تولید داده ایجاد امضا / داده درستی‌سنجی امضا تولید می‌کند، داده ایجاد امضا (SCD) را برای محصول بارگذاری می‌کند، و

[1] assurance lifecycle class

داده درستی‌سنجی امضا (SVD) را به برنامه‌کاربردی تولید گواهی (CGA) ارسال می‌کند. محصول ممکن است زوج داده ایجاد امضا / داده درستی‌سنجی امضا را وارد و ذخیره کند.

۳) تولید گواهی (واجد شرایط) از میان موارد دیگر شامل موارد زیر است (مراجعه شود به پیوست ۲ منبع [۱])

أ. داده درستی‌سنجی امضا (SVD) متناظر با داده ایجاد امضا (SCD) که تحت کنترل صاحب‌امضا است؛

ب. نام صاحب‌امضا و یا یک نام مستعار، که به این عنوان شناخته خواهد شد،

ج. نشانه‌ای از آغاز و پایان دوره زمانی اعتبار گواهی.

۴) آماده‌سازی ممکن است شامل بارگذاری اختیاری اطلاعات گواهی در افزاره ایجاد امضای امن (SSCD) برای راحتی صاحب‌امضا باشد.

تامین‌کننده خدمات صدور گواهی (CSP) زوج داده ایجاد امضا / داده درستی‌سنجی امضا را تولید و داده ایجاد امضا (SCD) و داده درستی‌سنجی امضا (SVD) را به صورت اختیاری وارد افزاره ایجاد امضای امن (SSCD) می‌کند، تامین‌کننده خدمات صدور گواهی (CSP) اطمینان حاصل می‌کند که:

أ. بین داده ایجاد امضا (SCD) و داده درستی‌سنجی امضا (SVD) مطابقت وجود دارد،

ب. الگوریتم و اندازه کلید داده درستی‌سنجی امضا (SVD) مناسب هستند.

لطفاً توجه داشته باشید که تأیید این که آیا هویت ادعا شده امضا کننده از چیزی که افزاره ایجاد امضای امن (SSCD) داده است سرچشمه می‌گیرد باید توسط تامین‌کننده خدمات صدور گواهی (CSP) استفاده‌کننده از برنامه‌کاربردی تولید گواهی (CGA) است صورت گیرد.

اگر محصول برای ایجاد امضای الکترونیک پیشرفته مورد استفاده قرار گیرد گواهی، داده درستی‌سنجی امضا را به فرد (به طور مثال صاحب‌امضا) پیوند می‌دهد و هویت آن فرد را تأیید می‌کند (مراجعه شود به منبع [۱]، ماده ۲، بند ۹).

این پروفایل حفاظتی به محصول برای ارائه سازوکارهایی برای ورود داده ایجاد امضا (SCD)، پیاده‌سازی داده ایجاد امضا (SCD) و شخصی‌سازی نیاز دارد. فرض می‌شود که محیط از همه فرایندهای دیگر برای آماده‌سازی محصول محافظت می‌کند به عنوان مثال انتقال داده ایجاد امضا (SCD) بین افزاره تولید داده

ایجاد امضا / داده درستی‌سنجی امضا و محصول، و انتقال داده درستی‌سنجی امضا (SVD) بین افزاره تولید داده ایجاد امضا / داده درستی‌سنجی امضا و برنامه‌کاربردی تولید گواهی (CGA). تامین‌کننده خدمات صدور گواهی (CSP) ممکن است داده درستی‌سنجی امضا (SVD) را برای استفاده داخلی توسط محصول (به طور مثال، خود آزمایی) به محصول صادر کند.

قبل از تولید یک گواهی (واجد شرایط)، انتظار می‌رود تامین‌کننده خدمات صدور گواهی (CSP) ابتدا داده ایجاد امضا (SCD)را در یک افزاره ایجاد امضای امن (SSCD) ذخیره کند. یک کانال امن ممکن است برای پشتیبانی از این فرایند مورد استفاده محصول قرار گیرد که از یکپارچگی داده ایجاد امضا (SCD) در طول انتقال به محصول اطمینان می‌یابد.

۳-۳-۲- مرحله استفاده عملیاتی

در این مرحله از چرخه حیات، صاحب‌امضا می‌تواند از محصول برای ایجاد امضای الکترونیک پیشرفته استفاده کند.

فاز عملیاتی محصول زمانی آغاز می‌شود که حداقل یک زوج داده ایجاد امضا / داده درستی‌سنجی امضا توسط تامین‌کننده خدمات صدور گواهی (CSP) تولید شده باشد و داده ایجاد امضا (SCD) به افزاره ایجاد امضای امن (SSCD) وارد شده و صاحب‌امضا بر محصول کنترل دارد و داده ایجاد امضا (SCD) را عملیاتی می‌سازد. صاحب‌امضا محصول را تنها همراه با یک برنامه‌کاربردی ایجاد امضا (SCA) قابل‌اعتماد در یک محیط امن مورد استفاده قرار می‌دهد. فرض می‌شود برنامه‌کاربردی ایجاد امضا (SCA) در طول انتقال به محصول از داده‌ای که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن (DTBS/R) محافظت می‌کند.

صاحب‌امضا همچنین می‌تواند با افزاره ایجاد امضای امن (SSCD) برای انجام وظایف مدیریتی تعامل داشته باشد، به عنوان مثال زمانی که کلمه‌عبور یا پین در داده مرجع از بین رفت و یا مسدود شده باشد مقدار داده احراز هویت مرجع (RAD) را مجدداً تنظیم می‌کند و یا از شمارنده استفاده می‌کند. چنین وظایف مدیریتی‌ای نیازمند یک محیط امن است.

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

محصول ممکن است از توابع تولید کلیدهای امضای اضافی پشتیبانی کند. اگر محصول این کارکردها را پشتیبانی کند از کارکردهای بیشتری برای کسب امن گواهی برای کلیدهای جدید پشتیبانی خواهد کرد.

برای یک کلید اضافی ممکن است صاحب‌امضا اجازه انتخاب نوع گواهی (واجد شرایط و یا فاقد شرایط) را برای به دست آوردن داده درستی‌سنجی امضا (SVD) از کلید جدید داشته باشد. همچنین ممکن است صاحب‌امضا اجازه داشته باشد برخی از داده‌ها را هنگام درخواست گواهی انتخاب کند به عنوان مثال استفاده از اسم مستعار به جای نام قانونی در گواهی[1]. چنانچه شرایط کسب یک گواهی واجد شرایط برآورده شود، کلید جدید نیز برای ایجاد امضاهای الکترونیک پیشرفته قابل استفاده است. توابع اختیاری محصول برای تولید کلید اضافی و گواهی ممکن است نیازمند توابع امنیتی اضافی در محصول و تعامل با تأمین کننده خدمات تدارک افزاره ایجاد امضای امن (SSCD) در یک محیط امن باشد.

چرخه حیات محصول به عنوان افزاره ایجاد امضای امن (SSCD) زمانی به پایان می‌رسد که تمام داده‌های ایجاد امضای (SCD) ذخیره شده در محصول از بین بروند. این ممکن است شامل حذف گواهی‌های متناظر باشد.

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.

۴-۱-۱- دارایی‌ها و موجودیت‌های غیرفعال

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

۲.داده درستی‌سنجی امضا (SVD): کلید عمومی پیوند داده شده به داده ایجاد امضا (SCD) است که برای انجام درستی‌سنجی امضای 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

---

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

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[۱] ممکن است به عنوان موجودیت فعال مدیر سیستم[۲] در نقش مدیر سیستم[۳] و یا به عنوان موجودیت فعال صاحب‌امضا[۴] در نقش صاحب‌امضا[۵] ایفای نقش کند.

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.

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

تهدیدات	توضیحات

[۱] S.User

[۲] S.Admin

[۳] R.Admin

[۴] S.Sigy

[۵] R.Sigy

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

۴-۳- خط‌مشی‌های امنیت سازمانی

خط‌مشی‌ها	توضیحات

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

۴-۴- مفروضات

مفروضات	توضیحات
A.CGA	برنامه‌کاربردی تولید گواهی (CGA) از اصالت‌سنجی نام و یا اسم مستعار صاحب‌امضا و داده درستی‌سنجی امضا (SVD) در گواهی (واجد شرایط) توسط امضای الکترونیکی پیشرفته تامین‌کننده خدمات صدور گواهی (CSP) محافظت می‌کند.
A.SCA	صاحب‌امضا تنها از یک برنامه‌کاربردی ایجاد امضا (SCA) قابل‌اعتماد استفاده می‌کند. برنامه‌کاربردی ایجاد امضا (SCA) از داده‌هایی که صاحب‌امضا می‌خواهد امضا نماید داده‌ای که باید امضا شود یا بازنمایی منحصر به فرد متعلق به آن (DTBS/R) را به شکل مناسبی برای امضا کردن توسط محصول تولید و ارسال می‌کند.
A.CSP	تامین‌کننده خدمات صدور گواهی (CSP) تنها از افزاره‌های قابل‌اعتماد برای تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) استفاده می‌کند و اطمینان می‌یابد که این افزاره تنها مورد استفاده کاربر مجاز قرار خواهد گرفت. تامین‌کننده خدمات صدور گواهی (CSP) اطمینان حاصل می‌کند که داده ایجاد امضا (SCD) تولید شده عملاً تنها یکبار رخ می‌دهد، این داده ایجاد امضا (SCD) تولید شده و داده درستی‌سنجی امضا (SVD) در عمل با هم مطابقت دارند و این داده ایجاد امضا (SCD) را نمی‌توان از داده درستی‌سنجی امضا (SVD) استنتاج کرد. تامین‌کننده خدمات صدور گواهی (CSP) از محرمانگی داده ایجاد امضا (SCD) را در طول تولید و صادر شدن به محصول اطمینان می‌یابد، از داده ایجاد امضا (SCD) برای ایجاد هیچ امضایی استفاده نمی‌کند و داده ایجاد امضا (SCD) را بعد از صدور به محصول در محیط عملیاتی به شکل برگشت ناپذیری حذف می‌کند.

۵- اهداف امنیتی

۵-۱- کلیات

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

۵-۲- اهداف امنیتی برای محصول

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

تعدادی از اهداف امنیتی محصول این پروفایل حفاظتی عیناً همان‌هایی هستند که در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید تعریف شده‌اند، این اهداف امنیتی مستقل از این واقعیت هستند که آیا داده ایجاد امضا (SCD) از محیط عملیاتی وارد شده و یا توسط خود محصول تولید شده است و شامل موارد زیر هستند:

هدف امنیتی امنیت چرخه‌حیات (OT.Lifecycle_Security)، 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_I)، هدف امنیتی مقاومت در برابر دست‌کاری (OT.Tamper_Resistance).

اهداف امنیتی زیر مربوط به محصول در پروفایل حفاظتی اصلی افزاره ایجاد امضای امن – تولید کلید در این پروفایل حفاظتی مورد نیاز نیستند چرا که تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) بیرون از محصول اتفاق می‌افتد.

هدف امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) مجاز (OT.SCD/SVD_Auth_Gen)، هدف امنیتی یکتایی داده ایجاد امضا (OT.SCD_Unique) و هدف امنیتی تناظر بین داده درستی‌سنجی امضا و داده ایجاد امضا (OT.SCD_SVD_Corresp).

هدف امنیتی	توضیحات
OT.Lifecycle_Security CGA امنیت چرخه‌حیات	محصول باید نقص‌ها را در طول مقداردهی اولیه، شخصی‌سازی و کاربری عملیاتی تشخیص دهد. محصول باید قابلیت کارکردی تخریب امن داده ایجاد امضا (SCD) را فراهم آورد. **نکته کاربردی ۱:** محصول ممکن است بیش از یک مجموعه داده ایجاد امضا (SCD) را دربرداشته باشد. هیچ نیازی به تخریب داده ایجاد امضا (SCD) در موارد تولید مجدد داده ایجاد امضا (SCD) نیست. صاحب‌امضا باید به عنوان مثال بعد از منقضی‌شدن گواهی (واجد شرایط) برای داده درستی‌سنجی امضا (SVD) متناظر قادر به تخریب داده ایجاد امضا (SCD) ذخیره شده در افزاره امن ایجاد امضا (SSCD) باشد.
OT.SCD_Auth_Imp ورود داده ایجاد امضا مجاز	محصول باید ویژگی‌های امنیتی ارائه دهد تا اطمینان حاصل کند که تنها کاربران مجاز ممکن است ورود داده ایجاد امضا (SCD) را فراخوانی کنند.
OT.SCD_Secrecy رازمانی داده ایجاد امضا	رازمانی[۱] داده ایجاد امضا (SCD) (استفاده شده برای ایجاد امضا) بایستی به صورت قابل قبولی در مقابل حملات با پتانسیل بالای حمله بیمه شود. **نکته کاربردی ۲:** محصول باید محرمانگی داده ایجاد امضا (SCD) را در هر زمانی به خصوص در طول تولید داده ایجاد امضا (SCD)، عملیات امضای داده ایجاد امضا (SCD)، انبارش و تخریب امن حفظ کند
OT.Sig_Secure امنیت رمزنگاری امضای الکترونیک	محصول باید امضاهای دیجیتالی را تولید کند که بدون دانستن داده ایجاد امضا (SCD) از طریق تکنیک‌های رمزنگاری قوی، قابل جعل کردن نباشد. داده ایجاد امضا (SCD) نباید با استفاده از امضاهای دیجیتال یا هر داده دیگر صادرشده از محصول قابل بازسازی باشد. امضاهای دیجیتالی باید در مقابل این حملات مقاوم باشند، حتی اگر با پتانسیل بالایی برای حمله اجرا می‌شوند.
OT.Sigy_SigF تابع ایجاد امضا تنها برای صاحب‌امضای قانونی	محصول باید تابع ایجاد امضای دیجیتالی را تنها برای صاحب‌امضای قانونی فراهم آورده و از داده ایجاد امضا (SCD) در برابر استفاده دیگران محافظت کند. محصول باید در برابر حملات با پتانسیل بالای حمله مقاوم باشد.

۱ Secrecy

OT.DTBS_Integrity_TOE یکپارچگی داده‌ای که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن درون هدف ارزیابی	محصول نباید داده‌ای را که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن (DTBS/R) را تغییر دهد، این هدف در تضاد با فرایند ایجاد امضایی نیست که در آن محصول از داده‌ای که باید امضا شود (DTBS) و برای ایجاد امضا (به صورت جزئی یا به صورت کامل) ارائه شده‌است چکیده‌سازی می‌کند.
OT.EMSEC_Design ارائه امنیت برون‌تابی‌های فیزیکی	محصول باید به روشی طراحی و ساخته شود که تولید برون‌تابی‌های[1] معلوم را در محدوده‌های مشخص کنترل کند.
OT.Tamper_ID آشکارسازی دست‌کاری	محصول باید ویژگی‌های سامانه‌ای را ارائه دهد که دست‌کاری فیزیکی مؤلفه‌هایش را تشخیص داده و از آن ویژگی‌ها برای محدود کردن رخنه‌های امنیتی استفاده کند.
OT.Tamper_Resistance مقاومت در برابر دست‌کاری	محصول باید در مقابل دست‌کاری‌های فیزیکی افزاره‌ها و مؤلفه‌های سامانه مشخص، جلوگیری یا مقاومت کند.

۵-۳- اهداف امنیتی برای محیط عملیاتی

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

اهداف امنیتی برای محیط عملیاتی در این پروفایل حفاظتی که عیناً در پروفایل حفاظتی افزاره ایجاد امضای امن – تولید کلید عنوان شده‌اند. این اهداف امنیتی مستقل از این حقیقت هستند که آیا داده ایجاد امضا (SCD) از محیط عملیاتی وارد شده یا توسط خود محصول تولید شده است وشامل موارد زیر هستند؛

هدف امنیتی تولید داده ایجاد امضا / داده درستی‌سنجی امضا (OE.SCD/SVD_Gen)، 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 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)، هدف امنیتی التزام امنیتی صاحب‌امضا (OE.Signatory).

[1] physical-emanation

چهار هدف امنیتی باقیمانده زیر که در این پروفایل حفاظتی بیان شده است در پروفایل حفاظتی افزاره ایجاد امضای امن – تولید کلید ارائه نشده‌اند، چرا که این اهداف امنیتی تنها زمانی کاربردی هستند که محصول ورود کلید را پشتیبانی کند:

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 محیط عملیاتی	توضیحات
OE.SCD/SVD_Auth_Gen تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا مجاز	تامین‌کننده خدمات صدور گواهی (CSP) باید ویژگی‌های امنیتی فراهم آورد تا از این موضوع اطمینان حاصل شود که تنها کاربران مجاز می‌توانند تولید داده ایجاد امضا (SCD) و داده درستی‌سنجی امضا (SVD) را فراخوانی کنند.
OE.SCD_Secrecy رازمانی داده ایجاد امضا	تامین‌کننده خدمات صدور گواهی (CSP) باید از محرمانگی داده ایجاد امضا (SCD) در طول تولید و صدور به محصول محافظت کند. تامین‌کننده خدمات صدور گواهی (CSP) نباید از داده ایجاد امضا (SCD) برای ایجاد هیچ امضایی استفاده کند و باید داده ایجاد امضا (SCD) را در محیط عملیاتی پس از صدور به محصول به شکل برگشت ناپذیری حذف نماید.
OE.SCD_Unique یکتایی داده ایجاد امضا	تامین‌کننده خدمات صدور گواهی (CSP) باید از کیفیت رمزنگاری زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SVD/SCD) تولید شده در محیط برای امضای الکترونیکی پیشرفته و یا واجد شرایط اطمینان حاصل کند. داده ایجاد امضا (SCD) مورد استفاده برای ایجاد امضا باید عملاً فقط یکبار رخ دهد به طور مثال احتمال داده‌های ایجاد امضا (SCD) یکسان باید قابل چشم‌پوشی باشد و داده ایجاد امضا (SCD) نباید از داده درستی‌سنجی امضا (SVD) قابل بازسازی باشد.
OE.SCD_SVD_Corresp تناظر بین داده درستی‌سنجی امضا و داده ایجاد امضا	تامین‌کننده خدمات صدور گواهی (CSP) باید از مطابقت بین داده درستی‌سنجی امضا (SVD) و داده ایجاد امضای (SCD) تولید شده توسط تامین‌کننده خدمات صدور گواهی (CSP) اطمینان حاصل کند. این شامل تناظر بین داده درستی‌سنجی امضا (SVD) ارسالی به برنامه‌کاربردی تولید گواهی (CGA) و داده ایجاد امضا (SCD) صادر شده به محصول صاحب‌امضای شناسایی‌شده در گواهی داده درستی‌سنجی امضا (SVD) است.
OE.SVD_Auth اصالت‌سنجی داده درستی‌سنجی امضا	محیط عملیاتی باید از اصالت‌سنجی داده درستی‌سنجی امضا (SVD) فرستاده شده از تامین‌کننده خدمات صدور گواهی (CSP) به برنامه‌کاربردی تولید گواهی (CGA) اطمینان حاصل کند. برنامه‌کاربردی تولید گواهی (CGA)، تناظر بین داده ایجاد امضا (SCD) در افزاره ایجاد امضای امن (SSCD) صاحب‌امضا و داده درستی‌سنجی امضا (SVD) در گواهی واجد شرایط را بررسی می‌کند.

OE.CGA_QCert تولید گواهی واجد شرایط	برنامه‌کاربردی تولید گواهی (CGA) باید یک گواهی واجد شرایط شامل موارد زیر را تولید کند: أ. نام صاحب‌امضای کنترل‌کننده محصول، ب. داده درستی‌سنجی امضا (SVD) منطبق بر داده ایجاد امضای (SCD) ذخیره شده در محصول تحت کنترل انحصاری صاحب‌امضا، ج.امضای پیشرفته تامین‌کننده خدمات صدور گواهی (CSP). برنامه‌کاربردی تولید گواهی (CGA) باید با گواهی واجد شرایط تولیده‌شده تصدیق کند که داده ایجاد امضا (SCD) متناظر با داده درستی‌سنجی امضا (SVD) در افزاره ایجاد امضای امن (SSCD) ذخیره شده است.
OE.SSCD_prov_ Service ایجاد امضای امن موثق ارائه شده توسط خدمات تدارک افزاره ایجاد امضای امن	خدمات تدارک افزاره ایجاد امضای امن (SSCD) باید برای صاحب‌امضا نسخه موثقی از محصول را مقداردهی اولیه و شخصی‌سازی کند و این نسخه را به عنوان افزاره ایجاد امضای امن (SSCD) به صاحب‌امضا تحویل دهد.
OE.HID_VAD حفاظت از داده درستی‌سنجی احرازهویت	اگر یک افزاره خارجی رابط انسانی برای احرازهویت کاربر فراهم آورد، این افزاره باید از محرمانگی و یکپارچگی داده درستی‌سنجی احراز هویت (VAD) به گونه‌ای اطمینان حاصل کند که مورد نیاز روش احرازهویت استفاده‌شده از ورود از طریق رابط انسانی‌اش تا ورود از طریق رابط محصول می‌باشد. به خصوص زمانی که محصول برای ورود داده درستی‌سنجی احراز هویت (VAD) به کانال قابل‌اعتماد نیاز دارد، افزاره رابط انسانی[1] (HID) باید کاربری این کانال قابل‌اعتماد را پشتیبانی کند.

[1] Human Interface Device

OE.DTBS_Intend ارسال داده در نظر گرفته شده برای امضا توسط برنامه‌کاربردی ایجاد امضا	صاحب‌امضا باید از برنامه‌کاربردی ایجاد امضا (SCA) قابل‌اعتمادی استفاده کند که: أ. داده‌ای که باید امضا شود یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) را از داده‌ای تولید می‌کند که به عنوان داده‌ای که باید امضا شود (DTBS) ارائه شده و صاحب‌امضا آن را برای امضا در نظر گرفته است به شکلی که برای امضا کردن توسط محصول مناسب است. ب. داده‌ای که باید امضا شود یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) را به محصول می‌فرستد و درستی‌سنجی یکپارچگی داده‌ای که باید امضا شود یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) توسط محصول را فعال می‌سازد. ج.امضای تولید شده توسط محصول را به داده‌ها پیوست می‌کند و یا آن را به شکل جداگانه‌ای ارائه می‌دهد. **نکته کاربردی ۳:** برنامه‌کاربردی ایجاد امضا (SCA) باید قادر به پشتیبانی از امضای الکترونیک پیشرفته باشد. در حال حاضر سه قالب موجود تعریف شده توسط مؤسسه استانداردهای مخابراتی اروپا[۱] (ETSI) برای برآوردن الزامات مورد نیاز توسط امضاهای الکترونیک پیشرفته تشخیص داده شده است: امضای الکترونیک پیشرفته نحو پیام رمزنگاری[۲] (CadES)، امضای الکترونیک پیشرفته زبان نشانه‌گذاری توسعه‌پذیر[۳] (XadES) و امضای الکترونیک پیشرفته قالب فایل قابل‌حمل[۴] (PadES). این سه قالب گنجاندن چکیده‌پیام گواهی کلید عمومی امضاکننده را در داده‌ای که باید امضا شوند اجباری می‌کنند. به منظور پشتیبانی از تحرک امضاکننده، توصیه می‌شود اطلاعات گواهی روی افزاره ایجاد امضای امن (SSCD) ذخیره گردد تا توسط برنامه‌کاربردی ایجاد امضا (SCA) و برای شناسایی داده ایجاد امضا (SCD) متناظر هنگامی که بیش از یک داده ایجاد امضا (SCD) بر روی افزاره ایجاد امضای امن (SSCD) ذخیره شده است مورد استفاده قرار گیرد.

[۱] European Telecommunications Standards Institute

[۲] CMS (Cryptographic Message Syntax) Advanced Electronic Signatures

[۳] XML (Extensible Markup Language) Advanced Electronic Signatures

[۴] PDF (Portable Document Format) Advanced Electronic Signatures

OE.DTBS_Protect محافظت از داده‌های در نظر گرفته شده برای امضا توسط برنامه‌کاربردی ایجاد امضا	محیط عملیاتی باید اطمینان حاصل کند که داده‌ای که باید امضا شود یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) در گذر بین برنامه‌کاربردی ایجاد امضا (SCA) و محصول تغییر نخواهد کرد. به خصوص، هنگامی که محصول به کانال قابل‌اعتمادی برای ورود داده‌ای که باید امضا شود یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) نیاز دارد، برنامه‌کاربردی ایجاد امضا (SCA) باید کاربری این کانال قابل‌اعتماد را پشتیبانی کند
OE.Signatory التزام امنیتی صاحب‌امضا	صاحب‌امضا باید بررسی کند که داده ایجاد امضا (SCD) ذخیره شده در افزاره ایجاد امضای امن (SSCD) که از خدمات تدارک افزاره ایجاد امضای امن (SSCD) دریافت شده است، در حالت غیر عملیاتی قرار دارد. صاحب‌امضا باید محرمانگی داده درستی‌سنجی احرازهویت (VAD) خود را حفظ کند.

۵-۴- منطق اهداف امنیتی

۵-۴-۱- پیمایش معکوس اهداف امنیتی

جدول ۱ نگاشت تعریف مسأله امنیتی به اهداف امنیتی

	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	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.CGA_QCert	OE.SVD_Auth	OE.Dev_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory
T.SCD_Divulg		×	×							×	×									
T.SCD_Derive				×								×								
T.Hack_Phys			×				×	×	×											
T.SVD_Forgery													×		×					×
T.SigF_Misuse	×				×	×											×	×	×	×
T.DTBS_Forgery						×												×	×	
T.Sig_Forgery				×								×		×						
P.CSP_QCert	×	×								×			×	×					×	
P.QSign				×	×									×				×		

	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	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp	OE.CGA_QCert	OE.SVD_Auth	OE.Dev_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory
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

تهدیدات اهداف امنیتی	توضیحات

T.SCD_Divulg تهدید ذخیره‌سازی، نسخه‌برداری و انتشار داده ایجاد امضا	همانگونه که در بند (۱۸) دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا آمده است تهدیدات را در برابر اعتبار قانونی امضای الکترونیک به علت انبارش و نسخه‌برداری از داده ایجاد امضا (SCD) بیرون از محصول مورد توجه قرار می‌دهد [۱]. این تهدید با موارد زیر مورد مقابله قرار می‌گیرد: - هدف امنیتی برای محیط عملیاتی – رازمانی داده ایجاد امضا (OE.SCD_Secrecy)، که از رازمانی داده ایجاد امضا (SCD) در محیط تامین‌کننده خدمات صدور گواهی (CSP) اطمینان حاصل می‌کند. - هدف امنیتی برای محصول – رازمانی داده ایجاد امضا (OT.SCD_Secrecy)، که از رازمانی داده ایجاد امضا (SCD) در طول استفاده توسط محصول برای ایجاد امضا، اطمینان حاصل می‌کند. علاوه بر این، تولید و یا ورود داده ایجاد امضا (SCD) شناخته‌شده توسط یک مهاجم با استفاده از هدف امنیتی برای محیط عملیاتی - تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا مجاز (OE.SCD/SVD_Auth_Gen) و هدف امنیتی برای محصول - ورود داده ایجاد امضا مجاز (OT.SCD_Auth_Imp) مقابله می‌شود، که هدف امنیتی برای محیط عملیاتی - تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا مجاز (OE.SCD/SVD_Auth_Gen) اطمینان حاصل می‌کند که تنها تولید داده ایجاد امضا (SCD) مجاز در محیط امکان پذیر است، و هدف امنیتی برای محصول - ورود داده ایجاد امضا (SCD) مجاز (OT.SCD_Auth_Imp) اطمینان حاصل می‌کند که تنها ورود داده ایجاد امضا (SCD) مجاز ممکن است.

T.SCD_Derive تهدید استخراج داده ایجاد امضا	این تهدید که با حمله‌هایی روی داده ایجاد امضا (SCD) سروکار دارد که از طریق داده عمومی شناخته‌شده که داده درستی‌سنجی امضا (SVD) و امضاهای ایجاد شده با داده ایجاد امضا (SCD) هستند و توسط محصول تولید شده‌اند صورت می‌گیرند. هدف امنیتی برای محیط عملیاتی - یکتایی داده ایجاد امضا (OE.SCD_Unique) با پیاده‌سازی تولید امن رمزنگاری‌شده زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SVD/SCD) با این تهدید مقابله می‌کند. هدف امنیتی برای محصول - امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure)، از امضاهای الکترونیک امن رمزنگاری‌شده اطمینان حاصل می‌کند.
T.Hack_Phys تهدید بهره‌برداری از آسیب‌پذیری‌های فیزیکی	این تهدید با حملات فیزیکی‌ای سر وکار دارد که از آسیب‌پذیری‌های فیزیکی محصول بهره‌برداری می‌کند. هدف امنیتی برای محصول - رازمانی داده ایجاد امضا (OT.SCD_Secrecy) از رازمانی داده ایجاد امضا (SCD) را محافظت می‌کند. هدف امنیتی برای محصول - فراهم آوردن امنیت برون‌تابی‌های فیزیکی (OT.EMSEC_Design) با حملات فیزیکی از طریق رابط‌های محصول و مشاهده برون‌تابی‌های محصول مقابله می‌کند. هدف امنیتی برای محصول آشکارسازی دست‌کاری (OT.Tamper_ID) و هدف امنیتی برای محصول مقاومت در برابر دست‌کاری (OT.Tamper_Resistance) با شناسایی و مقاومت در برابر حملات دستکاری با تهدید بهره‌بردای از آسیب‌پذیری‌های فیزیکی (T.Hack_Phys) مقابله می‌کنند.

T.SVD_Forgery تهدید جعل داده درستی‌سنجی امضا	این تهدید با جعل داده درستی‌سنجی امضا (SVD) داده‌شده 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 محیط عملیاتی - تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا (OE.SCD_SVD_Corresp) که از تناظر میان داده درستی‌سنجی امضا (SVD) و داده ایجاد امضا (SCD) اطمینان حاصل می‌کند، و - هدف امنیتی برای محیط عملیاتی - اصالت‌سنجی داده درستی‌سنجی امضا (OE.SVD_Auth) که از اصالت‌سنجیِ داده درستی‌سنجی امضا (SVD) داده‌شده به برنامه‌کاربردی تولید گواهی (CGA) تامین‌کننده خدمات صدور گواهی (CSP) اطمینان حاصل می‌کند.

T.SigF_Misuse	این تهدید، سوءاستفاده از تابع ایجاد امضای محصول را برای ایجاد موجودیت غیرفعال داده امضاشده (SDO) توسط دیگران به جای صاحب‌امضا هنگام ایجاد موجودیت غیرفعال داده امضاشده (SDO) برای 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 امضا (SCD) بر حسب تقاضای صاحب‌امضا است. 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 برنامه‌کاربردی تولید امضا (OE.DTBS_Intend) اطمینان حاصل می‌کند که برنامه‌کاربردی ایجاد امضا (SCA)، داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) را تنها برای داده‌ای که صاحب‌امضا قصد امضای آن‌ها را دارد، می‌فرستد و هدف امنیتی برای محیط عملیاتی - محافظت از داده‌های در نظر گرفته شده برای امضا توسط برنامه‌کاربردی ایجاد امضا (OE.DTBS_Protect) با دستکاری داده‌ای که باید امضا شود (DTBS) در طول انتقال بر روی کانال بین برنامه‌کاربردی ایجاد امضا (SCA) و محصول مقابله می‌کند. هدف امنیتی برای محصول - یکپارچگی داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) درون محصول (OT.DTBS_Integrity_TOE) از تغییر داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) در درون محصول محافظت می‌کند. اگر برنامه‌کاربردی ایجاد امضا (SCA) رابط انسانی را برای احراز هویت کاربر فراهم کند، هدف امنیتی برای محیط عملیاتی - محافظت از داده درستی‌سنجی احرازهویت (OE.HID_VAD) به گونه‌ای محرمانگی و یکپارچگی داده درستی‌سنجی احراز هویت (VAD) را فراهم می‌آورد که مورد نیاز روش احراز هویت به کار گرفته شده است. همچنین هدف امنیتی برای محیط عملیاتی - التزام امنیتی صاحب‌امضا (OE.Signatory) اطمینان حاصل می‌کند که صاحب‌امضا داده درستی‌سنجی احراز هویت (VAD) خود را به صورت

T.DTBS_Forgery تهدید جعل داده‌ای که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن	این تهدید، تهدید برخاسته از تغییرات در داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) که برای امضا کردن به محصول فرستاده شده‌است را مورد توجه قرار می‌دهد که هیچ‌گونه مطابقتی با داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) متناظر با داده‌ای که باید امضا شود (DTBS) و صاحب‌امضا قصد امضایش را داشته ندارد. محیط فناوری اطلاعات محصول تهدید جعل داده‌ای که باید امضا شود یا بازنمایی منحصربه‌فرد متعلق به آن (T.DTBS_Forgery) را با مفاهیم زیر مورد توجه قرار می‌دهد: - هدف امنیتی برای محیط عملیاتی - ارسال داده‌های درنظر گرفته شده برای امضا توسط برنامه‌کاربردی تولید امضا (OE.DTBS_Intend) که اطمینان حاصل می‌کند که برنامه‌کاربردی ایجاد امضا (SCA) تنها داده‌ای که باید امضا شود (DTBS) را ارسال می‌کند که صاحب‌امضا قصد امضای آن را دارد. - هدف امنیتی برای محیط عملیاتی - محافظت از داده‌های در نظر گرفته شده برای امضا توسط برنامه‌کاربردی ایجاد امضا (OE.DTBS_Protect) اطمینان حاصل می‌کند که داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) در طول انتقال بین برنامه‌کاربردی ایجاد امضا (SCA) و محصول قابل تغییر نیست. محصول با این عامل تهدید با استفاده از هدف امنیتی برای محصول - یکپارچگی داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) درون محصول (OT.DTBS_Integrity_TOE) و با حصول اطمینان از یکپارچگی داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن (DTBS/R) در درون محصول مقابله می‌کند.

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

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

خط‌مشی اهداف امنیتی	توضیحات

P.CSP_QCert خط‌مشی تولید گواهی‌های واجد شرایط توسط تامین‌کننده خدمات صدور گواهی	این خط‌مشی امنیت سازمانی تعیین می‌کند که تامین‌کننده خدمات صدور گواهی (CSP) گواهی واجد شرایط یا غیر واجد شرایطی را تولید می‌کند، که صاحب‌امضا و داده درستی‌سنجی امضا (SVD) پیاده‌سازی‌شده در افزاره ایجاد امضا امن (SSCD) تحت کنترل انحصاری این صاحب‌امضا را به یکدیگر پیوند می‌دهد. خط‌مشی گواهی واجد شرایط (P.CSP_QCert) مورد توجه موارد زیر است: - هدف امنیتی برای محصول - امنیت چرخه‌حیات (OT.Lifecycle_Security) که برای شناسایی نقص‌های موجود در طول مقداردهی اولیه، شخصی‌سازی و کاربری عملیاتی به محصول نیاز دارد، - هدف امنیتی برای محیط عملیاتی - تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا مجاز (OE.SCD/SVD_Auth_Gen) که اطمینان حاصل می‌کند تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا (SCD/SVD) تنها می‌تواند توسط کاربران مجاز فراخوانی شود، - هدف امنیتی برای محصول - ورود داده ایجاد امضا مجاز (OT.SCD_Auth_Imp) که اطمینان حاصل می‌کند تنها کاربران مجاز امکان فراخوانی ورود داده ایجاد امضا (SCD) را داشته باشند، - هدف امنیتی برای محیط عملیاتی تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا (OE.SCD_SVD_Corresp) که برای حصول اطمینان از تناظر بین داده درستی‌سنجی امضا (SVD) و داده ایجاد امضا (SCD) در طول تولید آن‌ها به تامین‌کننده خدمات صدور گواهی (CSP) نیاز دارد، - هدف امنیتی برای محیط عملیاتی - تولید گواهی‌های واجد شرایط (OE.CGA_Qcert) برای تولید گواهی‌های واجد شرایط یا غیر واجد شرایط، که به برنامه‌کاربردی تولید گواهی (CGA) نیاز دارد تا تصدیق نماید که داده درستی‌سنجی امضا (SVD) با داده ایجاد امضا (SCD) پیاده‌سازی‌شده در محصول که تحت کنترل انحصاری صاحب‌امضا می‌باشد مطابقت دارد.

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

	این خط‌مشی مستلزم آن است که محصول الزامات پیوست ۲ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا را برآورده سازد [۱]. این اطمینان از طرق زیر حاصل می‌شود: - هدف امنیتی برای 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 محیط عملیاتی - یکتایی داده ایجاد امضا (OE.SCD_Unique)، هدف امنیتی برای محصول - رازمانی داده ایجاد امضا (OT.SCD_Secrecy) و هدف امنیتی برای محیط عملیاتی - رازمانی داده ایجاد امضا (OE.SCD_Secrecy) پاراگراف (a)۱ پیوست ۳ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا [۱] را با الزاماتی برای حصول اطمینان از رازمانی داده ایجاد امضا (SCD) برآورده می‌سازد. هدف امنیتی برای محصول - فراهم آوردن امنیت برون‌تابی‌های فیزیکی (OT.EMSEC_Design) و هدف امنیتی برای محصول - مقاومت در برابر دست‌کاری (OT.Tamper_Resistance) اهداف مشخص برای اطمینان از رازمانی داده ایجاد امضا (SCD) در برابر حملات مشخص را مدنظر قرار می‌دهد. - هدف امنیتی برای محصول - رازمانی داده ایجاد امضا (OT.SCD_Secrecy) و هدف امنیتی برای محصول - امنیت رمزنگاری امضای الکترونیک (OT.Sig_Secure) پاراگراف (b) ۱پیوست ۳ دستورالعمل چارچوب عمومی برای امضای الکترونیک پارلمان اروپا [۱] را با الزاماتی برآورده می‌سازد که اطمینان حاصل می‌کند که داده ایجاد امضا (SCD) نمی‌تواند از داده درستی‌سنجی امضا (SVD)، امضای دیجیتالی یا هر داده دیگر صادر شده به بیرون از محصول به دست آید. - هدف امنیتی برای محصول - تابع ایجاد امضا تنها برای صاحب‌امضای قانونی (OT.Sigy_SigF) و هدف امنیتی برای محیط عملیاتی -

	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 زوج داده ایجاد امضا / داده درستی‌سنجی امضا مجاز (OE.SCD/SVD_Auth_Gen)، هدف امنیتی برای محیط عملیاتی - رازمانی داده ایجاد امضا (OE.SCD_Secrecy) و هدف امنیتی برای محیط عملیاتی - یکتایی داده ایجاد امضا (OE.SCD_Unique) امنیت داده ایجاد امضا (SCD) را در محیط تامین‌کننده خدمات صدور گواهی (CSP) تضمین می‌کنند. هدف امنیتی برای محیط عملیاتی - رازمانی داده ایجاد امضا (OE.SCD_Secrecy) از محرمانگی داده ایجاد امضا (SCD) در طول تولید، هنگام و پس از صدور به محصول اطمینان حاصل می‌کند. تامین‌کننده خدمات صدور گواهی (CSP) از داده ایجاد امضا (SCD) برای ایجاد هیچ امضایی استفاده نمی‌کند و داده ایجاد امضا (SCD) را به شکل برگشت‌ناپذیری بعد از صدور به محصول حذف می‌کند. هدف امنیتی برای محیط عملیاتی - یکتایی داده ایجاد امضا (OE.SCD_Unique) این امکان را فراهم می‌آورد که داده ایجاد امضا (SCD) صاحب‌امضا عملاً فقط یکبار اتفاق بیفتد. هدف امنیتی برای محیط عملیاتی - تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا (OE.SCD_SVD_Corresp) تضمین می‌کند که داده درستی‌سنجی امضا (SVD) موجود در گواهی صاحب‌امضا با داده ایجاد امضا (SCD) پیاده‌سازی‌شده در نسخه محصول صاحب‌امضا مطابقت داشته باشد. هدف امنیتی برای محیط عملیاتی - تولید گواهی‌های واجد شرایط (OE.CGA_Qcert) اطمینان حاصل می‌کند که گواهی اجازه شناسایی

۵-۴-۲-۱- مفروضات و کفایت اهداف امنیتی

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

	(OE.SCD/SVD_Auth_Gen) است، و این موضوع که داده ایجاد امضا (SCD) تولید شده یکتا باشد و با داده درستی‌سنجی امضا (SVD) قابل استنتاج نباشد مورد توجه هدف امنیتی برای محیط عملیاتی - یکتایی داده ایجاد امضا (OE.SCD_Unique) می‌باشد، و این موضوع که داده ایجاد امضا (SCD) و داده درستی‌سنجی امضا (SVD) با یکدیگر متناظرند مورد توجه هدف امنیتی برای محیط عملیاتی - تناظر بین داده ایجاد امضا و داده درستی‌سنجی امضا (OE.SCD_SVD_Corresp) می‌باشد و این مسئله که داده ایجاد امضا (SCD) به صورت محرمانه حفظ می‌گردد، برای تولید امضا در محیط مورد استفاده قرار نمی‌گیرد و هنگامی که به محصول صادر شد پاک می‌شوند مورد توجه هدف امنیتی برای محیط عملیاتی - رازمانی داده ایجاد امضا (OE.SCD_Secrecy) است.

۶- الزامات کارکرد امنیتی

۶-۱- قراردادها

معیار مشترک امکان اجرای چندین عملیات روی الزامات کارکردی پالایش، انتخاب، اختصاص، و تکرار را فراهم می‌آورد. هر یک از این عملیات در این پروفایل حفاظتی مورد استفاده قرار گرفته است. عملیاتی که در این پروفایل حفاظتی اجرا نمی‌شوند به منظور 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 برای یک الزام مورد استفاده قرار گرفته است. پالایش الزامات امنیتی (۱) با واژه "پالایش" به شکل **پر رنگ** نشان داده شده است و واژگان اضافه شده و یا تغییر یافته نوشته **پر رنگی** هستند، یا (۲) در متن به عنوان نوشته **پر رنگ** گنجانده شده و با زیرنویسی مشخص شده است. در مواردی که کلمات از یک الزام معیار مشترک حذف شده باشد، پیوست جداگانه‌ای کلماتی که حذف شده است را نشان می‌دهد و یا اینکه کلمات حذف شده به سادگی خط می‌خورند (به طور مثال مانند ~~کلمات حذف شده~~)

عملیات **انتخاب** برای انتخاب یک یا تعداد بیشتری از گزینه‌های ارائه شده توسط معیار مشترک در شرح الزامات مورد استفاده قرار می‌گیرد. انتخابی که توسط نویسندگان پروفایل حفاظتی انجام شده 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 نشان دهنده 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 مورد استفاده است. به شکل نوشته زیرخط‌دار نشان داده می‌شود و متن اصلیِ مؤلفه به صورت زیرنویس داده می‌شود. اختصاصی که توسط نویسنده هدف امنیتی ارائه شده است در براکتی با نشانی ظاهر می‌شود که نشان دهنده این است یک اختصاص انجام شده، [اختصاص:]، و با *حروف مورب* نشان داده شده است.

عملیات **تکرار** موقعی مورد استفاده 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 (لطفاً توجه داشته باشید که الزامات کارکرد امنیتی ورود داده کاربر بدون مشخصه‌های امنیتی، محرمانگی تبادل داده‌های پایه و کانال قابل‌اعتماد درونی محصول بدین شکل نشان داده شده‌اند در حالیکه در این پروفایل حفاظتی تکرار نشده‌اند. این به خاطر این واقعیت است که نامگذاری همسان برای "پروفایل حفاظتی افزاره ایجاد امضای امن – قسمت ۶: الحاقی بر افزاره با ورود کلید و کانال قابل اعتماد برای برنامه‌کاربردی ایجاد امضا " که در آن ورود داده کاربر بدون مشخصه‌های امنیتی، محرمانگی تبادل داده‌های پایه و کانال قابل اعتماد درونی محصول تغییر کرده‌اند، مطلوب است.).

الزامات کارکرد امنیتی افزاره ایجاد امضای امن – ورود کلید، با توجه به الزاماتی که در استاندارد ارزیابی معیار مشترک مطرح گردیده، به‌صورت خلاصه در جدول زیر آورده شده است.

جدول ۲ الزامات کارکردی افزاره ایجاد امضای امن – ورود کلید

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**مدیریت کلید رمزنگاری ۶**	FCS_CKM._EXT.4.1
۲	**عملیات رمزنگاری ۱ (۱)**	FCS_COP.1.1(1)
۳	**عملیات رمزنگاری ۱ (۲)**	FCS_COP.1.1(2)
۴	**کنترل دسترسی زیر مجموعه / ورود داده ایجاد امضا ۱**	FDP_ACC.1.1/SCD_Import
۵	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا ۱**	FDP_ACF.1.1/SCD/SVD_Generation_SFP
۶	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا ۲**	FDP_ACF.1.2/SCD/SVD_Generation_SFP
۷	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا ۳**	FDP_ACF.1.3/SCD/SVD_Generation_SFP
۸	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا ۴**	FDP_ACF.1.4/SCD/SVD_Generation_SFP
۹	**کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا ۱**	FDP_ACC.1.1/SVD_Transfer_SFP
۱۰	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا ۱**	FDP_ACF.1.1/SVD_Transfer_SFP
۱۱	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا ۲**	FDP_ACF.1.2/SVD_Transfer_SFP
۱۲	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا ۳**	FDP_ACF.1.3/SVD_Transfer_SFP
۱۳	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی انتقال داده درستی‌سنجی امضا ۴**	FDP_ACF.1.4/SVD_Transfer_SFP
۱۴	**کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد**	FDP_ACC.1.1/Signature_creation_SFP

شماره الزام	نام الزام	تطابق الزام با استاندارد
	امنیتی ایجاد امضا ۱	
۱۵	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی ایجاد امضا ۱**	FDP_ACF.1.1/Signature_creation_SFP
۱۶	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی ایجاد امضا ۲**	FDP_ACF.1.2/Signature_creation_SFP
۱۷	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی ایجاد امضا ۳**	FDP_ACF.1.3/Signature_creation_SFP
۱۸	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی ایجاد امضا ۴**	FDP_ACF.1.4/Signature_creation_SFP
۱۹	**حفاظت از اطلاعات باقیمانده زیرمجموعه ۱**	FDP_RIP.1.1
۲۰	**نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / ماندگاری ۱**	FDP_SDI.2.1/Persistent
۲۱	**نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / ماندگاری ۲**	FDP_SDI.2.2/Persistent
۲۲	**نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / داده‌ای که باید امضا شود ۱**	FDP_SDI.2.1/DTBS
۲۳	**نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / داده‌ای که باید امضا شود ۲**	FDP_SDI.2.2/DTBS
۲۴	**زمانبندی شناسایی ۱**	FIA_UID.1.1
۲۵	**زمانبندی شناسایی ۲**	FIA_UID.1.2
۲۶	**زمانبندی احرازهویت ۱**	FIA_UAU.1.1
۲۷	**زمانبندی احرازهویت ۲**	FIA_UAU.1.2
۲۸	**ساماندهی شکست در احرازهویت ۱**	FIA_AFL.1.1
۲۹	**ساماندهی شکست در احرازهویت ۲**	FIA_AFL.1.2
۳۰	**نقش‌های امنیتی ۱**	FMT_SMR.1.1
۳۱	**نقش‌های امنیتی ۲**	FMT_SMR.1.2
۳۲	**مشخصات کارکردهای مدیریت امنیت ۱**	FMT_SMF.1.1
۳۳	**مدیریت رفتار توابع امنیتی ۱**	FMT_MOF.1.1
۳۴	**مدیریت مشخصه‌های امنیتی / مدیر سیستم ۱**	FMT_MSA.1.1/Admin
۳۵	**مدیریت مشخصه‌های امنیتی / صاحب‌امضا ۱**	FMT_MSA.1.1/Signatory
۳۶	**مشخصه‌های امنیتی امن ۱**	FMT_MSA.2.1
۳۷	**مقداردهی اولیه مشخصه ایستا ۱**	FMT_MSA.3.1
۳۸	**مقداردهی اولیه مشخصه ایستا ۲**	FMT_MSA.3.2

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

۶-۲- کلاس پشتیبانی رمزنگاری

شماره الزام	نام الزام
۱	**مدیریت کلید رمزنگاری ۶**

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

- با پاک کردن کلید رمزگذاری کلید (KEK) که کلید هدف با آن رمز شده است.
- در مورد حافظه های فرار ، تخریب باید [انتخاب:
  - با بازنویسی مستقیم اطلاعات دیگر روی حافظه انجام شود [انتخاب:
    - یک الگوی شبه تصادفی با استفاده از RBG محصول (همان‌طور که FCS_RBG_EXT.1 در تعیین شد)،

- بیت های صفر
- بیت های یک
- مقدار یک کلید جدید
- [اختصاص: مقداری که شامل یک داده حساس امنیتی نباشد.]

- قطع برق حافظه
- نابود کردن ارجاع به کلید و بلافاصله بعد از آن درخواست بازیافت حافظه

- برای حافظه های غیر فرار که دارای رابطی است که به پلتفرم زمینه فرمان میدهد که مشخص کننده کلید را پاک کند یا به طور منطقی اشاره میکند به محل ذخیره سازی کلید و بازنویسی یکباره یا چندباره را به صورت زیر انجام می‌دهد:
  - یک الگوی شبه تصادفی با استفاده از RBG محصول (همان‌طور که FCS_RBG_EXT.1 در تعیین شد)،
  - بیت های صفر
  - بیت های یک
  - مقدار یک کلید جدید
  - [اختصاص: مقداری که شامل یک داده حساس امنیتی نباشد.]

نکته کاربردی ۱:

رابط ذکر شده در الزام می‌تواند فرم‌های مختلفی بگیرد. مرسوم‌ترین آنها یک API به هسته سیستم عامل است. سطوح مختلفی از انتزاع ممکن است قابل مشاهده باشد. برای مثال در یک پیاده‌سازی برنامه مورد نظر ممکن است به جزئیات فایل سیستم دسترسی داشته باشد و قادر به ادرس دهی منطقی به بخش‌های خاص از حافظه باشد. در پیاده سازی های دیگر، برنامه دسترسی محدودی به یک منبع دارد و صرفا می‌تواند از

پلتفرم درخواست کند که آن منبع را پاک کند. سطح جزئیاتی که محصول به آن دسترسی دارد در بخش TSSاز ST بیان شده است.

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

وراثت از هیچ مؤلفه دیگر ندارد.

وابستگی: [ورود داده کاربر بدون مشخصه‌های امنیتی، یا ورود داده کاربر با مشخصه‌های امنیتی یا تولید کلید رمزنگاری]، تخریب کلید رمزنگاری

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

[انتخاب:

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

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

نکته کاربردی ۲:

سند هدف امنیتی باید مشخص کند که آیا محصول، به تنهایی یا در ترکیب با محیط عملیاتی الگوریتم‌ها را اجرا می‌کند. برای هر یک از پلت‌فرم‌های محصول تحت پشتیبانی، نیاز به مدارکی است که نشان دهد این پلت‌فرم قادر است الزامات را از جانب محصول، برآورده سازد. نویسنده محصول باید الگوریتمی را برای پیاده‌سازی انتخاب کند تا کار امضای دیجیتال را انجام دهد؛ اگر بیش از یک الگوریتم در دسترس باشد،این الزام (و الزام مربوط به تولید کلید) باید تکرار شوند تا کارکرد آن تعیین شود. در مورد الگوریتم انتخابی،

نویسنده هدف امنیتی باید اختصاص/انتخاب‌های مناسبی اتخاذ کند تا پارامترهای الگوریتم پیاده‌سازی شده، تعیین شوند. در مورد الگوهای رمزگذاری خم‌های بیضوی ، اندازه کلید اشاره به لگاریتم پایه ۲ نقطه پایه دارد. به عنوان رویکرد ارجح در امضاهای دیجیتال، ECDSA برای کاربردهای آتی از این پروفایل، الزامی است.	
۳	**عملیات رمزنگاری ۱ (۲)(درهم‌سازی رمزنگاری)**
محصول باید [خدمات درهم‌سازی رمزنگاری] را مطابق با یک الگوریتم رمزنگاری مشخص [انتخاب: *SHA-256, SHA-384, SHA-512*] و اندازه‌ی خلاصه پیام[۱][انتخاب: *۱۶۰، ۲۵۶، ۳۸۴ و ۵۱۲ بیت*] که مطابق با استاندارد FIPS 180-4، «استاندارد درهم‌ساز امن» باشد، انجام دهد. **نکته کاربردی ۳:** انتخاب الگوریتم درهم‌سازی باید متناسب با اندازه خلاصه پیام باشد. برای کاربردهای مربوط به تولید امضای دیجیتال الگوریتم SHA-1 نا امن شناخته می‌شود. ولی برای سایر کاربردها قابل استفاده است.	

۶-۳- کلاس محافظت از داده‌های کاربری

مشخصه‌های امنیتی و وضعیت مرتبط با موجودیت‌های فعال و غیرفعال شامل موارد زیر می‌باشد:

جدول ۳ موجودیت‌های فعال و مشخصه‌های امنیتی برای کنترل دسترسی

موجودیت‌های فعال و غیرفعال مرتبط با مشخصه‌های امنیتی	نوع مشخصه امنیتی	مقدار مشخصه امنیتی
موجودیت فعال کاربر	نقش	نقش مدیر سیستم، نقش صاحب‌امضا
موجودیت فعال کاربر	مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا	مجاز، غیر مجاز
داده ایجاد امضا	داده ایجاد امضا عملیاتی	نه، بله

[۱] Message Digest Sizes

نکته کاربردی ۳: نویسنده پروفایل حفاظتی یا هدف امنیتی ممکن است موجودیت‌های غیرفعال و مشخصه‌های امنیتی دیگری تعریف کند.

شماره الزام	نام الزام
۴	**کنترل دسترسی زیر مجموعه / ورود داده ایجاد امضا ۱**
وراثت از هیچ مؤلفه دیگر ندارد. وابستگی: مشخصه امنیتی بر اساس کنترل دسترسی[۱] محصول باید خط‌مشی کارکرد امنیتی ورود داده ایجاد امضا[۲] را روی موارد زیر اجرا کند: (۱) موجودیت‌های فعال: موجودیت فعال کاربر (۲) موجودیت‌های غیرفعال: داده ایحاد امضا (۳) عملیات: ورود داده ایجاد امضا [۳]	
۵	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / ورود داده ایجاد امضا ۱**
وراثت از هیچ مؤلفه دیگر ندارد. وابستگی: کنترل دسترسی زیر مجموعه[۴] مقداردهی اولیه مشخصه ایستا محصول باید خط‌مشی کارکرد امنیتی ورود داده ایجاد امضا[۵] را برای موجودیت‌های غیرفعال بر اساس آنچه در ادامه می‌آید اعمال کنند: موجودیت فعال کاربر مرتبط با مشخصه امنیتی "مدیریت داده ایجاد امضا /	

[۱] FDP_ACF.1

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

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

[۴] FDP_ACC.1

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

داده درستی‌سنجی امضا"[1].	
۶	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / ورود داده ایجاد امضا ۲**
محصول باید نقش‌های زیر را اعمال کنند تا تعیین کنند آیا عملیاتی در میان موجودیت‌های فعال و غیرفعال کنترل شده مجاز شده است: موجودیت فعال کاربر به همراه مشخصه امنیتی "مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا" که به شکل "مجاز" تنظیم می‌شود مجاز به ورود داده ایجاد امضا است[2].	
۷	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / ورود داده ایجاد امضا ۳**
محصول باید به وضوح اجازه دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را بر اساس قوانین اضافی زیر صادر کند: هیچ[3].	
۸	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / ورود داده ایجاد امضا ۴**
محصول بایستی به وضوح دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را بر اساس قوانین اضافی زیر انکار کند: موجودیت فعال کاربر به همراه مشخصه امنیتی "مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا" که به شکل "غیر مجاز" تنظیم می‌شود مجاز به ورود داده ایجاد امضا نیست[4].	
۹	**کنترل دسترسی زیر مجموعه / ایجاد امضا ۱**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: مشخصه‌های امنیتی مبتنی بر کنترل دسترسی	

[1] [اختصاص: *فهرستی از موجودیت‌های فعال و غیرفعال تحت کنترل خط‌مشی کارکرد امنیتی مشخص شده، و برای هر کدام مشخصه‌های امنیتی مرتبط با خط‌مشی کارکرد امنیتی، یا گروه‌های نامگذاری شده مشخصه‌های امنیتی مرتبط با خط‌مشی کارکرد امنیتی*]

[2] [اختصاص: *قوانین حاکم بر دسترسی در بین موجودیت‌های فعال کنترل شده و موجودیت‌های غیرفعال کنترل شده مورد استفاده عملیات کنترل شده بر روی موجودیت‌های کنترل شده*]

[3] [اختصاص: *قوانین، بر اساس مشخصه‌های امنیتی، که به وضوح اجازه دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را صادر می‌کند*]

[4] [اختصاص: *قوانین، بر اساس مشخصه‌های امنیتی، که به وضوح اجازه دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را انکار می‌کند*]

محصول باید خط‌مشی کارکرد امنیتی ایجاد امضا[1] را روی موارد زیر اعمال کنند:

(۱) موجودیت‌های فعال: موجودیت فعال کاربر

(۲) موجودیت‌های غیرفعال: داده ایجاد امضا، داده‌ای که باید امضا شود و یا بازنمایی منحصر به فرد متعلق به آن

(۳) عملیات: ایجاد امضا[2].

۱۰	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / ایجاد امضا ۱**

وراثت: از هیچ مؤلفه دیگر ندارد

وابستگی: کنترل دسترسی زیر مجموعه

مقداردهی اولیه مشخصه ایستا

محصول باید خط‌مشی کارکرد امنیتی ایجاد امضا[3] را برای موجودیت‌های غیرفعال بر اساس موارد زیر اعمال کنند:

(۱) موجودیت فعال کاربر مرتبط با مشخصه امنیتی "نقش"، و

(۲) داده ایجاد امضا با مشخصه امنیتی " داده ایجاد امضای عملیاتی"[4].

۱۱	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / ایجاد امضا ۲

محصول باید نقش‌های زیر را اعمال کنند تا تعیین کنند آیا عملیاتی در میان موجودیت‌های فعال و غیرفعال کنترل شده مجاز شده است:

نقش صاحب‌امضا مجاز به ایجاد امضای الکترونیک برای داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن داده با داده ایجاد امضایی است که مشخصه امنیتی " داده ایجاد امضای عملیاتی"، "بله"

---

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

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

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

[4] [اختصاص: *فهرستی از موجودیت‌های فعال و غیرفعال تحت کنترل خط‌مشی کارکرد امنیتی مشخص شده، و برای هر کدام مشخصه‌های امنیتی مرتبط با خط‌مشی کارکرد امنیتی، یا گروه‌های نامگذاری شده مشخصه‌های امنیتی مرتبط با خط‌مشی کارکرد امنیتی*]

تنظیم شده است.[1].	
۱۲	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / ایجاد امضا ۳
محصول باید به وضوح اجازه دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را بر اساس قوانین اضافی زیر صادر کند: هیچ[2].	
۱۳	مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / ایجاد امضا ۴
محصول بایستی به وضوح دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را بر اساس قوانین اضافی زیر انکار کند: موجودیت فعال کاربر مجاز به ایجاد امضای الکترونیک برای داده‌ای که باید امضا شود و یا بازنمایی منحصر به‌فرد متعلق به آن داده با داده ایجاد امضایی نیست که مشخصه امنیتی "داده ایجاد امضای عملیاتی"، "نه" تنظیم شده است[3].	
۱۴	ورود داده کاربر بدون مشخصه‌های امنیتی / داده ایجاد امضا ۱
وابستگی: [کنترل دسترسی زیر مجموعه، یا کنترل جریان اطلاعات زیر مجموعه]، مقداردهی اولیه مشخصه ایستا محصول باید خط‌مشی کارکرد امنیتی ورود داده ایجاد امضا[4] را هنگام ورود داده کاربر، تحت کنترل خط مشی کارکرد امنیتی، بیرون از محصول اعمال کنند.	
۱۵	ورود داده کاربر بدون مشخصه‌های امنیتی / داده ایجاد امضا ۲
محصول باید هرگونه مشخصه امنیتی مرتبط با داده ایجاد امضا را هنگامی که از بیرون از محصول وارد شده است رد کند.	

[1] [اختصاص: *قوانینی که بر دسترسی در بین موجودیت‌های فعال کنترل شده و موجودیت‌های غیرفعال کنترل شده مورد استفاده عملیات کنترل شده بر روی موجودیت‌های کنترل شده حاکمیت می‌کند*]

[2] [اختصاص: *قوانین، بر اساس مشخصه‌های امنیتی، که به وضوح اجازه دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را صادر می‌کند*]

[3] [اختصاص: *قوانین، بر اساس مشخصه‌های امنیتی، که به وضوح اجازه دسترسی موجودیت‌های فعال به موجودیت‌های غیرفعال را انکار می‌کند*]

[4] [اختصاص: *قوانین، بر اساس مشخصه‌های امنیتی، که به وضوح اجازه دسترسی موجودیت‌های فعال به موجودیت‌های غ*

۱۶	ورود داده کاربر بدون مشخصه‌های امنیتی / داده ایجاد امضا ۳

محصول باید قوانین زیر را هنگام ورود داده کاربر تحت کنترل خط‌مشی کارکرد امنیتی بیرون از محصول اعمال کنند: [اختصاص: *قوانین کنترل ورود اضافی*].

۱۷	محرمانگی تبادل داده‌های پایه / داده ایجاد امضا ۱

وابستگی: [کانال قابل‌اعتماد درون توابع هدف امنیتی[۱]، یا مسیر قابل اعتماد[۲]]، [کنترل دسترسی زیر مجموعه، یا کنترل جریان اطلاعات زیر مجموعه]

محصول باید خط‌مشی کارکرد امنیتی ورود داده ایجاد امضا[۳] را برای دریافت[۴] ~~داده کاربر~~ داده ایجاد امضا در یک روش محافظت شده در برابر افشای غیر مجاز، اعمال کنند.

نکته کاربردی ۴: الزام کارکرد امنیتی محرمانگی تبادل داده‌های پایه / داده ایجاد امضا ۱ به منظور حصول اطمینان از محرمانگی داده ایجاد امضا در طول ورود به محصول نیاز دارد. پالایش جایگزینی "داده کاربر" توسط "داده ایجاد امضا" مشخص می‌سازد که محرمانگی دیگر داده‌های کاربر وارد شده، مانند داده‌ای که باید امضا شود، مورد نیاز نیست.

۱۸	حفاظت از اطلاعات باقیمانده زیر مجموعه ۱

محصول باید اطمینان حاصل کند که هرگونه محتوای اطلاعات قبلی از یک منبع به هنگام عدم تخصیص منبع از[۵] موجودیت‌های غیرفعالی که در ادامه می‌آید، از دسترس خارج شده است: داده ایجاد امضا[۶]

داده‌های زیر که به‌صورت ماندگار توسط محصول ذخیره می‌شود، مشخصه داده کاربر را "کنترل یکپارچگی داده‌های ذخیره‌شده پایدار" را دارد:

۱. داده ایجاد امضا

۲. داده درستی‌سنجی امضا (درصورتی‌که به‌صورت ماندگار توسط محصول ذخیره شده باشد).

داده‌ای که باید امضا شوند یا بازنمایی منحصربه‌فرد متعلق به آن که به‌صورت موقت توسط محصول ذخیره

یرفعال را ان
کار می‌کند]

[۳][اختصاص: *کنترل دسترسی SFP(ها) و یا کنترل جریان اطلاعات SPF(ها)*]

[۴][انتخاب: *ارسال، دریافت*]

[۵][انتخاب: *اختصاص منابع به، عدم اختصاص منابع از*]

[۶][اختصاص: *فهرستی از موجودیت‌ها*]

شده‌است، مشخصه داده کاربر " داده ذخیره‌شده کنترل‌شده از نظر یکپارچگی" را دارد.	
۱۹	نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / ماندگاری ۱
وراثت: از نظارت بر یکپارچگی داده ذخیره‌شده[۱] وابستگی: ندارد محصول باید بر روی داده‌های کاربر که در مجموعه‌ای تحت کنترل محصول ذخیره‌شده است، نظارت کند تا خطاهای یکپارچگی[۲] را بر روی تمام موجودیت‌های غیرفعال بر اساس مشخصاتی که در ادامه می‌آید تشخیص دهد: داده ذخیره‌شده کنترل‌شده از نظر یکپارچگی[۳]	
۲۰	نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / ماندگاری ۲
در صورت آشکارسازی خطای یکپارچگی داده، محصول باید (۱) استفاده از داده‌های تغییر یافته را منع کند. (۲) موجودیت فعال صاحب‌امضا را از خطای یکپارچگی مطلع کند.[۴]	
۲۱	نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن/ داده‌ای که باید امضا شود ۱
وراثت: از نظارت بر یکپارچگی داده ذخیره‌شده وابستگی: ندارد محصول باید بر روی داده‌های کاربر که در مجموعه‌ای تحت کنترل محصول ذخیره‌شده‌است، نظارت کند تا خطاهای یکپارچگی[۵] را بر روی تمام موجودیت‌های غیرفعال بر اساس مشخصاتی که در ادامه می‌آید تشخیص دهد: داده‌ای که باید امضا شود و ذخیره‌شده کنترل‌شده از نظر یکپارچگی[۶]	
۲۲	نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن/ داده‌ای که باید امضا شود ۲
در صورت تشخیص خطای یکپارچگی داده، محصول باید: (۱) استفاده از داده‌های تغییر یافته را منع کند.	

[۱] FDP_SDI.1

[۲] [اختصاص: *خطاهای یکپارچگی*]

[۳] [اختصاص: *مشخصات داده‌های کاربر*]

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

[۵] [اختصاص: خطاهای یکپارچگی]

[۶] [اختصاص: *مشخصات داده‌های کاربر*]

(۲) موجودیت فعال صاحب‌امضا را از خطای یکپارچگی مطلع کند.[۱]

نکته کاربردی ۵: یکپارچگی داده امنیتی مانند داده احرازهویت مرجع باید حفظ شود تا از اثربخشی احرازهویت کاربر اطمینان حاصل شود. این حفاظت، جنبه خاصی از معماری امنیتی می‌باشد (به الزامات تضمین امنیت طراحی معماری با جداسازی دامنه‌ها و بدون قابلیت دور زدن[۲] رجوع شود).

۶-۴- کلاس شناسایی و احراز هویت

شماره الزام	نام الزام
۲۳	زمانبندی شناسایی ۱
محصول باید به موارد زیر اجازه بدهد: (۱) خودآزمائی بر اساس آزمون توابع هدف امنیتی (۲) [اختصاص: *فهرستی از اقدامات اضافه‌ای که محصول واسطه آن هستند*][۳] قبل از اینکه کاربر شناسایی شود، در سمت کاربر انجام می‌شود.	
۲۴	زمانبندی شناسایی ۲
محصول باید مستلزم آن باشد که قبل از اینکه اجازه هرگونه اقدامی که محصول واسطه آنند را در سمت کاربر بدهد، هر کاربری به‌طور موفقیت‌آمیز شناسایی شود. **نکته کاربردی ۶:** نویسنده هدف امنیتی باید عملیات ازدست‌رفته در الزام کارکرد امنیتی زمانبندی شناسایی ۱را انجام دهد. فهرست اقدامات اضافه‌ای که محصول واسطه آنند ممکن است خالی باشد (به‌عنوان‌مثال، اختصاص "هیچ‌چیز") یا شامل اقداماتی باشد که محصول واسطه آن هستند مانند برقراری یک مسیر قابل‌اعتماد بین کاربرانی که در حال استفاده از رابط انسانی[۴] (کاربری) یک افزاره بیرونی هستند. محصول ممکن است به‌طور پیش‌فرض یا با انتخاب نقش و داده احرازهویت مرجع در برابر احرازهویتی که صورت خواهد گرفت، کاربر را شناسایی کند. شناسایی به‌طور پیش‌فرض، معمولا به چرخه‌حیات محصول پیوند داده می‌شود به‌عنوان‌مثال محصول ممکن است قبل از اینکه داده احرازهویت مرجع صاحب‌امضا ایجاد	

---

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

[۲] ADV_ARC.1

[۳] [اختصاص: *فهرستی از اقدامات انجام شده به واسطه توابع امنیتی هدف ارزیابی*]

[۴] HI

شود به‌طور پیش‌فرض مدیر سیستم را شناسایی کند، و اگر داده احرازهویت مرجع صاحب‌امضا وجود داشته باشد صاحب‌امضا را شناسایی کند. در مورد کارت‌های هوشمند چند کاربردی (به‌عبارت‌دیگر کارت‌های هوشمندی که کاربردی بیش از کاربرد ایجاد امضا را ارائه می‌دهند)، کارکرد با انتخاب فایل راهنمای فایل‌ها و مسیرها[1] برنامه‌کاربردی امضا، خود را به‌عنوان صاحب‌امضا شناسایی کرده و بنابراین احرازهویت پین بر اساس پین صاحب‌امضا انجام خواهد شد. کاربر ممکن است با انتخاب کلید احرازهویت، خود را به‌عنوان مدیر سیستم شناسایی کرده و بنابراین احرازهویت با احراز اصالت بیرونی یا احرازهویت افزاره دو طرفه انجام خواهد شد.

۲۵	زمانبندی احرازهویت ۱

وابستگی: زمانبندی شناسایی

محصول باید اجازه موارد زیر را بدهد:

(۱) انجام خودآزمائی مطابق آزمون توابع هدف امنیتی

(۲) شناسایی کاربر به‌وسیله محصول موردنیاز توسط الزام کارکرد امنیتی زمانبندی شناسایی

(۳) [اختصاص: *فهرستی از اقدامات اضافی که محصول واسطه آن هستند*][2]

قبل از اینکه کاربر احرازهویت شود در سمت کاربر انجام می‌شود.

۲۶	زمانبندی احرازهویت ۲

محصول باید مستلزم آن باشد که قبل از اینکه به هر اقدام دیگری که محصول واسطه آن هستند در طرف کاربر انجام شود، هر کاربری با موفقیت احرازهویت شود.

نکته کاربردی ۷: نویسنده هدف امنیتی باید عملیات ازدست‌رفته در زمانبندی احرازهویت ۱ را انجام دهد. فهرست اقدامات افزوده‌ای که محصول واسطه آن هستند ممکن است خالی باشد (به‌عنوان‌مثال، اختصاص"هیچ‌چیز") یا شامل اقداماتی باشد که محصول واسطه آن هستند مانند برقراری یک مسیر قابل اعتماد بین کاربرانی که در حال استفاده از افزاره رابط انسانی (کاربری) یک افزاره بیرونی هستند.

۲۷	ساماندهی شکست در احرازهویت ۱

وابستگی: زمانبندی احراز هویت

محصول باید زمانی که [اختصاص: عدد صحیح مثبت] عدد صحیح مثبت قابل تنظیم توسط مدیر سیستم به همراه [اختصاص: گستره‌ای از مقادیر قابل قبول] تلاش‌های احرازهویت ناموفق مربوط به تلاش‌های

[1] directory

[2] اختصاص: *فهرستی ازاقدامات انجام شده به واسطه توابع امنیتی هدف ارزیابی*]

احرازهویت شکست‌خورده متوالی[1] اتفاق می‌افتد را تشخیص دهد.	
۲۸	ساماندهی شکست در احرازهویت ۲
هنگامی که با تعداد تعریف شده‌ای از تلاش‌های احراز هویت ناموفق مواجه شد[2]، محصول باید داده احراز هویت مرجع را مسدود کنند.[3] **نکته کاربردی ۸:** نویسنده هدف امنیت باید عملیات ازدست‌رفته در الزام کارکرد امنیتی ساماندهی شکست در احراز هویت ۱ را انجام دهد. اختصاص باید با سازوکار احرازهویت پیاده‌سازی‌شده سازگار بوده و در برابر حملات با پتانسیل حمله بالا، مقاوم باشد.	

۶-۵- کلاس مدیریت امنیت

شماره الزام	نام الزام
۲۹	نقش‌های امنیتی ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: زمانبندی شناسایی محصول باید نقش‌های مدیر سیستم و صاحب‌امضا[4] را حفظ کند.	
۳۰	نقش‌های امنیتی ۲
محصول باید بتوانند کاربران را به نقش‌ها مرتبط کنند.	
۳۱	مشخصات کارکردهای مدیریت امنیت ۱
محصول باید بتواند کارکردهای مدیریتی زیر را اجرا کنند: (۱) ایجاد و تغییر داده احرازهویت مرجع، (۲) فعال کردن تابع ایجاد امضا، (۳) تغییر مشخصه‌های امنیتی مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا، داده ایجاد امضا عملیاتی،	

[1] [اختصاص: *فهرستی از اقداماتی که توابع هدف امنیتی واسطه آنند*]
[2] [انتخاب: *مواجه شدن، پیش افتادن*]
[3] [اختصاص: *فهرستی از اقدامات*]
[4] [اختصاص: *نقش‌های شناسایی شده مجاز*]

(۴) تغییر مقدار پیش‌فرض مشخصه امنیتی شناسه داده ایجاد امضا،

(۵) [اختصاص: *فهرستی از دیگر کارکردهای مدیریت امنیت که باید توسط محصول ارائه شود*][۱].

نکته کاربردی ۹:
نویسنده هدف امنیتی باید عملیات ازدست‌رفته در الزام کارکرد امنیتی مشخصات کارکردهای مدیریت امنیت ۱ را انجام دهد. فهرست دیگر کارکردهای مدیریت امنیتی که باید توسط محصول انجام شود، ممکن است خالی باشد (به‌عبارت‌دیگر: اختصاص "هیچ‌چیز").

۳۲	مدیریت رفتار توابع امنیتی ۱

وابستگی: نقش‌های امنیتی، مشخصات کارکردهای مدیریت امنیت

محصول باید توانایی فعال‌سازی[۲] کارکردهای تابع ایجاد امضا[۳] را به نقش صاحب‌امضا[۴] محدود کند.

۳۳	مدیریت مشخصه‌های امنیتی / مدیر سیستم ۱

وابستگی: [کنترل دسترسی زیرمجموعه یا کنترل جریان اطلاعات زیرمجموعه[۵]]، نقش‌های امنیتی، مشخصات کارکردهای مدیریت امنیت

محصول باید خط‌مشی کارکرد امنیتی ورود داده ایجاد امضا[۶] را اجرا کند تا توانایی تغییر [اختصاص: *عملیات دیگر*][۷] مشخصه‌های امنیتی مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا[۸] را به نقش مدیر سیستم[۹] محدود کند.

۳۴	مدیریت مشخصه‌های امنیتی / صاحب‌امضا ۱

وابستگی: [کنترل دسترسی زیرمجموعه یا کنترل جریان اطلاعات زیرمجموعه]، نقش‌های امنیتی،

---

[۱] [اختصاص: *فهرستی از کارکردهای مدیریتی‌ای که توسط توابع هدف امنیتی فراهم می‌شود*]

[۲] [انتخاب: *تعیین رفتار، فعال کردن، غیرفعال کردن، تغییر رفتار*]

[۳] [اختصاص: *فهرستی از توابع*]

[۴] [اختصاص: *نقش‌های مجاز شناسایی شده*]

[۵] FDP_IFC.1

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

[۷] [انتخاب: *تغییر_پیش فرض، پرس و جو، تغییر، حذف، [اختصاص: عملیات دیگر]*]

[۸] [اختصاص: *فهرستی از مشخصه‌های امنیتی*]

[۹] [اختصاص: *فهرستی از نقش‌های مجاز شناسایی شده*]

مشخصات کارکردهای مدیریت امنیت

محصول باید خط‌مشی کارکرد امنیتی ایجاد امضا[۱] را اجراکند تا توانایی تغییر[۲] مشخصه‌های امنیتی داده‌های ایجاد امضا عملیاتی[۳] را به نقش صاحب‌امضا[۴] محدود کند.

۳۵	مشخصه‌های امنیتی امن ۱

وابستگی: [کنترل دسترسی زیرمجموعه یا کنترل جریان اطلاعات زیرمجموعه]، نقش‌های امنیتی، مشخصات کارکردهای مدیریت امنیت

محصول باید اطمینان یابد که تنها مقادیر امن برای مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا و داده ایجاد امضا عملیاتی[۵] پذیرفته شده‌اند.

نکته کاربردی ۱۰:
نویسنده هدف امنیتی باید تعریف کند که کدام یک از مقادیر مشخصه‌های امنیتی مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا برای محصول و چرخه حیات محصول مورد نظر امن هستند به‌عبارت‌دیگر اگر محصول از تولید زوج‌های داده ایجاد امضا / داده درستی‌سنجی امضا توسط صاحب‌امضا و کانال قابل‌اعتماد برای صدور داده درستی‌سنجی امضا به برنامه‌کاربردی تولید گواهی پشتیبانی کند، پس موجودیت فعال صاحب‌امضا ممکن است "بله" را به مشخصه امنیتی مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا اختصاص بدهد یا ممکن است این کار را انجام ندهد. اگر محصول از تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا در فاز آماده‌سازی در محیط امن پشتیبانی کند تنها محصول باید "بله" را به ویژگی امنیتی مدیریت داده ایجاد امضا / داده درستی‌سنجی امضا مربوط به موجودیت فعال مدیر سیستم اختصاص داده و "خیر" را به این ویژگی مربوط به موجودیت فعال صاحب‌امضا اختصاص دهد.

۳۶	مقداردهی اولیه مشخصه ایستا ۱

وابستگی: مدیریت مشخصه‌های امنیتی[۶]، نقش‌های امنیتی

محصول باید خط‌مشی کارکرد امنیتی ورود داده ایجاد امضا و خط‌مشی کارکرد امنیتی ایجاد امضا[۷] را به‌منظور ارائه مقادیر پیش‌فرض محدودکننده[۸] برای مشخصه‌های امنیتی‌ای اجرا کند که جهت اجرای

---

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

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

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

[۴] [اختصاص: *فهرستی از نقش‌های مجاز شناسایی شده*]

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

[۶] FMT_MSA.1

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

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

خط‌مشی کارکرد امنیتی استفاده شده است.	
مقداردهی اولیه مشخصه ایستا ۲	**۳۷**
محصول باید به نقش مدیر سیستم[۱] اجازه دهد تا هنگامیکه یک موجودیت غیرفعال یا اطلاعات ایجاد می‌شود مقادیر اولیه جایگزینی را برای ابطال مقادیر پیش‌فرض مشخص کند.	
ارث‌بری مقادیر مشخصه‌های امنیتی ۱	**۳۸**
وابستگی: کنترل دسترسی زیرمجموعه یا کنترل جریان اطلاعات زیرمجموعه محصول باید از قوانین زیر برای تنظیم مقادیر مشخصه‌های امنیتی استفاده کند: ۱) اگر موجودیت فعال مدیر سیستم داده ایجاد امضا را در حالی وارد کند که موجودیت فعال صاحب‌امضا احرازهویت شده است، مشخصه امنیتی «داده ایجاد امضای عملیاتی» از داده ایجاد امضا باید بعد از ورود داده ایجاد امضا به‌عنوان یک عملیات یکتا، «خیر» تنظیم گردد. اگر موجودیت فعال صاحب‌امضا داده ایجاد امضا را در حالی وارد کند که موجودیت فعال صاحب‌امضا احراز هویت شده‌است، مشخصه امنیتی « داده ایجاد امضای عملیاتی» از داده ایجاد امضا باید بعد از ورود داده ایجاد امضا به‌عنوان یک عملیات یکتا، «بله» تنظیم شود[۲].	
مدیریت داده‌های امنیتی / مدیر سیستم ۱	**۳۹**
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: مشخصات کارکردهای مدیریت امنیت نقش‌های امنیتی محصول باید توانایی ایجاد[۳]داده احرازهویت مرجع[۴] را به نقش مدیر سیستم[۵] محدود کند.	
مدیریت داده امنیتی / صاحب‌امضا ۱	**۴۰**
وابستگی: مشخصات کارکردهای مدیریت امنیت	

[۱] [اختصاص: *فهرستی از نقش‌های مجاز شناسایی شده*]

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

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

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

[۵] [اختصاص: *نقش‌های مجاز مشخص‌شده*]

نقش‌های امنیتی

محصول باید توانایی تغییر [اختصاص: *سایر عملیات*][1] داده احرازهویت مرجع[2] را به نقش صاحب‌امضا[3] محدود کند.

نکته کاربردی ۱۱:
نویسنده هدف امنیتی باید عملیات ازدست‌رفته در الزام کارکردی امنیت مدیریت داده امنیتی ۱ را اجرا کند. اختصاص موارد ازدست‌رفته ممکن است "هیچ" باشد.

۴۱	حفظ حالت امن در صورت شکست ۱

محصول باید زمانی که انواع شکست‌های زیر رخ می‌دهد، حالت امن را حفظ کند.

(۱) خودآزمائی مطابق شکست‌های خودآزمائی توابع هدف امنیتی[4]

(۲) [اختصاص: *فهرستی از انواع شکست‌ها در توابع هدف امنیتی*][5]

نکته کاربردی ۱۲:
نویسنده هدف امنیتی باید اختصاص‌های ازدست‌رفته در الزام کارکرد امنیتی حفظ حالت امن در صورت شکست اجرا کند. اختصاص (۱) شکست‌هایی را که توسط خودآزمائی شکست خورده تشخیص داده‌شده و نیاز به اقدامات مناسب برای جلوگیری از تخلف امنیتی را مورد رسیدگی قرار می‌دهد. زمانی که محصول در حالت امن قرار دارد، محصول نباید هیچگونه عملیات رمزنگاری را انجام دهد و تمام رابط‌های خروجی داده باید توسط محصول مهار شوند.

۴۲	آشکارسازی انفعالی حمله فیزیکی ۱

محصول باید آشکارسازی بدون ابهامی از دستکاری‌های فیزیکی ارائه دهد که ممکن است محصول را در معرض خطر قرار دهند.

۴۳	آشکارسازی انفعالی حمله فیزیکی ۲

محصول باید قابلیتی را ارائه دهد که تعیین کند آیا دست‌کاری فیزیکی با افزاره‌های محصول یا اجزای محصول اتفاق افتاده است یا خیر.

۴۴	مقاومت در مقابل حمله فیزیکی ۱

محصول باید با پاسخگویی خودکار مانند الزامات کارکرد امنیتی‌ای که همیشه به کار گرفته می‌شوند مانع

---

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

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

[3] [اختصاص: *نقش‌های مشخص مجاز*]

[4] FPT TST

[5] [اختصاص: *فهرستی از انواع شکست‌ها در توابع امنیتی هدف ارزیابی*]

[اختصاص: *سناریوهای دست‌کاری فیزیکی*] در [اختصاص: *فهرستی از افزاره‌ها یا اجزای توابع هدف امنیتی*] شوند.

نکته کاربردی ۱۳:
محصول اقدامات مناسبی را به‌طور مداوم برای مقابله با دستکاری‌های فیزیکی اجرا خواهد کرد که ممکن است داده ایجاد امضا را در معرض خطر قرار دهد. "پاسخگویی خودکار" در الزام کارکرد امنیتی مقاومت در مقابل حمله فیزیکی ۱ بدان معنی است که (۱) فرض شده است که ممکن است در هر زمانی یک حمله وجود داشته‌باشد و (۲) اقدامات مقابله‌ای در هر زمانی ارائه‌شده‌اند. به واسطه ماهیت این حملات، محصول می‌تواند بدون هیچ ابزاری حملات را در تمام اجزای خود تشخیص دهد (به عنوان مثال محصول خراب شده است). اما دستکاری‌های فیزیکی نباید اطلاعاتی از داده ایجاد امضا را فاش کند، به‌عنوان‌مثال محصول ممکن است در حالت خاموشِ به‌طور فیزیکی دست‌کاری شود (مانند کارت هوشمند) که به محصول اجازه نوشتن مجدد داده ایجاد امضا را نمی‌دهد اما منجر به تخریب فیزیکی حافظه و تمام اطلاعات موجود در آن درباره داده ایجاد امضا می‌شود. در صورت دست‌کاری فیزیکی، محصول ممکن است توابع در نظر گرفته شده برای تولید زوج داده ایجاد امضا / داده درستی‌سنجی امضا یا ایجاد امضا را ارائه ندهد اما با مسدود کردن این توابع از محرمانگی داده ایجاد امضا اطمینان حاصل کند. الزام کارکرد امنیتی آشکارسازی انفعالی حمله فیزیکی مستلزم آن است که محصول به دستکاری‌های فیزیکی به‌گونه‌ای واکنش نشان دهد که صاحب‌امضا بتواند تشخیص دهد که محصول به‌طور فیزیکی دست‌کاری شده است یا نه. به‌عنوان‌مثال، محصول ممکن است پیغام مناسبی را در هنگام راه‌اندازی نشان دهد یا مستندات راهنما یک شکست در هنگام راه‌اندازی محصول را به‌عنوان نشانه‌ای از دست‌کاری فیزیکی توصیف کنند.

۴۵	آزمون محصول ۱
محصول باید مجموعه‌ای از خودآزمائی‌ها را اجرا کند [انتخاب: در طول راه‌اندازی اولیه، به‌صورت دوره‌ای در حین عملیات عادی، به هنگام درخواست کاربر مجاز، تحت شرایطی [اختصاص: شرایطی که تحت آن خودآزمائی باید صورت گیرد]] تا عملکرد صحیح توابع هدف امنیتی[۱] را نشان دهد.	
۴۶	آزمون محصول ۲
محصول باید این قابلیت را برای کاربران مجاز فراهم آورند تا بتوانند یکپارچگی داده امنیتی[۲] را بررسی کنند.	
۴۷	آزمون محصول ۳
محصول باید این قابلیت را برای کاربران مجاز فراهم آورند تا بتوانند یکپارچگی توابع هدف امنیتی[۳] را بررسی بررسی کنند.	

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

نکته کاربردی ۱۴:
نویسنده هدف امنیتی باید عملیات موجود در الزام کارکرد امنیتی آزمون محصول ۱ را اجرا کند. الزام کارکرد امنیتی آزمون محصول تنها خودآزمائی محصول یا قسمت‌هایی از محصول را مورد توجه قرار می‌دهد. اگر محصول متکی بر مشخصه‌های امنیتی سکوی سخت‌افزاری قسمتی از محصول باشد، نویسنده هدف امنیتی باید الزام کارکرد امنیتی آزمودن موجودیت‌های بیرونی۱ را بگنجاند که به محصول برای آزمودن این ویژگی‌ها برای عملکرد صحیح محصول وابسته نیاز دارد.

خانواده برون‌تابی محصول

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

- **رفتار خانواده برون‌تابی محصول:**

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

- **سطح‌بندی مؤلفه:**

برون‌تابی محصول دو جزء اصلی دارد:

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

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

---

[۱] FPT_TEE.1

[۲] FPT_EMS

[۳] Simple Power Analysis

[۴] Differential Power Analysis

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

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

- **اقدامات مدیریتی برون‌تابی محصول**

هیچگونه فعالیت مدیریتی پیش‌بینی نشده‌است.

- **اقدامات ممیزی برون‌تابی محصول**

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

شماره الزام	نام الزام
۴۸	برون‌تابی محصول ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد محصول نباید [اختصاص: *انواع تابش‌های امواج*[۲]] را بیش از [اختصاص: *محدوده مشخص*] ساتع کند که امکان دسترسی به داده احرازهویت مرجع[۳] و داده ایجاد امضا[۴] را میسر می‌کند.	
۱	برون‌تابی محصول ۲
محصول باید اطمینان حاصل کند [اختصاص: *انواع کاربران*] قادر به استفاده از رابط‌ها [اختصاص: *انواع اتصالات*] به‌منظور دسترسی به داده احرازهویت مرجع[۵] و داده ایجاد امضا[۶] نیستند. **نکته کاربردی ۱۵:** محصول باید از حملات علیه داده ایجاد امضا و دیگر داده‌های محرمانه که مبتنی بر پدیده‌ها و آثار فیزیکی	

[۱] FAU_GEN

[۲] emissions

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

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

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

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

قابل‌مشاهده بیرونی محصول می‌باشند، جلوگیری کند. چنین حملاتی ممکن است در واسط‌های محصول قابل مشاهده باشد یا ممکن است از عملیات درونی محصول نشأت بگیرد یا ممکن است از مهاجمی نشأت بگیرد که محیط فیزیکی که محصول در آن عمل می‌کند را تغییر می‌دهد. مجموعه آثار فیزیکی قابل اندازه‌گیری تحت تأثیر تکنولوژی به‌کار رفته در پیاده‌سازی محصول قرار دارد. مثال‌هایی از این آثار قابل‌اندازه‌گیری، تغییر در مصرف نیرو، زمان‌بندی انتقال حالات درونی، تشعشعات الکترومغناطیس ناشی از عملیات درونی، تابش امواج رادیویی می‌باشد.

با توجه به اینکه ماهیت تکنولوژی‌هایی که ممکن است باعث چنین برون‌تابی‌هایی شوند ناهمگن است، ارزیابی در برابر حملات پیشرفته کاربردپذیر در تکنولوژی‌های به‌کارگرفته شده در محصول، فرض شده‌است. مثال‌هایی از این حملات می‌تواند شامل این موارد باشد البته محدود به این موارد نیستند: ارزیابی تشعشعات الکترومغناطیس محصول، تحلیل ساده نیرو[۱] (SPA)، تحلیل تفاضلی نیرو[۲] (DPA)، حملات زمان‌بندی شده و غیره.

۶-۶- کلاس کانال‌ها و یا مسیرهای مورد اعتماد

شماره الزام	نام الزام
۴۹	کانال قابل‌اعتماد درون محصول / داده ایجاد امضا ۱
وراثت: از هیچ مؤلفه دیگر ندارد وابستگی: ندارد محصول باید کانال ارتباطی‌ای بین خود و دیگر محصولات فناوری اطلاعاتی قابل‌اعتماد فراهم آورد که منطقاً از دیگر کانال‌های ارتباطی مجزا هستند و شناسایی تضمین شده‌ای از نقاط پایانی‌اش و محافظت از داده کانال در برابر تغییر یا افشا فراهم آورد.	
۵۰	کانال قابل‌اعتماد درون محصول / داده ایجاد امضا ۲
محصول باید اجازه دهند دیگر محصولات فناوری اطلاعاتی قابل‌اعتماد[۳] ارتباط را از طریق کانال قابل‌اعتماد آغاز کنند.	

[۱] Simple Power Analysis

[۲] Differential Power Analysis

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

۵۱	کانال قابل‌اعتماد درون محصول / داده ایجاد امضا ۳

محصول باید ارتباط از طریق کانال قابل‌اعتماد را برای موارد زیر آغاز کنند:

(۱) یکپارچگی تبادل داده طبق الزام کارکرد امنیتی محرمانگی تبادل داده پایه

(۲) [اختصاص: *فهرستی از توابع دیگر که برای یک کانال قابل‌اعتماد مورد نیاز است*][۱]

نکته کاربردی ۱۶:

الزام کارکرد امنیتی کانال قابل‌اعتماد درون توابع هدف امنیتی[۲] به محصول نیاز دارد تا از کانال قابل‌اعتماد برقرار شده با دیگر محصولات فناوری اطلاعاتی قابل‌اعتماد پشتیبانی کند که زوج داده ایجاد امضا / داده درستی‌سنجی امضا را به‌نحو توصیف شده در الزام کارکرد امنیتی محرمانگی تبادل داده پایه جهت ورود داده ایجاد امضا تولید می‌کنند. نویسنده هدف امنیتی باید عملیات از دست رفته در عنصر الزام کارکرد امنیتی کانال قابل‌اعتماد درون محصول / داده ایجاد امضا ۳ را انجام دهد. اگر محصول استفاده از کانال قابل‌اعتماد را برای توابع دیگر اجرا نکرد، عملیات در عنصر کانال قابل‌اعتماد درون محصول / داده ایجاد امضا ۳ "هیچ" است.

[۱] [اختصاص: *فهرستی از توابع مورد نیاز برای کانال قابل اعتماد*]

[۲] FTP_ITC.1

۷- الزامات تضمین امنیتی

جدول ۴ الزامات تضمین: سطح تضمین ارزیابی ۴ تکمیل شده با تحلیل آسیب‌پذیری روشمند هوشمند

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

	ASE_TSS.1	خلاصه مشخصه هدف ارزیابی

۸- منطق

۸-۱- توجیه الزامات امنیتی

۸-۱-۱- پوشش الزامات امنیتی

جدول ۵ نگاشت الزامات کارکردیِ اهداف امنیتی برای محصول

اهداف امنیتی محصول / الزامات کارکردی	OT.Lifecycle_Security	OT_SCD_Auth_Imp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TO	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance
FCS_CKM.4	×		×						
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					×	×			
FIA_AFL.1					×				
FIA_UAU.1		×			×				
FIA_UID.1		×			×				
FMT_MOF.1	×				×				
FMT_MSA.1/Admin	×								
FMT_MSA.1/Signatory	×				×				

اهداف امنیتی محصول / 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
FMT_MSA.2	×				×				
FMT_MSA.3	×				×				
FMT_MSA.4	×				×				
FMT_MTD.1/Admin	×				×				
FMT_MTD.1/Signatory	×				×				
FMT_SMR.1	×				×				
FMT_SMF.1	×				×				
FPT_EMS.1			×				×		
FPT_FLS.1			×						
FPT_PHP.1								×	
FPT_PHP.3			×						×
FPT_TST.1	×		×	×					
FPT_ITC.1/SCD	×		×						

۸-۱-۲-کفایت الزامات امنیتی محصول

هدف امنیتی	توضیحات
OT.Lifecycle_Security امنیت چرخه‌حیات	امنیت چرخه حیات توسط الزامات کارکرد امنیتی به نحوی که در ادامه می‌آید تامین شده‌است. ورود داده ایجاد امضا توسط محصول مطابق کنترل دسترسی زیر مجموعه / ورود داده ایجاد امضا ، مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / ورود داده ایجاد امضا و ورود داده کاربر بدون مشخصه‌های امنیتی / داده ایجاد امضا کنترل می‌شود. محرمانگی داده ایجاد امضا در طول ورود مطابق الزام کارکرد امنیتی محرمانگی تبادل داده‌های پایه / داده ایجاد امضا در کانال قابل‌اعتماد الزام کارکرد امنیتی کانال قابل اعتماد درونی محصول / داده ایجاد امضا محافظت می‌شود. کاربری امن داده ایجاد امضا به شیوه رمزنگاری‌شده‌ای طبق الزام کارکرد امنیتی عملیات رمزنگاری تضمین می‌گردد. کاربری داده ایجاد امضا تحت کنترل دسترسی الزام کارکرد امنیتی کنترل دسترسی زیر مجموعه / ایجاد امضا و الزام کارکرد امنیتی مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / ایجاد امضا کنترل می‌شود که مبتنی بر مشخصه‌های امنیتی مدیریت محصول امن مطابق الزامات کارکرد امنیتی مدیریت رفتار توابع امنیتی، مدیریت مشخصه‌های امنیتی / مدیر سیستم، مدیریت مشخصه‌های امنیتی / صاحب‌امضا، مشخصه‌های امنیتی امن، مقداردهی اولیه مشخصه ایستا، ارث‌بری مقادیر مشخصه‌های امنیتی، مدیریت داده امنیتی / مدیر سیستم و مدیریت داده امنیتی / صاحب‌امضا می‌باشد. الزامات کارکرد امنیتی مشخصات کارکردهای مدیریت امنیت و نقش‌های امنیتی قوانین و کارکردهای مدیریت امنیتی را تعریف می‌کنند. تابع آزمون الزام کارکرد امنیتی آزمودن محصول آشکارسازی خرابی را در سر تا سر چرخه حیات فراهم می‌کند. الزام کارکردی امنیت تخریب کلید رمزنگاری تخریب امن داده ایجاد امضا را تضمین می‌کند.

OT.SCD_AUT_IMP ورود داده ایجاد امضای مجاز	این هدف با توابع امنیتی مشخص‌شده توسط الزامات کارکرد امنیتی زیر تامین شده است. الزامات کارکرد امنیتی زمان‌بندی شناسایی و زمان‌بندی احراز هویت اطمینان حاصل می‌کند که قبل از اینکه داده ایجاد امضا بتواند وارد شود کاربر شناسایی و احراز هویت شده باشد. الزامات کارکرد امنیتی کنترل دسترسی زیر مجموعه / ورود داده ایجاد امضا و مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / ورود داده ایجاد امضا تضمین می‌کند که تنها کاربران مجاز بتوانند داده ایجاد امضا را وارد کنند.

OT.SCD_Secrecry رازمانی داده ایجاد امضا	این هدف با توابع امنیتی مشخص‌شده توسط الزامات کارکرد امنیتی زیر تامین شده است. الزامات کارکرد امنیتی محرمانگی تبادل داده‌های پایه / داده ایجاد امضا و کانال قابل اعتماد درونی محصول / داده ایجاد امضا، محرمانگی ورود داده ایجاد امضا را تضمین می‌کنند. توابع امنیتی مشخص شده توسط الزامات کارکرد امنیتی حفاظت از اطلاعات باقیمانده زیر مجموعه و تخریب کلید رمزنگاری تضمین می‌کنند که اطلاعات باقیمانده روی داده ایجاد امضا بعد از استفاده از داده ایجاد امضا برای ایجاد امضا از بین خواهند رفت و تخریب داده ایجاد امضا هیچ اطلاعات باقیمانده‌ای بر جای نخواهد گذاشت. تابع امنیتی مشخص شده توسط الزام کارکرد امنیتی نظارت بر یکپارچگی داده‌های ذخیره شده و اقدامی برای آن / ماندگاری تضمین می‌کند که هیچ داده حیاتی‌ای به گونه‌ای تغییر نیابد که بتواند کارایی توابع امنیتی را تغییر دهد و یا اطلاعات داده ایجاد امضا را فاش کند. الزام کارکرد امنیتی آزمودن محصول شرایط کار کردن محصول را می‌آزماید و زمانی که یکپارچگی مورد تخلف قرار گرفته باشد الزام کارکرد امنیتی حفظ حالت امن در صورت شکست حالت امنی را تضمین می‌کند و اطمینان می‌دهد که توابع امنیتی خاصی عملیاتی هستند. نمونه‌ای که در آن شرایط خطای تهدیدآمیز با الزام کارکرد امنیتی حفظ حالت امن در صورت شکست پاسخ داده می‌شود، تزریق خطا برای تحلیل خطای تفاضلی[1] (DFA) می‌باشد. الزامات کارکرد امنیتی برون‌تابی محصول ۱ و مقاومت در مقابل حمله فیزیکی به ویژگی‌های امنیتی بیشتری برای حصول اطمینان از محرمانگی داده ایجاد امضا نیاز دارد.

[1] Differential Fault Analysis

OT.Sig_Secure امنیت رمزنگاری امضای الکترونیک	این هدف که توسط الگوریتم رمزنگاری مشخص‌شده توسط الزام کارکردی عملیات رمزنگاری فراهم می‌شود و قدرت رمزنگاری الگوریتم‌های امضا را تضمین می‌کند. الزام کارکرد امنیتی نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / ماندگاری مربوط به یکپارچگی داده ایجاد امضای پیاده‌سازی توسط محصول می‌باشد و الزام کارکرد امنیتی آزمون محصول این اطمینان را می‌دهد که خودآزمائی برای تضمین ایجاد امضای صحیح صورت گرفته‌است.

OT.Sigy_SigF تابع ایجاد امضا تنها برای صاحب‌امضای قانونی	این هدف با الزام کارکرد امنیتی برای شناسایی احرازهویت و کنترل دسترسی تامین شده‌است. الزامات کارکرد امنیتی زمانبندی احرازهویت و زمانبندی شناسایی تضمین می‌کنند که هیچ تابع ایجاد امضایی نمی‌تواند قبل از اینکه صاحب‌امضا شناسایی و احرازهویت شود، فراخوانی گردد. توابع امنیتی توصیف شده توسط الزامات کارکرد امنیتی مدیریت داده امنیتی / مدیر سیستم و مدیریت داده امنیتی / صاحب‌امضا توابع احرازهویت را مدیریت می‌کنند. الزام کارکرد امنیتی ساماندهی شکست در احرازهویت در برابر تعدادی از حملات ازجمله استخراج رمزنگاری اطلاعات باقیمانده، حملات جستجوی فراگیر[1] در مقابل احرازهویت محافظت می‌کند. تابع امنیتی توصیف شده توسط الزام کارکرد امنیتی نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / داده‌ای که باید امضا شود، یکپارچگی DTBS ذخیره‌شده را تضمین می‌کند. توابع امنیتی مشخص‌شده توسط الزامات کارکرد امنیتی کنترل دسترسی زیرمجموعه / خط‌مشی کارکرد امنیتی ایجاد امضا و مشخصه‌های امنیتی مبتنی بر کنترل دسترسی / خط‌مشی کارکرد امنیتی ایجاد امضا، کنترل دسترسی را بر اساس مشخصه‌های امنیتی مدیریت شده طبق الزامات کارکرد امنیتی مدیریت داده امنیتی / صاحب‌امضا، مشخصه‌های امنیتی امن، مقداردهی اولیه مشخصه ایستا و ارث‌بری مقادیر مشخصه‌های امنیتی ارائه می‌دهد. الزام کارکرد امنیتی مدیریت رفتار توابع امنیتی توانایی فعال‌سازی تابع ایجاد امضا را به صاحب‌امضا محدود می‌کند. الزامات کارکرد امنیتی، مشخصات کارکردهای مدیریت امنیت و نقش‌های امنیتی این کارکردها و نقش‌های مدیریتی را فهرست می‌کنند. این الزامات این اطمینان را حاصل می‌کند که فرایند امضا به صاحب‌امضا محدود شود. علاوه بر این، قابلیت کارکرد امنیتی مشخص شده توسط الزام کارکرد امنیتی حفاظت از اطلاعات باقیمانده زیر مجموعه این اطمینان را حاصل می‌کند که زمانی که داده ایجاد امضا توسط صاحب‌امضای قانونی حذف می‌شود، هیچ مهاجمی نتواند داده ایجاد امضا را (برای ایجاد امضا بیرون از محصول) تصرف کند.

[1] Brute force

OT.DTBS_Integrity_TOE یکپارچگی داده‌هایی که باید امضا شوند یا بازنمایی منحصربه‌فرد متعلق به درون محصول	این هدف تضمین می‌کند که داده‌هایی که باید امضا شوند یا بازنمایی منحصربه‌فرد متعلق به آن‌ها توسط محصول تغییر نمی‌کند. درستی سنجی این موضوع که داده‌هایی که باید امضا شوند یا بازنمایی منحصربه‌فرد متعلق به آن‌ها به وسیله محصول تغییر نکرده است با توابع مشخص شده توسط الزام کارکرد امنیتی نظارت بر یکپارچگی داده‌های ذخیره‌شده و اقدامی برای آن / داده‌ای که باید امضا شود ارائه شده است.
OT.EMSEC_Design فراهم‌آوردن امنیت برون‌تانی فیزیکی	این هدف این موضوع را پوشش می‌دهد که هیچ‌گونه اطلاعات قابل‌فهمی به بیرون ساتع نشود. این هدف با الزام کارکرد امنیتی برون‌تابی محصول ۱ تامین می‌شود.
OT.Tamper_ID آشکارسازی دست‌کاری	این هدف با الزام کارکرد امنیتی آشکارسازی انفعالی حمله فیزیکی از طریق آشکارسازی انفعالی حملات فیزیکی، تامین می‌شود.
OT.Tamper_Resistance مقاومت در برابر دست‌کاری	این هدف با الزام کارکرد امنیتی مقاومت در مقابل حمله فیزیکی برای مقابله با حملات فیزیکی تامین می‌شود.

۸-۲- برآوردن وابستگی‌های الزامات امنیتی

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

جدول ۶ برآوردن وابستگی‌های الزامات کارکرد امنیتی

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

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
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 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/SCD_Import, FMT_MSA.3
FDP_UCT.1/SCD	[FTP_ITC.1 or FTP_TRP.1], [FDP_ACC.1 or FDP_IFC.1]	FPT_ITC.1/SCD, FDP_ACC.1/SCD_Import
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_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 or 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 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/SCD_Import, FMT_SMR.1, FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD_Import, FMT_SMR.1 FMT_MSA.1/Admin, FMT_MSA.1/Signatory,
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 _Import FDP_ACC.1/ Signature_Creation
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1

الزامات کارکردی	وابستگی‌ها	برآورده شده توسط
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
FPT_ITC.1/SCD	بدون وابستگی	N/A

جدول ۷ 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 انتخاب شده

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 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 رابط انسانی (کاربری)
IT	Information Technology	فناوری اطلاعات
OE	Operational Environment	محیط عملیاتی
OSP	Organizational Security Policy	خط‌مشی امنیتی سازمانی
RAD	Reference Authentication data	داده 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 3, CCMB-2009-07-001, July 2009

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

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

[5] Protection Profile Secure Signature Creation Device Type 3, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-00062002, also short SSCD-PP or CWA14169

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

[7] 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

[8] 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

[9] 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