به نام خدا

پروفایل حفاظتی سرویس‌دهنده‌های ایمیل

بهمن ۱۴۰۲

نسخه ۱,۰

پیشگفتار

امروزه با رشد سریع علوم کامپیوتر و توسعه‌ی روزافزون اینترنت در کشورها استفاده از سرویس ایمیل به یک نیاز روزمره و حیاتی برای کاربران اینترنت تبدیل‌شده است به‌طوری‌که مبنای بسیاری از مکاتبات رسمی و غیررسمی را تشکیل می‌دهد. این مسئله تأمین امنیت پیغام‌های کاربران و محافظت از آن‌ها در مقابل حملات مختلف را به یک نیاز اساسی تبدیل کرده است. شاید در گذشته سرویس ایمیل از امنیت چندانی برخوردار نبود ولی در سال‌های اخیر این مسئله موضوع بحث و گفتگو در سازمان‌های مرجع و تعریف‌کننده در حوزه‌ی امنیت شبکه بوده و معماری‌های جامع و تست‌شده‌ای در این خصوص ارائه‌شده است. سند پیش‌رو با بررسی مجموعه استانداردهای امنیتی تدوین‌شده توسط سازمان‌های 3GPP و NIST برای یک سرویس‌دهنده ایمیل و با تکیه بر الگوهای معیار مشترک در نگارش پروفایل‌های حفاظتی تدوین‌شده است، به‌طوری‌که با الگو قرار دادن آخرین نسخه از پروفایل حفاظتی مرجع برای محصولات شبکه مجموعه الزامات کارکردی-امنیتی لازم برای ساخت یک سرویس‌دهنده ایمیل امن را تعریف و چارچوب اعتبارسنجی این الزامات توسط ارزیاب را نیز بیان کرده است.

این سند در ۹ فصل، تدوین شده است. فصل اول به‌طور گذرا به بررسی معماری استاندارد و امن ارائه‌شده برای یک سرویس‌دهنده ایمیل می‌پردازد. فصل دوم انطباق سند با سطوح معیار مشترک را ذکر می‌کند. فصل سوم به معرفی دارایی‌ها، فرضیات، سیاست‌های سازمانی و تهدیدات می‌پردازد. فصل چهارم با دو زیر بخش، نخست به تشریح تهدیدات امنیتی موجود می‌پردازد به‌طوری‌که به‌صورت خلاصه و تیتروار به الزامات کارکردی-امنیتی در نظر گرفته‌شده برای رفع هر تهدید نیز اشاره می‌کند. همچنین در زیر بخش دوم از آن نگاشت اهداف به فرضیات، سیاست‌های سازمانی و تهدیدات ذکرشده است. اما بخش اصلی از این سند فصل پنجم است که به بیان الزامات کارکردی-امنیتی موردنظر برای رفع تهدیدها می‌پردازد. همچنین در ادامه در فصل ۶ نیز رویه‌ها و الزامات در نظر گرفته‌شده برای ارزیابی یک سرویس‌دهنده ایمیل توسط ارزیاب و نحوه تعیین پایبندی آن به الزامات کارکردی-امنیتی ذکرشده است. فصل‌های ۷ و ۸ نیز به الزامات کارکردی-امنیتی اختیاری و انتخابی اختصاص دارد که در فصل ۵ به آن‌ها اشاره خواهد شد. فصل ۹ نیز لیست مراجع مورد استفاده در نگارش این سند را ارائه می‌دهد.

این پروفایل حفاظتی محصولات امنیتی با همکاری سازمان فناوری اطلاعات ایران، مرکز مدیریت راهبردی افتا، پژوهشگاه ارتباطات و فناوری اطلاعات و مرکز تحقیق و توسعه همراه اول تهیه، تدوین و انتشاریافته است.

فهرست مطالب

عنوان **صفحه**

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

فهرست جدول‌ها

عنوان **صفحه**

فهرست شکل‌ها

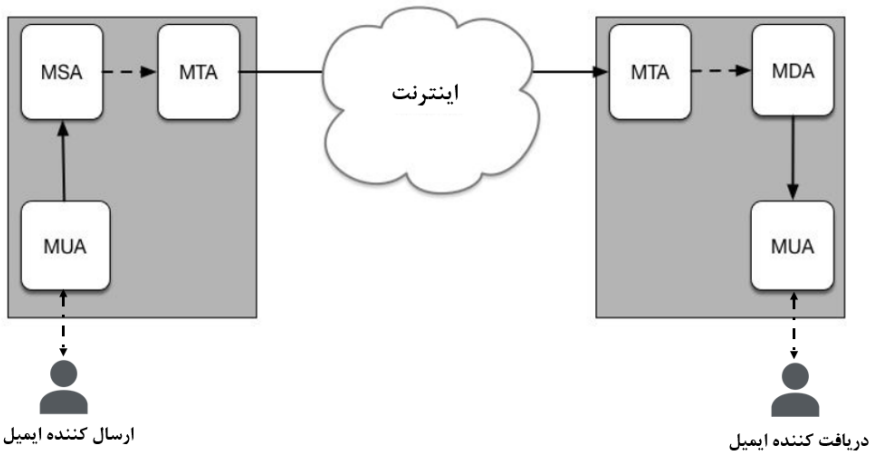
عنوان **صفحه**

فصل ۱– معرفی محصول مورد ارزیابی (TOE)

محصول موردبررسی در این پروفایل حفاظتی یک سرویس‌دهنده‌ی ایمیل است. وظیفه اصلی یک سرویس‌دهنده‌ی ایمیل، فراهم کردن مکانیزم‌هایی امن برای دریافت، ارسال و تحویل ایمیل است.

۱–۱– مکانیزم کاری و مؤلفه‌های اصلی یک سرویس‌دهنده ایمیل

شکل زیر مکانیزم کاری و مؤلفه‌های نرم‌افزاری درگیر در فرایند ایجاد، ارسال و دریافت ایمیل در بستر اینترنت را نشان می‌دهد.



شکل ۱-۱ مؤلفه‌های شرکت‌کننده در فرایند ایجاد، ارسال و دریافت ایمیل

وظیفه‌ی مؤلفه‌های نرم‌افزاری ذکرشده در تصویر از قرار زیر است:

مؤلفه MUA (Mail User Agent) : این مؤلفه‌ی نرم‌افزاری امکان استفاده از سرویس ایمیل را برای کاربر نهایی فراهم می‌کند. کاربر نهایی می‌تواند از طریق آن ایمیل ساخته و ارسال کند و یا به ایمیل‌های موجود در جعبه‌ی ایمیل[۱] خود دسترسی داشته باشد. مؤلفه MUA عموماً به دو صورت دسترسی وب و نیز نرم‌افزار قابل‌نصب بر روی موبایل یا کامپیوتر کاربر ارائه می‌شود. همچنان که در شکل ۱-۱ مشخص است، این مؤلفه برای دسترسی به ایمیل‌ها یا ارسال ایمیل جدید نیازمند ارتباط با سرویس‌دهنده ایمیل

[۱] Mail Box

مربوط به خود (مؤلفه MSA یا MDA از آن) است. این اتصال با بهره‌گیری از پروتکل‌های مختلفی انجام می‌شود که جلوتر به آن‌ها اشاره خواهد شد.

مؤلفه MSA (Mail Submission Agent): این مؤلفه با دریافت ایمیل از مؤلفه‌ی MUA پردازش‌های اولیه ازجمله احراز هویت ارسال‌کننده را انجام داده و آن را جهت ارسال به مقصد به مؤلفه‌ی MTA تحویل می‌دهد.

مؤلفه MDA (Mail Delivery Agent): این مؤلفه با تحویل ایمیل از مؤلفه‌ی MTA آن را در جعبه‌ی ایمیل مربوطه قرار می‌دهد و امکان دسترسی مؤلفه (های) MUA به ایمیل‌ها را فراهم می‌کند.

مؤلفه MTA (Mail Transfer Agent): این مؤلفه وظیفه ارسال ایمیل به مقصد را دارد. قابل‌ذکر است که یک ایمیل ممکن است از مؤلفه‌های MTA متعدد در مسیر بگذرد تا به مؤلفه MTA در مقصد برسد.

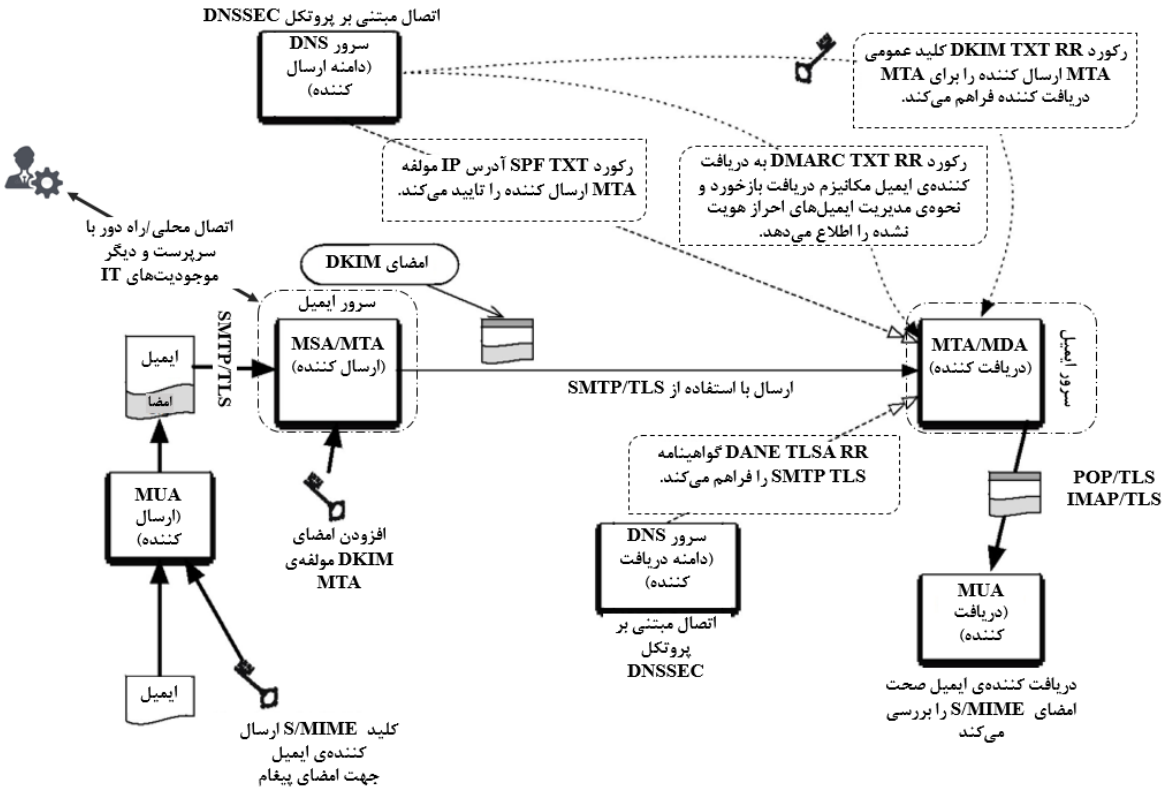
به‌طور کل، یک سرویس‌دهنده‌ی ایمیل از سه نوع مؤلفه‌ی MDA، MSA و MTA و همچنین مؤلفه‌ی MUA در حالت دسترسی وب تشکیل می‌شود. مؤلفه MUA در حالتی که به‌صورت نرم‌افزار قابل‌نصب بر روی کامپیوتر یا گوشی کاربر باشد، در سمت کاربر قرارگرفته و این کارکرد که «کاربر سرویس ایمیل» نامیده می‌شود در این سند بررسی نشده است.

۲-۱-معماری امنیتی و انواع اتصالات در یک سرویس‌دهنده ایمیل

مطابق با اسناد سازمان NIST که ارائه‌دهنده‌ی مدون‌ترین و جدیدترین استانداردها در حوزه‌ی تأمین امنیت برای سرویس ایمیل است، نمای بصری از معماری امنیتی یک سرویس‌دهنده‌ی ایمیل با تأکید بر مکانیزم ارسال ایمیل به‌صورت زیر است[3,4]:

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)



شکل ۱-۲ چارچوب امنیتی یک سرویس‌دهنده‌ی ایمیل [3]

مطابق با شکل فوق، چارچوب امنیتی یک سرویس ایمیل را در دو حوزه می‌توان بررسی کرد:

۱. مدیریت سرویس‌دهنده ایمیل و امنیت اتصالات آن با دیگر موجودیت‌های IT: این حوزه اشاره به مدیریت دسترسی‌ها در سرور و نیز اتصالات آن با دیگر موجودیت‌های IT دارد. این موجودیت می‌تواند یک سرپرست سرور باشد که از اتصال راه دور برای ارتباط با آن استفاده می‌کند، یا یک سرور خارجی برای ارسال رکوردهای ممیزی و یا یک پایگاه داده خارجی باشد.

۲. امنیت مکانیزم‌های ارسال و دریافت ایمیل: این حوزه اشاره به پروتکل‌ها و رویه‌های مورداستفاده جهت تأمین سه مؤلفه‌ی احراز هویت[۱]، محرمانگی[۲] و صحت داده[۳] در طول فرایند دریافت ایمیل از مؤلفه‌ی MUA ارسال‌کننده تا تحویل آن به مؤلفه‌ی متناظر در سمت دریافت‌کننده دارد.

---

[۱] Authentication

[۲] Confidentiality

[۳] Data Integrity

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

شکل ۱-۲ با تأکید بیشتری به تشریح این فرایند می‌پردازد. در این قسمت به‌طور خلاصه و تیتروار به بیان این مکانیزم می‌پردازیم. قابل‌ذکر است که شرح جزییات این چارچوب خارج از هدف این سند بوده و خواننده باید به مرجع [3] مراجعه کند.

- پیشنهاد این چارچوب برای پروتکل مورداستفاده جهت ارسال ایمیل استفاده از پروتکل SMTP[۱] مبتنی بر TLS[۲] است. این پروتکل باید در تمام‌مسیر از مؤلفه‌ی MUA ارسال‌کننده تا مؤلفه MDA در سرور مقصد استفاده شود. به‌طورمعمول هردو عملکرد MTA و MDA در سرویس‌دهنده ایمیل را یک مؤلفه انجام می‌دهد ولی اگر این مخلفه‌ها جدا از هم باشند آنگاه ارتباط آن‌ها نیز باید با استفاده از SMTP مبتنی بر TLS باشد.
- در سمت دریافت‌کننده، MUA باید از پروتکل‌های POP و IMAP مبتنی بر TLS برای دسترسی و برداشتن ایمیل استفاده کند.
- نکته مهم در این چارچوب استفاده از یک مکانیزم مبتنی بر DNS[۳] برای احراز هویت مؤلفه MTA ارسال‌کننده و نیز فراهم کردن گواهینامه X.509 یا کلید عمومی MTA ارسال‌کننده برای MTA دریافت‌کننده است. ازاین‌رو اتصال با سرور DNS باید مبتنی بر پروتکل DNSSEC[۴] باشد تا امنیت اتصال به DNS تضمین شود. همچنین فرض بر این است که سرور DNS از امنیت لازم برخوردار است و تأمین امنیت DNS هدف این سند نیست.
- احراز هویت مؤلفه MTA ارسال‌کننده جهت جلوگیری از آسیب‌هایی چون وجود MTA تقلبی انجام می‌شود. بدین منظور، سرویس‌دهنده ایمیل می‌تواند با استفاده از چارچوب SPF[۵] و ثبت رکوردهای مربوطه بر روی سرور DNS ، آدرس‌های IP معتبر برای مؤلفه‌های MTA خود را تعیین کند تا بدین طریق سرور دریافت‌کننده از معتبر بودن MTA ارسال‌کننده اطمینان حاصل کند.

---

[۱] Simaple Mail Transfer Protocol (SMTP)

[۲] Transport Layer Security (TLS)

[۳] Domain Name System (DNS)

[۴] Domain Name System Security Extensions (DNSSEC)

[۵] Sender Policy Framework (SPF)

- همچنین برای تکمیل احراز هویت و جلوگیری از ایجاد تغییر در سرآیند ایمیل (مانند تغییر در آدرس ایمیل ارسال‌کننده)، MTA ارسال‌کننده باید از مکانیزم DKIM[۱] و تولید امضا از ایمیل و سرآیند آن استفاده کند. با توجه به استفاده از رمزنگاری نامتقارن برای تولید این امضا، برای دسترسی MTA دریافت‌کننده به کلید عمومی ارسال‌کننده از DNS و رکوردهای DKIM TXT RR استفاده می‌شود.

- با استفاده از دو مکانیزم SPF و DKIM سرور دریافت‌کننده‌ی ایمیل می‌تواند از احراز هویت MTA ارسال‌کننده اطمینان حاصل کند و ایمیل‌های نامرتبط را دور ریخته یا قرنطینه کند. حال برای اینکه سرور ارسال‌کننده آماری از ایمیل‌های جعلی ارسالی از جانب خود به دست آورد می‌تواند از مکانیزم DMARC[۲] و رکوردهای DNS مربوطه استفاده و از سرور دریافت‌کننده ایمیل بخواهد تا با تناوب مشخصی گزارش‌های آماری برای او ارسال کند. همچنین بدین طریق می‌تواند چگونگی برخورد با ایمیل‌های احراز هویت نشده را برای دریافت‌کننده مشخص کند و حتی از او بخواهد تا این ایمیل‌ها را در صورت بهره‌مندی از برخی ویژگی‌ها به مقصد تحویل دهد. اهمیت این قابلیت از آنجایی است که ممکن است در یک سرویس‌دهنده ایمیل توزیع‌شده با مؤلفه‌های MTA متعدد آدرس برخی از آن‌ها در رکوردهای SPF ثبت‌نشده یا با توجه به برخی ملاحظات قابل ثبت نباشد.

- با اینکه استفاده از پروتکل SMTP/TLS امنیت لازم برای جلوگیری از شنود و تغییر محتوای ایمیل را فراهم می‌کند اما با توجه به اینکه این پروتکل بین مؤلفه‌ها استفاده‌شده و یک ایمیل ممکن است از مؤلفه‌های MTA متعدد عبور کند تا به مقصد برسد، لذا وجود یک مؤلفه جعلی در میانه راه کافی است تا محتوای ایمیل افشا شود. ازاین‌رو برای تأمین امنیت به‌صورت «جعبه‌ی ایمیل-به-جعبه‌ی ایمیل»[۳] دو پروتکل S/MIME و OpenPGP در این چارچوب پیشنهادشده است. توجه شود که در این حالت فقط محتوای ایمیل رمزنگاری‌شده و سرآیند دخیل نخواهد بود، چراکه برای تعیین مقصد ایمیل، سرور باید قادر به خواندن سرآیند ایمیل باشد. اهمیت امضای DKIM که پیش‌تر اشاره شد نیز ازاین‌جهت است که پس از تعیین شدن مسیر می‌تواند از سرآیند محافظت کند.

---

[۱] DomainKeys Identified Mail (DKIM)

[۲] Domain-based Message Authentication Reporting and Conformance (DMARK)

[۳] MailBox to MailBox

- برای توزیع گواهی‌های TLS ، S/MIME و OpenPGP نیز این چارچوب استفاده از پروتکل DANE بر اساس DNS را پیشنهاد داده است.

به‌طور کل، هدف اصلی این پروفایل حفاظتی تأمین امنیت برای اتصالات، مکانیزم‌ها و کارکردهای ذکرشده با تعیین مجموعه‌ای از الزامات کارکردی-امنیتی است که سازنده‌ی محصول باید آن‌ها را رعایت و پیاده‌سازی کند.

۳-۱- کارکرد محصول

به‌عنوان یک سرویس‌دهنده‌ی ایمیل باهدف دریافت، ارسال و تحویل ایمیل، این پروفایل حفاظتی دو حوزه کارکردی زیر را پوشش خواهد داد:

۱. ارسال و دریافت ایمیل : در این حوزه که تمرکز اصلی این سند هست تأکید بر روی امن سازی سه عملکرد کلیدی یک سرویس‌دهنده ایمیل شامل موارد زیر است :

۱-۱ دریافت ایمیل از مؤلفه MUA در مبدأ

۱-۲ تحویل ایمیل به مؤلفه MUA در مقصد

۱-۳ فرایند ارسال ایمیل از MTA مبدأ به مقصد است.

در مورد مؤلفه‌ی MUA در حالت دسترسی وب که توسط سرویس‌دهنده ایمیل فراهم و مدیریت می‌شود، تمرکز بر روی امنیت فرایند دسترسی به ایمیل‌ها ، ایجاد و ارسال ایمیل به MSA و همچنین تأمین امنیت ایمیل‌ها به‌صورت «جعبه‌ی ایمیل-به-جعبه‌ی ایمیل» (میان دو مؤلفه‌ی MUA در مبدأ و مقصد) خواهد بود.

۲. مدیریت سرویس‌دهنده‌ی ایمیل به‌عنوان یک موجودیت از شبکه: این حوزه مدیریت سرور و نیز دسترسی‌ها به آن و همچنین اتصالات آن با دیگر موجودیت‌های IT در شبکه را شامل می‌شود. قابل‌ذکر است که عملکردهای دیگری چون محافظت از پایگاه داده خارج از هدف این سند است.

فصل ۲- معیار مشترک CC[1] (ASE_CCL)

ادعای انطباق این پروفایل حفاظتی با CC به این شرح است:

- تطابق با سری استانداردهای ملی ایران به شماره ۱۵۴۰۸ نسخه ۳,۱ (بازنگری پنجم)
- تطابق با الزامات کارکردی امنیت: تطبیق با استاندارد ملی ایران به شماره ۲-۱۵۴۰۸
- تطابق با الزامات تضمین امنیت: تطبیق با استاندارد ملی ایران به شماره ۳-۱۵۴۰۸

قابل‌ذکر است با وجود اینکه این پروفایل حفاظتی با تکیه بر پروفایل حفاظتی مرجع برای محصولات شبکه نگاشته شده است اما به‌منظور پوشش کامل نیازمندی‌های امنیتی در یک سرویس‌دهنده‌ی ایمیل، علاوه بر الزامات عمومی مطرح‌شده در پروفایل مرجع، الزامات اختصاصی‌تری نیز تعریف‌شده است. برخی از این الزامات به‌عنوان بندهای جدید و در بین همان الزامات مطرح‌شده در پروفایل مرجع ذکرشده است، ولی برای بیان موارد اختصاصی‌تر، الزامات جدیدی نیز تعریف‌شده است. این الزامات با توسعه خانواده FCS و FIA و با پسوند EXT و به‌منظور پوشش نیازمندی‌های اختصاصی برای امن کردن فرایند دریافت، ارسال و تحویل ایمیل ذکرشده است. مشابه با سری الزام FCS_DNSSEC_EXT که برای پروتکل DNSSEC تعریف‌شده است، این الزامات به‌طور عمومی شامل پروتکل‌ها و مکانیزم‌های اختصاصی برای یک سرویس‌دهنده‌ی ایمیل امن است. ازاین‌رو، این پروفایل حفاظتی هیچ خانواده جدیدی از الزامات تعریف نکرده و تنها خانواده‌های ذکرشده توسعه داده‌شده است. جزییات هر الزام در بخش الزامات کارکردی-امنیتی در فصل ۵ در دسترس است.

انطباق محض[2] با این پروفایل حفاظتی (PP) در صورت ادعای انطباق با آن در دیگر پروفایل‌های حفاظتی یا در هر سند هدف امنیتی (ST) الزامی است. به جهت یادآوری، میزان تطابق ST با هر PP به دو صورت ذیل می‌تواند باشد:

- انطباق محض: ST شامل یا فراتر از PP است.
  - تعریف مسئله امنیت: ST باید کاملاً حاوی تعریف مسئله امنیت موجود در PP باشد. فرضیات ST می‌تواند کمتر باشد و افزودن فرض اضافی، به‌شرط عدم ایجاد تهدید جدید، ممکن است.

[1] Common Criteria

[2] Strict Conformance

- اهداف امنیتی: تمامی اهداف امنیتی PP باید برای ST نیز باشد و علاوه بر آن، ST می‌تواند اهداف بیشتری نیز داشته باشد.
- الزامات امنیتی: ST حاوی تمامی الزامات کارکردی و تضمین امنیت PP است و علاوه بر آن، می‌تواند الزامات اضافی نیز داشته باشد.

- انطباق قابل‌اثبات[1]: ST می‌تواند با ارائه دلایل منطقی، برخی موارد PP را تقلیل دهد یا مقید سازد.

این PP هیچ ادعایی برای انطباق با PP دیگری ندارد. همچنین این PP در انطباق با سطح یک تضمین ارزیابی یا EAL1 است. سطوح تضمین ارزیابی در **شکل ۱-۳** نشان داده‌شده است.

[1] Demonstrable

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

شکل ۱-۳ سطح تضمین ارزیابی بر اساس کلاس‌های تضمین

فصل ۳– تعریف مسئله امنیت (ASE_SPD)

تعریف مسئله امنیت شامل بیان دارایی‌ها، تهدیدات، فرضیات و سیاست‌های امنیتی سازمان است.

۳–۱– دارایی‌ها

۱. FIRMWARE: سفت افزار سرور که کارکرد آن را کنترل و مدیریت می‌کند.
۲. USER_DATA: اطلاعات حساب‌های کاربری و نیز ایمیل‌های کاربران که یکی از مهم‌ترین دارایی‌ها در سرور به‌حساب می‌آید.
۳. SERVER_DATA: اطلاعات پیکربندی، کنترلی و ترافیکی مربوط به سرور که به کمک آن‌ها به دیگر تجهیزات شبکه وصل می‌شود.
۴. SECURITY_DATA: کلیدهای رمزنگاری، گواهی‌های امنیتی، اطلاعات احراز هویت، شناسه‌ها و غیره که در سرور نگه‌داری می‌شوند.

۳–۲– تهدیدات

همچنان که پیش‌تر اشاره شد، وظیفه اصلی یک سرویس‌دهنده ایمیل دریافت، ارسال و تحویل ایمیل به مقصد است. این فرایند با تهدیدات مختلفی همراه است و مهاجم به روش‌های مختلفی می‌تواند به شنود یا تغییر ایمیل‌ها اقدام کرده و یا حتی با حملات منع سرویس اقدام به از کار انداختن سرویس‌دهنده ایمیل کند. لذا امنیت این فرایند باید حتماً تضمین شود.

اما جدا از این نقش، به‌عنوان یک مؤلفه از شبکه، سرویس‌دهنده ایمیل ممکن است به مؤلفه‌های دیگری از شبکه مانند یک سرور خارجی جهت ذخیره رکوردهای ممیزی یا به‌روزرسانی نرم‌افزار متصل باشد، و یا جهت پیکربندی سرور، سرپرست آن از اتصال راه دور استفاده کند. لذا گستره تهدیدات می‌تواند لیست طولانی‌تری را شامل شود. همچنین ذخیره‌سازی داده‌های امنیتی مانند رمز عبور سرپرست یا کلیدهای رمزنگاری نیز بستر تهدیدات امنیتی بیشتری را فراهم می‌کند. تلاش در شناسایی کارکردهای امنیتی دارای مشکل نیز همواره از روش‌های مطلوب برای تهدید سیستم است. از سویی دیگر عامل تهدیدکننده همواره سعی خواهد کرد تا هیچ اثری از خود باقی نگذارد. ازاین‌رو، کلیه فعالیت‌ها در سیستم باید به‌صورت رکوردهای ممیزی ثبت و ضبط شود. بر مبنای توضیحات ارائه‌شده، تهدیدات شناسایی‌شده برای یک سرویس‌دهنده ایمیل از قرار زیر است:

۱. T.UNAUTHORIZED_SERVER_OAM_ACCESS: منظور از این تهدید، تلاش یک مهاجم یا عامل بیگانه برای نفوذ به سرویس‌دهنده ایمیل ضمن کسب دسترسی در سطح سرپرست است. عامل مربوطه به روش‌های مختلفی می‌تواند این حمله را انجام دهد؛ ازجمله اینکه خود را به‌عنوان سرپرست به سرور معرفی کند و وارد آن شود، یا به‌طور معکوس در حالت

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

پیکربندی سرور از راه دور، در میانه کانال ارتباطی میان سرور و سرپرست قرارگرفته و خود را به‌عنوان سرور به سرپرست معرفی کند و از طریق ذخیره پیام‌های احراز هویتی که از جانب سرپرست به سرور ارسال می‌شود و باز ارسال آن‌ها در همان زمان یا وقت دیگری دسترسی در سطح سرپرست به سرور پیدا کند. با برخورداری از چنین سطح از دسترسی، ضمن سرقت اطلاعات، مهاجم می‌تواند با نصب بدافزار روی سیستم‌عامل سرور در کار آن اخلال ایجاد کند و یا شروع به ارسال ایمیل‌های جعلی به کاربران کرده و اطلاعات آن‌ها را به سرقت ببرد.

۲. T.CHANNEL_EAVESDROP_AND_MANIPULATION: این تهدید اشاره به شنود، دست‌کاری و ایجاد اختلال در کانال تشکیل‌شده میان سرویس‌دهنده ایمیل و دیگر موجودیت‌های IT مانند سرور رکوردهای ممیزی، سرور پایگاه داده و یا کانال ارتباطی میان سرور و یک سرپرست راه دور دارد. مهاجم با قرار گرفتن در مسیر انتقال اطلاعات میان سرور و این موجودیت‌ها می‌تواند به استراق سمع ، جاسوسی و یا حتی تغییر اطلاعات بپردازد. لذا کانال ارتباطی میان سرور و دیگر موجودیت‌های IT باید با استفاده از پروتکل‌های امن باشد.

۳. T.UNAUTHORIZED_EMAIL_SENDER/RECEIVER: این تهدید اشاره به وجود یک مؤلفه‌ی MTA تقلبی در درون شبکه‌ی سرویس‌دهنده ایمیل دارد. این مؤلفه‌ی تقلبی هم در سمت سرور ارسال‌کننده‌ی ایمیل و هم در سمت سرور دریافت‌کننده، ممکن است وجود داشته باشد. در این حالت مؤلفه‌ی مذکور با بهره‌مندی از فضای IP شبکه‌ی سرور اقدام به ارسال یا دریافت ایمیل می‌کند. با توجه به معتبر بودن آدرس IP و دامنه، ایمیل‌های ارسالی معتبر شناخته خواهند شد. همچنین به‌عنوان دریافت‌کننده‌ی تقلبی، با پذیرش ایمیل‌های آلوده راه برای نفوذ به شبکه دریافت‌کننده بازخواهد شد. حالت‌های مختلفی برای رخ دادن این تهدید وجود دارد، مانند نصب شدن یک بدافزار بر روی یکی از سرورها یا کامپیوتر یکی از کارکنان در درون شرکت ارائه‌دهنده‌ی سرویس ایمیل و یا وجود یک عامل نفوذی.

۴. T.EMAIL_ADDRESS_SPOOFING: این تهدید اشاره به ارسال ایمیل شامل یک آدرس جعلی برای بخش ارسال‌کننده است. در این حالت مهاجم سعی می‌کند تا خود را بجای فرد دیگری جا زده و حمله شونده را فریب دهد. این تهدید از آنجایی است که در پروتکل SMTP می‌توان آدرس ارسال‌کننده را تغییر و یا مقدار دلخواه تعیین کرد. به‌طور مشابه ممکن است مهاجم با استفاده از یک عنوان جعلی برای ایمیل، خود را مدیر شبکه معرفی کرده و اطلاعات حساس از کاربران دریافت کند.

۵. EMAIL_CONTENT_EAVESDROP_AND_MODIFICATION: این تهدید اشاره به شنود یا تغییر محتوای ایمیل در مسیر رسیدن به مقصد دارد.

۶. T.PHISHING : این نوع حمله که برای سرویس‌های ایمیل بسیار رایج است با ارسال ایمیل‌های جعلی به کاربران و باهدف جمع‌آوری اطلاعات حساس مانند اطلاعات کارت‌بانکی یا

نصب بدافزار بر روی سیستم کاربر انجام می‌شود. این کار معمولاً با درخواست از کاربر برای فشردن یک لینک جعلی انجام می‌شود. در حالت عادی معمولاً این ایمیل‌های جعلی به طیف وسیعی از کاربران ارسال می‌شوند ولی در حالت پیشرفته‌تر که Spear Phishing نامیده می‌شود افراد خاصی هدف قرار داده می‌شوند. راه‌های مختلفی برای انجام این نوع حمله وجود دارد که یکی از آن‌ها استفاده از Address Spoofing است که در مورد چهارم به آن اشاره‌شده است، اما در حالت پیشرفته‌تر ممکن است از ایمیل‌های معتبر برای این کار استفاده شود که در این حالت سرویس‌دهنده ایمیل باید قادر به شناسایی و فیلترینگ محتوای ایمیل‌ها بر اساس کلیدواژه‌های خاص و لینک‌های جعلی باشد.

۷. T.DNS_CACHE_POISONING: این تهدید اشاره به وجود رکوردهای جعلی بر روی سرور DNS دارد. برای جلوگیری از این حمله باید تمامی مؤلفه‌های اتصالی به سرور DNS از پروتکل امن DNSSEC استفاده کنند. لذا اگرچه تأمین امنیت DNS خارج از هدف این سند است ولی مطابق با این سند، سرویس‌دهنده ایمیل باید از DNSSEC برای اتصال به سرور DNS استفاده کند.

۸. T.EMAIL_BOMBING: این تهدید اشاره به ارسال گسترده‌ی ایمیل‌ها (معمولاً با ضمیمه‌های حجیم) به یک سرویس‌دهنده ایمیل باهدف مشغول کردن سرور و از کار انداختن آن است به‌گونه‌ای که قادر به دریافت ایمیل‌های واقعی نباشد. در این تهدید که به حمله‌ی منع سرویس[1] نیز مشهور است، حمله‌کننده ممکن است از سرورها و آدرس‌های واقعی برای ارسال ایمیل‌ها استفاده کند.

۹. T.DEVICE_FUNTIONALITY_FAILURE_ EXPLOIT: این تهدید اشاره به کارکرد نادرست کارکردهای امنیتی و شناسایی شدن و بهره‌برداری از آن‌ها توسط مهاجم برای نفوذ به سرویس‌دهنده ایمیل دارد.

۱۰. T.ATTACK_ON_STORED_CREDENTIALS: این تهدید اشاره به دسترسی غیرمجاز به اطلاعات پیکربندی و امنیتی مختلف ذخیره‌شده بر روی سرویس‌دهنده ایمیل دارد. اطلاعاتی مانند نام کاربری و رمز عبور سرپرستان سیستم، کلیدهای رمزنگاری عمومی و خصوصی و گواهینامه‌های X.509.

[1] Denial Of Service (DOS)

۱۱. T.MALICIOUS_UPDATE: این تهدید اشاره به آلوده شدن سرویس‌دهنده ایمیل به‌واسطه به‌روزرسانی‌های نامعتبر دارد.

۱۲. T.UNDETECTED_ACTIONS: این تهدید اشاره به برجای نگذاشتن رد از خود توسط مهاجم دارد که نتیجه آن می‌تواند عدم توانایی در شناخت آسیب‌های رسیده و عامل آن باشد.

۳-۳- سیاست‌های امنیتی سازمانی

هر سازمان یا به‌طورکلی هر محصولی مجموعه‌ای از قوانین و مقررات و یا فرضیات خاص خود را برای محافظت از محصول یا سازمان خود دارد. در صورت وجود، این قوانین باید به هنگام دسترسی کنسول به سرور برای سرپرست مربوطه نمایش داده‌شده و در صورت موافقت با موارد ذکرشده اجازه دسترسی به سرور را پیدا کند.

۱. OSP.ACCESS_BANNER: به هنگام لاگین کنسول در سرور، محصول باید قادر به نمایش بنری باشد که مجموعه قوانین و رویه‌های موردنظر سازمان (یا محصول) جهت دسترسی به سرور را نشان دهد. بدون اعلام موافقت با قوانین مربوطه نباید اجازه ورود داده شود.

الزام کارکردی امنیتی[۱] در نظر گرفته‌شده:

- الزام FTA_TAB.1 نمایش و پیکربندی این بنر دسترسی را تعریف می‌کند.

۴-۳- فرضیات

۱. A.PHYSICAL_PROTECTION: فرض بر این است که سرور در محیط عملیاتی خود به‌صورت فیزیکی محافظت‌شده و در معرض حملات فیزیکی و خسارت‌های ناشی از آن‌ها قرار ندارد. فرض می‌شود که این محافظت برای تأمین امنیت و داده‌های آن کافی است. درنتیجه، این پروفایل حفاظتی شامل هیچ الزامی در زمینه حفاظت فیزیکی و ابزارهای لازم برای کاستن از خسارت‌های ناشی از حملات فیزیکی نیست. این پروفایل از خود محصول انتظار ندارد که از دسترسی فیزیکی به دستگاه جلوگیری به عمل آورد. دسترسی فیزیکی به موجودیت‌های غیرمجاز امکان می‌دهد تا داده‌ها را استخراج کنند، سایر کنترل‌ها را دور بزنند یا به هر طریق دیگری دستگاه را دست‌کاری کنند.

[۱] Security Functional Requirements (SFR)

۲. A.TRUSTED_ADMIN: محصول دارای دفترچه راهنما است و توسط فرد متخصص نصب و پیکربندی اولیه آن صورت می‌گیرد. علاوه بر این، اعتماد کامل به این فرد متخصص ازنظر پیکربندی و تنظیم کلمات عبور وجود دارد.

۳. A.LIMITED_FUNCTIONALITY: فرض بر این است که محصول قرار است نقش یک سرویس‌دهنده‌ی ایمیل را به‌عنوان کارکرد اصلی خود ارائه دهد و سرویس‌های همه‌منظوره و غیر مرتبط با این نقش را ارائه نمی‌دهد.

۴. A.REGULAR_UPDATES: فرض بر این است که در صورت منتشر شدن به‌روزرسانی‌های جدید در پاسخ به آسیب‌پذیری‌های شناسایی‌شده، سرپرست محصول آن را به‌صورت منظم به‌روزرسانی می‌کند.

۵. A.ADMIN_CREDENTIALS_SECURE: فرض می‌شود که اطلاعات محرمانه سرپرست (مانند کلید خصوصی) که برای دسترسی (محلی یا راه دور) به سرویس‌دهنده ایمیل استفاده می‌شوند، توسط سیستمی که روی آن قرار دارند محافظت می‌گردند (منظور از سیستم سرویس‌دهنده ایمیل نیست، بلکه فرضاً کامپیوتر شخصی سرپرست برای اتصال راه دور به سرور هست).

۶. A.RESIDUAL_INFORMATION: فرض می‌شود که برای اطلاعات حساس باقیمانده (مانند کلیدهای رمزنگاری، اجزای سازنده کلید، رمزهای عبور و غیره) روی سرویس‌دهنده ایمیل، زمانی که سرور از محیط عملیاتی حذف یا برداشته می‌شود، امکان دسترسی غیرمجاز وجود ندارد.

فصل ۴– اهداف امنیتی (ASE_OBJ)

در این پروفایل حفاظتی، اهداف امنیتی ذیل به‌منظور ارزیابی امنیتی سرویس‌دهنده‌ی ایمیل در نظر گرفته‌شده است.

۴–۱– اهداف امنیتی برای سرویس‌دهنده‌ی ایمیل

در این قسمت ضمن بیان اهداف امنیتی در نظر گرفته‌شده، الزامات کارکردی-امنیتی مربوطه برای رفع تهدیدات و رسیدن به این اهداف نیز لیست شده است. شرح این الزامات در بخش بعدی بیان‌شده است.

۱. O. SERVER_ ACCESS_CONTROL: سرویس‌دهنده ایمیل باید تعریف و پیاده‌سازی دقیقی از نقش‌ها و دسترسی‌های امنیتی ارائه کند و از مکانیزم‌های امن برای دسترسی و نیز مدیریت نشست‌های برقرارشده استفاده کند.

الزامات کارکردی امنیتی در نظر گرفته‌شده:

- نقش‌های امنیتی در سری الزام FMT_SMR.2 و قابلیت‌ها و دسترسی‌های مدیریتی-امنیتی مربوطه در الزامات FMT_SMF.1 و FMT_MTD.1/CoreData تعریف‌شده است. همچنین امکانات و دسترسی‌های بیشتری نیز در الزامات انتخابی FMT_MOF.1/Services و FMT_MOF.1/Functions در نظر گرفته‌شده است.
- الزام FIA_UIA_EXT.1 سرویس‌های قابل‌ارائه بدون نیاز به انجام احراز هویت به همراه الزام به احراز هویت پیش از انجام کارهای مدیریتی و FTA_TAB.1 نیز امکان نمایش یک بنر شامل پیام هشدار در زمان ورود به سرور را بررسی می‌کنند.
- نیازمندی‌های مربوط به احراز هویت و لاگین سرپرست سرور در الزام FIA_UAU_EXT.2 لحاظ شده است.
- الزامات FTA_SSL_EXT.1، FTA_SSL.3 و FTA_SSL.4 چگونگی مدیریت نشست‌های مدیریتی راه دور و محلی را بررسی می‌کنند.
- اطمینان از امن بودن نشست‌های مدیریتی راه دور در الزام FTP_TRP.1/Admin و با تأکید بر ایجاد یک کانال امن تضمین‌شده است.
- به الزامات مرتبط با شناسایی رویدادهای مشکوک و محافظت از اطلاعات امنیتی مانند رمزهای عبور نیز در ادامه این بخش به‌طور جداگانه اشاره‌شده است.

۲. O. CONNECTION_SECURITY: به‌طورکلی تأمین هر سه شاخصه‌ی محرمانگی، صحت داده و احراز هویت برای اتصال با دیگر موجودیت‌های IT ضروری است و باید از پروتکل‌های امن برای تشکیل این کانال استفاده شود.

الزامات کارکردی امنیتی در نظر گرفته‌شده:

- الزامات FTP_ITC.1 و FTP_TRP.1/Admin با پیشنهاد پروتکل‌های مناسب برای برقراری کانال راه دور امن میان سرور و سرپرست یا با دیگر مؤلفه‌های شبکه، اطمینان از انجام احراز هویت امن را نیز تضمین می‌دهند. همچنین بر اساس انتخاب انجام‌شده در خصوص پروتکل ایجاد کانال، الزامات مربوط به آن پروتکل نیز باید از بخش الزامات انتخابی در این سند رعایت شود. علاوه بر این، الزامات FIA_X509_EXT.1، FIA_X509_EXT.2 و FIA_X509_EXT.3 نیز در صورت تمایل به استفاده از گواهینامه‌های کلید عمومی باید رعایت شوند.
- الزامات FCS_CKM.1 و FCS_CKM.2 در خصوص تولید و استقرار کلید[1] رمزنگاری در نظر گرفته‌شده است.
- الزامات FCS_COP.1/DataEncryption، FCS_COP.1/SigGen، FCS_COP.1/Hash و FCS_COP.1/KeyedHash نیز برای انجام رمزنگاری، تولید امضا و تضمین صحت داده لحاظ شده است.
- الزام FCS_RBG_EXT.1 برای تولید بیت تصادفی مورداستفاده در تولید کلید لحاظ شده است.
- مدیریت کارکردهای امنیتی نیز در الزام FMT_SMF.1 اعمال می‌شود.

۳. O. EMAIL_SENDER/RECEIVER_AUTHENTICATION: برای جلوگیری از ارسال ایمیل توسط مؤلفه‌های MTA جعلی باید از مکانیزم‌هایی امن، استفاده شود. یک سرویس‌دهنده ایمیل باید امکان سوءاستفاده از شبکه خود توسط مهاجمین و تعبیه یک مؤلفه MTA جعلی را به حداقل برساند. همچنین در مقام گیرنده ایمیل باید قادر به احراز هویت ارسال‌کننده‌های معتبر MTA باشد.

الزامات کارکردی امنیتی در نظر گرفته‌شده:

- چهار مجموعه الزام FCS_SPF_EXT.1.X، FCS_ DKIM_EXT.1.X ، FCS_DMARK_EXT.1.X و FCS_DANE_EXT.1.X ابزار و امکان لازم برای تضمین احراز هویت طرفین را فراهم می‌کنند. مجموعه الزام FIA_X509.X نیز در خصوص گواهینامه‌های X.509 و احراز هویت طرفین هم برای این هدف و هم در پروتکل‌هایی چون TLS کارکرد دارد.

۴. O. ADDRESS_SPOOFING _PREVENTION:

الزامات کارکردی امنیتی در نظر گرفته‌شده:

[1] Key Establishment

- سری الزام FCS_ DKIM_EXT.1.X در این خصوص در نظر گرفته‌شده است.

۵. O. EMAIL_CONTENT_SECURITY: باید از شنود و تغییر محتوای ایمیل‌ها در طول مسیر ارسال از مبدأ به مقصد جلوگیری شود.

الزامات کارکردی امنیتی در نظر گرفته‌شده:

- سری الزام FCS_TLSC_EXT.1.X و FCS_TLSS_EXT.1.X برای تأمین امنیت اتصالات SMTP و POP/IMAP در نظر گرفته‌شده است.
- FCS_HTTPS_EXT.X دسترسی تحت وب را امن می‌کند.
- سری الزام FCS_S/MIME_EXT.1.X برای رمزنگاری محتوای ایمیل‌ها در نظر گرفته‌شده است.

۶. O. PHISHING_PREVENTION: برای جلوگیری و کاهش آسیب حملات ناشی از Phishing، سرویس‌دهنده ایمیل باید از مکانیزمی مناسب برای وارسی محتوای ایمیل‌ها از لینک‌ها و کلیدواژه‌های استفاده کند.

الزامات کارکردی امنیتی در نظر گرفته‌شده:

- الزامات FIA_UED_EXT.1 و FIA_UED_EXT.2 در این خصوص در نظر گرفته‌شده است.

۷. O. DNS_CONNECTION_SECURITY: اتصال با سرور DNS باید با استفاده از پروتکل امن DNSSEC باشد تا از امکان حمله‌ی DNS Cache Poisoning جلوگیری شود.

الزامات کارکردی امنیتی در نظر گرفته‌شده:

- سری الزام FCS_DNSSEC_EXT.1.X برای امن کردن اتصال با سرور DNS است.

۸. O. SERVER_AVAILABILITY: با استفاده از سیاست‌ها و مکانیزم‌های مناسب باید از آسیب حملات DOS و DDOS جلوگیری شود.

الزامات کارکردی امنیتی در نظر گرفته‌شده:

- الزامات FIA_UED_EXT.1.X و FIA_UED_EXT.3.X در این خصوص در نظر گرفته‌شده است.

۹. O. DEVICE_FUNTIONALITY_ASSURANCE: سرور باید از سلامت کارکردهای امنیتی خود اطمینان حاصل کند.

الزامات کارکردی امنیتی در نظر گرفته‌شده:

- الزام FPT_TST_EXT.1 پیاده‌سازی انجام تست خودکار را اعمال می‌کند.

۱۰. O. CREDENTIALS_SECURITY: سرور باید قادر به محافظت از اطلاعات امنیتی ذخیره‌شده روی آن مانند نام کاربری و رمز عبور سرپرستان سرور، کلیدهای رمزنگاری عمومی و خصوصی و گواهینامه‌های X.509 بوده و سرپرستان را مجبور به تعیین رمزهای عبور امن، کند.

الزامات کارکردی امنیتی در نظر گرفته‌شده:

- الزام FPT_SKP_EXT.1 به محافظت از کلیدهای عمومی و خصوصی می‌پردازد.
- پاک‌سازی یا نابودسازی کلیدها در الزام FCS_CKM.4 اعمال می‌شود.
- الزام FMT_SMF.1 برای مدیریت کلیدها و الزام اختیاری FMT_MTD.1/CryptoKeys نیز به محدود کردن این دسترسی به سرپرستان سرور اختصاص دارد.
- الزامات FIA_UAU.7، FIA_AFL.1، FPT_APW_EXT.1 و FIA_PMG_EXT.1 به موارد مختلفی ازجمله طول و سختی رمز عبور سرپرستان، جلوگیری از نمایش رمز عبور در زمان واردکردن و ذخیره امن آن‌ها روی سرور می‌پردازند.

۱۱. O. UPDATE_SECURITY: برای حفظ آمادگی سرور در جلوگیری از حملات جدید، نرم‌افزار و در صورت نیاز سفت افزار آن باید به‌صورت مرتب به‌روزرسانی شود. اما پیش از به‌روزرسانی باید اصالت محتوا و نیز مبدأ انجام دهنده آن تأیید هویت شوند. در غیر این صورت احتمال آلوده شدن سرور و نفوذ مهاجمین بالا خواهد بود.

الزامات کارکردی امنیتی در نظر گرفته‌شده:

- مجموعه الزام FPT_TUD_EXT.1 برای امن کردن فرایند به‌روزرسانی لحاظ شده است. همچنین به دنبال انتخاب انجام‌شده در این الزام برای سازوکار تصدیق فایل به‌روزرسانی، نیازمندی‌های بیشتری نیز باید پیاده‌سازی شود که در همان مجموعه الزام FPT_TUD_EXT.1 به آن‌ها اشاره‌شده است.
- الزامات FMT_SMF.1 و FMT_MOF.1/ManualUpdate و همچنین مورد اختیاری FMT_MOF.1/AutoUpdate نیز برای مدیریت و تنظیم فرایند به‌روزرسانی در نظر گرفته‌شده‌اند.

۱۲. O. ACTION_MONITORING: تولید و ثبت رکوردهای ممیزی از فعالیت‌های انجام‌گرفته در سرور، کمک شایانی به سرپرست در بررسی وضعیت آن، شناسایی خطاهای موجود، تولید گزارش و نیز در امور مربوط به حسابرسی سیستم می‌کند. لذا بسیار مهم است که در وهله اول تمامی فعالیت‌های دارای اهمیت رکورد شود و در وهله دوم این رکوردها از تغییر و دست‌کاری در امان باشند، بخصوص در حالتی که از یک سرور syslog خارجی برای ارسال رکوردهای مربوطه استفاده می‌شود.

طبق این پروفایل حفاظتی و نیز با استناد به پروفایل حفاظتی عمومی ثبت‌شده برای تجهیزات شبکه، سرور باید قابلیت ارسال رکوردهای ممیزی به یک سرور syslog خارجی را از طریق یک کانال امن داشته باشد.

الزامات کارکردی امنیتی در نظر گرفته‌شده:

- الزامات FAU_GEN.1 و FAU_GEN.2 به ثبت رکوردهای ممیزی اختصاص دارد. همچنین الزام FPT_STM_EXT.1 به ثبت مهر زمانی روی رکوردهای ممیزی و نیز در صورت استفاده از سرور NTP برای تنظیم زمان، الزام FCS_NTP_EXT.1 نیز به امن کردن کانال ارتباطی با سرور مربوطه اختصاص دارد.
- الزام FAU_STG_EXT.1 به مدیریت چگونگی ذخیره‌سازی رکوردهای ممیزی روی دیسک محلی و نیز ارسال آن‌ها به یک سرور syslog خارجی اشاره دارد.
- الزام اختیاری FAU_STG.1 مربوط به محافظت از رکوردهای ممیزی ذخیره‌شده روی سرویس‌دهنده ایمیل است و دیگر الزام اختیاری FAU_STG_EXT.2/LocSpace به ثبت آمار از تعداد رکوردهای ازدست‌رفته یا رونویسی شده در مواقعی که حافظه سرور پر می‌شود، اشاره دارد.
- در صورت قابل پیکربندی بودن پارامترهای مختلفی چون پروتکل ارتباطی با سرور syslog خارجی یا تعیین چگونگی رونویسی رکوردها در زمان پر شدن حافظه، الزام FMT_MOF.1/Functions انجام چنین پیکربندی‌هایی را به سرپرستان مجاز محدود می‌کند.

۲-۴- اهداف امنیتی برای محیط عملیاتی

۱. OE.PHYSICAL_DEVICE_PROTECTION: امنیت فیزیکی سرویس‌دهنده ایمیل و داده‌هایی که در آن قرار دارند، توسط محیط باید تضمین شود.

۲. OE.TRUSTED_OAM: این هدف اشاره به این دارد که سرپرستان باید قابل‌اعتماد باشند و تمام موارد ذکرشده در اسناد راهنما را به‌طور صحیح انجام دهند و به‌طور عمدی محصول و اطلاعات موجود روی آن را در معرض تهدید قرار ندهند.

۳. OE.NO_GENERAL_PURPOSE: به‌جز کارکرد اصلی که ارائه سرویس ایمیل است، سرویس جانبی دیگری ارائه نمی‌شود.

۴. REGULAR_UPDATE_CHECKING: نرم‌افزارها و میان‌افزارهای سرویس‌دهنده ایمیل باید به‌طور منظم توسط سرپرستان به‌روزرسانی شوند.

۵. OE. CREDENTIALS_SECURITY_OTHER_PLATFORMS

اطلاعات حساب کاربری سرپرستان (مانند کلید خصوصی) که مورداستفاده برای دسترسی به سرور است، در هر پلتفرمی که قرار دارند باید حفاظت‌شده باشند (مقصود در تجهیزات غیر از سرور است).

۶. OE.RESIDUAL_INFORMATION

سرپرست امنیتی باید اطمینان یابد که به اطلاعات باقیمانده حساس (مانند کلیدهای رمزنگاری، اجزای سازنده کلید، رمز عبورها و غیره) روی محصول، وقتی‌که محصول از محیط عملیاتی حذف یا برداشته می‌شود، امکان دسترسی غیرمجاز وجود ندارد.

۳-۴- منطق اهداف امنیتی

در این بخش به‌وسیله یک جدول، نگاشت اهداف امنیتی به تهدیدات، فرضیات و سیاست‌های سازمانی را نشان داده‌ایم. در ادامه توجیهات لازم برای این نگاشت‌ها نیز بیان‌شده است.

۱-۳-۴- نگاشت اهداف امنیتی به مسئله امنیت

در **جدول ۱-۱**، محور افقی اهداف امنیتی در نظر گرفته‌شده برای سرویس‌دهنده ایمیل و محیط عملیاتی آن را نشان داده و محور عمودی نیز تهدیدات، فرضیات و سیاست‌های سازمانی را نشان می‌دهد. هر خانه تیک خورده از جدول نشان می‌دهد که هدف امنیتی مربوطه به کدام تهدید(ات)، فرضیه(ها) و سیاست(های) سازمانی مرتبط می‌شود.

جدول ۱-۱ نگاشت تهدیدات/دارایی‌ها/سیاست‌های سازمان به اهداف امنیتی/محیط عملیات

	O. SERVER_ ACCESS_CONTROL	O. CONNECTION_SECURITY	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION	O. ADDRESS_SPOOFING _PREVENTION	O. EMAIL_CONTENT_SECURITY	O. PHISHING_PREVENTION	O. DNS_CONNECTION_SECURITY	O. SERVER_AVAILABILITY	O. DEVICE_FUNTIONALITY_ASSURANCE	O. CREDENTIALS_SECURITY	O. UPDATE_SECURITY	O. ACTION_MONITORING	OE.PHYSICAL_DEVICE_PROTECTION	OE.TRUSTED_OAM	OE.NO_GENERAL_PURPOSE	OE.REGULAR_UPDATE_CHECKING	OE.CREDENTIALS_SECURITY_OTHER_PLATFORMS	OE.RESIDUAL_INFORMATION_SECURITY
T.UNAUTHORIZED_SERVER_OAM_ACCESS	✓																	
T.CHANNEL_EAVESDROP_AND_MANIPULATION		✓																
T.UNAUTHORIZED_EMAIL_SENDER/RECEIVER			✓															
T.EMAIL_ADDRESS_SPOOFING				✓														
T.EMAIL_CONTENT_EAVESDROP_AND_MOD					✓													

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

	O. SERVER_ ACCESS_CONTROL	O. CONNECTION_SECURITY	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION	O. ADDRESS_SPOOFING _PREVENTION	O. EMAIL_CONTENT_SECURITY	O. PHISHING_PREVENTION	O. DNS_CONNECTION_SECURITY	O. SERVER_AVAILABILITY	O. DEVICE_FUNTIONALITY_ASSURANCE	O. CREDENTIALS_SECURITY	O. UPDATE_SECURITY	O. ACTION_MONITORING	OE.PHYSICAL_DEVICE_PROTECTION	OE.TRUSTED_OAM	OE.NO_GENERAL_PURPOSE	OE.REGULAR_UPDATE_CHECKING	OE.CREDENTIALS_SECURITY_OTHER_PLATFORMS	OE.RESIDUAL_INFORMATION_SECURITY
IFICATION																		
T.PHISHING						✓												
T.DNS_CACHE_POISONING							✓											
T.EMAIL_BOMBING								✓										
T.DEVICE_FUNTIONALITY_FAILURE_ EXPLOIT									✓									
T.ATTACK_ON_STORED_CREDENTIALS										✓								
T.MALICIOUS_UPDATE											✓							
T.UNDETECTED_ACTIONS												✓						
OSP.ACCESS_BANNER	✓																	
A.PHYSICAL_PROTECTION													✓					
A.TRUSTED_ADMIN														✓				
A.LIMITED_FUNCTIONALITY															✓			
A.REGULAR_UPDATES																✓		
A.ADMIN_CREDENTIALS_SECURITY																	✓	
A.RESIDUAL_INFORMATION																		✓

۲-۳-۴- استدلال نگاشت‌ها به اهداف امنیتی

در این قسمت استدلال نگاشت اهداف به تهدیدات، سیاست‌های امنیتی سازمان و فرضیات به‌طور مختصر ارائه‌شده است.

۱-۲-۳-۴- نگاشت تهدیدات

در این سند به ازای هر تهدید یک هدف برای مقابله با آن لحاظ شده است. به‌طور دقیق‌تر هر تهدید یا حذف کامل می‌شود یا به‌وسیله کاهش انگیزه مهاجم یا ایجاد محدودیت برای آن، به‌اندازه کافی تقلیل پیدا می‌کند. قابل‌ذکر است که رسیدن به اهدف امنیتی مربوطه نیز با رعایت الزامات کارکردی امنیتی محقق می‌شود که نگاشت آن در همان بخش اهداف برای هر هدف ذکر شد و توضیحات کامل این الزامات کارکردی امنیتی نیز در بخش بعد آورده شده است.

۱. T.UNAUTHORIZED_SERVER_OAM_ACCESS:
هدف SERVER_ACCESS_ CONTROL از طریق مجموعه الزامات مربوطه، راه را برای دسترسی غیرمجاز به سرور می‌بندد.

۲. T.CHANNEL_EAVESDROP_AND_MANIPULATION: هدف مرتبط با این تهدید با تأمین هر سه ویژگی امنیتی احراز هویت، صحت و محرمانگی اتصالات از شنود و تغییر آن‌ها جلوگیری می‌کند.

۳. T.UNAUTHORIZED_EMAIL_SENDER/RECEIVER: این تهدید از طریق هدف مربوطه و احراز هویت مؤلفه‌ی MTA ارسال‌کننده و دریافت‌کننده برطرف می‌شود.

۴. T.EMAIL_ADDRESS_SPOOFING:
هدف ADDRESS_SPOOFING _PREVENTION با استفاده از مکانیزم‌هایی چون امضای DKIM امکان شناسایی آدرس‌های جعلی یا تغییر داده‌شده برای فرستنده را فراهم می‌کند.

۵. T.EMAIL_CONTENT_EAVESDROP_AND_MODIFICATION:
هدف EMAIL_CONTENT_SECURITY به استفاده از مکانیزم‌ها و لایه‌های امنیتی مختلف برای جلوگیری از تغییر یا شنود محتوای ایمیل‌ها اختصاص دارد.

۶. T.PHISHING: هدف PHISHING_PREVENTION متناظر با این تهدید اختصاص به شناسایی و کاهش خطرات ناشی از تهدید Phishing دارد.

۷. T.DNS_CACHE_POISONING: این تهدید با تأکید بر استفاده از پروتکل امن DNSSEC برای اتصال به سرور DNS در هدف مربوطه رفع می‌شود.

۸. T.EMAIL_BOMBING: هدف SERVER_AVAILABILITY اختصاص به رعایت الزامات کارکردی مختلف برای جلوگیری و کاهش آسیب حملات DOS و DDSO از طریق email bombing دارد.

۹. T.DEVICE_FUNTIONALITY_FAILURE_ EXPLOIT: این تهدید باهدف نگاشت‌شده در جدول فوق از طریق انجام تست خودکار و اطمینان از کارکرد توابع امنیتی رفع می‌شود.

۱۰. T.ATTACK_ON_STORED_CREDENTIALS:

هدف CREDENTIALS_SECURITY به ارائه سیاست‌ها و مکانیزم‌های امن برای ذخیره اطلاعات محرمانه روی سرور اختصاص دارد.

۱۱. T.MALICIOUS_UPDATE: هدف UPDATE_SECURITY به تأیید صحت به‌روزرسانی‌ها ارتباط دارد.

۱۲. T.UNDETECTED_ACTIONS: هدف ACTION_MONITORING به تهیه رکوردهای ممیزی از رخدادهای مهم روی سرور ارتباط دارد.

۲-۲-۳-۴- نگاشت سیاست‌های امنیتی سازمان

۱. OSP.ACCESS_BANNER: هدف O. DEVICE_ ACCESS_CONTROL از طریق الزام کارکردی امنیتی FTA_TAB.1 امکان نمایش و پیکربندی این بنر دسترسی را برای نمایش سیاست‌های سازمانی فراهم می‌کند.

۳-۲-۳-۴- نگاشت فرضیات

همچنان که واضح است اهداف امنیتی در نظر گرفته‌شده برای محیط عملیاتی توسط فرضیات بیان‌شده تأمین می‌شوند. همچنین قرار بر این است که فرضیات بیان‌شده توسط محیط عملیاتی تأمین می‌شود و درنتیجه این سند هیچ الزام امنیتی برای تأمین اهداف امنیتی محیط عملیاتی بیان نمی‌کند.

۱. A.PHYSICAL_PROTECTION:

این فرض تأمین‌کننده هدف امنیتی OE.PHYSICAL_DEVICE_PROTECTION خواهد بود و فرض بر این است که امنیت فیزیکی سرور توسط محیط، تأمین خواهد شد.

۲. A.TRUSTED_ADMIN:

این فرض تأمین‌کننده هدف امنیتی OE.TRUSTED_OAM است. به‌عبارت دیگر کلیه عملیات مدیریتی سرویس‌دهنده ایمیل توسط سرپرستان قابل‌اعتماد، انجام می‌شود.

۳. A.LIMITED_FUNCTIONALITY:

این فرض به هدف OE.NO_GENERAL_PURPOSE نگاشت شده و بیان می‌کند که قرار بر این است که سرویس‌دهنده ایمیل تنها نقش مختص خود را ایفا کرده و الزامی به ایفای نقش‌های بیشتر نیست.

۴. A.REGULAR_UPDATES:

ایـن فـرض بـه هـدف OE.REGULAR_UPDATE_CHECKING نگاشـت شـده و تضـمین می‌دهد که سرویس‌دهنده ایمیل به‌طور مرتب به‌روزرسانی خواهد شد.

۵. A.ADMIN_CREDENTIALS_SECURE:

این فرض با نگاشت به هدف مربوطه بیان می‌کند، فرض بر این است که اطلاعات ذخیره‌شده روی تجهیزات دیگر (مانند کلید خصوصی روی کامپیوتر یک سرپرست) امن بوده و وسیله‌ای برای حمله نخواهد شد.

۶. A.RESIDUAL_INFORMATION:

این فرض با نگاشت به هدف OE.RESIDUAL_INFORMATION_SECURITY بیان می‌کند که در صورت خاموش کردن و جدا کردن سرویس‌دهنده ایمیل از محیط عملیاتی توسط سرپرست، اطلاعات باقی‌مانده در آن مانند کلیدهای نامتقارن امن خواهند بود.

فصل ۵– الزامات کارکردی–امنیتی (ASE_REQ_SFR)

در این بخش الزامات کارکردی-امنیتی اشاره‌شده در بخش تهدیدات شرح داده خواهند شد. مطابق با سند مرجع Common Criteria یا CC که استاندارد و الگوی اصلی و پیروی شده در نگارش این پروفایل حفاظتی است، الزامات مربوطه به‌صورت کلاس‌بندی شده شرح داده خواهند شد، به‌طوری‌که هر کلاس شامل الزامات مرتبط است.

شایان‌ذکر است که پیاده‌سازی تمامی الزامات که در این بخش شرح داده می‌شوند برای یک سرویس‌دهنده ایمیل که مدعی انطباق و التزام با این پروفایل حفاظتی است اجباری می‌باشد. همچنان که جلوتر خواهیم دید برای پیاده‌سازی برخی از الزامات، مانند کانال ارتباطی با دیگر مؤلفه‌های IT، امکان انتخاب از میان گزینه‌های موجود فراهم‌شده است. این نوع الزامات را انتخابی می‌نامیم. همچنین برخی از الزامات اختیاری است که بالطبع پیاده‌سازی آن‌ها نیز اختیاری خواهد بود. هریک از موارد اختیاری یا انتخابی به‌صورت [اختیاری] و [انتخابی] در طول سند مشخص‌شده است. علاوه بر این، ممکن است در داخل الزامات [انتخابی] یکی از گزینه‌ها برای انتخاب با عنوان [اختصاص] مطرح شود که منظور از آن عموماً این است که نویسنده سند هدف امنیتی خود می‌تواند موارد جدیدی را با توجه به ویژگی‌های سرویس‌دهنده ایمیل خود به بخش مربوطه اضافه کند. پیاده‌سازی موارد اختیاری همان‌طور که از عنوان آن نیز مشخص است اختیاری است، اما برای برخی از موارد انتخابی الزاماتی نیز در بخش پیوست در نظر گرفته‌شده که باید پیاده‌سازی شوند. به‌عنوان‌مثال، در صورت انتخاب پروتکل IPSec برای پیکربندی کانال امن باید الزامات پروتکل IPSec نیز از بخش الزامات انتخابی پیاده‌سازی شود.

جدول ۱-۲ نگاشت میان الزامات کارکردی امنیتی و اهداف امنیتی ذکرشده را نشان می‌دهد. این الزامات تحقق اهداف مربوطه را تضمین خواهند کرد.

جدول ۱-۲ نگاشت الزامات کارکردی امنیتی به اهداف

شماره الزام	الزام	هدف
۱	تولید داده ممیزی ۱,۱ (FAU_GEN.1.1)	O. ACTION_MONITORING
۲	تولید داده ممیزی ۲,۱ (FAU_GEN.1.2)	O. ACTION_MONITORING
۳	تولید داده ممیزی۲ (FAU_GEN.2)	O. ACTION_MONITORING
۴	محل ذخیره‌سازی داده‌های ممیزی ۱ (FAU_ STG_EXT.1.1)	O. ACTION_MONITORING
۵	محل ذخیره‌سازی داده‌های ممیزی ۲	O. ACTION_MONITORING

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

شماره الزام	الزام	هدف
	(FAU_ STG_EXT.1.2)	
۶	محل ذخیره‌سازی داده‌های ممیزی (FAU_ STG_EXT.1.3)۳	O. ACTION_MONITORING
۷	مدیریت کلید رمزنگاری ۱ (FCS_CKM.1)	O. CONNECTION_SECURITY
۸	مدیریت کلید رمزنگاری ۲ (FCS_CKM.2.1)	O. CONNECTION_SECURITY
۹	نابودسازی کلید رمزنگاری (FCS_CKM.4.1)	O. CONNECTION_SECURITY
۱۰	عملیات رمزنگاری/ رمزنگاری داده‌ها (FCS_COP.1/DataEncryption)	O. CONNECTION_SECURITY
۱۱	عملیات رمزنگاری/ تولید و تأیید امضا (FCS_COP.1/SigGen)	O. CONNECTION_SECURITY
۱۲	عملیات رمزنگاری/الگوریتم درهم‌ساز (FCS_COP.1/Hash)	O. CONNECTION_SECURITY
۱۳	عملیات رمزنگاری/الگوریتم درهم‌ساز مبتنی بر کلید (FCS_COP.1/KeyedHash)	O. CONNECTION_SECURITY
۱۴	عملیات رمزنگاری/تولید بیت تصادفی ۱ (FCS_RBG_EXT.1)	O. CONNECTION_SECURITY
۱۵	عملیات رمزنگاری/تولید بیت تصادفی ۲ (FCS_RBG_EXT.2)	O. CONNECTION_SECURITY
۱۶	مدیریت احراز هویت ناموفق ۱ (FIA_AFL.1.1)	O. CREDENTIALS_SECURITY O. SERVER_ ACCESS_CONTROL
۱۷	مدیریت احراز هویت ناموفق ۲ (FIA_AFL1.2)	O. CREDENTIALS_SECURITY O. SERVER_ ACCESS_CONTROL
۱۸	مدیریت رمز عبور ۱ (FIA_PMG_EXT.1)	O. CREDENTIALS_SECURITY O. SERVER_ ACCESS_CONTROL
۱۹	شناسایی و احراز هویت کاربر ۱ (FIA_UIA_EXT.1.1)	O. SERVER_ ACCESS_CONTROL

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

شماره الزام	الزام	هدف
۲۰	شناسایی و احراز هویت کاربر ۲ (FIA_UIA_EXT.1.2)	O. SERVER_ ACCESS_CONTROL
۲۱	سازوکار احراز هویت بر اساس رمز عبور ۲(FIA_UAU_EXT.2.1)	O. SERVER_ ACCESS_CONTROL
۲۲	بازخورد امن در مکانیزم احراز هویت (FIA_UAU.7)	O. CREDENTIALS_SECURITY
۲۳	لیست‌های سیاه و سفید (FIA_UED_EXT.1)	O. SERVER_AVAILABILITY O. PHISHING_PREVENTION
۲۴	تحلیل محتوا (FIA_UED_EXT.2)	O. PHISHING_PREVENTION
۲۵	ایمیل‌های حجیم (FIA_UED_EXT.3)	O. SERVER_AVAILABILITY
۲۶	مدیریت کارکرد امنیتی ۱/ به‌روزرسانی دستی (FMT_MOF.1/ManualUpdate)	O. UPDATE_SECURITY
۲۷	مدیریت دسترسی به داده‌ها ۱ (FMT_MTD.1/CoreData)	O. SERVER_ ACCESS_CONTROL
۲۸	تعریف کارکردهای امنیتی ۱ (FMT_SMF.1)	مرتبط با تمامی اهداف
۲۹	مدیریت نقش‌های امنیتی ۱ (FMT_SMR.2.1)	O. SERVER_ ACCESS_CONTROL
۳۰	مدیریت نقش‌های امنیتی ۲ (FMT_SMR.2.2)	O. SERVER_ ACCESS_CONTROL
۳۱	مدیریت نقش‌های امنیتی ۳ (FMT_SMR.2.3)	O. SERVER_ ACCESS_CONTROL
۳۲	محافظت از کلیدهای رمزنگاری۱ (FPT_SKP_EXT.1.1)	O. CREDENTIALS_SECURITY
۳۳	محافظت از رمز عبور سرپرست ۱ (FPT_APW_EXT.1.1)	O. CREDENTIALS_SECURITY
۳۴	محافظت از رمز عبور سرپرست ۲ (FPT_APW_EXT.1.2)	O. CREDENTIALS_SECURITY

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

شماره الزام	الزام	هدف
۳۵	خودآزمایی خودکار ۱ (FPT_TST_EXT.1)	O. DEVICE_FUNTIONALITY_ ASSURANCE
۳۶	به‌روزرسانی امن ۱ (FPT_TUD_EXT.1.1)	O. UPDATE_SECURITY
۳۷	به‌روزرسانی امن ۲ (FPT_TUD_EXT.1.2)	O. UPDATE_SECURITY
۳۸	به‌روزرسانی امن ۳(FPT_TUD_EXT.1.3)	O. UPDATE_SECURITY
۳۹	مهر زمانی امن ۱(FPT_STM_EXT.1.1)	O. ACTION_MONITORING
۴۰	مهر زمانی امن ۲(FPT_STM_EXT.1.2)	O. ACTION_MONITORING
۴۱	قفل‌کردن و خاتمه دادن به نشست‌ها ۱ (FTA_SSL_EXT.1.1)	O. SERVER_ ACCESS_CONTROL
۴۲	قفل‌کردن و خاتمه دادن به نشست‌ها ۲ (FTA_SSL.3.1)	O. SERVER_ ACCESS_CONTROL
۴۳	قفل‌کردن و خاتمه دادن به نشست‌ها ۳ (FTA_SSL.4.1)	O. SERVER_ ACCESS_CONTROL
۴۴	بنر هشدار (FTA_TAB.1.1)	O. SERVER_ ACCESS_CONTROL
۴۵	کانال امن/ سرویس‌دهنده ایمیل با دیگر موجودیت‌های IT ۱ (FTP_ITC.1.1)	O. CONNECTION_ SECURITY
۴۶	کانال امن/ سرویس‌دهنده ایمیل با دیگر موجودیت‌های IT ۲ (FTP_ITC.1.2)	O. CONNECTION_ SECURITY
۴۷	کانال امن/ سرویس‌دهنده ایمیل با دیگر موجودیت‌های IT ۳ (FTP_ITC.1.3)	O. CONNECTION_ SECURITY
۴۸	کانال امن/ سرویس‌دهنده ایمیل با سرپرست ۱ (FTP_TRP.1.1/Admin)	O. CONNECTION_ SECURITY
۴۹	کانال امن/ سرویس‌دهنده ایمیل با سرپرست ۲ (FTP_TRP.1.2/Admin)	O. CONNECTION_ SECURITY

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

شماره الزام	الزام	هدف
۵۰	کانال امن/ سرویس‌دهنده ایمیل با سرپرست ۳ (FTP_TRP.1.3/Admin)	O. CONNECTION_ SECURITY
۵۱	الزامات پروتکل TLS Client (۱) (FCS_TLSC_EXT.1.1)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۵۲	الزامات پروتکل TLS Client (۲) (FCS_TLSC_EXT.1.2)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۵۳	الزامات پروتکل TLS Client (۳) (FCS_TLSC_EXT.1.3)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۵۴	الزامات پروتکل TLS Client (۴) (FCS_TLSC_EXT.1.4)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۵۵	الزامات پروتکل TLS Client (۵) (FCS_TLSC_EXT.1.5)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۵۶	الزامات پروتکل TLS Server (۱) (FCS_TLSS_EXT.1.1)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۵۷	الزامات پروتکل TLS Server (۲) (FCS_TLSS_EXT.1.2)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۵۸	الزامات پروتکل TLS Server (۳) (FCS_TLSS_EXT.1.3)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۵۹	الزامات پروتکل TLS Server (۴) (FCS_TLSS_EXT.1.4)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۶۰	الزامات پروتکل TLS Server (۵) (FCS_TLSS_EXT.1.5)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۶۱	الزامات پروتکل TLS Server (۶) (FCS_TLSS_EXT.1.6)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۶۲	الزامات گواهینامه‌های X.509/ تأیید گواهینامه (۱) (FIA_X509_EXT.1.1/Rev)	O. CONNECTION_ SECURITY
۶۳	الزامات گواهینامه‌های X.509/ تأیید گواهینامه (۲)	O. CONNECTION_ SECURITY

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

شماره الزام	الزام	هدف
	(FIA_X509_EXT.1.2/Rev)	
۶۴	الزامات گواهینامه‌های X.509/ احراز هویت (۱) (FIA_X509_EXT.2.1)	O. CONNECTION_ SECURITY
۶۵	الزامات گواهینامه‌های X.509/ احراز هویت (۲) (FIA_X509_EXT.2.2)	O. CONNECTION_ SECURITY
۶۶	الزامات گواهینامه‌های X.509/ درخواست گواهینامه (۱) (FIA_X509_EXT.3.1)	O. CONNECTION_ SECURITY
۶۷	الزامات گواهینامه‌های X.509/ درخواست گواهینامه (۲) (FIA_X509_EXT.3.2)	O. CONNECTION_ SECURITY
۶۸	الزامات پروتکل DNSSEC (۱) (FCS_DNSSEC_EXT.1.1)	O. DNS_CONNECTION_SECURITY
۶۹	الزامات پروتکل DNSSEC (۲) (FCS_DNSSEC_EXT.1.2)	O. DNS_CONNECTION_SECURITY
۷۰	الزامات پروتکل DNSSEC (۳) (FCS_DNSSEC_EXT.1.3)	O. DNS_CONNECTION_SECURITY
۷۱	الزامات پروتکل DNSSEC (۴) (FCS_DNSSEC_EXT.1.4)	O. DNS_CONNECTION_SECURITY
۷۲	الزامات پروتکل DNSSEC (۵) (FCS_DNSSEC_EXT.1.5)	O. DNS_CONNECTION_SECURITY
۷۳	الزامات پروتکل SPF (۱) (FCS_SPF_EXT.1.1)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۷۴	الزامات پروتکل SPF (۲) (FCS_SPF_EXT.1.2)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۷۵	الزامات پروتکل SPF (۳) (FCS_SPF_EXT.1.3)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۷۶	الزامات پروتکل SPF (۴) (FCS_SPF_EXT.1.4)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

شماره الزام	الزام	هدف
۷۷	الزامات پروتکل SPF (۵) (FCS_SPF_EXT.1.5)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۷۸	الزامات پروتکل SPF (۶) (FCS_SPF_EXT.1.6)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۷۹	الزامات متد DKIM (۱) (FCS_DKIM_EXT.1.1)	O. ADDRESS_SPOOFING _PREVENTION O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۸۰	الزامات متد DKIM (۲) (FCS_ DKIM_EXT.1.2)	O. ADDRESS_SPOOFING _PREVENTION O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۸۱	الزامات متد DKIM (۳) (FCS_ DKIM_EXT.1.3)	O. ADDRESS_SPOOFING _PREVENTION O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۸۲	الزامات متد DKIM (۴) (FCS_DKIM_EXT.1.4)	O. ADDRESS_SPOOFING _PREVENTION O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۸۳	الزامات متد DKIM (۵) (FCS_ DKIM_EXT.1.5)	O. ADDRESS_SPOOFING _PREVENTION O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۸۴	الزامات مکانیزم DMARK (۱) (FCS_DMARK_EXT.1.1)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۸۵	الزامات مکانیزم DMARK (۲) (FCS_DMARK_EXT.1.2)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

شماره الزام	الزام	هدف
۸۶	الزامات مکانیزم DMARK (۳) (FCS_DMARK_EXT.1.3)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۸۷	الزامات مکانیزم DMARK (۴) (FCS_DMARK_EXT.1.4)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۸۸	الزامات مکانیزم DMARK (۵) (FCS_DMARK_EXT.1.5)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۸۹	الزامات مکانیزم DMARK (۶) (FCS_DMARK_EXT.1.6)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۹۰	الزامات پروتکل S/MIME (۱) (FCS_S/MIME_EXT.1.1)	O. EMAIL_CONTENT_SECURITY
۹۱	الزامات پروتکل S/MIME (۲) (FCS_S/MIME_EXT.1.2)	O. EMAIL_CONTENT_SECURITY
۹۲	الزامات پروتکل S/MIME (۳) (FCS_S/MIME_EXT.1.3)	O. EMAIL_CONTENT_SECURITY
۹۳	الزامات پروتکل S/MIME (۴) (FCS_S/MIME_EXT.1.4)	O. EMAIL_CONTENT_SECURITY
۹۴	الزامات پروتکل DANE (۱) (FCS_DANE_EXT.1.1)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۹۵	الزامات پروتکل DANE (۲) (FCS_DANE_EXT.1.2)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۹۶	الزامات پروتکل DANE (۳) (FCS_DANE_EXT.1.3)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۹۷	الزامات پروتکل DANE (۴) (FCS_DANE_EXT.1.4)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۹۸	الزامات پروتکل DANE (۵) (FCS_DANE_EXT.1.5)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION

شماره الزام	الزام	هدف
۹۹	الزامات پروتکل DANE (۶) (FCS_DANE_EXT.1.6)	O. EMAIL_SENDER/RECEIVER_AUTHENTICATION
۱۰۰	الزامات پروتکل HTTPS (۱) (FCS_HTTPS_EXT.1)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۱۰۱	الزامات پروتکل HTTPS (۲) (FCS_HTTPS_EXT.2)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY
۱۰۲	الزامات پروتکل HTTPS (۳) (FCS_HTTPS_EXT.3)	O. CONNECTION_ SECURITY O. EMAIL_CONTENT_SECURITY

۱-۵- کلاس ثبت رکوردهای ممیزی از رویدادهای امنیتی

این کلاس شامل مجموعه‌ای از کارکردهای موردنیاز باهدف ثبت رکورد ممیزی برای هرگونه فعالیت امنیتی دارای اهمیت است که سرویس‌دهنده ایمیل در آن دخیل بوده است. هدف از این کار فراهم کردن اطلاعات لازم برای سرپرست سرور جهت شناسایی مشکلات عمدی و غیرعمدی رخداده درزمینه پیکربندی و/یا در هر یک از کارکردهای سیستم است. سرویس‌دهنده ایمیل باید این قابلیت را داشته باشد که داده‌های ممیزی موردنیاز برای تشخیص چنین فعالیت‌هایی را تولید کند.

ثبت این رکوردها از جهات مختلفی مفید و تأثیرگذار خواهد بود، به‌طور مثال ثبت رکورد ممیزی از فعالیت‌های مدیریتی منجر به تولید اطلاعاتی می‌شود که در صورت نیاز به تغییر پیکربندی سرور، می‌توان از تحلیل آن‌ها برای طراحی اقدامات اصلاحی و بازنگری درروش مدیریت آن استفاده کرد. همچنین ممیزی رویدادهای مرتبط با رمزنگاری نشان می‌دهد که آیا کارکردهای مربوطه به‌درستی اجرا می‌شوند یا سیستم در معرض شنود قرار دارد. از سویی دیگر این رکوردها به شناسایی فعالیت‌های غیرمعمول مانند ایجاد یک نشست کاربری در زمان مشکوک، شکست مکرر نشست‌ها یا احراز هویت ناموفق به سیستم کمک می‌کنند.

در برخی موارد، ممکن است حجم اطلاعات ممیزی تولیدشده به‌اندازه‌ای زیاد شود که سرپرست سرویس‌دهنده ایمیل را سردرگم کند. ازاین‌رو سرور باید بتواند اطلاعات ممیزی را به یک موجودیت مورد اعتماد خارجی ارسال کند. این اطلاعات باید دارای مهرهای زمانی قابل‌اعتماد باشند. این امر امکان مرتب کردن رکوردهای مربوطه بعد از ارسال به دستگاه خارجی را فراهم می‌کند. همچنین ارتباط با این سرور ممیزی خارجی باید از طریق برقراری یک کانال امن صورت پذیرد و در صورت قطع اتصال، باید از ارسال داده‌های ممیزی روی مسیر عادی و رمز نشده جلوگیری شود.

از سرور انتظار نمی‌رود که این رکوردهای ممیزی را همواره در خود ذخیره داشته باشد. هرچند که لازم است داده‌ها به‌صورت محلی در زمان تولید ذخیره شوند ولی در صورت تجاوز از ظرفیت ذخیره‌سازی، رونویسی رکوردهای قدیمی مجاز است.

شماره الزام	نام الزام
۱	تولید داده ممیزی ۱,۱ (FAU_GEN.1.1)

سرویس‌دهنده ایمیل باید قادر به تولید رکورد ممیزی از رویدادهای قابل ممیزی زیر باشد:

- ❖ آغاز و خاتمه اجرای [انتخاب: توابع ممیزی، تمامی توابع کارکردی] در هر بار اجرا
- ❖ تمامی رویدادهای ذکرشده به تفکیک الزام در جدول لیست رویدادهای قابل ممیزی
- ❖ تمامی اقدامات مدیریتی شامل موارد زیر:
  - ▪ورود و خروج مدیریتی به سیستم (درصورتی‌که سرپرستان سیستم دارای حساب کاربری شخصی باشند، نام حساب کاربری آن‌ها نیز باید ثبت شود)
  - ▪هرگونه تغییر در پیکربندی توابع امنیتی (علاوه بر گزارش اینکه تغییر رخداده، نوع تغییر انجام‌شده نیز باید مشخص شود.)
  - ▪تولید/واردکردن[۱] ، تغییر، یا پاک کردن کلیدهای رمزنگاری (علاوه بر گزارش رخداد مربوطه، نام کلید یا مرجع مشخص‌کننده آن باید تعیین شود)
  - ▪تغییر رمز عبور (نام حساب کاربری مربوطه نیز باید ثبت شود)
  - ▪انتخاب: [هیچ اقدام دیگر، اختصاص: [لیستی از دیگر اقدامات مدیریتی دارای اهمیت که قابل رکورد کردن باشد]]
- ❖ تمامی دیگر رویدادهای قابل ممیزی و دارای اهمیت که جزء موارد تأکید شده فوق نباشد.

نکات کاربردی:

- ✓ درصورتی‌که لیست ارائه‌شده برای ثبت ممیزی از اقدامات مدیریتی کافی نبوده و نویسنده سند هدف امنیتی تشخیص به لزوم ثبت اقدامات و فعالیت‌های مدیریتی بیشتری دهد، می‌تواند با استفاده از قسمت «اختصاص» که در «انتخاب» قرارگرفته است، اقدامات مدیریتی دیگری را به لیست اضافه کند.

[۱] Import (اشاره به ایمپورت یک کلید آماده دارد)

- ✓ در خصوص مورد اول برای ثبت رکورد ممیزی در مورد آغاز و خاتمه اجرای توابع کارکردی، سرور می‌تواند تنها برای اجرای توابع ممیزی چنین رکوردی ثبت کند، ولی بهتر است برای دیگر توابع کارکردی امنیتی نیز چنین رکوردی ثبت شود، هرچند که این سند آن را اجبار نمی‌کند.
- ✓ ثبت رکورد ممیزی از کلیدهای رمزنگاری تنها اشاره به کلیدهای غیرموقتی دارد که برای بیش از یک نشست استفاده می‌شوند.

۲	تولید داده ممیزی ۲,۱ (FAU_GEN.1.2)

در هر رکورد ممیزی دست‌کم اطلاعات زیر باید ذخیره شود:

- ❖ تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت انجام‌دهنده رویداد و نتیجه رویداد (موفقیت یا شکست)
- ❖ اطلاعات اضافی اختصاصی برای هر رویداد قابل ممیزی مطابق با ستون سوم از جدول زیر با نام لیست رویدادهای قابل ممیزی.

(همچنین برای موارد انتخابی و اختیاری باید به همین ترتیب و مطابق با جدول مربوطه با نام «لیست رویدادهای قابل ممیزی برای الزامات انتخابی/اختیاری» اطلاعات موردنیاز ثبت شود.)

جدول ۱-۳ لیست رویدادهای قابل ممیزی به تفکیک کارکردهای امنیتی مورد نیاز

کارکرد امنیتی موردنیاز	رویداد قابل ممیزی	اطلاعات اضافی مورد نیاز
FAU_GEN.1	×	×
FAU_GEN.2	×	×
FAU_STG_EXT.1	×	×
FCS_CKM.1	×	×
FCS_CKM.2	×	×
FCS_CKM.4	×	×
FCS_COP.1/DataEncryption	×	×
FCS_COP.1/SigGen	×	×
FCS_COP.1/Hash	×	×

FCS_COP.1/KeyedHash	×	×
FCS_RBG_EXT.1	×	×
FIA_AFL.1	ثبت لاگین ناموفق در سرویس‌دهنده ایمیل زمانی که تعداد آن به تعداد آستانه تعیین‌شده برسد.	در اتصال راه دور: مبدأ تلاش کننده برای لاگین (مانند آدرس IP آن)
FIA_PMG_EXT.1	×	×
FIA_UIA_EXT.1	هر نوع استفاده از سرویس‌های بدون نیاز به احراز هویت	در اتصال راه دور: مبدأ تلاش کننده (مانند آدرس IP آن)
FIA_UAU_EXT.2	انجام فرایند احراز هویت و ورود به سیستم	در اتصال راه دور: مبدأ تلاش کننده (مانند آدرس IP آن)
FIA_UAU_EXT.3	×	×
FIA_UAU.7	×	×
FIA_UED_EXT.1	• ثبت دریافت ایمیل از یک مبدأ مشکوک و موجود در لیست سیاه • هر نوع اضافه یا حذف آدرس در لیست سیاه و هویت انجام دهنده آن	×
FIA_UED_EXT.2	ثبت شناسایی یک	×

	ایمیل مشکوک و آدرس ارسال‌کننده‌ی آن	
FIA_UED_EXT.3	ثبت هر نوع ایمیل با ضمیمه‌ی حجیم و آدرس ارسال‌کننده‌ی آن	×
FMT_MOF.1/ManualUpdate	هر نوع تلاش برای شروع به‌روزرسانی دستی	×
FMT_MTD.1/CoreData	×	×
FMT_SMF.1	انجام هر نوع فعالیت و پیکربندی توسط سرپرست	×
FMT_SMR.2	×	×
FPT_SKP_EXT.1	×	×
FPT_APW_EXT.1	×	×
FPT_TST_EXT.1	×	×
FPT_TUD_EXT.1	• شروع به‌روزرسانی • نتیجه به‌روزرسانی (موفقیت یا شکست)	×
FPT_STM_EXT.1	هر نوع ایجاد تغییر و پیکربندی مجدد زمان (چه به‌صورت دستی توسط مدیر و چه به‌صورت اتوماتیک توسط سرور NTP)	• زمان قبلی و جدید • مبدأ انجام دهنده تغییر (مانند آدرس IP آن)

FTA_SSL_EXT.1 **(درصورتی‌که گزینه قفل‌کردن برای نشست‌های محلی غیرفعال پیاده‌سازی شده است.)**	هر نوع تلاش برای بازگشایی مجدد یک نشست قفل‌شده که به خاطر عدم فعالیت برای مدت‌زمان معین قفل‌شده است.	×
FTA_SSL_EXT.1 **(درصورتی‌که گزینه خاتمه دادن برای نشست‌های محلی غیرفعال پیاده‌سازی شده است.)**	ثبت رویداد خاتمه دادن به یک نشست غیرفعال محلی	×
FTA_SSL.3	ثبت رویداد خاتمه دادن به یک نشست راه دور غیرفعال	×
FTA_SSL.4	ثبت رویداد خاتمه دادن به نشست راه دور مربوطه توسط خودسرپرست راه دور	×
FTA_TAB.1	×	×
FTP_ITC.1	• آغاز برقراری یک کانال امن • خاتمه یافتن کانال امن • وقوع مشکل در کارکرد کانال امن	هویت شروع‌کننده و مقصد کانال امن دچار مشکل شده است.
FTP_TRP.1/Admin	• آغاز برقراری یک کانال امن با یک سرپرست راه دور • خاتمه یافتن کانال امن	×

	• وقوع مشکل در کارکرد کانال امن	
FCS_TLSC_EXT.1	شکست در ایجاد یک نشست TLS	دلیل شکست
FCS_TLSS_EXT.1	شکست در ایجاد یک نشست TLS	دلیل شکست
FIA_X509_EXT.1.x/Rev	تلاش‌های ناموفق برای اعتبارسنجی یک گواهینامه	دلیل شکست
FIA_X509_EXT.2	×	×
FIA_X509_EXT.3	×	×
FCS_DNSSEC_EXT.1	شکست در ایجاد یک اتصال DNSSEC	دلیل شکست
FCS_SPF_EXT.1	×	×
FCS_ DKIM_EXT.1	هرگونه شناسایی امضای نادرست	فرستنده ایمیل ثبت شود.
FCS_DMARK_EXT.1	×	×
FCS_S/MIME_EXT.1	هرگونه شناسایی امضای نادرست یا مشکل در رمزگشایی ایمیل	فرستنده ایمیل ثبت شود.
FCS_DANE_EXT.1	×	×
FCS_HTTPS_EXT.1	شکست در ایجاد یک نشست HTTPS	دلیل شکست
۳	تولید داده ممیزی۲ (FAU_GEN.2)	

در مورد آن دسته از اقداماتی که توسط سرپرستان احراز هویت شده انجام می‌شوند، سرویس‌دهنده ایمیل باید بتواند رویداد قابل ممیزی را با درج هویت سرپرست انجام دهنده آن ثبت کند.	
۴	محل ذخیره‌سازی داده‌های ممیزی ۱ (FAU_ STG_EXT[۱].1.1)
همچنان که پیش‌تر گفته شد، سرور باید قادر به ذخیره رکوردهای ممیزی روی هارد خود باشد و در صورت پر شدن فضای ذخیره‌سازی آن اقدام مناسب برای رونویسی را مطابق با الزام ۶ انجام دهد. اما درعین‌حال باید قادر به ارسال داده‌های ممیزی تولیدشده به یک موجودیت IT خارجی با استفاده از یک کانال امن مطابق با الزام FTP_ITC.1 باشد. شایان‌ذکر است که در صورت استفاده از هریک از پروتکل‌های HTTPS، TLS، DTLS، SSH یا IPsec به‌عنوان پروتکل ارتباطی امن، تمامی الزامات مربوط به آن پروتکل نیز باید تکمیل و به سند هدف امنیتی اضافه گردد. همچنین در صورت قطع شدن کانال ارتباطی امن، مکانیزم مناسب برای جلوگیری از ارسال داده‌های ممیزی تا زمان اتصال مجدد کانال باید اتخاذ شود. نکات کاربردی: ✓ از آنجایی‌که سرور ممیزی خارجی قسمتی از سرویس‌دهنده ایمیل نیست، به‌جز الزام برقراری کانال امن FTP_ITC.1 الزام دیگری برای آن تعریف نمی‌شود. همچنین پس از پیکربندی، سرور باید توانایی ارسال اتوماتیک داده‌های ممیزی را بدون مداخله سرپرست داشته باشد. به‌عبارتی‌دیگر، انتقال دستی نمی‌تواند الزامات را برآورده کند. ارسال می‌تواند به‌صورت بلادرنگ یا دوره‌ای انجام شود. ✓ اگر ارسال به‌صورت بلادرنگ انجام نمی‌شود، باید مشخص شود در چه زمانی و با چه تناوبی این ارسال‌ها انجام می‌گیرند. این تناوب باید قابل‌قبول باشد.	
۵	محل ذخیره‌سازی داده‌های ممیزی ۲ (FAU_ STG_EXT.1.2)
سرویس‌دهنده ایمیل باید بتواند داده‌های ممیزی تولیدشده را در خود ذخیره کند.	
۶	محل ذخیره‌سازی داده‌های ممیزی ۳ (FAU_ STG_EXT.1.3)

[۱] الزاماتی که انتهای آن‌ها با EXT تمام می‌شود، الزاماتی هستند که با توسعه‌ی خانواده مربوطه از الزامات و به‌طور خاص روی کارکردهای اختصاصی از سرویس‌دهنده ایمیل تمرکز دارند. این الزامات اغلب فاقد بیان عام و کلیات هستند و در عوض، روی جزئیات متمرکزشده‌اند.

با پر شدن حافظه محلی برای ذخیره‌سازی رکوردهای ممیزی، سرور باید [انتخاب: ۱) داده‌های ممیزی جدید را ابتدا روی یک موجودیت خارجی IT (سرور syslog) یا مکان مناسبی ثبت نماید و سپس آن‌ها را دور بریزد، ۲) داده‌های ممیزی قدیمی را با داده‌های جدید بازنویسی کند و ۳) از این رویکرد استفاده کند: [اختصاص: قوانین بازنویسی رکوردهای قدیمی]، [اختصاص: اقدامات دیگر]] الزام فوق امکان سه انتخاب را برای رونویسی رکوردهای قدیمی فراهم می‌کند: ۱) دور ریختن رکوردهای جدید که این حالت توصیه نمی‌شود، ولی درهرصورت موجودیت خارجی IT باید رکوردهای جدید را داشته باشد. ۲) رکوردهای قدیمی رونویسی شود. بدین منظور قسمت اختصاص امکان تعریف قاعده رونویسی را به خودسرپرست می‌سپارد. ۳) سرپرست خود می‌تواند در مورد رکوردهای جدید تصمیم‌گیری کند. به‌عنوان‌مثال می‌تواند ارسال رکوردهای جدید به یک سرور syslog خارجی را انتخاب کند.

۲-۵- کلاس پشتیبانی از رمزنگاری

در این بخش الزامات پایه‌ای مرتبط با رمزنگاری شرح داده خواهند شد. این الزامات شامل تولید کلید و بیت تصادفی، روش‌های استقرار کلید، از بین بردن کلید، روش‌های مختلف رمزنگاری برای پیاده‌سازی رمزنگاری/رمزگشایی AES، تأیید و تصدیق امضای دیجیتال و نیز متدهای ساده یا مبتنی بر کلید برای درهم‌سازی است.

*** توجه شود که الزامات و الگوریتم‌های ذکرشده در این قسمت با پروتکل‌های انتخابی در بخش‌های بعدی مانند TLS، IPSEC، DKIM، DNSSEC و ... مرتبط است و انتخاب‌های این بخش باید با مجموعه‌های رمز انتخابی برای پروتکل‌های مذکور متناسب باشند.

در میان الزامات این بخش، موارد مختلفی از گزینه [انتخاب] را خواهید دید که بالطبع بر اساس انتخاب انجام‌شده نیازمند پیاده‌سازی الزامات مربوطه از بخش پیوست است.

شماره الزام	نام الزام
۷	مدیریت کلید رمزنگاری ۱ (FCS_CKM.1)
سرویس‌دهنده ایمیل باید تولید کلیدهای رمزنگاری نامتقارن را با انتخاب یکی از متدهای مقابل برای تولید کلید انجام دهد:[انتخاب: ❖ روش RSA با طول کلید ۲۰۴۸ بیت یا بزرگ‌تر که الزامات ذکرشده در پیوست B.3 از سند FIPS PUB 186-4 با عنوان استاندارد امضای دیجیتال DSS را رعایت کند. ❖ روش ECC بر مبنای منحنی NIST Curves [انتخاب: P-256, P-384, P-521] که الزامات ذکرشده در پیوست B.4 از سند FIPS PUB 186-4 با عنوان استاندارد امضای دیجیتال DSS	

را رعایت کند.

- ❖ روش FFC با طول کلید ۲۰۴۸ بیت یا بزرگ‌تر که الزامات ذکرشده در پیوست B.1 از سند FIPS PUB 186-4 با عنوان استاندارد امضای دیجیتال DSS را رعایت کند.
- ❖ روش FFC با استفاده از گروه‌های "safe-prime" که الزامات ذکرشده در سند زیر "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

و [انتخاب: RFC 3526, RFC 7919] را رعایت کند.

]

نکات کاربردی:

- ✓ این الزام چهار نوع الگوی تولید کلید برای استفاده در راستای استقرار کلید و نیز احراز هویت سیستم‌ها فراهم می‌کند که می‌توان از میان آن‌ها یک مورد را انتخاب کرد.
- ✓ درصورتی‌که هدف از انتخاب انجام‌شده در این الزام برای استقرار کلید باشد، انتخاب انجام‌شده باید با انتخابی که در الزام «مدیریت کلید رمزنگاری ۲» و نیز پروتکل‌های رمزنگاری انجام می‌شود، مطابقت داشته باشد.
- ✓ همچنین درصورتی‌که هدف برای احراز هویت دستگاه‌ها باشد، باید علاوه بر ssh-rsa، ecdsa-sha2-nistp256، ecdsa-sha2-nistp384 و ecdsa-sha2-nistp521، کلید عمومی نیز مرتبط با گواهینامه X.509v3 باشد.
- ✓ اگر سرویس‌دهنده ایمیل به‌عنوان یک دریافت‌کننده در الگوهای استقرار کلید عمل کند و برای پشتیبانی از احراز هویت دوطرفه پیکربندی نشده باشد، سرویس‌دهنده ایمیل نیاز به پیاده‌سازی تولید کلید ندارد.

۸	مدیریت کلید رمزنگاری ۲ (FCS_CKM.2.1)

سرویس‌دهنده ایمیل باید استقرار کلید رمزنگاری را بر اساس یک روش استاندارد استقرار کلید رمزنگاری انجام دهد: [انتخاب:

- ❖ الگوهای استقرار کلید RSA که ویژگی‌های مشخص‌شده در بخش ۷,۲ از RFC3447 با نام RSAES-PKCS1-v1_5 را رعایت کنند.
- ❖ الگوهای استقرار کلید مبتنی بر روش Elliptic curve که ویژگی‌های مشخص‌شده در نسخه بازبینی‌شده ۲ از سند NIST SP 800-56A با عنوان " Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" را رعایت کند.
- ❖ الگوهای استقرار کلید مبتنی بر روش Finite field که ویژگی‌های مشخص‌شده در نسخه بازبینی‌شده ۲ از سند NIST SP 800-56A با عنوان " Recommendation for Pair-Wise

Key Establishment Schemes Using Discrete Logarithm Cryptography" را رعایت کند. ❖ الگوهای استقرار کلید FFC با استفاده از گروه‌های "safe-prime" که ویژگی‌های مشخص‌شده در نسخه بازبینی‌شده ۳ از سند NIST SP 800-56A با عنوان " Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" و [انتخاب: RFC 3526، RFC 7919] را رعایت کند.]	
۹	نابودسازی کلید رمزنگاری (FCS_CKM.4.1)
سرویس‌دهنده ایمیل باید قابلیت نابودسازی کلیدهای تولیدشده را داشته باشد: [اختصاص: ❖ برای کلیدهای متن-ساده (رمز نشده) که در حافظه گذرا قرار دارند، نابودسازی باید از طریق [انتخاب: بازنویسی ساده از طریق [انتخاب: تولید عبارت شبه تصادفی با استفاده از تابع تولید بیت تصادفی، یک عبارت تماماً صفر، یک عبارت تماماً یک، یک مقدار جدید از کلید، [اختصاص: یک مقدار ثابت یا پویا که شامل هیچ CSP نباشد]]، یا نابودسازی مرجع کلید (مستقیماً با درخواست زباله روبی) باشد] ❖ برای کلیدهای متن-ساده (رمز نشده) که در حافظه پایدار قرار دارند، نابودسازی باید از طریق یک واسط فراهم‌شده توسط خود سرویس‌دهنده ایمیل انجام شود که [انتخاب: ▪ به‌صورت منطقی مکان ذخیره‌سازی کلید را آدرس می‌دهد و بازنویسی را برای [انتخاب: یک‌بار، [اختصاص: لیست دفعات]] [1] انجام می‌دهد که شامل [انتخاب: تولید عبارت شبه تصادفی با استفاده از تابع تولید بیت تصادفی، عبارت تماماً صفر، عبارت تماماً یک، یک مقدار جدید از کلید، [اختصاص: یک مقدار ثابت یا پویا که شامل هیچ CSP[2] نباشد]] است. ▪ به یک ماژول دستور دهد تا اشاره‌کننده معرف کلید را پاک کند. نکات کاربردی: ✓ برای عبارت «واسط فراهم‌شده توسط خود سرویس‌دهنده ایمیل»، بخش خلاصه مشخصات	

[1] منظور از این عبارت این است که بازنویسی یک‌بار یا برای اطمینان و به انتخاب سازنده چندین بار انجام شود.

[2] Content Security Policy

محصول باید این «بخش» و واسط مرتبط با آن را مشخص و معرفی کند. واسط اشاره‌شده می‌تواند در سرویس‌دهنده ایمیل‌های مختلف، اشکال متفاوتی داشته باشد. شاید مشهودترین شکل آن یک برنامه کاربردی روی یک سیستم‌عامل باشد. ✓ زمانی که از روش‌های تخریب یا نابودسازی مختلفی برای کلیدهای مختلف و/یا موقعیت‌های تخریب مختلف استفاده می‌شود، این روش‌ها و کلیدها/موقعیت‌های متفاوت بکار گرفته‌شده باید در بخش خلاصه مشخصات محصول توصیف شوند. بخش خلاصه مشخصات باید همه کلیدهای مرتبط استفاده‌شده در پیاده‌سازی الزامات کارکردی-امنیتی را توصیف کند، همچنین مواردی که محل ذخیره شدن کلیدها به‌صورت متن آشکار است را شامل می‌شود. ✓ در بعضی از اختصاص‌های ذکرشده، از عبارت «شامل هیچ CSP نباشد» استفاده‌شده است. این جمله به این معنی است که سرویس‌دهنده ایمیل از برخی داده‌های خاص استفاده کند که شامل هیچ‌کدام از مقادیر تولیدشده توسط تولیدکننده بیت تصادفی موجود در الزام FCS_RBG_EXT یا مقادیر لیست شده در این الزام، به‌طور مثال موارد لیست شده در اولین انتخاب از اولین اختصاص این الزام، نیست. درواقع وجود عبارت «شامل هیچ CSP نباشد» برای مطمئن شدن از این موضوع است که حتماً بازنویسی داده با دقت انجام‌شده و مقدار مورداستفاده برای بازنویسی احیاناً یک کلید یا داده حساس را شامل نشود. ✓ مهم: لازم به ذکر است که کلیدهای رمزنگاری در این الزام، شامل کلیدهای نشست نیز می‌شود. همچنین قابل‌ذکر است که الزام نابودسازی کلید برای کلیدهای عمومی در جفت کلید نامتقارن، اعمال نمی‌شود.	
۱۰	عملیات رمزنگاری/ رمزنگاری داده‌ها (FCS_COP.1/DataEncryption)
سرویس‌دهنده ایمیل باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES در حالت [انتخاب:CBC، GCM، CTR] و در اندازه کلید [انتخاب: ۱۲۸ بیتی، ۱۹۲ بیتی، ۲۵۶ بیتی] و با توجه به استاندارد AES که در ISO ۱۸۰۳۳-۳ تعریف‌شده است و استاندارد [انتخاب: CBC که در ISO ۱۰۱۱۶ تعریف‌شده است، GCM که در ISO ۱۹۷۷۲ تعریف‌شده است، CTR که در ISO ۱۰۱۱۶ تعریف‌شده است] انجام دهد. نکات کاربردی: ✓ نخست حالت یا مد کاری الگوریتم AES و سپس اندازه کلید آن و استانداردهای مربوطه باید انتخاب شوند. ✓ مد و اندازه کلید انتخاب‌شده در این مرحله متناظر با انتخاب مجموعه رمز برای الزام کانال امن است.	
۱۱	عملیات رمزنگاری/ تولید و تأیید امضا (FCS_COP.1/SigGen)
سرویس‌دهنده ایمیل باید سرویس امضای دیجیتال (تولید و تأیید) را بر اساس الگوریتم‌های رمزنگاری	

زیر ارائه کند: [انتخاب:

الگوریتم امضای دیجیتال RSA و کلید رمزنگاری با اندازه‌های [اختصاص: ۲۰۴۸ بیتی یا بزرگ‌تر]

الگوریتم امضای دیجیتال Elliptic Curve و کلید رمزنگاری با اندازه‌های [اختصاص: ۲۵۶ بیتی یا بزرگ‌تر]

]

و با رعایت موارد زیر:

[انتخاب:

برای الگوریتم RSA: قسمت ۵,۵ از سند FIPS PUB 186-4 با عنوان «استاندارد امضای دیجیتال DSS»،

برای الگوریتم Elliptic Curve: قسمت ۶ و پیوست D از سند FIPS PUB 186-4 با عنوان «استاندارد امضای دیجیتال DSS»

]

نکات کاربردی:

- ✓ نویسنده هدف امنیتی باید الگوریتم مورداستفاده برای اجرای امضای دیجیتال را انتخاب کند.
- ✓ نویسنده هدف امنیتی باید سازگار بودن انتخاب انجام‌شده در این قسمت با دیگر الزامات رمزنگاری را بررسی کند، خصوصاً زمانی که از Elliptic Curve استفاده شود.

۱۲	عملیات رمزنگاری/الگوریتم درهم‌ساز (FCS_COP.1/Hash)

سرویس‌دهنده ایمیل باید عملیات درهم‌سازی مبتنی بر رمزنگاری را بر اساس الگوریتم رمزنگاری [انتخاب: SHA-1، SHA-256، SHA-384، SHA-512] و اندازه خلاصه پیام [۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیتی و با رعایت استاندارد ISO/IEC 10118-3:2004 انجام دهد.

نکات کاربردی:

- ✓ اکیداً توصیه می‌شود که از پروتکل‌های به‌روزرسانی شده که از خانواده SHA-2 پشتیبانی می‌کنند، استفاده شود. تا زمانی که پروتکل‌های بروز شده پشتیبانی شوند، این پروفایل حفاظتی اجازه پشتیبانی از پیاده‌سازی SHA-1 را منطبق بر SP 800-131A فراهم می‌کند.
- ✓ توجه: بر اساس نقشه راه SP 800-131A، استفاده از الگوریتم SHA-1 فقط می‌تواند برای عملیاتی غیر از امضای دیجیتال همچون درهم‌سازی رمز عبور و غیره استفاده شود. در نسخه‌های آتی از پروفایل حفاظتی مرجع برای محصولات شبکه، SHA-256 کمینه الزام خواهد بود.
- ✓ انتخاب الگوریتم درهم‌ساز باید با توجه به قدرت الگوریتم مورداستفاده برای الزام «عملیات

رمزنگاری۱/ رمزنگاری داده‌ها» و الزام «عملیات رمزنگاری۱/ تولید و تأیید امضا» انجام شود (مثلاً SHA-256 برای کلیدهای ۱۲۸ بیتی).	
۱۳	عملیات رمزنگاری/الگوریتم درهم‌ساز مبتنی بر کلید (FCS_COP.1/KeyedHash)
سرویس‌دهنده ایمیل باید احراز هویت پیام مبتنی بر کلید درهم‌سازی شده را بر اساس الگوریتم رمزنگاری [انتخاب: HMAC-SHA-1]، HMAC-SHA256، HMAC-SHA-384، HMAC-SHA-512 و سایز کلید رمزنگاری [اختصاص: اندازه کلید به بیت که در HMAC استفاده‌شده] و اندازه خلاصه پیام [۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲] بیتی و با رعایت نکات ذکرشده در بخش ۷ از سند ISO/IEC 9797-2:2011 انجام دهد. نکات کاربردی: ✓ اندازه کلید k در عبارت «اختصاص» بین L1 و L2 خواهد بود (تعریف‌شده در ۱۰۱۱۸ IEC/ISOمربوط به توابع درهم‌ساز). به‌طور مثال در مورد SHA-256 داریم: L2<=k<=L1 که L1=512, L2=256	
۱۴	عملیات رمزنگاری/تولید بیت تصادفی ۱ (FCS_RBG_EXT.1)
سرویس‌دهنده ایمیل باید سرویس تولید بیت تصادفی را بر اساس استاندارد ISO/IEC 18031:2011 و با استفاده از [انتخاب: Hash_DRBG (any)، HMAC_DRBG (any)، CTR_DRBG (AES)] فراهم کند. نکات کاربردی: ✓ برای Hash_DRBG و HMAC_DRBG از هریک از SHA-1، SHA-256، SHA-384، SHA-512 می‌توان استفاده کرد، ولی برای CTR_DRBG پیاده‌سازی‌های مبتنی بر AES باید استفاده شود.	
۱۵	عملیات رمزنگاری/تولید بیت تصادفی ۲ (FCS_RBG_EXT.2)
تابع تولید بیت تصادفی برای تولید رشته‌های تصادفی، خود نیازمند تغذیه شدن با رشته‌های نویزی یا تصادفی است که توسط منابع نرم‌افزاری و سخت‌افزاری دیگر تولید می‌شوند. ازاین‌رو، تابع تولیدکننده بیت تصادفی RBG باید حداقل توسط یک منبع آنتروپی تغذیه شود؛ و این منبع باید آنتروپی‌ها را از [انتخاب: [اختصاص: تعداد] منبع نرم‌افزاری برای تولید آنتروپی، [اختصاص: تعداد] منبع سخت‌افزاری برای تولید آنتروپی] با حداقل سایز آنتروپی [انتخاب: ۱۲۸، ۱۹۲، ۲۵۶] بیتی گردآوری کند. همچنین سایز آنتروپی باید معادل یا بزرگ‌تر از طولانی‌ترین یا قوی‌ترین کلیدی باشد که در سرویس‌دهنده ایمیل تولید و استفاده خواهد شد. نکات کاربردی: ✓ منظور از منبع تولید آنتروپی یک یا چند منبع سخت‌افزاری یا نرم‌افزاری است که قادر به	

تولید رشته‌های تصادفی هستند که توسط تابع RBG یا Deterministic RBG برای تولید رشته‌های نهایی موردنیاز برای تولید کلید استفاده خواهند شد. ✓ در قسمت اختصاص، منظور از عبارت «تعداد»، تعداد منابع مورداستفاده است. مثلاً ۲ منبع نرم‌افزاری برای تولید آنتروپی.

۳-۵- کلاس شناسایی و احراز هویت

به‌عنوان ابزاری امن برای ورود، سرویس‌دهنده ایمیل باید یک سازوکار ورود مبتنی بر رمز عبور را در اختیار سرپرستان خود قرار دهد. سرویس‌دهنده ایمیل باید سرپرست را ملزم به انتخاب یک رمز عبور قدرتمند کرده و نیز او را ملزم به تغییر مرتب این رمز عبور کند. همچنین برای جلوگیری از حملاتی که در آن‌ها فرد مهاجم نوشتن رمز عبور یا فرایند ورود سرپرست به سرویس‌دهنده را می‌بیند، رمز عبور باید در هنگام ورود به حالت محو و ناخوانا دیده شود. قفل‌کردن و یا خاتمه دادن اتوماتیک به هر نشست غیرفعال بعد از یک مدت‌زمان معین را نیز می‌توان برای جلوگیری از ورود غیرمجاز به سرویس‌دهنده ایمیل به‌وسیله دزدیدن نشست‌های قبلی قرار داد. همچنین رمزهای عبور باید به شکل محو و ناخوانا در حافظه ذخیره شوند، به‌گونه‌ای که هیچ واسطی برای خواندن آن به شکل متن ساده وجود نداشته باشد.

در این بخش ضمن بیان الزامات پاسخ‌دهنده به نگرانی‌های فوق، زیربخشی نیز برای تعریف اقدامات تکمیلی جهت شناسایی و تشخیص ایمیل‌های جعلی در نظر گرفته‌شده است.

شماره الزام	نام الزام
۱۶	مدیریت احراز هویت ناموفق ۱ (FIA_AFL.1)
سرویس‌دهنده ایمیل باید قادر به تشخیص مواقعی باشد که در آن تعداد دفعات تلاش یک موجودیت برای احراز هویت و لاگین کردن به‌عنوان سرپرست سرویس‌دهنده ایمیل به‌صورت راه دور از تعداد معینی [اختصاص: تعداد دفعات] فراتر می‌رود. همان‌طور که در اختصاص مشخص‌شده است، این تعداد معین باید توسط سرپرست قابل تنظیم باشد.	
۱۷	مدیریت احراز هویت ناموفق ۲ (FIA_AFL.2)
با رسیدن به تعداد دفعات ناموفق تعیین‌شده در لاگین کردن، سرویس‌دهنده ایمیل باید [انتخاب: اکانت راه دور مذکور را تا زمانی که یک [اختصاص: اقدام] توسط یک سرپرست محلی انجام شود در حالت قفل نگه دارد؛ اکانت تخطی کننده را قفل کند تا وقتی‌که یک دوره زمانی تعریف‌شده توسط سرپرست سپری شود] نکات کاربردی: ✓ منظور از قفل‌کردن در الزام فوق، اجازه ندادن برای احراز هویت و ورود به سیستم است.	

✓ این الزام تنها به سرپرستان راه دور اعمال می‌شود و نه سرپرستان محلی که به‌طور مثال با کابل قصد اتصال به سرویس‌دهنده ایمیل را دارند. رسیدن به این مهم نیازمند وجود اکانت‌های سرپرستی محلی و راه دور جداگانه یا داشتن سازوکار احراز هویتی است که بتواند انواع ورود محلی و راه دور را به‌صورت متمایز تشخیص دهد. ✓ در خصوص قسمت اختصاص و تعیین یک اقدام مناسب برای آن به‌طور مثال می‌توان به بازنشانی‌کردن[1] رمز عبور و یا خارج کردن اکانت مذکور از حالت قفل اشاره کرد. ✓ بخش خلاصه مشخصات محصول باید بیان کند که سرویس‌دهنده ایمیل چگونه این اطمینان را ایجاد می‌کند که مسدود شدن موقت یا دائم یک سرپرست راه دور به دلیل شکست‌های مداوم در احراز هویت، باعث به وجود آمدن عدم دسترس‌پذیری محلی سرپرست نمی‌شود (به‌طور مثال با تعریف کردن یک اکانت محلی که مسدودسازی برای آن اعمال نمی‌شود).

۱۸	مدیریت رمز عبور ۱ (FIA_PMG_EXT.1)

سرویس‌دهنده ایمیل باید امکانات زیر را برای تعریف رمز عبور یا رمزهای عبور مدیریتی، فراهم کند:

۱ رمز عبور را باید بتوان با هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای ویژه مطرح‌شده در این بخش ساخت:
[انتخاب: ")"،"("،"*"،"&"،"^"،"%"،"$"،"#"،"@"،"!"،[اختصاص: سایر کاراکترها]]

۲ حداقل طول رمز عبور باید قابل پیکربندی به یک عدد مابین [اختصاص: کمترین تعداد کاراکترهای قابل پشتیبانی توسط سرویس‌دهنده ایمیل] و [اختصاص: تعداد کاراکترهای بزرگ‌تر مساوی با ۱۵] باشد.

نکات کاربردی:

✓ نویسنده هدف امنیتی کاراکترهای ویژه قابل‌استفاده در رمز عبور را انتخاب می‌کند. وی می‌تواند با استفاده از عبارت اختصاص در بند ۱، کاراکترهای دیگری را به لیست اضافه کند.

✓ منظور از واژه «رمز عبور مدیریتی» رمزهای عبوری هستند که توسط سرپرستان سیستم در کنسول محلی یا برای پروتکل‌هایی که از رمز عبور پشتیبانی می‌کنند مانند SSH و HTTPS مورد استفاده، قرار می‌گیرند. این رمزهای عبور گاهی نیز برای ارائه آن دسته از داده‌های پیکربندی که از دیگر الزامات کارکرد امنیتی در سرویس‌دهنده ایمیل پشتیبانی می‌کنند، مورداستفاده قرار می‌گیرند.

[1] Reset

✓ اختصاص دوم از بند ۲، باید به بزرگ‌ترین مقداری که می‌تواند برای کمینه طول رمز عبور توسط سرپرست پیکربندی شود، تنظیم گردد.	
شناسایی و احراز هویت کاربر ۱ (FIA_UIA_EXT.1.1)	۱۹
به هنگام اتصال یک موجودیت خارجی مانند یک سرپرست انسانی به سرویس‌دهنده ایمیل، پیش از انجام فرایند احراز هویت، سرویس‌دهنده ایمیل باید اجازه انجام فعالیت‌های زیر را بدهد: ۱. نمایش بنر هشدار با توجه به الزام FTA_TAB.1 (این بنر در مورد دسترسی غیرمجاز به سرویس‌دهنده هشدار می‌دهد.) ۲. [انتخاب: هیچ اقدامی، [اختصاص: لیستی از سرویس‌ها و اقداماتی که سرویس‌دهنده ایمیل می‌تواند بدون نیاز به احراز هویت برای کاربر فراهم کند.]] نکات کاربردی: ✓ ممکن است در مواردی امکان ارائه برخی از سرویس‌ها بدون نیاز به احراز هویت در سرویس‌دهنده برای کاربران فراهم شود. به‌طور مثال کاربر بتواند پیش از احراز هویت و اتصال به سرویس‌دهنده ایمیل با انجام سرویس ping از اتصال آن به اینترنت مطمئن شود. این‌گونه سرویس‌ها را می‌توان در قسمت اختصاص از مورد ۲ گنجاند.	
شناسایی و احراز هویت کاربر ۲ (FIA_UIA_EXT.1.2)	۲۰
پیش از آن‌که سرویس‌دهنده ایمیل امکان انجام اقدامات مدیریتی در خود را فراهم آورد، باید هر مدیر سیستم را ملزم کند که به‌صورت موفق شناسایی و احراز هویت شود. ✓ احراز هویت می‌تواند مبتنی بر رمز عبور و از طریق کنسول محلی و یا از طریق پروتکلی صورت گیرد که از رمزهای عبور، پشتیبانی می‌کند (مانند SSH) و یا بر اساس گواهینامه انجام شود (مانند SSH و TLS)	
سازوکار احراز هویت بر اساس رمز عبور ۲ (FIA_UAU_EXT.2.1)	۲۱
سرویس‌دهنده ایمیل باید یک سازوکار احراز هویت محلی مبتنی بر [انتخاب: رمز عبور، کلید عمومی SSH[۱]، گواهینامه[۲]، [اختصاص: مکانیزم‌های احراز هویت دیگر]] برای احراز هویت سرپرستان محلی فراهم کند.	

[۱] SSH public key-based

[۲] certificate-based

نکات کاربردی: ✓ عبارت اختصاص برای مشخص کردن دیگر سازوکارهای محلی احراز هویت پشتیبانی شده است. ✓ سازوکارهای احراز هویت محلی درواقع آن‌هایی هستند که از طریق کنسول محلی انجام می‌شوند. نشست‌های مدیریتی راه دور و سازوکارهای احراز هویت مربوط به آن‌ها در الزام FTP_TRP.1/Admin مشخص‌شده‌اند.	
۲۲	بازخورد امن در مکانیزم احراز هویت (FIA_UAU.7)
هنگامی‌که فرایند احراز هویت روی کنسول محلی در حال جریان است، سرویس‌دهنده ایمیل تنها باید بازخورد مبهم[1] را در اختیار سرپرست سرویس‌دهنده ایمیل قرار دهد. نکات کاربردی: ✓ «بازخورد مبهم» به معنی بازخوردی است که در آن سرویس‌دهنده ایمیل داده‌های احراز هویت واردشده توسط کاربر را به‌صورت واضح و قابل‌خواندن نشان نمی‌دهد؛ البته ممکن است روند پیشرفت به شکل مبهم نشان داده شود (مانند یک ستاره برای هر کاراکتر). ✓ بازخورد مبهم همچنین نشان می‌دهد که سرویس‌دهنده ایمیل در جریان احراز هویت هیچ اطلاعاتی را که ممکن است نشان‌دهنده داده‌های احراز هویت باشد، نمایش نمی‌دهد.	

۱-۳-۵- الزامات تکمیلی برای مقابله با ایمیل‌های جعلی و ناخواسته

ترکیب SPF، DKIM و DMARK، که در ادامه به الزامات هر یک اشاره‌شده است، تا حد زیادی می‌تواند خطر ایمیل‌های جعلی را برطرف کند، اما درصورتی‌که بازبینی‌های SPF و DKIM درست باشد ایمیل به مقصد تحویل داده خواهد شد. به‌عبارتی‌دیگر، حمله‌کننده ممکن است از یک دامنه معتبر برای حمله استفاده کند و شناسایی آن دشوار باشد. ازاین‌رو همواره باید از اقدامات تکمیلی نیز بهره جست که در این قسمت به آن‌ها اشاره‌شده است.

قابل‌ذکر است که الزامات مذکور با توسعه خانواده FIA و به‌صورت FIA_UED_EXT.1 ذکرشده است که UED مخفف عبارت Unsolicited Email Detection است.

شماره الزام	نام الزام

[1] Obscured feedback

۲۳	لیست‌های سیاه و سفید (FIA_UED_EXT.1)
با تکیه‌بر لیست سیاه از ارسال‌کننده‌های ایمیل، سرویس‌دهنده ایمیل باید قادر به فیلترینگ بر اساس آدرس IP ارسال‌کننده‌ها باشد. نکات کاربردی: ✓ سرویس‌دهنده ایمیل باید آدرس‌های تهدیدکننده را در طول زمان شناسایی کند و از دریافت ایمیل از آدرس‌های مذکور خودداری کند. سایت‌ها و سازمان‌هایی وجود دارد که لیستی از آدرس‌های تهدیدکننده را تهیه و مدام به‌روزرسانی می‌کنند.	
۲۴	تحلیل محتوا (FIA_UED_EXT.2)
سرویس‌دهنده ایمیل باید از مکانیزمی هوشمند برای شناسایی ایمیل‌های تهدیدکننده و جعلی با تکیه‌بر بررسی محتوای ایمیل‌ها از وجود لینک‌ها، عکس‌ها و هرگونه عبارات و الگوهای تکرارشونده در ایمیل‌های مشابه استفاده کند. نکات کاربردی: ✓ با توجه به سربار این روش، این مکانیزم باید به‌عنوان آخرین اقدام در شناسایی ایمیل‌های جعلی استفاده شود. ✓ این نوع ایمیل‌ها عموماً باهدف دسترسی به اطلاعات شخصی یا ارجاع به صفحات Phishing ارسال می‌شوند و تحلیل محتوا کمک زیادی به شناسایی آن‌ها خواهد کرد، هرچند که قادر به رفع کامل آن نیست.	
۲۵	ایمیل‌های حجیم (FIA_UED_EXT.3)
سرویس‌دهنده ایمیل باید از دریافت ایمیل‌هایی که ضمیمه‌های حجیم دارند خودداری کند و مقدار آستانه باید قابل تنظیم توسط سرپرست باشد. نکات کاربردی: ✓ ایمیل‌های حجیم می‌توانند حافظه و پردازش کننده‌ی سرور را شدیداً مشغول کنند. ✓ سرپرست سرویس‌دهنده ایمیل باید قادر به تنظیم حد آستانه برای ضمیمه ایمیل‌ها باشد.	

۴-۵- کلاس مدیریت امنیت

این کلاس شامل چهار دسته الزام برای مدیریت کارکردهای امنیتی در سرویس‌دهنده ایمیل است:

- FMT_MOF: مدیریت فرایند به‌روزرسانی
- FMT_MTD: مدیریت دسترسی به داده‌های پیکربندی
- FMT_SMR: تعریف نقش‌های امنیتی
- FMT_SMF: تعریف حداقل قابلیت‌های امنیتی که در اختیار سرپرستان خواهد بود.

در کنار این الزامات مدیریتی اصلی، برخی الزامات اختیاری نیز در پیوست اول و تعدادی الزامات انتخابی نیز در پیوست دوم ذکرشده‌اند.

شماره الزام	نام الزام
۲۶	مدیریت کارکرد امنیتی ۱/ به‌روزرسانی دستی (FMT_MOF.1/ManualUpdate)
سرویس‌دهنده ایمیل باید امکان استفاده از توابع به‌روزرسانی دستی را به سرپرست‌های امنیتی محدود کند. نکات کاربردی: ✓ این الزام امکان آغاز به‌روزرسانی دستی را به سرپرست سرویس‌دهنده ایمیل محدود می‌کند.	
۲۷	مدیریت دسترسی به داده‌ها ۱ (FMT_MTD.1/CoreData)
سرویس‌دهنده ایمیل باید امکان «مدیریت» داده‌های امنیتی، مانند اطلاعات پیکربندی سرویس‌دهنده ایمیل، را به سرپرست‌های امنیتی محدود کند. نکات کاربردی: ✓ منظور از «مدیریت» می‌تواند هر یک از اقدامات مقابل و حتی موارد دیگری ازاین‌دست باشد: مشاهده، تولید، مقداردهی اولیه، تغییر مقدار پیش‌فرض، تغییر مقدار داده، پاک کردن و اضافه کردن مقدار جدید. ✓ الزام حاضر همچنین شامل بازگرداندن[۱] رمز عبور کاربر به حالت پیش‌فرض توسط سرپرست سرویس‌دهنده ایمیل است.	

[۱] Reset

✓ عبارت" CoreData" در نام این الزام برای جداسازی آن با الزام ذکرشده در قسمت الزامات اختیاری با نام FMT_MTD.1/CryptoKeys است.	
۲۸	تعریف کارکردهای امنیتی ۱ (FMT_SMF.1)
سرویس‌دهنده ایمیل باید امکانات و توابع مدیریتی زیر را ارائه کند: • امکان مدیریت کردن سرویس‌دهنده ایمیل به‌صورت محلی و راه دور • پیکربندی بنر هشدار (اشاره‌شده در الزام FTA_TAB.1) • پیکربندی مدت‌زمان ممکن برای غیرفعال بودن یک نشست پیش از قفل‌کردن یا خاتمه دادن به آن (برای الزامات FTA_SSL_EXT.1 و FTA_SSL.3) • امکان به‌روزرسانی سرویس‌دهنده ایمیل و امکان تأیید به‌روزرسانی‌ها با استفاده از [انتخاب: امضای دیجیتال، مقایسه مقدار درهم‌سازی] پیش از نصب شدن به‌روزرسانی‌های مربوطه (مرتبط با الزامات FMT_MOF.1/ManualUpdate و FPT_TUD_EXT.1.) • پیکربندی پارامترهای مرتبط با شکست احراز هویت برای الزام FIA_AFL.1 • اضافه یا حذف دستی آدرس IP از لیست سیاه • امکان تعیین حد آستانه برای ضمیمه‌های حجیم • امکان تعریف قواعد DMARK و SPF • امکان تعیین دوره زمانی برای ارسال گزارش‌های DMARK به سرورهای طرف مقابل • [انتخاب: ▪ امکان شروع کردن یا خاتمه دادن به هر سرویس ▪ پیکربندی نحوه ذخیره‌سازی رکوردهای ممیزی (مثلاً تغییر محل ذخیره‌سازی به یک سرور خارجی syslog) ▪ مطابق با FIA_UIA_EXT.1 امکان فراهم کردن لیستی از سرویس‌ها که بدون نیاز به احراز هویت در سرویس‌دهنده ایمیل قابل‌ارائه خواهد بود. ▪ مدیریت کلیدهای رمزنگاری	

- مدیریت توابع رمزنگاری
- پیکربندی حد آستانه برای ایجاد مجدد کلید در پروتکل SSH
- پیکربندی طول عمر برای IPSec SAs[1]
- پیکربندی تعامل بین مؤلفه‌های سرویس‌دهنده ایمیل
- فعال‌سازی مجدد حساب سرپرست
- تنظیم زمان برای مهرهای زمانی
- امکان انجام پیکربندی‌های مرتبط با پروتکل NTP
- امکان تعیین trust store[2] برای گواهینامه‌های X509.v3 و همچنین تعیین گواهینامه‌های موردنظر به‌عنوان trust anchor
- امکان اضافه کردن گواهینامه‌های X509.v3 به trust store
- هیچ قابلیت دیگر

]

نکات کاربردی:

- ✓ دقت شود که مورد آخر از موارد ذکرشده، انتخاب است.
- ✓ همان‌طور که واضح است هریک از امکانات فوق دست‌کم مرتبط با یکی از الزامات ذکرشده در بخش‌های دیگر این سند است و همان‌طور که مشخص است در برخی موارد صریحاً به الزام یا الزامات مربوطه اشاره‌کرده‌ایم. سرویس‌دهنده ایمیل باید برای هر مورد، قابلیت(های) تعریف‌شده در الزام مربوطه را پیاده‌سازی کند.
- ✓ در مورد قابلیت‌های مربوط به IPsec تنها درصورتی‌که الزام مربوطه انتخاب‌شده است باید قابلیت ذکرشده پیاده‌سازی شود.

[1] IPSec Security Association

[2] برای سهولت در دریافت منظور این پروفایل حفاظتی، دو مفهوم اساسی trust store و trust anchor در حوزه تولید گواهینامه‌های x509 بدون ترجمه ذکرشده است.

۲۹	مدیریت نقش‌های امنیتی ۱ (FMT_SMR.2.1)
سرویس‌دهنده ایمیل باید حداقل نقش امنیتی زیر را فراهم کند: • سرپرست امنیتی نکات کاربردی: ✓ سرویس‌دهنده ایمیل باید با امکان تعریف سرپرستان محلی و راه دور، امکان مدیریت سرویس‌دهنده ایمیل را فراهم کند. ✓ توجه شود که می‌توان انواع نقش سرپرست با دسترسی‌ها و قابلیت‌های مختلف تعریف کرد و لزوماً نیاز نیست یک نقش قادر به انجام تمام قابلیت‌های تعریف‌شده در FMT_SMF.1 باشد و یا قادر به مدیریت راه دور یا محلی باشد. ✓ برای مدیریت راه دور باید با رعایت الزامات FPT_ITT.1،FTP_ITC.1 و/یا FTP_TRP.1/Admin برقراری اتصال امن تضمین شود.	
۳۰	مدیریت نقش‌های امنیتی ۲ (FMT_SMR.2.2)
سرویس‌دهنده ایمیل باید بتواند برای کاربران تعریف‌شده نقش تعیین کند.	
۳۱	مدیریت نقش‌های امنیتی ۳ (FMT_SMR.2.3)
سرویس‌دهنده ایمیل باید از فراهم بودن نقش‌های زیر اطمینان حاصل کند: • نقش سرپرست امنیتی برای اداره سرویس‌دهنده ایمیل به‌صورت محلی • نقش سرپرست امنیتی برای مدیریت سرویس‌دهنده ایمیل از راه دور	

۵-۵- کلاس محافظت از محصول

این کلاس شامل چهار دسته الزام به ترتیب برای محافظت از داده‌های امنیتی ذخیره‌شده در سرویس‌دهنده ایمیل مانند کلیدهای رمزنگاری و رمزهای عبور، انجام خودآزمایی خودکار برای کسب اطمینان از کارکرد صحیح توابع امنیتی، فراهم کردن رویه‌های قابل‌اعتماد برای انجام به‌روزرسانی و نیز تضمین درستی مهرهای زمانی برای ثبت رکوردهای ممیزی است.

۱-۵-۵- محافظت از داده‌های امنیتی

شماره الزام	نام الزام
۳۲	محافظت از کلیدهای رمزنگاری۱ (FPT_SKP_EXT.1.1)
سرویس‌دهنده ایمیل به‌هیچ‌وجه نباید اجازه خوانده‌شدن مقادیر کلیدهای از پیش به اشتراک گذاشته‌شده، کلیدهای متقارن و کلیدهای خصوصی را بدهد. نکات کاربردی: ✓ این داده‌ها باید تنها برای کارکردهای امنیتی مربوطه قابل‌دسترسی باشند و نیازی به دسترسی و نمایش آن‌ها در هر زمان دیگر نیست.	
۳۳	محافظت از رمز عبور سرپرست ۱ (FPT_APW_EXT.1.1)
سرویس‌دهنده ایمیل نباید رمزهای عبور را به شکل متن ساده، ذخیره کند.	
۳۴	محافظت از رمز عبور سرپرست ۲ (FPT_APW_EXT.1.2)
سرویس‌دهنده ایمیل باید از خوانده شدن رمزهای عبور، جلوگیری کند. نکات کاربردی: ✓ هدف از دو الزام اخیر این است که داده‌های خام مربوط به احراز هویت از طریق رمز عبور، به شکل واضح ذخیره نشوند و هیچ کاربر و سرپرست سرویس‌دهنده ایمیل نیز نتواند این رمزهای عبور را به‌صورت متن ساده از طریق واسط «عادی» بخواند. البته سرپرست سرویس‌دهنده ایمیل که تمام دسترسی‌ها را داشته باشد، می‌تواند رمزهای عبور را بخواند، اما به وی اعتماد می‌شود و فرض می‌گردد که وی این کار را نخواهد کرد.	

۲-۵-۵ خودآزمایی خودکار عملگرهای امنیتی

برای شناسایی وقوع مشکل در سازوکارهای امنیتی، سرویس‌دهنده ایمیل باید از طریق خودآزمایی از صحت کارکرد آن‌ها اطمینان حاصل کند. میزان و حجم این خودآزمایی‌ها به تصمیم تولیدکننده

سرویس‌دهنده ایمیل بستگی دارد، اما هر چه خودآزمایی‌های جامع‌تری انجام شوند، پلتفرم قابل‌اعتمادتری پدید خواهد آمد. همچنین شایان‌ذکر است که تعدادی الزام مبتنی بر انتخاب برای این مؤلفه در پیوست دو ارائه‌شده‌اند.

۳۵	خودآزمایی خودکار ۱ (FPT_TST_EXT.1)
سرویس‌دهنده ایمیل باید مجموعه‌ای از خودآزمایی‌های [اختصاص: لیستی از خودآزمایی‌ها] را در مواقع [انتخاب: در مرحله راه‌اندازی اولیه (روشن شدن دستگاه)، به‌طور دوره‌ای در حین کارکرد دستگاه، در صورت درخواست کاربر مجاز، در شرایط [اختصاص: شرایطی که باید در آن خودآزمایی انجام شود]] انجام دهد.	

۳-۵-۵- به‌روزرسانی امن محصول

عدم موفقیت سرپرست سرویس‌دهنده ایمیل در تأیید به‌روزرسانی‌های سیستم ممکن است کل سیستم را در معرض خطر قرار دهد. برای اعتماد به منبع به‌روزرسانی، سیستم می‌تواند مجموعه‌ای از فرایندها و سازوکارهای مبتنی بر رمزنگاری را مورداستفاده قرار دهد. به‌طور مثال از طریق سازوکار امضای دیجیتال از هویت منبع به‌روزرسانی اطمینان حاصل کند.

لازم به ذکر است که تعدادی الزام مبتنی بر انتخاب برای این خانواده در بخش الزامات انتخابی ارائه‌شده است.

۳۶	به‌روزرسانی امن ۱ (FPT_TUD_EXT.1.1)
سرویس‌دهنده ایمیل باید این امکان را به سرپرستان امنیتی خود بدهد که به نسخه فعلی (در حال استفاده) نرم‌افزار/میان‌افزار سرویس‌دهنده ایمیل و [انتخاب: جدیدترین نسخه نصب‌شده از نرم‌افزار/میان‌افزار روی سرویس‌دهنده ایمیل، هیچ نسخه دیگری از نرم‌افزار/میان‌افزار سرویس‌دهنده ایمیل] دسترسی داشته باشد. نکات کاربردی: ✓ منظور از الزام فوق این است که اگر امکان نصب ولی فعال‌سازی در یک‌زمان دیگر برای یک نسخه جدید از نرم‌افزار/میان‌افزار سرویس‌دهنده ایمیل وجود دارد، آنگاه باید هر دو گزینه نسخه در حال استفاده و نیز جدیدترین نسخه نصب‌شده از نرم‌افزار/میان‌افزار برای سرپرست نمایش	

داده شود. در غیر این صورت تنها نسخه در حال استفاده نمایش داده شود.	
۳۷	به‌روزرسانی امن ۲ (FPT_TUD_EXT.1.2)
سرویس‌دهنده ایمیل باید این امکان را برای سرپرستان امنیتی خود فراهم کند که به‌روزرسانی نرم‌افزار/میان‌افزار سرویس‌دهنده ایمیل را به‌صورت دستی انجام دهد و [انتخاب: از جستجوی خودکار به‌روزرسانی‌ها پشتیبانی کند، از به‌روزرسانی خودکار پشتیبانی کند، از هیچ سازوکار به‌روزرسانی دیگری پشتیبانی نکند].	
۳۸	به‌روزرسانی امن ۳ (FPT_TUD_EXT.1.3)
سرویس‌دهنده ایمیل باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، با استفاده از یک سازوکار مبتنی بر [انتخاب: امضای دیجیتال، گواهینامه x509، درهم‌سازی] ابزاری را برای احراز هویت به‌روزرسانی‌ها فراهم کند. نکات کاربردی: ✓ در صورت انتخاب سازوکار مبتنی بر گواهینامه‌های x509 الزام‌های FIA_X509_EXT.1/Rev و FIA_X509_EXT.2.1 باید در خصوص بررسی و احراز هویت گواهینامه‌های مربوطه پیاده‌سازی شوند. ✓ الگوریتم امضای دیجیتال باید مطابق با مورد انتخاب‌شده در الزام FCS_COP.1/SigGen باشد. ✓ الگوریتم امضای دیجیتال علاوه بر حالتی که در سازوکار مبتنی بر گواهینامه‌های x509 استفاده می‌شود، به‌صورت یک مکانیزم واحد و همراه با الگوریتم GPG و یا با کلیدهای عمومی خام نیز می‌تواند استفاده شود. ✓ برای مکانیزم مبتنی بر درهم‌سازی، الگوریتم انتخاب‌شده باید مبتنی بر الزام FCS_COP.1/Hash باشد. ✓ در صورت استفاده از سازوکار مبتنی بر درهم‌سازی، به یک مکانیزم «مجوزدهی فعال» توسط سرپرست امنیتی سرویس‌دهنده ایمیل نیز نیاز خواهد بود. منظور از این مکانیزم مجوزدهی، تولید مقدار چکیده فایل به‌روزرسانی و مقایسه آن با مقدار چکیده ارسال‌شده است. سرویس‌دهنده ایمیل می‌تواند به هر نحوی که مناسب آن باشد این فرایند را به‌صورت دستی یا	

خودکار پیاده‌سازی کند. قابل‌ذکر است که فرایند ارسال مقدار چکیده به سرویس‌دهنده ایمیل نیز باید به‌طور کامل شرح داده‌شده و قابل‌اطمینان بودن این فرایند انتقال باید تضمین شود.

۴-۵-۵- مهرهای زمانی قابل‌اعتماد

۳۹	مهر زمانی امن ۱ (FPT_STM_EXT.1.1)
سرویس‌دهنده ایمیل باید قابلیت ارائه مهرهای زمانی قابل‌اطمینان برای استفاده خودش را داشته باشد.	
۴۰	مهر زمانی امن ۲ (FPT_STM_EXT.1.2)
سرویس‌دهنده ایمیل باید [انتخاب: به سرپرست امنیتی اجازه دهد که زمان را تنظیم کند، زمان را با منابع خارجی NTP همگام سازد]. نکات کاربردی: ✓ مهرهای زمانی قابل‌اطمینان جهت استفاده در دیگر توابع امنیتی سرویس‌دهنده ایمیل، موردنظر هستند، به‌عنوان‌مثال، برای ثبت زمان وقوع رخداد در رکوردهای ممیزی. ✓ این زمان می‌تواند به‌صورت دستی توسط سرپرست امنیتی تنظیم شود و یا با استفاده از یک یا چند منبع خارجی مانند سرور NTP تنظیم گردد. ✓ در صورت استفاده از سرور خارجی NTP الزام FCS_NTP_EXT.1 هم باید رعایت و اضافه شود.	

۶-۵- کلاس دسترسی به محصول

این کلاس به الزامات مرتبط با چگونگی مدیریت نشست‌های محلی و راه دور برقرارشده میان سرپرستان و سرویس‌دهنده ایمیل اختصاص دارد. مواردی چون بستن یک نشست بعد از یک مدت‌زمان معین از عدم فعالیت و نیز نمایش بنر هشدار در ابتدای هر نشست در این کلاس قرار می‌گیرند.

شماره الزام	نام الزام
۴۱	قفل‌کردن و خاتمه دادن به نشست‌ها ۱ (FTA_SSL_EXT.1.1)
در مورد نشست‌های محلی، سرویس‌دهنده ایمیل باید پس از اتمام زمان غیرفعال بودن که توسط سرپرست سرویس‌دهنده ایمیل تعیین‌شده است، [انتخاب:	

❖ نشست را قفل کند: یعنی امکان دسترسی سرپرست به منوهای مختلف را قفل کرده و تنها گزینه «بازگشایی از حالت قفل» را به آن نشان دهد. برای بازگشایی نیز سرپرست را مجبور به احراز هویت مجدد کند. ❖ نشست را به‌طور کامل خاتمه دهد. [	
۴۲	قفل‌کردن و خاتمه دادن به نشست‌ها ۲ (FTA_SSL.3.1)
در مورد نشست‌های راه دور، درصورتی‌که نشست تعاملی برای مدت معینی غیرفعال باشد، سرویس‌دهنده ایمیل باید نشست تعاملی را خاتمه دهد. مدت‌زمان مجاز برای غیرفعال بودن توسط سرپرست سرویس‌دهنده ایمیل تعیین می‌شود.	
۴۳	قفل‌کردن و خاتمه دادن به نشست‌ها ۳ (FTA_SSL.4.1)
سرویس‌دهنده ایمیل باید به سرپرست سرویس‌دهنده ایمیل اجازه دهد که نشست تعاملی خود را خاتمه دهد.	
۴۴	بنر هشدار (FTA_TAB.1.1)
قبل از برقراری نشست میان سرپرست اجرایی و سرویس‌دهنده ایمیل، سرویس‌دهنده ایمیل باید توصیه‌های مشخص‌شده توسط سرپرست امنیتی و همچنین تأییدیه استفاده از سرویس‌دهنده ایمیل را نشان دهد. نکات کاربردی: ✓ این الزام تنها در مورد نشست‌های تعاملی بین یک کاربر انسانی و سرویس‌دهنده ایمیل اعمال می‌شود. برای دیگر موجودیت‌های IT مانند اتصال اتوماتیک سرور خارجی syslog از طریق IPSec نیازی به رعایت این الزام نیست.	

۷-۵- کلاس کانال‌ها/مسیرهای مورد اعتماد

الزامات این کلاس اختصاص به چگونگی برقراری یک کانال امن میان سرویس‌دهنده ایمیل و یک موجودیت خارجی مانند یک سرور خارجی syslog برای ارسال رکوردهای ممیزی دارد. این کانال امن

باید داده‌های ارسالی را از شنود و تغییر حفظ کند و نیز با فراهم کردن احراز هویت دوطرفه از حملاتی مثل مرد میانی، جلوگیری کند.

رسیدن به این هدف با استفاده از یکی از پنج پروتکل IPsec، TLS،SSH ، DTLS و HTTPS فراهم می‌شود.

شماره الزام	نام الزام
۴۵	کانال امن/ سرویس‌دهنده ایمیل با دیگر موجودیت‌های IT ۱ (FTP_ITC.1.1)
سرویس‌دهنده ایمیل باید بتواند کانال ارتباطی امنی را با استفاده از پروتکل(های) [انتخاب: IPsec، SSH، TLS، DTLS، HTTPS] میان خود و دیگر موجودیت‌های IT معتبر شامل: سرور ممیزی، [انتخاب: سرور احراز هویت، [اختصاص: لیستی از سرورهای دیگر که نیاز به امن کردن کانال دارند]، هیچ سرور دیگر] برقرار کند تا ضمن فراهم کردن احراز هویت دوطرفه، از داده‌های مورد تبادل در برابر تغییر و افشاء محافظت کند و تغییرات را تشخیص دهد. تذکر: در صورت استفاده از هر یک از پروتکل‌های مذکور به‌عنوان پروتکل ارتباطی امن، لازم است از بخش الزامات انتخابی تمامی الزامات مربوط به آن پروتکل نیز تکمیل و به سند هدف امنیتی اضافه گردد. نکات کاربردی: ✓ این الزام تضمین می‌دهد که اطلاعات مورد تبادل میان تجهیز مربوطه و سرویس‌دهنده ایمیل در یک ارتباط راه دور در معرض افشا و تغییر قرار نخواهد گرفت. ✓ بسیار مهم است که چگونگی مدیریت کردن شرایطی که کانال مربوطه قطع می‌شود نیز شرح داده شود. باید تضمین داده شود که در صورت قطع شدن کانال تا برقراری مجدد کانال، هیچ داده‌ای تحت هیچ شرایطی روی مسیر عادی ارسال نخواهد شد.	
۴۶	کانال امن/ سرویس‌دهنده ایمیل با دیگر موجودیت‌های IT ۲ (FTP_ITC.1.2)
سرویس‌دهنده ایمیل باید اجازه داشته باشد یا به دیگر موجودیت معتبر IT اجازه دهد تا پس از برقراری	

کانال امن میان آن‌ها، ارتباط را از طریق این کانال آغاز کنند.	
۴۷	کانال امن/ سرویس‌دهنده ایمیل با دیگر موجودیت‌های IT ۳ (FTP_ITC.1.3)
سرویس‌دهنده ایمیل باید ارتباطات را از طریق کانال امن برای [اختصاص: لیست سرویس‌هایی که سرویس‌دهنده ایمیل می‌تواند برای آن‌ها ارتباطات را آغاز کند] شروع کند.	
۴۸	کانال امن/ سرویس‌دهنده ایمیل با سرپرست ۱ (FTP_TRP.1.1/Admin)
سرویس‌دهنده ایمیل باید بتواند کانال ارتباطی امنی را با استفاده از پروتکل(های) [انتخاب: IPsec، SSH، TLS، DTLS، HTTPS] میان خود و یک سرپرست راه دور برقرار کند تا ضمن فراهم کردن احراز هویت دوطرفه، از داده‌های مورد تبادل در برابر تغییر و افشاء محافظت کند و تغییرات را تشخیص دهد. نکات کاربردی: ✓ این الزام تضمین می‌دهد که اطلاعات حساس میان سرپرست و سرویس‌دهنده ایمیل در یک ارتباط راه دور در معرض افشا و تغییر قرار نخواهند گرفت.	
۴۹	کانال امن/ سرویس‌دهنده ایمیل با سرپرست ۲ (FTP_TRP.1.2/Admin)
سرویس‌دهنده ایمیل باید به سرپرست راه دور سرویس‌دهنده ایمیل اجازه دهد تا ارتباطات را از طریق کانال امن ایجادشده آغاز کند.	
۵۰	کانال امن/ سرویس‌دهنده ایمیل با سرپرست ۳ (FTP_TRP.1.3/Admin)
سرویس‌دهنده ایمیل باید استفاده از کانال امن را برای احراز هویت اولیه سرپرست و تمامی فعالیت‌های مدیریتی راه دور الزامی کند.	

۸-۵- الزامات پروتکل TLS

استفاده از پروتکل TLS برای امن کردن اتصالات SMTP، POP و IMAP از الزامات اساسی در این پروفایل حفاظتی به شمار می‌آید. همچنین می‌توان از TLS به‌منظور ایجاد کانال امن میان سرویس‌دهنده ایمیل و یک موجودیت خارجی IT مانند سرور syslog استفاده کرد که به آن اشاره شد.

قابل‌ذکر است که با توجه به کارکرد این پروتکل به فرم client/server، الزامات مربوطه نیز برای هر یک از نقش‌های client یا server جداگانه بیان‌شده است. به‌طورمعمول شروع‌کننده‌ی اتصال نقش server و

مخاطب آن نقش client را به خود می‌گیرد. واضح است که بسته به نوع اتصالات موردنیاز در فرایند دریافت، ارسال و تحویل ایمیل، مؤلفه‌های سرویس‌دهنده ایمیل شامل MTA، MDA، MSA و MUA باید قادر به پیاده‌سازی هر یک از دو نقش client/server باشند.

جدول زیر لیست مجموعه‌های رمزنگاری برای پیاده‌سازی TLS و DTLS را نشان می‌دهد.

جدول ۱-۴ لیست مجموعه‌های رمزنگاری برای پروتکل‌های TLS و DTLS

TLS_RSA_WITH_AES_128_CBC_SHA مطابق با3268 RFC
TLS_RSA_WITH_AES_256_CBC_SHAمطابق با 3268 RFC
TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با 3268 RFC
TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با 3268 RFC
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با 4492 RFC
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با 4492 RFC
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با 4492 RFC
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با 4492 RFC
TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با 5246 RFC
TLS_RSA_WITH_AES_256_CBC_ SHA256 مطابق با 5246 RFC
TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 مطابق با 5246 RFC
TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 مطابق با 5246 RFC
TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با 5288 RFC
TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با 5288 RFC
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با 5288 RFC
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با 5288 RFC
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با 5289 RFC
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با 5289 RFC
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با 5289 RFC
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با 5289 RFC
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با 5289 RFC
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با 5289 RFC

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289

شماره الزام	نام الزام
۵۱	الزامات پروتکل TLS Client (۱) (FCS_TLSC_EXT.1.1)
TLS Client باید [انتخاب: TLS 1.3 (RFC 8446)، TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و از دیگر نسخه‌های TLS و SSL استفاده نکند. همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر، پیاده‌سازی کند: [انتخاب: یکی از مجموعه‌های رمزنگاری لیست شده در «لیست مجموعه‌های رمزنگاری برای پروتکل‌های TLS»]	
۵۲	الزامات پروتکل TLS Client (۲) (FCS_TLSC_EXT.1.2)
TLS Client باید مطابقت شناسه[۱] ارائه‌شده با شناسه مرجع را با توجه به بخش 6 از RFC 6125، تأیید کند. نکات کاربردی: قوانین مربوط به تأیید شناسه در بخش 6 از RFC 6125 توضیح داده‌شده‌اند.	
۵۳	الزامات پروتکل TLS Client (۳) (FCS_TLSC_EXT.1.3)
TLS Client باید کانال امن را فقط در صورت معتبر بودن گواهینامه TLS server برقرار سازد. اگر	

[۱] Identifier

گواهینامه TLS server نامعتبر به نظر رسید، client باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات.]].	
الزامات پروتکل TLS Client (۴) (FCS_TLSC_EXT.1.4)	۵۴
TLS Client باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Extension Supported Elliptic Curves را به همراه NIST curveهای [انتخاب:secp384r1, secp521r1 ,secp256r1] و هیچ منحنی دیگری] در پیام Client Hello ارائه دهد. نکات کاربردی: ✓ اگر در الزام «الزامات پروتکل TLS Client (۱)» مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام مربوطه هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب نگردد، عبارت "Supported Elliptic Curves Extension را ارائه نکند" باید انتخاب شود. ✓ این الزام مجموعه‌های رمز بیضوی مجاز برای احراز هویت و توافق کلید را به منحنی‌های NIST از الزام‌های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌هایی که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند الزامی است.	
الزامات پروتکل TLS Client (۵) (FCS_TLSC_EXT.1.5)	۵۵
TLS Client باید از احراز هویت دوطرفه TLS server بر مبنای گواهینامه‌های X.509v3 پشتیبانی کند.	
الزامات پروتکل TLS Server (۱) (FCS_TLSS_EXT.1.1)	۵۶
TLS server باید [انتخاب: TLS 1.3 (RFC 8446) ، TLS 1.2 (RFC 5246)، TLS 1.1 (RFC 4346)] را پیاده‌سازی کند و از دیگر نسخه‌های TLS و SSL استفاده نکند. همچنین TLS را با پشتیبانی از مجموعه‌های رمز زیر، پیاده‌سازی کند: [انتخاب: یکی از مجموعه‌های رمزنگاری لیست شده در «لیست الگوریتم‌های رمزنگاری برای پروتکل‌های TLS و	

«DTLS]	
۵۷	الزامات پروتکل TLS Server (۲) (FCS_TLSS_EXT.1.2)
TLS server باید برای کلاینت‌های دارای درخواست SSL 2.0، SSL 3.0، TLS 1.0 و [انتخاب: TLS 1.1، TLS 1.2، TLS 1.3 ، هیچ موردی]، اتصال را ایجاد نکند. نکات کاربردی: ✓ تمامی نسخه‌های SSL و TLS v1.0 رد می‌شوند. هر نسخه‌ای از TLS که در الزام «الزامات پروتکل TLS Server (۱)» انتخاب نگردد، باید در بخش انتخاب فوق، انتخاب شود.	
۵۸	الزامات پروتکل TLS Server (۳) (FCS_TLSS_EXT.1.3)
TLS server باید استقرار کلید را با استفاده از [انتخاب: RSA با اندازه کلید [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲بیت، ۴۰۹۶ بیت] ، دیفی- هلمن با پارامترهایی با سایز [۲۰۴۸ بیت، ۳۰۷۲بیت، ۴۰۹۶ بیت، ۶۱۴۴ بیت، ۸۱۹۲ بیت]، دیفی-هلمن با گروه‌های [انتخاب: ffdhe2048، ffdhe3072، ffdhe4096، ffdhe6144، ffdhe8192، هیچ گروه دیگر]، منحنی‌های ECDHE [انتخاب:secp521r1 ,secp256r1, secp384r1] و هیچ منحنی دیگری] انجام دهد.	
۵۹	الزامات پروتکل TLS Server (۴) (FCS_TLSS_EXT.1.4)
TLS server باید از احراز هویت دوطرفه TLS client بر مبنای گواهینامه‌های X.509v3 پشتیبانی کند.	
۶۰	الزامات پروتکل TLS Server (۵) (FCS_TLSS_EXT.1.5)
به هنگام برقراری کانال امن، TLS server بدون تأیید گواهینامه TLS client نباید با آن تشکیل کانال دهد. در صورت غیر معتبر بودن گواهینامه، TLS server در ادامه همچنین باید [انتخاب: هیچ کار دیگری نکند، درخواست مجوز برای تشکیل کانال بدهد]	
۶۱	الزامات پروتکل TLS Server (۶) (FCS_TLSS_EXT.1.6)
بدون تأیید اینکه distinguished name (DN) و Subject Alternative Name (SAN) موجود در گواهینامه با شناسه‌های مورد انتظار برای کاربر تطابق ندارند، TLS server نباید با TLS client کانال امن تشکیل دهد.	

۹-۵- الزامات گواهینامه‌های X.509

گواهینامه‌های X.509 در TLS ، S/MIME و به عبارتی در سرتاسر معماری امن تعریف‌شده برای یک سرویس‌دهنده ایمیل کاربرد دارند. این بخش الزامات مرتبط با چگونگی اعتبار سنجی این گواهینامه‌ها را بیان می‌کند.

شماره الزام	نام الزام
۶۲	الزامات گواهینامه‌های X.509/ تأیید گواهینامه (۱) (FIA_X509_EXT.1.1/Rev)
سرویس‌دهنده ایمیل باید گواهینامه‌ها را بر اساس قوانین زیر تأیید کند: • بر اساس RFC 5280 برای تأیید گواهینامه و مسیر آن که از حداقل طول مسیر سه گواهینامه پشتیبانی می‌کند. • مسیر گواهینامه باید به یک گواهینامه CA امن ختم شود. • برای تأیید مسیر گواهینامه باید اطمینان حاصل شود که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهینامه‌های CA به حالت ”True“تنظیم‌شده است. • وضعیت فسخ گواهینامه باید با استفاده از [انتخاب: پروتکل OCSP مشخص‌شده در RFC 6960، لیست فسخ گواهینامه (CRL) مشخص‌شده در RFC 5280 بخش۶.۳ ، لیست فسخ گواهینامه (CRL) مشخص‌شده در RFC 5759 بخش ۵، هیچ روش فسخ] تأیید شود. • فیلد extendedKeyUsage باید بر اساس قوانین زیر تأیید شود: ▪ گواهینامه‌های مورداستفاده برای تأیید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی، باید دارای هدف "Code Signing Purpose" (id-kp3 با OID 1.3.6.1.5.5.7.3.3) در فیلد extendedKeyUsage باشند. ▪ گواهینامه‌های سرور ارائه‌شده برای TLS باید هدف ”Server Authentication“ id-kp1 با OID 1.3.6.1.5.5.7.3.1) در فیلد extendedKeyUsage خود داشته باشند. ▪ گواهینامه‌های کلاینت ارائه‌شده برای TLS باید هدف ”Client Authentication“	

(id-kp1 با OID 1.3.6.1.5.5.7.3.2) در فیلد extendedKeyUsage خود داشته باشند. ▪ گواهینامه‌های OCSP مورداستفاده برای پاسخ‌های OCSP باید هدف "OCSP Signing" (id-kp9 با OID1.3.6.1.5.5.7.3.9) در فیلد extendedKeyUsage خود داشته باشند.	
الزامات گواهینامه‌های X.509/ تأیید گواهینامه (۲) (FIA_X509_EXT.1.2/Rev)	۶۳
تنها درصورتی‌که افزونه مربوط به basicConstraints از پیش تنظیم‌شده باشد و پرچم CA به حالت "TRUE" تنظیم‌شده باشد یک گواهینامه را به‌عنوان گواهینامه CA پذیرفته می‌شود.	
الزامات گواهینامه‌های X.509/ احراز هویت (۱) (FIA_X509_EXT.2.1)	۶۴
سرویس‌دهنده ایمیل باید جهت پشتیبانی از احراز هویت در [انتخاب: DTLS, TLS, HTTPS, SSH ,IPsec] و [انتخاب: امضای کد[۱] برای به‌روزرسانی‌های نرم‌افزاری سیستم، امضای کد برای تأیید یکپارچگی، [اختصاص: سایر کاربردها]، هیچ کاربرد دیگر] از گواهینامه‌های X.509v3 مطابق با RFC 5280 استفاده کند.	
الزامات گواهینامه‌های X.509/ احراز هویت (۲) (FIA_X509_EXT.2.2)	۶۵
زمانی که سرویس‌دهنده ایمیل نمی‌تواند اتصال موردنیاز برای تأیید اعتبار یک گواهینامه را برقرار کند، باید [انتخاب: به سرپرست سرویس‌دهنده ایمیل اجازه دهد که در این مورد تصمیم‌گیری کند، گواهینامه را بپذیرد، گواهینامه را نپذیرد.]	
الزامات گواهینامه‌های X.509/ درخواست گواهینامه (۱)(FIA_X509_EXT.3.1)	۶۶
سرویس‌دهنده ایمیل باید مطابق با آنچه در RFC 2986 تشریح شده است، یک پیام Request Certificate تولید کند و بتواند اطلاعاتی شامل کلید عمومی و [انتخاب: اطلاعات مخصوص به	

[۱] Code Signing

سرویس‌دهنده ایمیل، Common Name، Organization، Organization Unit، Country] را در درخواست فراهم کند. نکات کاربردی: ✓ منظور از کلید عمومی درواقع بخش کلید عمومی از جفت کلیدهای عمومی-خصوصی است که در الزام FCS_CKM.1 شرح داده‌شده است و توسط سرویس‌دهنده ایمیل تولید می‌شود.	
الزامات گواهینامه‌های X.509/ درخواست گواهینامه (۲)(FIA_X509_EXT.3.2)	۶۷
با دریافت پاسخ CA Certificate Response، سرویس‌دهنده ایمیل باید زنجیره گواهینامه‌ها را با شروع از Root CA اعتبارسنجی کند.	

۱۰-۵- الزامات پروتکل DNSSEC

این بخش به بیان الزامات پروتکل DNSSEC[1] می‌پردازد که برای ارتباط با سرور DNS باید مورداستفاده قرار گیرد. این پروتکل امکان احراز هویت مبدأ و همچنین تضمین صحت داده برای پاسخ‌های دریافتی در ازای درخواست‌های DNS را فراهم می‌کند. به‌عبارتی‌دیگر، سرویس‌دهنده ایمیل مطمئن خواهد شد که پاسخ دریافتی از سرویس‌دهنده DNS معتبر است.

شماره الزام	نام الزام
۶۸	الزامات پروتکل DNSSEC (۱) (FCS_DNSSEC_EXT.1.1)
سرویس‌دهنده ایمیل باید پروتکل DNSSEC (RFC 4033) را با توجه به لیست مجموعه رمز زیر برای انجام DNSSEC Validation پیاده‌سازی کند. مطابق با این پروتکل، سرویس‌دهنده باید قادر به انجام احراز هویت زنجیره‌ای برای تائید امضای موجود در جواب‌های دریافتی از سرویس‌دهنده DNS دارد. ستون «نیازمندی» الزام به پیاده‌سازی هر مجموعه را مشخص کرده و ستون مرجع نیز الگو و استاندارد	

[1] Domain Name System Security Extensions

موردنیاز در پیاده‌سازی را مشخص می‌کند.

جدول ۱-۵ مجموعه رمز برای انجام DNSSEC Validation

الگوریتم	مرجع	نیازمندی
RSA/SHA-1	RFC 3110	لازم
RSASHA1-NSEC3-SHA1	RFC 5155	لازم
RSA/SHA-256	RFC 5702	لازم
RSA/SHA-512	RFC 5702	لازم
ECDSA/SHA-256	RFC 6605	لازم
ECDSA/SHA-384	RFC 6605	توصیه‌شده
Ed25519	RFC 8080	توصیه‌شده
Ed448	RFC 8080	توصیه‌شده
GOST R 34. 10-2001	RFC 5933	اختیاری

۶۹	الزامات پروتکل DNSSEC (۲) (FCS_DNSSEC_EXT.1.2)

سرویس‌دهنده ایمیل باید از پروتکل DNSSEC برای تمامی اتصالات با سرور DNS استفاده کند.

نکات کاربردی:

- ✓ مطابق با این الزام، سرویس‌دهنده ایمیل باید از سرویس‌دهنده‌های DNS ای بهره بگیرد که از DNSSEC پشتیبانی می‌کنند.
- ✓ مطابق با معماری DNSSEC، سرور ایمیل نقش Security-aware resolver را ایفا خواهد کرد.

۷۰	الزامات پروتکل DNSSEC (۳) (FCS_DNSSEC_EXT.1.3)

به‌منظور دریافت کردن[1] رکوردهای DNS در حافظه محلی، سرویس‌دهنده ایمیل باید طول عمر امضای رکوردها را نیز در نظر بگیرد. نکات کاربردی: ✓ عموماً هدف از دریافت کردن رکوردهای DNS در حافظه محلی صرفه‌جویی در زمان و نیز کمک به کاهش بار کاری سرویس‌دهنده DNS است. ✓ توجه به طول عمر امضاهای دیجیتال بر روی رکوردهای DNS (RRSIG) برای جلوگیری از نگهداری و استفاده از رکوردهای تاریخ گذشته ضروری است.	
الزامات پروتکل DNSSEC (۴) (FCS_DNSSEC_EXT.1.4)	۷۱
درصورتی‌که از موجودیت مجزایی برای ارسال درخواست‌های DNS و دریافت و تائید اصالت پاسخ‌ها استفاده شود، کانال ارتباطی میان سرویس‌دهنده ایمیل و موجودیت مربوطه باید از کلاس «کانال‌ها/مسیرهای مورد اعتماد» پیروی کند. نکات کاربردی: ✓ ممکن است در شرایط خاص و به دلایل امنیتی از مؤلفه‌ی مطمئن مجزایی به‌مانند یک Proxy جهت ارسال درخواست‌های DNS استفاده‌شده و موجودیت مربوطه مسئول دریافت و احراز اصالت پاسخ‌ها باشد. در چنین شرایطی باید کانال امنی میان موجودیت مربوطه و سرویس‌دهنده ایمیل برقرار باشد.	
الزامات پروتکل DNSSEC (۵) (FCS_DNSSEC_EXT.1.5)	۷۲
در صورت استفاده از یک موجودیت مجزا، سرویس‌دهنده ایمیل باید اطمینان حاصل کند که موجودیت مربوطه اصالت امضا در پاسخ دریافتی از سرویس‌دهنده DNS را به‌طور کامل احراز کرده است.	

[1] Cash

نکات کاربردی: ✓ سرویس‌دهنده می‌تواند با چک کردن بیت AD (Authenticated Data) در هدر پیغام دریافتی از موجودیت مربوطه این کار را انجام دهد.

۱۱-۵- الزامات چارچوب SPF

چارچوب SPF به سرویس‌دهنده‌ی ایمیل این امکان را می‌دهد تا آدرس‌های IP معتبر برای مؤلفه‌های MTA خود را در سرویس‌دهنده‌ی DNS ثبت کرده و بدین طریق به گیرندگان این امکان را دهد تا با چک کردن آدرس MTA ارسال‌کننده‌ی ایمیل با آدرس‌های معتبر ثبت‌شده برای دامنه‌ی مربوطه ایمیل‌های جعلی را شناسایی کنند و از وقوع حملاتی چون Phishing و جعل هویت جلوگیری شود.

شماره الزام	نام الزام
۷۳	الزامات پروتکل SPF (۱) (FCS_SPF_EXT.1.1)
سرویس‌دهنده ایمیل باید چارچوب SPF را مطابق با RFC 7208 و به‌روزرسانی‌های آن در نسخه‌های 7372، 8553 و 8616 پیاده‌سازی کند.	
۷۴	الزامات پروتکل SPF (۲) (FCS_SPF_EXT.1.2)
سرویس‌دهنده ایمیل باید آدرس(های) IP معتبر برای مؤلفه(های) MTA خود را به‌صورت رکوردهای SPF TXT در سرویس‌دهنده‌ی DNS مربوط به خود ثبت کند. نکات کاربردی: ✓ ممکن است به دلایلی سرویس‌دهنده امکان ثبت تمامی آدرس‌های IP مربوطه را در رکورد SPF نداشته باشد. در این حالت باید قواعد SPF مناسب برای نحوه‌ی پردازش ایمیل‌هایی که از IP های لیست شده نیامده‌اند تعیین شود که در ادامه به آن اشاره‌شده است.	
۷۵	الزامات پروتکل SPF (۳) (FCS_SPF_EXT.1.3)
سرویس‌دهنده ایمیل می‌تواند تعداد [انتخاب: ۱، تعداد بیشتر، هیچ] آدرس دامنه‌ی third-party را به‌عنوان آدرس دامنه‌ی تائید شده برای ارسال ایمیل در رکورد SPF خود مشخص کند.	

نکات کاربردی: ✓ رکوردهای SPF این امکان را می‌دهند تا علاوه بر تعیین IPهای معتبر، دامنه‌های third-party و مجاز به ارسال ایمیل از جانب دامنه اصلی را نیز با استفاده از کلیدواژه include تعیین کرد. به‌عبارتی‌دیگر ایمیل‌های رسیده از دامنه‌های مذکور نیز معتبر خواهند بود. در این حالت به‌عنوان گیرنده‌ی ایمیل، فرایند SPF record checking جهت شناسایی IPهای معتبر برای دامنه (های) مذکور نیز باید انجام شود.	
۷۶	الزامات پروتکل SPF (۴) (FCS_SPF_EXT.1.4)
رکوردهای SPF باید شامل قواعد لازم برای نحوه‌ی پردازش ایمیل‌هایی باشد که آدرس MTA ارسالی آن‌ها در لیست آدرس‌های ثبت‌شده موجود نباشد. سرویس‌دهنده نباید از قاعده all+ که به معنای پذیرش تمامی ایمیل‌های مذکور است استفاده کند.	
۷۷	الزامات پروتکل SPF (۵) (FCS_SPF_EXT.1.5)
در جایگاه دریافت‌کننده ایمیل، سرویس‌دهنده ایمیل باید قادر به پردازش رکوردهای SPF ثبت‌شده برای ارسال‌کننده و پردازش بر اساس قواعد مربوطه باشد.	
۷۸	الزامات پروتکل SPF (6) (FCS_SPF_EXT.1.6)
سرویس‌دهنده‌ی ایمیل باید از پروتکل DNSSEC برای اتصال با DNS و ثبت یا بررسی رکوردهای SPF استفاده کند.	

۱۲-۵- الزامات مکانیزم DKIM

متد DKIM با اضافه کردن یک DKIM Header به ایمیل که شامل یک امضای دیجیتال از سرآیند ایمیل و محتوای هش شده‌ی آن است، دامنه ارسال‌کننده را احراز هویت می‌کند. این متد در کنار SPF و DMARK تضمین می‌دهند که ایمیل رسیده از مرجع معتبری ارسال‌شده است.

شماره الزام	نام الزام
۷۹	الزامات متد DKIM (۱) (FCS_ DKIM_EXT.1.1)

سرویس‌دهنده ایمیل باید متد DKIM را بر اساس RFC 6376 و الگوریتم‌های RSA-SHA256 و Ed25519-SHA256 برای انجام امضای دیجیتال پیاده‌سازی کند.	
۸۰	الزامات متد DKIM (۲) (FCS_ DKIM_EXT.1.2)
سرویس‌دهنده ایمیل باید از الگوریتم‌های RSA-SHA1، RSA-SHA256 و Ed25519-SHA256 برای تائید اصالت امضای دیجیتال بر روی سرآیند DKIM پشتیبانی کند. نکات کاربردی: ✓ با توجه به آسیب‌پذیر بودن RSA-SHA1، استفاده از آن برای انجام امضا توصیه نمی‌شود ولی با توجه به اینکه ممکن است برای یک ایمیل دریافتی از یک سرور خارجی از این الگوریتم برای تولید امضا استفاده‌شده باشد، لذا پشتیبانی از آن برای تائید اصالت امضا اجباری است.	
۸۱	الزامات متد DKIM (۳) (FCS_ DKIM_EXT.1.3)
سرویس‌دهنده ایمیل باید قادر به تولید جفت کلید عمومی/خصوصی برای متد DKIM بر اساس الزام « مدیریت کلید رمزنگاری ۱» باشد.	
۸۲	الزامات متد DKIM (۴) (FCS_ DKIM_EXT.1.4)
سرویس‌دهنده ایمیل باید از رکوردهای DKIM DNS TXT برای قرار دادن کلید عمومی خود بر روی سرویس‌دهنده DNS استفاده کند تا گیرنده به کلید مربوطه دسترسی داشته باشد.	
۸۳	الزامات متد DKIM (۵) (FCS_ DKIM_EXT.1.5)
سرویس‌دهنده ایمیل باید از پروتکل DNSSEC برای ارتباط با سرویس‌دهنده DNS جهت قرار دادن کلید عمومی خود یا برداشتن کلید عمومی دیگر سرویس‌دهنده‌ها استفاده کند.	

۱۳-۵- الزامات مکانیزم DMARK

اهمیت DMARK برای یک سرویس‌دهنده ایمیل از دو نظر است:

۱) به سرور(های) دریافت‌کننده‌ی ایمیل اعلام می‌کند تا چگونه با ایمیل‌هایی که تست DKIM یا SPF آن‌ها ناموفق بوده رفتار کند (۱- به گیرنده تحویل دهد ۲- به‌عنوان Spam به گیرنده تحویل دهد ۳- دور بریزد).

۲) چگونه گزارش‌هایی از آمار ایمیل‌های سالم یا ناسالم رسیده از سرویس‌دهنده ایمیل را به او ارسال کند. بدین طریق، سرویس‌دهنده ایمیل از ارسال ایمیل‌های جعلی یا وجود مشکل در امضای DKIM و ... آگاه خواهد شد.

شماره الزام	نام الزام
۸۴	الزامات مکانیزم DMARK (۱) (FCS_DMARK_EXT.1.1)
سرویس‌دهنده ایمیل باید مکانیزم DMARK را مطابق با RFC 7489 پیاده‌سازی کند.	
۸۵	الزامات مکانیزم DMARK (۲) (FCS_DMARK_EXT.1.2)
با ثبت رکوردهای DMARK DNS TXT در سرور DNS، سرویس‌دهنده ایمیل باید نحوه رفتار با ایمیل‌های ارسالی از جانب او و نیز ارسال گزارش‌های آماری به خود را تعیین کند.	
۸۶	الزامات مکانیزم DMARK (۳) (FCS_DMARK_EXT.1.3)
برای فیلدهای p و aspf از رکوردهای DMARK، سرویس‌دهنده مجاز به استفاده از تمامی مقادیر موجود است (none, quarantine و reject برای p و s و r برای aspf). اما برای فیلد adkim تنها حالت s که ملزم به چک کردن امضای DKIM می‌کند مجاز است.	
۸۷	الزامات مکانیزم DMARK (۴) (FCS_DMARK_EXT.1.4)
برای دریافت گزارش‌های DMARK، سرویس‌دهنده می‌تواند از آدرس مستقیم خود یا یک سرور third-party استفاده کند. نکات کاربردی: ✓ استفاده از یک سرور دیگر برای دریافت گزارش‌ها ازاین‌جهت مجاز است که می‌تواند از بار کاری سرویس‌دهنده ایمیل کاسته و بدین‌وسیله سرویس‌دهنده یک سرور اختصاصی برای دریافت و تحلیل گزارش‌های مربوطه در نظر بگیرد.	

۸۸	الزامات مکانیزم DMARK (۵) (FCS_DMARK_EXT.1.5)
در جایگاه دریافت‌کننده ایمیل، رفتار سرویس‌دهنده ایمیل با ایمیل‌های ناسالم (عدم تائید امضای DKIM یا دارای آدرس فرستنده خارج از لیست SPF) باید مطابق با قواعد DMARK ثبت‌شده توسط سرور فرستنده باشد. در صورت نبود رکورد DMARK، مختار به دور ریزی یا تحویل این ایمیل‌ها با مهر spam است.	
۸۹	الزامات مکانیزم DMARK (۶) (FCS_DMARK_EXT.1.6)
سرویس‌دهنده ایمیل باید از پروتکل DNSSEC برای ارتباط با سرویس‌دهنده DNS جهت قرار دادن رکورد DMARK خود یا بررسی رکورد دیگر سرویس‌دهنده‌ها استفاده کند.	

۱۴-۵- الزامات پروتکل S/MIME

کارکرد پروتکل S/MIME بر روی مؤلفه‌های MUA و جهت تأمین امنیت محتوای ایمیل‌ها به‌صورت انتها-به-انتها یعنی جعبه ایمیل-به-جعبه ایمیل است. مبنای کاری این پروتکل در استفاده از امضای دیجیتال و رمزنگاری نامتقارن برای تأمین احراز هویت، عدم انکار مبدأ[۱]، صحت داده و محرمانگی محتوای ایمیل‌ها (و نه سرآیند ایمیل) است.

از آنجایی‌که توصیه اکید NIST در حال حاضر در استفاده از S/MIME با استفاده از یک گواهینامه امضاشده توسط یک CA معتبر است لذا در این سند به الزامات OpenPGP اشاره‌ای نشده و این پروتکل (OpenPGP) جز الزامات نخواهد بود.

شماره الزام	نام الزام
۹۰	الزامات پروتکل S/MIME (۱) (FCS_S/MIME_EXT.1.1)

[۱] Non-repudiation

سرویس‌دهنده ایمیل باید پروتکل S/MIME را مطابق با RFC 8551 و مجموعه رمز زیر پیاده‌سازی کند:

۱. برای الگوریتم امضای دیجیتال:

با پشتیانی از (ECDSA با منحنی P-256 و SHA-256)، (EdDSA با منحنی 25519 و با استفاده از مد PureEdDSA)، (RSA PKCS #1 v1.5 با SHA-256) و [انتخاب: RSASSA-PSS، هیچ الگوریتم دیگری]

۲. رمزنگاری محتوا:

با پشتیبانی از AES-128 and 256 GCM، AES-128 CBC و [انتخاب: ChaCha20-Poly1305، هیچ الگوریتم دیگری]

۳. مدیریت و استقرار کلید:

ECDH با مد ephemeral-static برای P-256، ECDH با مد ephemeral-static برای x25519 با استفاده از HKDF-256 برای KDF، RSA و [انتخاب: RSAES-OAEP، هیچ الگوریتم دیگری]

۴. تولید چکیده پیغام:

SHA-256، SHA-512

۹۱	الزامات پروتکل S/MIME (۲) (FCS_S/MIME_EXT.1.2)

سرویس‌دهنده ایمیل باید مکانیزمی امن برای تولید و دسترس‌پذیری گواهینامه‌های X.509 کاربران ایمیل (email client) فراهم کند.

نکات کاربردی:

- ✓ برای توزیع و دسترس‌پذیری گواهینامه‌ها می‌توان از سرورهای LDAP استفاده کرد، به‌طوری‌که به‌عنوان‌مثال در زمان ارسال ایمیل توسط کاربر۱ به کاربر۲، کاربر ۱ بتواند

گواهینامه‌ی کاربر ۲ را از سرور مربوطه بازیابی کرده و با استفاده از آن رمزنگاری محتوا را انجام دهد. ✓ توصیه می‌شود تا گواهینامه‌ها حداقل توسط یک CA معتبر امضا شوند و اعتبار سنجی گواهینامه‌ها با استفاده از متدولوژی PKIX انجام گیرد.	
الزامات پروتکل S/MIME (۳) (FCS_S/MIME_EXT.1.3)	۹۲
سرویس‌دهنده ایمیل باید پروتکل S/MIME را با استفاده از پروتکل DANE و مکانیزم SMIMEA برای فرایند دسترس‌پذیری و تائید اصالت گواهینامه‌ها پیاده‌سازی کند. نکات کاربردی: ✓ یک مانع بزرگ در راه توسعه‌ی S/MIME نیاز به گواهینامه‌ی گیرنده برای انجام رمزنگاری و ارسال ایمیل به اوست. در حالتی که توسعه S/MIME تنها محدود به کاربران داخلی سرویس‌دهنده ایمیل باشد، این دسترسی به‌طور مثال با استفاده از سرورهای LDAP (الزام قبل) قابل فراهم کردن است. اما زمانی که مبنا ارسال ایمیل از یک سرویس‌دهنده به یک سرویس‌دهنده دیگر باشد این راهکار پاسخگو نیست. این محدودیت با توسعه DANE برای S/MIME حل‌شده و رکوردهای SMIMEA علاوه بر امکان اعتبار سنجی، امکان فراهم کردن گواهینامه‌های X.509 کاربران را نیز ممکن می‌کنند.	
الزامات پروتکل S/MIME (۴) (FCS_S/MIME_EXT.1.4)	۹۳
ایمیل‌ها پیش از ذخیره در جعبه ایمیل هر کاربر باید از حالت رمز شده خارج شوند. نکات کاربردی: ✓ اهمیت این الزام از آنجایی است که با هربار دسترسی کاربر به هر ایمیل موجود در جعبه ایمیل نیاز به رمزگشایی مجدد با کلید خصوصی کاربر نباشد. این مسئله برای در دسترس نبودن دائمی کلید خصوصی و افزایش امنیت در نگهداری از آن اهمیت دارد. ✓ توصیه می‌شود تا برای تأمین امنیت ایمیل‌ها در جعبه ایمیل از روش‌هایی چون رمزنگاری دیسک استفاده گردد. اما درصورتی‌که نگهداری از آن‌ها به‌صورت رمزشده ضروری باشد، بهتر است تا ایمیل‌ها با استفاده از کلیدهای موقتی مبتنی بر نشست و ایمیل محور رمز شده و	

نگهداری شوند.

۱۵-۵- الزامات پروتکل DANE

پروتکل DANE مکانیزمی امن و مطمئن برای ذخیره و دسترس‌پذیری کلیدهای عمومی PGP و گواهینامه‌های TLS و S/MIME فراهم می‌کند. همچنین در صورت عدم پشتیبانی یک سرویس‌دهنده‌ی ایمیل از TLS، سرویس‌دهنده‌ی مقابل می‌تواند با استفاده از ایده‌ی جستجو برای وجود رکورد DANE از این موضوع مطمئن شود و بدین‌وسیله از حمله‌ی تنزل به SMTP یا POP/IMAP ساده جلوگیری شود.

شماره الزام	نام الزام
۹۴	الزامات پروتکل DANE (۱) (FCS_DANE_EXT.1.1)
سرویس‌دهنده ایمیل باید پروتکل DANE را بر اساس RFC 7671 برای TLS (مورداستفاده در SMTP، POP و IMAP) پیاده‌سازی کرده و قادر به ثبت و خوانش رکوردهای TLSA باشد.	
۹۵	الزامات پروتکل DANE (۲) (FCS_DANE_EXT.1.2)
مطابق با RFC 7672، در زمان استفاده از DANE برای اتصالات SMTP به‌صورت MTA-to-MTA نباید از گزینه PKIX-TA و PKIX-EE در فیلد Certificate Usage از رکوردهای TLSA استفاده کرد. نکات کاربردی: ✓ اعمال این محدودیت دلایل امنیتی-کارکردی دارد که در بخش ۳,۱,۳ از RFC شرح داده‌شده است. ✓ توصیه می‌شود تا از هر دو نوع رکورد DANE-TA و DANE-EE برای افزایش امنیت استفاده شود. همچنین برای فیلد Selector و Matching Type نیز به ترتیب SPKI و SHA-256 توصیه می‌شود که برای هر سه فیلد معادل با "1 1 2" و "1 1 3" خواهد بود.	
۹۶	الزامات پروتکل DANE (۳) (FCS_DANE_EXT.1.3)
سرویس‌دهنده ایمیل باید از مقادیر ۰، ۱، [انتخاب: ۲، هیچ گزینه دیگری] برای فیلد Matching از	

رکوردهای TLSA پشتیبانی کند. نکات کاربردی: پشتیبانی از SHA2-512 (مقدار ۲) اختیاری است.	
۹۷	الزامات پروتکل DANE (۴) (FCS_DANE_EXT.1.4)
سرویس‌دهنده ایمیل باید پروتکل DANE را بر اساس RFC 8162 برای S/MIME پیاده‌سازی کند و قادر به ثبت و خوانش رکوردهای DNS SMIMEA Resource Record باشد. نکات کاربردی: ✓ استفاده و کارکرد DNS و پروتکل DANE برای S/MIME مشابه با کارکرد ذکرشده برای TLS جهت افزایش امنیت در احراز اصالت کلیدهای عمومی و گواهینامه‌های x509 است و رکوردهای SMIMEA Resource Record نیز ساختار مشابهی دارند. ✓ قابل‌ذکر است که در خصوص S/MIME استفاده از هر چهار مقدار ۰، ۱، ۲ و ۳ برای فیلد Certificate Usage مجاز است.	
۹۸	الزامات پروتکل DANE (۵) (FCS_DANE_EXT.1.5)
هر گروه اتصال با سرور DNS برای ثبت و خوانش رکوردهای DANE باید با استفاده از پروتکل DNSSEC باشد.	
۹۹	الزامات پروتکل DANE (۶) (FCS_DANE_EXT.1.6)
مطابق با سند مرجع NIST [3] برای معماری امن یک سرویس‌دهنده ایمیل و با توجه به عدم پشتیبانی از DANE توسط برخی از سرویس‌دهنده‌های ایمیل، سرویس‌دهنده ایمیل باید از مکانیزم جایگزین MTA-STS مطابق با RFC 8461 نیز علاوه بر DANE پشتیبانی کند.	

۱۶-۵- الزامات پروتکل HTTPS

سرویس‌دهنده ایمیل باید با استفاده از اتصال HTTPS دسترسی تحت وب کاربران به سرویس ایمیل را امن کند. HTTPS برای تشکیل کانال امن هم کاربرد دارد که در بخش کانال امن به آن اشاره‌شده است.

شماره الزام	نام الزام
۱۰۰	الزامات پروتکل HTTPS (۱) (FCS_HTTPS_EXT.1.1)
سرویس‌دهنده ایمیل باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند. نکته کاربردی: ✓ نویسنده سند هدف امنیتی باید اطلاعات کافی را فراهم آورد و مشخص کند که پیاده‌سازی این پروتکل مطابق استانداردهای تعریف‌شده است.	
۱۰۱	الزامات پروتکل HTTPS (۲) (FCS_HTTPS_EXT.1.2)
سرویس‌دهنده ایمیل باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	
۱۰۲	الزامات پروتکل HTTPS (۳) (FCS_HTTPS_EXT.1.3)
درصورتی‌که گواهینامه همتا ارائه‌شده باشد و نامعتبر باشد، سرویس‌دهنده ایمیل باید [انتخاب: اتصال را برقرار نکند، برای برقراری اتصال درخواست مجوز کند، هیچ اقدام دیگری انجام ندهد.] نکته کاربردی: ✓اعتبارسنجی گواهینامه از طریق بررسی و تأیید فیلدهای شناسه گواهینامه، مسیر گواهینامه[۱]، تاریخ انقضاء و وضعیت ابطال[۲] آن مطابق با RFC 5280 تعیین می‌گردد. همچنین نحوه اعتبارسنجی گواهینامه بر اساس قواعد تعریف‌شده در الزام FIA_X509_EXT.1/Rev انجام می‌شود.	

[۱] Certificate path

[۲] Revocation status

فصل ۶– الزامات تضمین امنیت (ASE_REQ_SAR)

الزامات موجود در این بخش عملاً فصل‌ها و بخش‌های موردنیاز در سند «هدف امنیتی» را شرح می‌دهند. همچنان که پیش‌تر نیز گفته‌شده است، یکی از اسناد مهم همراه با محصول، سند «هدف امنیتی» است که به شرح محصول و چگونگی پیاده‌سازی الزامات ذکرشده در این پروفایل حفاظتی می‌پردازد و باید دست‌کم شامل فصل‌هایی مطابق با الزامات زیر باشد.

شماره الزام	الزام	شرح الزام
(۱)	ادعای التزام به پروفایل(های) حفاظتی (ASE_CCL.1)	مطابق با این الزام باید لیست و ورژن پروفایل(های) حفاظتی که سرویس‌دهنده‌ی ایمیل ادعای التزام و پیاده‌سازی آن‌ها را دارد، ذکر شود.
(۲)	تعریف مؤلفه‌های توسعه‌یافته (ASE_ECD.1)	درصورتی‌که علاوه بر الزامات ذکرشده در این پروفایل حفاظتی، الزامات بیشتری نیز بنا به قابلیت‌های سرویس‌دهنده‌ی ایمیل قابل‌بیان بوده و در آن نیز پیاده‌سازی شده باشد، می‌توان آن‌ها را به‌صورت الزامات توسعه‌یافته در بخش «الزامات امنیتی تبیین شده» از سند هدف امنیتی بیان کرد. اما باید در نظر داشت که این الزامات باید با خانواده مربوطه که توسعه داده می‌شود همخوانی داشته و مطابق با استانداردهای معیار مشترک در تعریف الزامات کارکردی-امنیتی باشند. مؤلفه‌های توسعه‌یافته باید شامل المان‌های هدفمند و قابل‌اندازه‌گیری باشد، طوری که انطباق و عدم انطباق با این المان‌ها، قابل‌اثبات باشد (این بخش اختیاری بوده و جهت جلوگیری از مشکلات احتمالی در تعریف این الزامات، پیاده‌سازی آن توصیه نمی‌شود).
(۳)	معرفی سرویس‌دهنده‌ی ایمیل	مطابق با این الزام م باید سرویس‌دهنده‌ی ایمیل معرفی و مؤلفه‌ها و اجزای مختلف آن به همراه ویژگی‌ها، قابلیت‌ها

	(ASE_INT.1)	و محدودیت‌هایش شرح داده شوند. معرفی محصول باید نحوه استفاده و ویژگی‌های اصلی آن را بیان کند. این معرفی باید حوزه فیزیکی و منطقی کارکرد سرویس‌دهنده‌ی ایمیل را توصیف کند.
(۴)	اهداف امنیتی برای محیط عملیاتی (ASE_OBJ.1)	مطابق با این الزام، اهداف امنیتی در نظر گرفته‌شده برای محیط عملیاتی بیان شوند (به اهداف امنیتی ذکرشده در این سند رجوع شود).
(۵)	تعریف مشکلات و تهدیدات امنیتی (ASE_SPD.1)	مطابق با این الزام، تهدیدات امنیتی موجود باید بیان شوند (به تهدیدات امنیتی ذکرشده در این سند رجوع شود).
(۶)	الزامات امنیتی تبیین شده (ASE_REQ.1)	مطابق با این سند مجموعه‌ای از الزامات برای سرویس‌دهنده‌ی ایمیل ذکرشده است که برخی اجباری، برخی اختیاری و برخی وابسته به انتخاب انجام‌گرفته در الزامات دیگر بودند. لازم است تا در سند «هدف امنیتی» کلیه الزامات رعایت شده، مطابق با این سند شرح داده شوند.
(۷)	خلاصه مشخصات محصول (ASE_TSS.1)	لازم است تا سرویس‌دهنده‌ی ایمیل با جزئیات کامل به تشریح چگونگی پیاده‌سازی الزامات ذکرشده بپردازد.

اقدامات ارزیاب

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

هدف امنیت (ASE)	مؤلفه: (ASE_CCL.1E) شرح مؤلفه: ارزیاب باید تأیید کند که توضیحات ارائه‌شده و مشخصات پروفایل‌های حفاظتی ذکرشده، کامل می‌باشند و پروفایل‌ها وجود خارجی دارند.
	مؤلفه: (ASE_ECD.1E) شرح مؤلفه: ارزیاب باید تأیید کند که هیچ مؤلفه توسعه‌یافته‌ای به‌وسیله مؤلفه‌های موجود به صورت شفاف قابل‌بیان نیست و تعریف مؤلفه توسعه‌یافته صحیح انجام‌شده است.
	مؤلفه: (ASE_INT.1E) شرح مؤلفه: ارزیاب باید تأیید کند که اطلاعات موردنیاز برای بخش معرفی محصول کامل بوده و زیربخش‌های آن با یکدیگر سازگار هستند.
	مؤلفه: (ASE_OBJ.1E) شرح مؤلفه: ارزیاب باید تأیید کند که اطلاعات ارائه‌شده برای اهداف امنیتی کامل است.
	مؤلفه: (ASE_SPD.1E) شرح مؤلفه: ارزیاب باید تأیید کند که لیست و شرح ارائه‌شده برای تهدیدات امنیتی کامل است.
	شماره مؤلفه: (ASE_REQ.1E) شرح مؤلفه: ارزیاب باید تأیید کند که لیست و شرح ارائه‌شده برای الزامات کامل است و هیچ الزام اجباری یا انتخابی مربوطه‌ای نادیده گرفته نشده است.
	شماره مؤلفه: (ASE_TSS.1E)

	شرح مؤلفه: ارزیاب باید تأیید کند اطلاعات ارائه‌شده برای خلاصه مشخصات سرویس‌دهنده‌ی ایمیل تمامی الزامات ذکرشده را پیاده‌سازی کرده و از جامعیت و شفافیت کامل در شرح مکانیزم برخوردار است.

۱-۶- کلاس توسعه

شماره الزام	الزام	شرح الزام
(۸)	شرح پایه‌ای از مشخصات کارکردی محصول (ADV_FSP.1)	مطابق با این الزام باید واسط‌ها و اینترفیس‌های تعریف‌شده برای پیاده‌سازی توابع و کارکردهای امنیتی موردنیاز به‌طور مختصر تشریح شوند. پارامترهای مرتبط با هر اینترفیس باید بیان شود. ارتباط هر اینترفیس با کارکرد(های) امنیتی مربوطه باید بیان شود. نیاز به تشریح جامعی از این اینترفیس‌ها نبوده و بیشتر منظور اینترفیس‌هایی است که سرپرست با آن‌ها سروکار دارد و برای باقی اینترفیس‌ها (مانند اینترفیس‌های متصل به محیط عملیاتی) یک شرح مختصر کافی است. نیاز به سند جداگانه‌ای برای این الزام نبوده و توضیحات موردنیاز را می‌توان در مستندات راهنما و بخش خلاصه مشخصات سرویس‌دهنده‌ی ایمیل از سند هدف امنیتی گنجاند.

اقدامات ارزیاب

شرح پایه‌ای از مشخصات کارکردی محصول (ADV_FSP)	مؤلفه: (ADV_FSP.1.1E) شرح مؤلفه: ارزیاب باید تأیید کند که اطلاعات ارائه‌شده تمام موارد خواسته‌شده را برآورده می‌کند.
	مؤلفه: (ADV_FSP.1.2E) شرح مؤلفه: ارزیاب باید مشخص کند که اینترفیس‌های تعریف‌شده نمونه کامل و دقیقی از کارکردهای امنیتی موردنیاز را فراهم می‌کنند.

۲-۶- کلاس اسناد راهنما

مستند(ات) راهنما همراه با سند هدف امنیتی ارائه خواهند شد. این اسناد باید مشخص کنند که هر نوع سرپرست در سرویس‌دهنده ایمیل چگونه می‌تواند از آن استفاده کرده و وظایف خود را انجام دهد. به‌عبارت‌دیگر چگونه می‌تواند از امکانات امنیتی مربوط به نقش خود استفاده کند.

اگر محصول قابلیت پشتیبانی از محیط‌های عملیاتی مختلف با ویژگی‌های متفاوت را دارد، برای هر محیط عملیاتی باید یک راهنمای جداگانه ارائه شود.

هر سند راهنما باید شامل موارد زیر باشد:

- دستورالعمل نصب موفقیت‌آمیز سرویس‌دهنده‌ی ایمیل در محیط عملیاتی
- دستورالعمل‌های لازم برای مدیریت امنیت آن به‌عنوان یک سرویس‌دهنده ایمیل تنها یا به‌عنوان بخشی از یک محیط عملیاتی بزرگ‌تر
- دستورالعمل‌ها و توصیه‌های مفید در اتخاذ استراتژی‌های امنیتی در شرایط مختلف با توجه به امکانات سرویس‌دهنده ایمیل
- دستورالعمل‌های مربوطه برای استفاده از هر یک از توابع و کارکردهای امنیتی

شماره الزام	الزام	شرح الزام

(۹)	راهنمای کاربر عملیاتی (AGD_OPE.1)	این سند باید همراه با محصول ارائه شود و یا محتوای مورد نیاز آن در اسناد دیگر گنجانده شود و یا به‌صورت آنلاین در اینترنت در دسترس باشد. این سند باید برای هر نوع نقش سرپرست، کارکردها و واسط‌های در دسترس، به‌خصوص تمام پارامترهای امنیتی تحت کنترل را توصیف و مقادیر امن را توصیه کند. باید برای هر نقش، رویدادهای امنیتی به کارکردهای در دسترس و قابل انجام توسط سرپرست مرتبط شوند. سند راهنمای کاربرد عملیاتی باید تمام مدهای عملیاتی سرویس‌دهنده‌ی ایمیل (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آن‌ها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نماید. این سند باید برای هر نوع نقش سرپرست، معیارهای امنیتی را که توسط سرپرست تبعیت شوند، توصیف کند تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده‌شده‌اند، کاملاً اجرا گردند.
(۱۰)	راهنمای آماده‌سازی (AGD_PRE.1)	این سند باید همراه با سرویس‌دهنده ایمیل ارائه شود. مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن سرویس‌دهنده ایمیل و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی در نظر گرفته‌شده برای محیط عملیاتی که در سند هدف امنیتی ذکرشده‌اند، شرح دهند.

اقدامات ارزیاب	
اسناد راهنما (AGD)	مؤلفه: (AGD_OPE.1.1E) شرح مؤلفه: ارزیاب باید تأیید کند که اطلاعات ارائه‌شده در سند راهنمای کاربرد عملیاتی تمام محتوای موردنیاز و ذکرشده در الزام را برآورده می‌کند.
	مؤلفه: (AGD_PRE.1.1E) شرح مؤلفه: ارزیاب باید تأیید کند که اطلاعات ارائه‌شده در سند راهنمای آماده‌سازی تمام محتوای موردنیاز و ذکرشده در الزام را برآورده می‌کند.
	مؤلفه: (AGD_PRE.1.2E) شرح مؤلفه: ارزیاب باید رویه‌های آماده‌سازی شرح داده‌شده در سند را بکار ببرد تا تأیید کند که سرویس‌دهنده‌ی ایمیل می‌تواند به‌صورت امن برای عمل کردن آماده شود.

۳-۶- کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که در این پروفایل حفاظتی ارائه‌شده است (EAL1)، کلاس پشتیبانی از چرخه حیات به ویژگی‌هایی از چرخه حیات محدود می‌گردد که توسط سرپرست قابل‌مشاهده باشد. این به آن معنی نیست که نحوه عمل توسعه‌دهنده نقش کمرنگی در قابل‌اعتماد بودن سرویس‌دهنده‌ی ایمیل دارد، بلکه در این سطح اطمینان تنها به این اطلاعات نیاز است.

شماره الزام	الزام	شرح الزام
(۱۱)	برچسب‌گذاری محصول CMC.1_ALC	توسعه‌دهنده باید سرویس‌دهنده‌ی ایمیل و مرجع آن را ارائه کند. به‌عبارتی‌دیگر محصول باید با یک مرجع یکتا برچسب زده شود. این برچسب می‌تواند یک برچسب کاغذی، نرم‌افزاری و یا حک‌شده باشد که آن را به‌صورت یک محصول یکتا در میان محصولات شرکت مربوطه معرفی می‌کند.

(۱۲)	پوشش پیکربندی محصول CMS.1_ALC	توسعه‌دهنده باید لیست موارد قابل پیکربندی سرویس‌دهنده ایمیل را در اسناد راهنما ارائه کند. لیست پیکربندی باید موارد قابل پیکربندی را به‌صورت یکتا معرفی کند.

اقدامات ارزیاب	
پشتیبانی از چرخه حیات(ALC)	مؤلفه: (ALC_CMC.1.1E) شرح مؤلفه: ارزیاب باید تأیید کند که محصول برچسب یکتا دارد.
	مؤلفه: (ALC_CMS.1.1E) شرح مؤلفه: ارزیاب باید تأیید کند که اطلاعات ارائه‌شده تمام محتوای موردنیاز را برآورده می‌کند.

۴-۶- کلاس آزمون

آزمون سرویس‌دهنده‌ی ایمیل توسط ارزیاب و برای بررسی و تست کارکردهای سیستم و همچنین تست وجود حفره‌های امنیتی که در محصولات مشابه شناسایی‌شده است، در نظر گرفته‌شده است. آزمون کارکردهای سیستم از طریق خانواده ATE_IND و آزمون نوع دوم نیز از طریق خانواده AVA_VAN صورت می‌گیرد که این مورد در ادامه شرح داده‌شده است. در این سطح از ارزیابی (سطح EAL1)، آزمون بر اساس کارکردهایی که برای سرویس‌دهنده ایمیل در نظر گرفته‌شده و واسط‌هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌شود. نتایج آزمون و تحلیل آسیب‌پذیری باید توسط ارزیاب در گزارش آزمون لحاظ شوند.

آزمون مستقل-انطباق: «آزمون مستقل-انطباق» برای تأیید کارکردهای سرویس‌دهنده ایمیل که در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی و مستندات «راهنما» ارائه‌شده، صورت

می‌گیرد. هدف اصلی از انجام آزمون، اطمینان از برآورده شدن الزامات کارکردی-امنیتی مشخص‌شده در سند هدف امنیتی است. ارزیاب باید در سند «گزارش آزمون»، طرح آزمون و نتایج آن را مستند کند.

شماره الزام	الزام	شرح الزام
(۱۳)	ATE_IND.1	توسعه‌دهنده باید محصول را برای آزمودن ارائه کند و محصول باید مناسب برای آزمون باشد.
اقدامات ارزیاب		
آزمون مستقل (ATE_IND)	مؤلفه: (ATE_IND.1.1E) شرح مؤلفه: ارزیاب باید تأیید کند که با توجه به اسناد و محتوای ارائه‌شده، محصول برای ارزیابی مناسب است یا نیست.	
	مؤلفه: (ATE_IND.1.2E) شرح مؤلفه: ارزیاب باید زیرمجموعه‌ای از توابع امنیتی سرویس‌دهنده‌ی ایمیل را تست کند تا تأیید شود که توابع امنیتی به‌صورت مشخص‌شده عمل می‌کنند.	

۵-۶- کلاس ارزیابی آسیب‌پذیری

این کلاس به شناسایی آسیب‌پذیری‌های قابل بهره‌برداری که در سرویس‌دهنده ایمیل ممکن است وجود داشته باشد، می‌پردازد.

شماره الزام	الزام	شرح الزام
(۱۴)	AVA_VAN.1	توسعه‌دهنده باید محصول را برای ارزیابی آسیب‌پذیری ارائه کند و محصول باید مناسب برای آزمون باشد.
اقدامات ارزیاب		

آسیب‌پذیری (AVA_VAN)	مؤلفه: (AVA_VAN.1.1E) شرح مؤلفه: ارزیاب باید تأیید کند که با توجه به اسناد و محتوای ارائه‌شده، محصول برای ارزیابی آسیب‌پذیری مناسب است یا نیست.
	مؤلفه: (AVA_VAN.1.2E) شرح مؤلفه: ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه و شناخته‌شده در سرویس‌دهنده‌ی ایمیل، در منابع عمومی جستجو انجام دهد.
	شماره مؤلفه: (AVA_VAN.1.3E) شرح مؤلفه: ارزیاب باید بر اساس آسیب‌پذیری‌های بالقوه شناسایی‌شده، آزمون نفوذ انجام دهد تا مقاومت سرویس‌دهنده‌ی ایمیل را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص کند.

فصل ۷- پیوست یک: الزامات اختیاری

این پیوست از الزاماتی تشکیل‌شده است که می‌توان آن‌ها را در هدف امنیتی گنجاند، اما برای انطباق با این پروفایل حفاظتی ضروری نیستند. اگر سرویس‌دهنده ایمیل هرکدام از این الزامات اختیاری را پشتیبانی می‌کند، توصیه می‌شود که قابلیت‌های کارکردی مرتبط به سند هدف امنیتی اضافه شود. نویسندگان سند هدف امنیتی آزاد هستند که هیچ، برخی یا تمامی الزامات مطرح‌شده در این بخش را انتخاب کنند.

۱-۷- کلاس ثبت رکوردهای ممیزی از الزامات اختیاری

مشابه با بخش الزامات اجباری در فصل ۵، جدول زیر لیست رویدادهای قابل ممیزی برای الزامات اختیاری را به تفکیک الزام و نیز اطلاعات اضافی موردنیاز برای هر رویداد را نشان می‌دهد. برای هرکدام از الزامات اختیاری که پیاده‌سازی شود باید حداقل اطلاعات ذکرشده در **جدول ۱-۶** برای آن الزام به‌صورت رکورد ممیزی ثبت شود.

جدول ۱-۶ لیست رویدادهای قابل ممیزی به تفکیک کارکردهای امنیتی اختیاری

کارکرد امنیتی مورد نیاز	رویداد قابل ممیزی	اطلاعات اضافی مورد نیاز
FAU_STG.1	×	×
FAU_STG_EXT.2/LocSpace	×	×
FAU_STG.3/LocSpace	اخطار کم بودن فضای ذخیره‌سازی برای رویدادهای قابل ممیزی	×
FCS_DTLSC_EXT.2 (DTLS Client با احراز هویت)	شکست در ایجاد یک نشست DTLS	دلیل شکست
	تشخیص حملات replay attack	هویت منبع حمله کننده (مثال: آدرس IP)
FCS_DTLSS_EXT.2	شکست در ایجاد یک نشست	دلیل شکست

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

کارکرد امنیتی مورد نیاز	رویداد قابل ممیزی	اطلاعات اضافی مورد نیاز
DTLS Server) با احراز هویت)	DTLS	
	تشخیص حملات replay attack	هویت منبع حمله‌کننده (مثال: آدرس IP)
FMT_MOF.1/Services	شروع و توقف هر سرویس	×
FMT_MTD.1/CryptoKeys	رویداد مدیریت کلیدهای رمزنگاری	×

در ادامه الزامات اختیاری مختص به کلاس ثبت رکوردهای ممیزی بیان‌شده است.

شماره الزام	نام الزام
۱	محافظت از داده‌های ممیزی ذخیره‌شده ۱ (FAU_STG.1.1)
سرویس‌دهنده ایمیل باید از پاک شدن غیرمجاز داده‌های ممیزی جلوگیری کند.	
۲	محافظت از داده‌های ممیزی ذخیره‌شده ۲ (FAU_STG.1.2)
سرویس‌دهنده ایمیل باید از دست‌کاری غیرمجاز داده‌های ممیزی جلوگیری کند.	
۳	شمارش رکوردهای ازدست‌رفته در فضای ذخیره‌سازی محلی (FAU_STG_EXT.2/LocSpace)
سرویس‌دهنده ایمیل در صورت پر شدن حافظه محلی، باید اطلاعات مربوط به تعداد رکوردهای ممیزی [انتخاب: ازدست‌رفته، بازنویسی شده، [اختصاص: سایر اطلاعات]] را ارائه کند.	
۴	اقدام در صورت از دست رفتن رکوردهای ممیزی روی حافظه محلی (FAU_STG_EXT.3.1/LocSpace)

درصورتی‌که حجم داده‌های ممیزی از ظرفیت ذخیره‌سازی محلی داده‌های ممیزی فراتر رود/سرریز کند، سرویس‌دهنده ایمیل باید با تولید اخطار، سرپرست را آگاه کند.

۲-۷- کلاس پشتیبانی از رمزنگاری

با توجه به اینکه پروتکل DTLS از احراز هویت دوطرفه پشتیبانی نمی‌کند، لذا پشتیبانی از این ویژگی به‌عنوان یک انتخاب اختیاری در نظر گرفته‌شده است که الزامات آن در این قسمت شرح داده‌شده است. درصورتی‌که این پروتکل انتخاب‌شده باشد، برای پشتیبانی از احراز هویت دوطرفه این قسمت باید رعایت شود.

با توجه به کارکرد این پروتکل به‌صورت client/server، الزامات مربوطه نیز برای هر یک از دو نقش DTLS server و DTLS client جداگانه بیان‌شده است که هریک از دو طرف سرویس‌دهنده ایمیل و موجودیت دوم مانند سرور خارجی رکوردهای ممیزی می‌توانند نقش کاربر DTLS یا سرور DTLS را بگیرند.

شماره الزام	نام الزام
۵	احراز هویت دوطرفه DTLS client (۱) (FCS_DTLSC_EXT.2.1)
DTLS client باید قادر به پشتیبانی از احراز هویت دوطرفه‌ی DTLS server بر مبنای گواهینامه‌های X.509v3 باشد.	
۶	احراز هویت دوطرفه DTLS client (۲) (FCS_DTLSC_EXT.2.2)
درصورتی‌که هر پیام دریافت شده از سمت DTLS server دارای مقدار MAC نادرست باشد، DTLS client باید [انتخاب: نشست را خاتمه دهد، به‌صورت خاموش پیام را نادیده بگیرد] نکات کاربردی: ✓ منظور از خاموش یعنی کنار گذاشتن بسته بدون فیدبک دادن یا ارسال Ack.	
۷	احراز هویت دوطرفه DTLS client (۳) (FCS_DTLSC_EXT.2.3)
DTLS client باید پیام‌های باز ارسال‌شده (مربوط به replay attack) برای:	

۱. رکوردهای DTLS که قبلاً دریافت شده‌اند (یعنی شماره ترتیب آن تکراری هست). ۲. رکوردهای DTLS بسیار قدیمی که شماره ترتیب آن‌ها در sliding receive window قرار نمی‌گیرد. را به‌صورت خاموش نادیده بگیرد. نکات کاربردی: ✓حمله replay attack در RFC 6347 برای DTLS 1.2 و RFC 4347 برای DTLS 1.0 شرح داده‌شده است.
۸ | احراز هویت دوطرفه DTLS server (۱) (FCS_DTLSS_EXT.2.1)
DTLS server باید از احراز هویت دوطرفه DTLS client بر مبنای گواهینامه‌های X.509v3 پشتیبانی کند.
۹ | احراز هویت دوطرفه DTLS server (۲) (FCS_DTLSS_EXT.2.2)
به هنگام برقراری کانال امن، DTLS server بدون تأیید گواهینامه client نباید با آن تشکیل کانال دهد. در صورت غیر معتبر بودن گواهینامه، DTLS server در ادامه همچنین باید [انتخاب: هیچ کار دیگری نکند، درخواست مجوز برای تشکیل کانال بدهد].
۱۰ | احراز هویت دوطرفه DTLS server (۳) (FCS_DTLSS_EXT.2.3)
بدون تأیید اینکه Distinguished Name (DN) و Subject Alternative Name (SAN) موجود در گواهینامه با شناسه‌های مورد انتظار برای DTLS client تطابق ندارند، DTLS server نباید با client کانال امن تشکیل دهد.

۳-۷- کلاس مدیریت امنیت

شماره الزام	نام الزام
۱۱	مدیریت کارکرد امنیتی ۱/سرویس‌ها (FMT_MOF.1/Services)
سرویس‌دهنده ایمیل باید امکان فعال/غیرفعال کردن توابع و سرویس‌ها را به سرپرستان امنیتی محدود کند.	
۱۲	مدیریت دسترسی به داده‌ها ۱/کلیدهای رمزنگاری (FMT_MTD.1/CryptoKeys)
سرویس‌دهنده ایمیل باید توانایی مدیریت کردن کلیدهای رمزنگاری را به سرپرست امنیتی محدود کند. نکته کاربردی: ✓این گزینه زمانی باید انتخاب گردد که سرپرست امنیتی امکان مدیریت کلیدهای رمزنگاری (برای مثال: اصلاح، حذف، تولید/واردکردن) را داشته باشد. این الزام مدیریت کلیدهای رمزنگاری را به سرپرست‌های امنیتی محدود می‌کند.	

فصل ۸– پیوست دو: الزامات انتخابی

این پیوست به بیان الزامات مبتنی بر انتخاب می‌پردازد. پیاده‌سازی الزامات این بخش بسته به انتخاب‌های انجام‌شده در فصل ۵ است. به‌طور مثال در صورت انتخاب پروتکل IPSEC برای امن کردن کانال ارتباطی میان سرویس‌دهنده ایمیل و موجودیت‌های خارجی مانند سرور خارجی ذخیره رکوردهای ممیزی، باید الزامات مربوط به IPSEC از این بخش پیاده‌سازی شود.

۸–۱– کلاس ثبت رکوردهای ممیزی از الزامات اختیاری

مشابه با بخش الزامات اجباری در فصل ۵، جدول زیر لیست رویدادهای قابل ممیزی برای الزامات انتخابی را به تفکیک الزام و نیز اطلاعات اضافی موردنیاز برای هر رویداد را نشان می‌دهد. برای هرکدام از الزامات انتخابی که پیاده‌سازی شود باید حداقل اطلاعات ذکرشده در **جدول ۱-۷** برای آن الزام به‌صورت رکورد ممیزی ثبت شود.

جدول ۱-۷ لیست رویدادهای قابل ممیزی به تفکیک کارکردهای امنیتی انتخابی

کارکرد امنیتی	رویداد قابل ممیزی	اطلاعات اضافی مورد نیاز
FCS_DTLSC_EXT.1	شکست در ایجاد یک نشست DTLS	دلیل شکست
FCS_DTLSS_EXT.1	شکست در ایجاد یک نشست DTLS	دلیل شکست
	تشخیص حملات replay attack	هویت منبع حمله‌کننده (مثال: آدرس IP آن)
FCS_IPSEC_EXT.1	شکست در ایجاد یک نشست HTTPS	دلیل شکست
FCS_SSHC_EXT.1	شکست در ایجاد یک نشست SSH	دلیل شکست
FCS_SSHS_EXT.1	شکست در ایجاد یک نشست SSH	دلیل شکست
FPT_TST_EXT.2	شکست در خودآزمایی	دلیل شکست (شامل شناسه گواهینامه نامعتبر)

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

کارکرد امنیتی	رویداد قابل ممیزی	اطلاعات اضافی مورد نیاز
FPT_TUD_EXT.2	شکست در به‌روزرسانی	دلیل شکست (شامل شناسه گواهینامه نامعتبر)
FMT_MOF.1/AutoUpdate	فعال‌سازی و غیر فعال‌سازی جستجوی خودکار به‌روزرسانی‌ها یا به‌روزرسانی‌های خودکار	×
FMT_MOF.1/Functions	اصلاح یا تغییر رفتار، انتقال داده‌های ممیزی به یک موجودیت IT خارجی، کنترل داده ممیزی، کارکرد موردنظر وقتی‌که فضای محلی ذخیره‌سازی ممیزی پر می‌شود.	×

۲-۸- کلاس پشتیبانی از رمزنگاری

۱-۲-۸- الزامات پروتکل DTLS

پیش از بیان الزامات DTLS لازم است تا بار دیگر به لیست مجموعه‌های رمزنگاری قابل‌استفاده برای DTLS و TLS اشاره‌کنیم. این لیست در جدول ۱-۸ آورده شده و در خلال الزامات DTLS به آن مراجعه خواهیم کرد.

جدول ۱-۸ لیست مجموعه‌های رمزنگاری برای پروتکل‌های TLS و DTLS

TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268
TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268
TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492
TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246
TLS_RSA_WITH_AES_256_CBC_ SHA256 مطابق با RFC 5246
TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 مطابق با RFC 5246
TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 مطابق با RFC 5246
TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288
TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289

در ادامه الزامات پروتکل DTLS بیان‌شده است. قابل‌ذکر است که در نسخه جدید از پروفایل حفاظتی برای محصولات شبکه، پیاده‌سازی قابلیت احراز هویت دوطرفه در DTLS به‌عنوان یک الزام اختیاری در نظر گرفته‌شده است. لذا این روند در این پروفایل حفاظتی نیز رعایت شده و در این قسمت الزامات پروتکل بدون احراز هویت دوطرفه را بیان کرده‌ایم و در صورت تمایل به پیاده‌سازی احراز هویت دوطرفه باید الزامات اختیاری ذکرشده در آن بخش نیز علاوه بر الزامات این بخش رعایت شود.

قابل‌ذکر است که با توجه به کارکرد این پروتکل به فرم client/server، الزامات مربوطه نیز برای هر یک از دو نقش DTLS server یا DTLS client جداگانه بیان‌شده است که هریک از دو طرف سرویس‌دهنده ایمیل و موجودیت دوم مانند سرور خارجی رکوردهای ممیزی می‌توانند نقش کاربر DTLS یا سروردTLS را بگیرند.

شماره الزام	نام الزام
۱	الزامات پروتکل DTLS Client بدون احراز هویت دوطرفه (۱) (FCS_DTLSC_EXT.1.1)
DTLS client باید [انتخاب: DTLS 1.3 (RFC 9147)، DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی کند: [انتخاب: یکی از مجموعه‌های رمزنگاری لیست شده در لیست مجموعه‌های رمزنگاری برای پروتکل‌های TLS و DTLS]	

۲	الزامات پروتکل DTLS Client بدون احراز هویت دوطرفه (۲) (FCS_DTLSC_EXT.1.2)
DTLS client باید مطابقت شناسه[۱] ارائه‌شده با شناسه مرجع را با توجه به بخش 6 از RFC 6125، تأیید کند. نکات کاربردی: ✓قوانین مربوط به تأیید شناسه در بخش 6 از RFC 6125 توضیح داده‌شده‌اند.	
۳	الزامات پروتکل DTLS Client بدون احراز هویت دوطرفه (۳) (FCS_DTLSC_EXT.1.3)
DTLS client باید کانال امن را فقط در صورت معتبر بودن گواهینامه سرور برقرار سازد. اگر گواهینامه DTLS server نامعتبر به نظر رسید، DTLS client باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات.]].	
۴	الزامات پروتکل DTLS Client بدون احراز هویت دوطرفه (۴) (FCS_DTLSC_EXT.1.4)
DTLS client باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Extension Supported Elliptic Curves را به همراه NIST curveهای [انتخاب:secp521r1 ,secp384r1 ,secp256r1] و هیچ منحنی دیگری] در پیام Client Hello ارائه دهد. نکات کاربردی: ✓اگر در الزام «الزامات پروتکل DTLS Client بدون احراز هویت (۱) » مجموعه‌های رمز دارای منحنی‌های بیضوی انتخاب گردند، در این الزام باید یک یا چند مورد از منحنی‌ها انتخاب شود. اگر در الزام مربوطه هیچ‌کدام از مجموعه‌های رمز دارای منحنی‌های بیضوی	

[۱] Identifier

انتخاب نگردد، عبارت" Supported Elliptic Curves Extension را ارائه نکند" باید انتخاب شود. ✓این الزام مجموعه‌های رمز بیضوی مجاز برای احراز هویت و توافق کلید را به منحنی‌های NIST از الزام‌های FCS_COP.1/SigGen و FCS_CKM.1 و FCS_CKM.2 محدود می‌سازد. این افزونه برای کلاینت‌هایی که از مجموعه‌های رمز بیضوی پشتیبانی می‌کنند، الزامی است.	
۵	الزامات پروتکل DTLS Server بدون احراز هویت دوطرفه (۱) (FCS_DTLSS_EXT.1.1)
DTLS server باید [انتخاب: DTLS 1.3 (RFC 9147)، DTLS 1.2 (RFC 6347)، DTLS 1.0 (RFC 4347)] را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی کند: [انتخاب: یکی از مجموعه‌های رمزنگاری لیست شده در لیست مجموعه‌های رمزنگاری برای پروتکل‌های TLS و DTLS]	
۶	الزامات پروتکل DTLS Server بدون احراز هویت دوطرفه (۲) (FCS_DTLSS_EXT.1.2)
DTLS server نباید برای کلاینت‌هایی که درخواست هیچ دارند، ارتباطات را ایجاد کند.	
۷	الزامات پروتکل DTLS Server بدون احراز هویت دوطرفه (۳) (FCS_DTLSS_EXT.1.3)
DTLS server نباید در صورت شکست خوردن اعتبارسنجی DTLS client، تلاش دست‌تکانی ارتباط را پیش ببرد. نکته کاربردی: ✓ فرآیند اعتبارسنجی کردن DTLS Client در بخش 4.2.1 از (RFC 6347) DTLS v1.2 و (RFC 4347) DTLS v1.0 تشریح شده است. سرویس‌دهنده ایمیل با نقش DTLS server، DTLS client را در طول فرایند برقراری اتصال (Handshaking) و پیش از ارسال پیام	

ServerHello اعتبارسنجی می‌کند. سرور بعد از دریافت پیام ClientHello، یک پیام HelloVerifyRequest را همراه با یک کوکی به کلاینت ارسال می‌کند. این کوکی درواقع یک پیام امضاءشده با استفاده از توابع چکیده ساز معرفی‌شده در الزام FCS_COP.1/KeyedHash است. در ادامه کلاینت دوباره یک پیام ClientHello دیگر را به همراه کوکی امضاءشده ذکرشده ارسال می‌کند. سرور در صورت تأیید کردن این کوکی ارسالی از جانب کلاینت، مطمئن می‌شود که کلاینت از آدرس IP جعلی استفاده نکرده است.	
۸	الزامات پروتکل DTLS Server بدون احراز هویت دوطرفه (۴) (FCS_DTLSS_EXT.1.4)
DTLS server باید استقرار کلید را با استفاده از [انتخاب: RSA با اندازه کلید [انتخاب: ۲۰۴۸ بیت، ۳۰۷۲بیت، ۴۰۹۶ بیت] ، دیفی-هلمن با پارامترهایی با سایز [۲۰۴۸ بیت، ۳۰۷۲بیت، ۴۰۹۶ بیت، ۶۱۴۴ بیت، ۸۱۹۲ بیت]، دیفی-هلمن با گروه‌های [انتخاب: ffdhe2048، ffdhe3072،ffdhe4096 ، ffdhe6144، ffdhe8192، هیچ گروه دیگر]، منحنی‌های ECDHE [انتخاب: secp521r1, secp384r1, secp256r1,] و هیچ منحنی دیگری] انجام دهد.	
۹	الزامات پروتکل DTLS Server بدون احراز هویت دوطرفه (۵) (FCS_DTLSS_EXT.1.5)
DTLS server باید هنگامی‌که یک پیام حاوی MAC نامعتبر دریافت می‌کند، [انتخاب: به نشست DTLS خاتمه دهد، بی‌صدا رکورد را دور بریزد.] نکته کاربردی: ✓ کد MAC در طی فاز دست تکانی DTLS و برای حفاظت از جامعیت پیام‌ها استفاده می‌شود. اگر تأیید MAC شکست بخورد، نشست باید خاتمه یابد یا رکورد دریافت شده، بی‌صدا دور انداخته شود.	
۱۰	الزامات پروتکل DTLS Server بدون احراز هویت دوطرفه (۶) (FCS_DTLSS_EXT.1.6)
DTLS server باید پیام‌های باز ارسال‌شده (مربوط به replay attack) برای: ۱. رکوردهای DTLS که قبلاً دریافت شده‌اند (یعنی شماره ترتیب آن تکراری هست). ۲. رکوردهای DTLS بسیار قدیمی که شماره ترتیب آن‌ها در sliding receive window قرار	

نمی‌گیرد. را به‌صورت خاموش نادیده بگیرد.

۲-۲-۸- الزامات پروتکل IPSEC

شماره الزام	نام الزام
۱۱	الزامات پروتکلIPSEC (۱) (FCS_IPSEC_EXT.1.1)
سرویس‌دهنده ایمیل باید پروتکل IPSEC را بر اساس آنچه در RFC 4301 مشخص‌شده است، پیاده‌سازی کند. نکات کاربردی: ✓ بر اساس RFC 4301 برای پیاده‌سازی IPSEC جهت محافظت از ترافیک IP از یک پایگاه داده امنیتی با نام SPD (Security Policy Database) استفاده می‌شود. ✓ با استفاده از SPD می‌توان تعیین کرد که بسته‌های IP چگونه باید مدیریت شوند. در این زمینه به سه قاعده زیر اشاره‌شده است: • PROTECT : محافظت از بسته‌ها با استفاده از رمزنگاری • BYPASS : عدم استفاده از سرویس‌های IPSEC (عدم استفاده از رمزنگاری) • DISCARD : دور ریختن بسته‌ها ✓ پایگاه داده مذکور را می‌توان به روش‌های مختلفی پیاده‌سازی کرد که از آن جمله می‌توان به پیاده‌سازی لیست‌های کنترل دسترسی[۱] در مسیریاب‌ها، مجموعه قوانین فیلترینگ بسته	

[۱] Access Control Lists

(packet filtering rule set) در فایروال‌ها و مواردی ازاین‌دست اشاره کرد. ✓ صرف‌نظر از روش پیاده‌سازی این پایگاه داده باید توجه داشت که مشابه با مثال‌های ذکرشده، قواعد (rule‌ها) باید ترتیب اعمال داشته و بسته‌های IP قابل‌تفکیک باشند. ✓ حتی می‌توان یک پایگاه داده برای هر واسط شبکه داشت اما الزامی در این زمینه وجود ندارد.	
الزامات پروتکلIPSEC (۲) (FCS_IPSEC_EXT.1.2)	۱۲
سرویس‌دهنده ایمیل باید یک قاعده پیش‌فرض (default rule) در SPD داشته باشد که با بسته‌های تطابق نیافته (match نشده) با قواعد دیگر تطابق یافته و کارکرد این قاعده نیز دور ریختن بسته‌های مذکور باشد.	
الزامات پروتکلIPSEC (۳) (FCS_IPSEC_EXT.1.3)	۱۳
سرویس‌دهنده ایمیل باید [انتخاب: مد انتقال (Transport) ، مد تونل (Tunnel)] را پیاده‌سازی کند. نکته کاربردی: ✓ نویسنده سند هدف امنیتی باید مدهای عملیاتی پشتیبانی شده برای IPSEC را مشخص کند. به‌عبارتی‌دیگر حداقل یک یا هر دو مد ذکرشده را پیاده‌سازی کند.	
الزامات پروتکلIPSEC (۴) (FCS_IPSEC_EXT.1.4)	۱۴
سرویس‌دهنده ایمیل باید بر اساس آنچه در RFC 4303 گفته‌شده است، فریمورک ESP از پروتکل IPSEC را با استفاده از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128، AES-CBC-192، AES-CBC-256 (تشریح شده در RFC 3602)، هیچ الگوریتم دیگری] به همراه یک HMAC مبتنی بر الگوریتم درهم‌سازی امن (SHA) [انتخاب: HMAC-SHA-1، HMAC-SHA-256، HMAC-SHA-384، HMAC-SHA-512، هیچ الگوریتم دیگری] و [انتخاب: AES-GCM-128، AES-GCM-192، AES-GCM-256 (تشریح شده در RFC 4106)، هیچ الگوریتم دیگری] پیاده‌سازی کند. نکته کاربردی: ✓ وقتی‌که الگوریتم AES-CBC انتخاب گردد، حداقل یک HMAC مبتنی بر SHA نیز باید	

انتخاب شود. اگر یک AES-GCM انتخاب گردد، نیاز نیست که HMAC انتخاب شود، زیرا AES-GCM محرمانگی و جامعیت را فراهم می‌کند. درصورتی‌که برای IPSEC با توجه به خروجی مورد انتظار، نوع خاصی از HMAC مبتنی بر SHA (مثال: a truncated version of HMAC) انتخاب گردد، در خلاصه مشخصات محصول باید معرفی گردد.	
الزامات پروتکل IPSEC (۵) (FCS_IPSEC_EXT.1.5)	۱۵
سرویس‌دهنده ایمیل باید یکی از این پروتکل‌ها را به کار گیرد: [انتخاب: ۱. IKEv1، با استفاده از مد اصلی برای انجام تبادلات فاز اول، طبق RFCهای 4109، 2409، 2408، 2407، [انتخاب: هیچ RFC دیگری برای شماره توالی‌های بسط یافته[۱]، RFC4304 برای شماره توالی‌های بسط یافته] و [انتخاب: هیچ RFC دیگری برای توابع درهم‌ساز، RFC 4868 برای توابع درهم‌ساز] ۲. IKEv2، مطابق با تعریف RFC 5996 و [انتخاب: بدون پشتیبانی از NAT Traversal، با پشتیبانی اجباری از NAT Traversal چنان‌که در بخش 2.23 از RFC 5996 تشریح شده است] و [انتخاب: هیچ RFC دیگر برای توابع درهم‌ساز، RFC 4868 برای توابع درهم‌ساز] نکات کاربردی: ✓ اگر سرویس‌دهنده ایمیل برای دو پروتکل IKEv1 یا IKEv2 از الگوریتم درهم‌ساز SHA-2 استفاده کند، نویسنده سند هدف امنیتی باید RFC 4868 را انتخاب کند. اگر سرویس‌دهنده ایمیل از HMACهای مبتنی بر SHA، کوتاه شده مطابق با RFC 4868 استفاده کند، باید در خلاصه مشخصات محصول، مشخص گردد.	

[۱] Extended Sequence Numbers

۱۶	الزامات پروتکل IPSEC (۶) (FCS_IPSEC_EXT.1.6)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که برای پیلود رمزشده در پروتکل [انتخاب: IKEv1،IKEv2] از الگوریتم‌های رمزنگاری [انتخاب: AES-CBC-128، AES-CBC-192، AES-CBC-256 (تشریح شده در RFC 3602)، AES-GCM-128، AES-GCM-192، AES-GCM-256 (تشریح شده در RFC 5282)]استفاده می‌شود. نکته کاربردی: ✓ ازآنجایی‌که هیچ RFC وجود ندارد که AES-GCM را برای IKEv1 تعریف کرده باشد، AES-GCM-128، AES-GCM-192 و AES-GCM-256 تنها در صورتی انتخاب می‌شوند که IKEv2 نیز انتخاب‌شده باشد.	
۱۷	الزامات پروتکلIPSEC (۷) (FCS_IPSEC_EXT.1.7)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که [انتخاب: سرپرست سرویس‌دهنده ایمیل می‌تواند طول عمر SA[1] فاز اول IKEv1 را بر اساس [انتخاب: • تعداد بایت منتقل‌شده؛ • مدت‌زمان سپری‌شده از زمان برقراری آن‌که این طول عمر آستانه را می‌توان در بازه [اختصاص: اعداد صحیح شامل 24] ساعت قرار داد] پیکربندی کند. سرپرست سرویس‌دهنده ایمیل می‌تواند طول عمر IKEv2 SA را بر اساس [انتخاب: • تعداد بایت منتقل‌شده؛ • مدت‌زمان سپری‌شده از زمان برقراری آن‌که این طول عمر آستانه را می‌توان در بازه [اختصاص: اعداد صحیح شامل 24] ساعت قرار داد] پیکربندی کند.]	

[1] Security Association

نکات کاربردی: ✓ تعیین طول عمر برای SAهای فاز اول به مدیر سرویس‌دهنده ایمیل محول شده و باید قابل پیکربندی باشد. این مقدار به‌طور پیش‌فرض معمولاً ۲۴ ساعت است. هر چه این مقدار کمتر باشد به لحاظ امنیتی بهتر است.	
الزامات پروتکلIPSEC (۸) (FCS_IPSEC_EXT.1.8)	۱۸
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که [انتخاب: سرپرست سرویس‌دهنده ایمیل می‌تواند طول عمر SA فاز دوم IKEv1 را بر اساس [انتخاب: • تعداد بایت منتقل‌شده؛ • مدت‌زمان برقراری نشست که مقدار طول عمر آن را می‌توان در بازه [اختصاص: بازه اعداد صحیح شامل ۸] ساعت قرار داد] پیکربندی کند. سرپرست سرویس‌دهنده ایمیل می‌تواند طول عمر IKEv2 Child SA را بر اساس [انتخاب: • تعداد بایت منتقل‌شده؛ • مدت‌زمان برقراری نشست که مقدار طول عمر آن را می‌توان در بازه [اختصاص: بازه اعداد صحیح شامل ۸] ساعت قرار داد] پیکربندی کند. [نکات کاربردی: ✓ تعیین طول عمر برای SAهای فاز اول به سرپرست سرویس‌دهنده ایمیل محول شده و باید قابل پیکربندی باشد. این مقدار به‌طور پیش‌فرض معمولاً ۸ ساعت است. هر چه این مقدار کمتر باشد، به لحاظ امنیتی بهتر است.	
الزامات پروتکلIPSEC (۹) (FCS_IPSEC_EXT.1.9)	۱۹
سرویس‌دهنده ایمیل باید مقدار x را که در تبادل کلید IKE DiffieHellman استفاده می‌شود (g ^ x mod p)، با استفاده از تولیدکننده بیت تصادفی که در الزام «تولید بیت تصادفی ۱» مشخص‌شده است تولید کند و اندازه آن نیز دست‌کم [اختصاص: تعداد بیتی که حداقل دو برابر قدرت امنیتی گروه Diffie-Hellman مذاکره شده باشد] بیت باشد.	

نکات کاربردی: ✓ برای مشاهده قدرت امنیتی گروه‌های مختلف دیفی-هلمن به جدول ۲ از سند NIST SP 800-57 با عنوان "Recommendation for Key Management –Part 1: General" می‌توانید مراجعه کنید.	
۲۰	الزامات پروتکل IPSEC (۱۰) (FCS_IPSEC_EXT.1.10)
سرویس‌دهنده ایمیل باید تک‌شمارهای مورداستفاده در تبادلات [انتخاب: IKEv1، IKEv2] را با طول [انتخاب: [اختصاص: قدرت امنیتی مربوط به گروه Diffie-Hellman مذاکره شده]، حداقل ۱۲۸ بیت و نیز حداقل نصف اندازه خروجی تابع درهم‌سازی شبه تصادفی[۱] مذاکره شده] تولید کند. نکته کاربردی: ✓ اگر IKEv2 انتخاب‌شده باشد (همان‌طور که در RFC5996 اجباری شده است)، نویسنده سند هدف امنیتی باید دومین گزینه را برای طول تک شمار انتخاب کند. نویسنده سند هدف امنیتی مجاز است هر یک از گزینه‌ها را برای IKEv1 انتخاب کند.	
۲۱	الزامات پروتکل IPSEC (۱۱) (FCS_IPSEC_EXT.1.11)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که پروتکل‌های IKE، گروه‌های دیفی-هلمن [انتخاب: ۱۴ (2048-bit MODP) و ۱۹ (256-bit Random ECP)، ۲۰ (384-bit Random ECP)، ۲۴ (2048-bit MODP with 256-bit POS)) را پیاده‌سازی می‌کنند. نکته کاربردی: ✓ قسمت «انتخاب» در این الزام جهت مشخص کردن این موضوع که گروه‌های DH اضافی	

[۱] Sudo random function

پشتیبانی شده است، بکار می‌رود. این الزام برای هر دو IKEv1 و IKEv2 اعمال می‌گردد.	
الزامات پروتکلIPSEC (۱۲) (FCS_IPSEC_EXT.1.12)	۲۲
سرویس‌دهنده ایمیل باید به‌صورت پیش‌فرض بتواند اطمینان حاصل کند که قدرت الگوریتم متقارنی (ازنظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [انتخاب: فاز 1 IKEv1، IKEv2 IKE_SA] مذاکره شده است، بیشتر یا مساوی قدرت الگوریتم متقارنی (ازنظر تعداد بیت‌های کلید) که برای حفاظت از اتصال [انتخاب: فاز 2 IKEv1، IKEv2 CHILD_SA] مذاکره شده است، باشد.	
الزامات پروتکل IPSEC (۱۳) (FCS_IPSEC_EXT.1.13)	۲۳
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که همه پروتکل‌های IKE احراز هویت همتا را با استفاده از [انتخاب: RSA، ECDSA] که از گواهینامه‌های X.509v3 مطابق با RFC4945 و [انتخاب: کلیدهای پیش اشتراکی، هیچ روش دیگری] استفاده می‌کند، انجام می‌دهند. نکات کاربردی: ✓ برای انطباق با این پروفایل حفاظتی، استفاده از حداقل یک روش احراز هویت همتا مبتنی بر کلید عمومی الزامی است. ✓ خلاصه مشخصات محصول باید تشریح کند که چگونه الگوریتم‌ها مورداستفاده قرار می‌گیرند. برای مثال RFC 2409 سه روش احراز هویت با استفاده از کلید عمومی را مشخص می‌کند، هرکدام که استفاده می‌شود، باید در خلاصه مشخصات محصول، ذکر گردد.	
الزامات پروتکل IPSEC (۱۴) (FCS_IPSEC_EXT.1.14)	۲۴
سرویس‌دهنده ایمیل باید کانال امن را فقط درصورتی‌که شناسه موجود در گواهینامه دریافتی با شناسه مرجع پیکربندی‌شده انطباق داشته باشد، برقرار کند. شناسه مرجع و ارائه‌شده از انواع زیر می‌توانند باشند: [انتخاب: آدرس IP، FQDN، FQDN کاربر، DN (Distinguished Name)] و [انتخاب: هیچ نوع شناسه مرجع دیگری، [انتخاب: دیگر انواع شناسه مرجع پشتیبانی شده]].	

۳-۲-۸- الزامات پروتکل SSH

الزامات این بخش نیز برای هر دو نقش کلاینت و سرور در اتصال SSH بیان‌شده است.

شماره الزام	نام الزام
۲۵	الزامات پروتکل Client SSH (۱) (FCS_SSHC_EXT.1.1)
سرویس‌دهنده ایمیل باید پروتکل SSH را مطابق با RFCهای 4251، 4252، 4253، 4254، [انتخاب: 4256، 4344، 5647، 5656، 6187، 6668، 8268، 8308 section 3.1، 8332] پیاده‌سازی کند. برای راهنمایی نویسنده محترم سند «هدف امنیتی» لیست زیر برای بخش انتخاب از این الزام ارائه‌شده است. • RFC 4256 در صورت فراهم بودن keyboard-interactive authentication • RFC 4344 در صورت فراهم بودن مد AES-128-CTR یا AES-256-CTR • RFC 5647 در صورت فراهم بودن AEAD_AES_128_GCM یا AEAD_AES_256_GCM • RFC 5656 در صورت فراهم بودن رمزنگاری elliptical curve • RFC 6187 در صورت فراهم بودن گواهینامه X.509 برای الگوریتم‌های مبتنی بر کلید عمومی • RFC 6668 در صورت فراهم بودن الگوریتم‌های HMAC-SHA-2 • RFC 8268 در صورت فراهم بودن گروه‌های FFC DH به همراه SHA-2 • RFC 8308 Section 3.1 در صورت انتخاب RFC 8332 • RFC 8332 در صورت فراهم بودن SHA-2 به همراه ssh-rsa برای الگوریتم‌های کلید عمومی	
۲۶	الزامات پروتکل SSH Client (۲) (FCS_SSHC_EXT.1.2)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که در پیاده‌سازی پروتکل SSH، روش‌های احراز هویت مقابل مطابق با آنچه در RFC 4252 توضیح داده‌شده است، پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، [انتخاب: احراز هویت مبتنی بر رمز عبور، هیچ روش دیگری].	
۲۷	الزامات پروتکل SSH Client (۳) (FCS_SSHC_EXT.1.3)
همان‌طور که در RFC 4253 توضیح داده‌شده است، سرویس‌دهنده ایمیل باید اطمینان حاصل کند که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک اتصال SSH، کنار گذاشته شوند.	

نکات کاربردی: RFC 4253 امکان پذیرش «بسته‌های بزرگ» را فراهم می‌کند، با این اخطار که بسته‌ها باید «طول معقولی» داشته باشند یا اینکه کنار گذاشته می‌شوند. توصیه می‌شود این اختصاص توسط نویسنده هدف امنیتی با در نظر گرفتن بیشترین اندازهٔ بستهٔ قابل‌پذیرش پر شود تا به این وسیله «طول معقول» برای سرویس‌دهنده ایمیل تعریف شود.	
۲۸	الزامات پروتکل SSH Client (۴) (FCS_SSHC_EXT.1.4)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که در پیاده‌سازی پروتکل انتقال SSH، از الگوریتم‌های رمزنگاری [انتخاب: AES128-CBC، AES-256-CBC، AES128-CTR، AES256-CTR، AEAD_AES_128_GCM، AEAD_AES_256_GCM] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند. نکات کاربردی: ✓ RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌کند. چنان‌که در این RFC مطرح‌شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌ها برای MAC نیز انتخاب گردند.	
۲۹	الزامات پروتکل SSH Client (۵) (FCS_SSHC_EXT.1.5)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که در پیاده‌سازی مکانیزم احراز هویت مبتنی بر کلید عمومی از [انتخاب: ecdsa-sha2-nistp256، ssh-rsa] و [انتخاب: ecdsa-sha2-nistp384، ecdsa-sha2-nistp521، x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384، x509v3-ecdsa- sha2-nistp521، هیچ الگوریتم کلید عمومی دیگری] به‌عنوان الگوریتم(های) کلید عمومی خود استفاده کند و همه الگوریتم‌های دیگر را رد کند (استفاده نکند).	
۳۰	الزامات پروتکل SSH Client (۶) (FCS_SSHC_EXT.1.6)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که در پیاده‌سازی پروتکل انتقال SSH از [انتخاب: hmac-sha1، hmac-sha1-96، hmac-sha2-256، hmac-sha2-512] و [انتخاب: AEAD_AES_128_GCM، AEAD_AES_256_GCM، هیچ الگوریتم MAC دیگری] به‌عنوان الگوریتم(های) MAC برای تأمین صحت داده استفاده می‌شود و سایر الگوریتم‌های MAC استفاده نمی‌شوند.	

نکات کاربردی:

- ✓ RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌کند. چنانکه در این RFC مطرح‌شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌های برای MAC نیز انتخاب گردند.
- ✓ RFC 6668 استفاده از sha2 را در SSH مشخص می‌کند.

۳۱	الزامات پروتکل SSH Client (۷) (FCS_SSHC_EXT.1.7)

سرویس‌دهنده ایمیل باید اطمینان حاصل کند که [انتخاب: .ecdh- diffie-hellman-group14-sha1 sha2- nistp256 و [انتخاب: ecdh-sha2-nistp384، ecdh-sha2-nistp521، هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.

۳۲	الزامات پروتکل SSH Client (۸) (FCS_SSHC_EXT.1.8)

سرویس‌دهنده ایمیل باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه (منظور از حد آستانه یعنی طول نشست بیشتر از یک ساعت نباشد و حجم داده مخابره شده بیشتر از 1 گیگابایت نباشد) استفاده می‌گردد. در صورت پر شدن حد آستانه، تولید مجدد کلید باید صورت بگیرد.

نکات کاربردی:

- ✓ این الزام حد آستانه‌هایی را برای حداکثر زمانی که کلید(های) نشست می‌تواند استفاده گردد و حداکثر مقدار داده‌ای که می‌تواند با یک سری کلید نشست انتقال یابد، مشخص می‌کند. هر دو حد آستانه باید پیاده‌سازی گردد و مجدد سازی کلید نیز وقتی هرکدام از دو مورد مذکور سر برسد باید بکار گرفته شود.
- ✓ برای محاسبه حداکثر داده انتقالی، داده‌هایی که به سرویس‌دهنده ایمیل وارد و از سرویس‌دهنده ایمیل خارج می‌شوند باید محاسبه گردد.
- ✓ مجدد سازی کلید باید روی تمام کلیدهای نشست (رمزنگاری، حفاظت از جامعیت) برای ترافیک ورودی و خروجی اعمال گردد.

✓ سرویس‌دهنده ایمیل همچنین می‌تواند مقادیری کمتر از مقادیر حد آستانه ذکرشده در این الزام را پیاده‌سازی کند. سند راهنمای سرویس‌دهنده ایمیل یا بخش خلاصه مشخصات محصول، باید نحوه پیکربندی این مقادیر و نحوه سر رسیدن آن‌ها و همچنین چگونگی امکان تعریف مقادیر کمتر از حد آستانه را تشریح کند.

۳۳	الزامات پروتکل SSH Client (۹) (FCS_SSHC_EXT.1.9)

سرویس‌دهنده ایمیل باید اطمینان حاصل کند که کلاینت SSH، سرور SSH را با استفاده از یک پایگاه داده محلی که نام هر میزبان را با کلید عمومی متناظر آن مرتبط می‌کند و یا [انتخاب: فهرستی از مراجع صدور گواهی مطمئن، هیچ روش دیگری] (تشریح شده در RFC 4251 بخش 4.1) احراز هویت می‌کند.

نکات کاربردی:

✓ تنها در صورتی می‌توان گزینه «فهرستی از مراجع صدور گواهی مطمئن» را انتخاب کرد که x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384 یا x509v3-ecdsa-sha2-nistp521 در FCS_SSHC_EXT.1.5 انتخاب‌شده باشد.

۳۴	الزامات پروتکلServer SSH (۱) (FCS_SSHS_EXT.1.1)

سرویس‌دهنده ایمیل باید پروتکل SSH را مطابق با RFCهای 4251، 4252، 4253، 4254، [انتخاب: 4256، 4344، 5647، 5656، 6187، 6668، 8268، 8308 section 3.1، 8332] پیاده‌سازی کند.

برای راهنمایی نویسنده محترم سند «هدف امنیتی» لیست زیر برای بخش انتخاب از این الزام ارائه‌شده است.

- RFC 4256 در صورت فراهم بودن keyboard-interactive authentication
- RFC 4344 در صورت فراهم بودن مد AES-128-CTRیا AES-256-CTR
- RFC 5647 در صورت فراهم بودن AEAD_AES_128_GCM یا AEAD_AES_256_GCM
- RFC 5656 در صورت فراهم بودن رمزنگاری elliptical curve
- RFC 6187 در صورت فراهم بودن گواهینامه X.509 برای الگوریتم‌های مبتنی بر کلید عمومی

• RFC 6668 در صورت فراهم بودن الگوریتم‌های HMAC-SHA-2 • RFC 8268 در صورت فراهم بودن گروه‌های FFC DH به همراه SHA-2 • RFC 8308 Section 3.1 در صورت انتخاب RFC 8332 • RFC 8332 در صورت فراهم بودن SHA-2 به همراه SSH-RSA برای الگوریتم‌های کلید عمومی	
۳۵	الزامات پروتکل Server SSH (۲) (FCS_SSHS_EXT.1.2)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که در پیاده‌سازی پروتکل SSH، همان‌طور که در RFC 4252 توضیح داده‌شده است، روش‌های احراز هویت مقابل پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، احراز هویت مبتنی بر رمز عبور.	
۳۶	الزامات پروتکل Server SSH (۳) (FCS_SSHS_EXT.1.3)
همان‌طور که در RFC 4253 توضیح داده‌شده است، سرویس‌دهنده ایمیل باید اطمینان حاصل کند که بسته‌های دارای بایت‌های بیشتر از [اختصاص: تعداد بایت‌ها] در یک اتصال SSH، کنار گذاشته شوند. نکات کاربردی: RFC 4253 امکان پذیرش «بسته‌های بزرگ» را فراهم می‌کند، با این اخطار که بسته‌ها باید «طول معقولی» داشته باشند یا اینکه کنار گذاشته می‌شوند. توصیه می‌شود این اختصاص توسط نویسنده هدف امنیتی با در نظر گرفتن بیشترین اندازهٔ بستهٔ قابل‌پذیرش پر شود تا به این وسیله «طول معقول» برای سرویس‌دهنده ایمیل تعریف شود.	
۳۷	الزامات پروتکل Server SSH (۴) (FCS_SSHS_EXT.1.4)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که در پیاده‌سازی پروتکل انتقال SSH، از الگوریتم‌های رمزنگاری [انتخاب: AES128-CBC، AES-256-CBC، AES128-CTR، AES256-CTR، AEAD_AES_128_GCM، AEAD_AES_256_GCM] استفاده می‌شود و سایر الگوریتم‌های رمزنگاری رد می‌شوند. نکات کاربردی: ✓ RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌کند. چنانکه در این RFC مطرح‌شده	

است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌ها برای MAC نیز انتخاب گردند.	
۳۸	الزامات پروتکل Server SSH (۵) (FCS_SSHS_EXT.1.5)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که در پیاده‌سازی مکانیزم احراز هویت مبتنی بر کلید عمومی از [انتخاب: ecdsa-sha2-nistp256، ssh-rsa] و [انتخاب: ecdsa-sha2-nistp384، ecdsa-sha2-nistp521، x509v3-ecdsa-sha2-nistp256، x509v3-ecdsa-sha2-nistp384، x509v3-ecdsa-sha2-nistp521، هیچ الگوریتم کلید عمومی دیگری] به‌عنوان الگوریتم(های) کلید عمومی خود استفاده کند و همه الگوریتم‌های دیگر را رد کند (استفاده نکند).	
۳۹	الزامات پروتکل Server SSH (۶) (FCS_SSHS_EXT.1.6)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که در پیاده‌سازی پروتکل انتقال SSH از [انتخاب: hmac-sha1، hmac-sha1-96، hmac-sha2-256، hmac-sha2-512] و [انتخاب: AEAD_AES_128_GCM، AEAD_AES_256_GCM، هیچ الگوریتم MAC دیگری] به‌عنوان الگوریتم(های) MAC برای تأمین صحت داده استفاده می‌شود و سایر الگوریتم‌های MAC استفاده نمی‌شوند. نکات کاربردی: ✓ RFC 5647 استفاده از الگوریتم‌های AEAD_AES_128_GCM و AEAD_AES_256_GCM را در SSH مشخص می‌کند. چنانکه در این RFC مطرح‌شده است، در صورتی می‌توان از دو الگوریتم مذکور استفاده کرد که همین الگوریتم‌ها برای MAC نیز انتخاب گردند. ✓ RFC 6668 استفاده از sha2 را در SSH مشخص می‌کند.	
۴۰	الزامات پروتکل Server SSH (۷) (FCS_SSHS_EXT.1.7)
سرویس‌دهنده ایمیل باید اطمینان حاصل کند که [انتخاب: diffie-hellman-group14-sha1، ecdh-sha2-nistp256] و [انتخاب: ecdh-sha2-nistp384، ecdh-sha2-nistp521، هیچ روش دیگری] تنها روش‌های مجاز تبادل کلید هستند که برای پروتکل SSH به کار می‌روند.	
۴۱	الزامات پروتکل Server SSH (۸) (FCS_SSHS_EXT.1.8)

سرویس‌دهنده ایمیل باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه (منظور از حد آستانه یعنی طول نشست بیشتر از یک ساعت نباشد و حجم داده مخابره شده بیشتر از یک گیگابایت نباشد) استفاده می‌گردد. در صورت پر شدن حد آستانه، تولید مجدد کلید باید صورت بگیرد. نکات کاربردی: ✓ این الزام حد آستانه‌هایی را برای حداکثر زمانی که کلید(های) نشست می‌تواند استفاده گردد و حداکثر مقدار داده‌ای که می‌تواند با یک سری کلید نشست انتقال یابد مشخص می‌کند. هر دو حد آستانه باید پیاده‌سازی گردد و مجدد سازی کلید نیز وقتی هرکدام از دو مورد مذکور سر برسد باید بکار گرفته شود.برای محاسبه حداکثر داده انتقالی، داده‌هایی که به سرویس‌دهنده ایمیل وارد و از سرویس‌دهنده ایمیل خارج می‌شوند باید محاسبه گردد. ✓ مجدد سازی کلید باید روی تمام کلیدهای نشست (رمزنگاری، حفاظت از جامعیت) برای ترافیک ورودی و خروجی اعمال گردد. ✓ سرویس‌دهنده ایمیل همچنین می‌تواند مقادیری کمتر از مقادیر حد آستانه ذکرشده در این الزام را پیاده‌سازی کند. سند راهنمای سرویس‌دهنده ایمیل یا بخش خلاصه مشخصات سرویس‌دهنده ایمیل، باید نحوه پیکربندی این مقادیر و نحوه سر رسیدن آن‌ها و همچنین چگونگی امکان تعریف مقادیر کمتر از حد آستانه را تشریح کند.

۳-۸- کلاس محافظت از محصول

۱-۳-۸- خودآزمایی خودکار عملگرهای امنیتی

شماره الزام	نام الزام
۴۵	خودآزمایی بر اساس گواهینامه (۱) (FPT_TST_EXT.2.1)
اگر برای انجام آزمون‌های خودآزمایی از یک گواهینامه استفاده شود و آن گواهینامه نامعتبر باشد، محصول باید در آزمون خودآزمایی ناموفق اعلام شود. نکات کاربردی:	

✓ می‌توان به‌صورت اختیاری از گواهینامه‌ها برای آزمون‌های خودآزمایی استفاده کرد. در این صورت باید سند هدف امنیتی آن را صریحاً بیان کرده و این الزام را اعمال کند.

۲-۳-۸- به‌روزرسانی امن محصول

شماره الزام	نام الزام
۴۶	به‌روزرسانی امن بر اساس گواهینامه (۱) (FPT_TUD_EXT.2.1)
درصورتی‌که کد امضای گواهینامه یک به‌روزرسانی نامعتبر باشد سرویس‌دهنده ایمیل نباید آن را نصب کند.	
۴۷	به‌روزرسانی امن بر اساس گواهینامه (۲) (FPT_TUD_EXT.2.2)
هنگامی‌که گواهینامه به علت انقضای آن، غیر معتبر اعلام‌شده است، سرویس‌دهنده ایمیل باید [انتخاب: اجازه بدهد که در این موارد سرپرست سرویس‌دهنده ایمیل در مورد پذیرش گواهی تصمیم‌گیری کند، گواهی را بپذیرد، گواهی را نپذیرد.]	

۴-۸- کلاس مدیریت امنیت

شماره الزام	نام الزام
۴۸	مدیریت کارکرد امنیتی ۱/توابع (FMT_MOF.1/Funtions)
سرویس‌دهنده ایمیل باید قابلیت [انتخاب: تعیین نحوه کارکرد، تغییر نحوه کارکرد] در خصوص [انتخاب: ارسال داده‌های ممیزی به یک موجودیت IT خارجی (سرور syslog)، کنترل داده ممیزی، نحوه عمل در زمان پر بودن فضای محلی ذخیره‌سازی] را به سرپرست امنیتی سرویس‌دهنده ایمیل محدود کند. نکته کاربردی: این الزام در صورتی انتخاب می‌گردد که یک یا چند مورد از سناریوهای زیر اعمال شوند: ✓ اگر پروتکل انتقال برای ارسال داده ممیزی به موجودیت IT خارجی که در الزام	

FAU_STG_EXT.1 تعریف‌شده است، قابل پیکربندی باشد و ارسال داده ممیزی به موجودیت IT خارجی انتخاب‌شده باشد. ✓ اگر کنترل داده ممیزی قابل پیکربندی باشد، «کنترل داده ممیزی» باید انتخاب گردد. عبارت «کنترل داده ممیزی» به گزینه‌های مختلفی برای انتخاب و اختصاص در الزامات FAU_STG_EXT.1.2، FAU_STG_EXT.1.3 و FAU_STG_EXT.2/LocSpace اشاره دارد.	
۴۹	مدیریت کارکرد امنیتی ۱/به‌روزرسانی خودکار (FMT_MOF.1/AutoUpdate)
سرویس‌دهنده ایمیل باید قابلیت [انتخاب: فعال کردن و غیرفعال کردن] توابع [انتخاب: جستجو برای به‌روزرسانی‌های خودکار، به‌روزرسانی خودکار] را به سرپرست امنیتی سرویس‌دهنده ایمیل محدود کند. نکات کاربردی: ✓ این الزام تنها زمانی قابل پیاده‌سازی است که سرویس‌دهنده ایمیل امکان پشتیبانی از جستجو برای به‌روزرسانی‌های خودکار و/یا به‌روزرسانی خودکار را فراهم کند و اجازه فعال و غیرفعال کردن این قابلیت‌ها را بدهد. ✓ گزینه «به‌روزرسانی خودکار» ممکن است فقط وقتی انتخاب شود که از امضای دیجیتال برای تأیید به‌روزرسانی امن، استفاده گردد.	

واژه‌نامه

واژه‌نامه انگلیسی به فارسی

واژه انگلیسی	برگردان فارسی
Protection Profile (PP)	پروفایل حفاظتی
Common Criteria (CC)	سند معیار مشترک
Security Target (ST)	هدف امنیتی
Target of Evaluation (TOF)	مودم (مودم)
Security Functional Requirement (SFR)	الزام کارکردی امنیتی
Email Server	سرویس‌دهنده ایمیل
Email Client	کاربر ایمیل
Mail Box	جعبه ایمیل
Mail Box-to-Mail Box	جعبه ایمیل-به-جعبه ایمیل
Strict Conformance	انطباق سخت (قطعی)
Demonstrable	قابل‌اثبات
Import	واردکردن
Authentication	احراز هویت
Confidentiality	محرمانگی
Data Integrity	صحت داده
Key Establishment	استقرار کلید
Public Key	کلید عمومی

پروفایل حفاظتی سرویس دهنده‌های ایمیل

(Email server)

واژه انگلیسی	برگردان فارسی
Certificate	گواهی
Obscured Feedback	بازخورد مبهم
Reset	بازنشانی‌کردن
Revocation Status	وضعیت ابطال
Extended Sequence Numbers	شماره‌های توالی بسط یافته
Sudo Random Function	تابع درهم‌سازی شبه تصادفی
Identifier	شناسه
Code Siging	امضای کد
Integrity Key	کلید یکپارچگی (صحت)
Cipher Key	کلید رمزنگاری
Replay Attack	حمله تکرار (باز ارسال)
Trust Anchor	لنگر اعتماد
Admin	سرپرست

علائم اختصاری

جدول علائم اختصاری

Abbreviation	Description
CC	Common Criteria
PP	Protection Profile
TOE	Target Of Evaluation
ST	Security Target
SFR	Security Functional Requirement
SAR	Security Assurane Requirement
SMTP	Simaple Mail Transfer Protocol
TLS	Transport Layer Security
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
SPF	Sender Policy Framework
DKIM	DomainKeys Identified Mail
DMARK	Domain-based Message Authentication Reporting and Conformance
HTTPS	Hypertext Transfer Protocol Secure
IPSEC	IP Security
SSL	Secure Sockets Layer
SSH	Secure Shell

فصل ۹– مراجع

1. “Common Criteria for Information Technology Security Evaluation”, Version 3.1, Revisoin 5, 2017
2. “collaborative Protection Profile for Network Devices”, Version 2.2e, 2020
3. “Trustworthy Email”, NIST Special Publication 800-177, Revision 1, 2019
4. “Guidelines on Eletronic Email Security”, NIST Special Publication 800-45, Revision 2, 2007