به نام خدا

پروفایل حفاظتی برای سرویس‌گیرنده ایمیل (Email Client)

آذر ماه ۱۴۰۲

نسخه ۱,۵

پیشگفتار

سند پیش‌رو به تبیین و ارائه‌ی مجموعه الزامات کارکردی-امنیتی موردنیاز برای ساخت یک سرویس‌گیرنده‌ی امنِ ایمیل پرداخته و چارچوب اعتبارسنجی این الزامات توسط ارزیاب را نیز بیان می‌کند. یک سرویس‌گیرنده‌ی ایمیل در قالبِ یک برنامه‌ی قابل‌نصب بر روی کامپیوتر شخصی یا تجهیزاتِ همراه مانند گوشی موبایل ارائه‌شده و امکانِ ارسال و دریافت ایمیل و دسترسی و مدیریت آن‌ها را فراهم می‌کند. برای تدوین این سند از سه نوع مرجع استفاده‌شده است که عبارتند از :

۱. مجموعه استانداردهای امنیتی تدوین‌شده توسط سازمان‌های ۳GPP و NIST برای سرویس ایمیل

۲. پروفایل‌های حفاظتی ارائه‌شده به زبان انگلیسی برای سرویس‌گیرنده‌ی ایمیل و نیز سند مرجع برای محصولات شبکه

۳. آخرین نسخه از سند الگوهای معیار مشترک (CC) برای نگارش پروفایل‌های حفاظتی.

سند در ۹ فصل تدوین‌شده است. فصل اول به بیان مقدمه و مراجع مورداستفاده اختصاص‌یافته و فصل دوم به‌طور گذرا به تشریح معماری استاندارد و امنِ ارائه‌شده برای سرویس ایمیل و نیز جایگاه سرویس‌گیرنده‌ی ایمیل در این معماری می‌پردازد. فصل سوم انطباق سند با سطوح معیار مشترک را ذکر می‌کند. فصل چهارم به معرفی دارایی‌ها، فرضیات، سیاست‌های سازمانی و تهدیدات می‌پردازد. فصل پنجم با دو زیر بخش، نخست به تشریح تهدیدات امنیتی موجود پرداخته و در زیر بخش دوم، نگاشت اهداف به فرضیات، سیاست‌های سازمانی و تهدیدات را ذکر می‌کند. اما بخش اصلی از این سند فصل ۶ام آن هست که به بیان الزامات کارکردی-امنیتی موردنظر برای رفع تهدیدها می‌پردازد. همچنین در ادامه در فصل ۷ نیز رویه‌ها و الزامات در نظر گرفته‌شده برای ارزیابی یک سرویس‌گیرنده‌ی ایمیل توسط ارزیاب و نحوه تعیین پایبندی آن به الزامات کارکردی-امنیتی ذکرشده است. فصل‌های ۸ و ۹ نیز به الزامات کارکردی-امنیتی اختیاری و انتخابی اختصاص دارد که در فصل ۶ به آن‌ها اشاره خواهد شد.

این پروفایل حفاظتی محصولات امنیتی با همکاری مرکز مدیریت راهبردی افتا، سازمان فناوری اطلاعات ایران و پژوهشگاه ارتباطات و فناوری اطلاعات تهیه، تدوین و انتشار یافته است.

فهرست مطالب

فهرست جدول‌ها

فهرست شکل‌ها

فصل ۱– مقدمه

امروزه با رشد سریع علوم کامپیوتر و توسعه‌ی روزافزون اینترنت در کشورها استفاده از سرویس ایمیل به یک نیازِ روزمره و گاهاً حیاتی برای کاربران اینترنت تبدیل‌شده است، بطوریکه 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. بدین منظور، سندِ پیش‌رو با تمرکز بر روی مؤلفه یا برنامه‌ی سرویس‌گیرنده در سرویسِ ایمیل به ارائه‌ی مجموعه الزامات کارکردی-امنیتی به‌منظور تأمین امنیتِ اتصالات و دسترسی‌های مربوطه جهت ارسال، دریافت، ذخیره و مدیریت ایمیل‌ها در جعبه-ی ایمیل می‌پردازد. بدین منظور از سه نوع مرجع استفاده‌شده است که عبارتند از :

۱. مجموعه استانداردهای امنیتی تدوین‌شده توسط سازمان‌های ۳GPP و NIST برای سرویس ایمیل

۲. پروفایل‌های حفاظتی ارائه‌شده به زبان انگلیسی برای سرویس‌گیرنده‌ی ایمیل و نیز سند مرجع برای محصولات شبکه

۳. آخرین نسخه از سند الگوهای معیار مشترک (CC) برای نگارش پروفایل‌های حفاظتی.

سازمان‌دهی این سند در ۹ فصل و بدین شکل است. فصل اول به بیان مقدمه و مراجعِ مورداستفاده اختصاص‌یافته و فصل دوم به‌طور گذرا به تشریح معماری استاندارد و امنِ ارائه‌شده برای سرویس ایمیل و نیز جایگاه سرویس‌گیرنده‌ی ایمیل در این معماری می‌پردازد. فصل سوم انطباق سند با سطوح معیار مشترک را ذکر می‌کند. فصل چهارم به معرفی دارایی‌ها، فرضیات، سیاست‌های سازمانی و تهدیدات می‌پردازد. فصل پنجم با دو زیر بخش، نخست به تشریح تهدیدات امنیتی موجود می‌پردازد بطوریکه 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. فصل ۶ام به بیان الزامات کارکردی-امنیتی موردنظر برای رفع تهدیدها می‌پردازد. همچنین در فصل ۷ رویه‌ها و الزامات در نظر گرفته‌شده برای ارزیابی یک سرویس‌گیرنده‌ی ایمیل توسط ارزیاب و نحوه تعیین پایبندی آن به الزامات کارکردی-امنیتی ذکرشده است. فصل‌های ۸ و ۹ نیز به الزامات کارکردی-امنیتی اختیاری و انتخابی اختصاص دارد که در فصل ۶ به آن‌ها اشاره خواهد شد.

۱-۱-واژه‌نامه

۱-۱-۱-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)	محصول مورد ارزیابی
Network Device	تجهیز شبکه
Security Functional Requirement (SFR)	الزام کارکردی امنیتی
Security Assurance Requirement (SAR)	الزامات تضمین امنیت
Key Establishment	استقرار کلید
Public Key	کلید عمومی
Security Certificate	گواهینامه امنیتی
Obscured Feedback	بازخورد مبهم
Reset	بازگرداندن
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
Cipher Key	کلید رمزنگاری
Replay Attack	حمله باز ارسال (تکرار)
Server	سرور
Client	کاربر - کلاینت

واژه انگلیسی	برگردان فارسی
Transport	انتقال
three-way handshake	دست تکانی سه مرحله‌ای
Tunnel	تونل
Trust Anchor	لنگر اعتماد
Admin	سرپرست

۲-۱-۱-علائم اختصاری

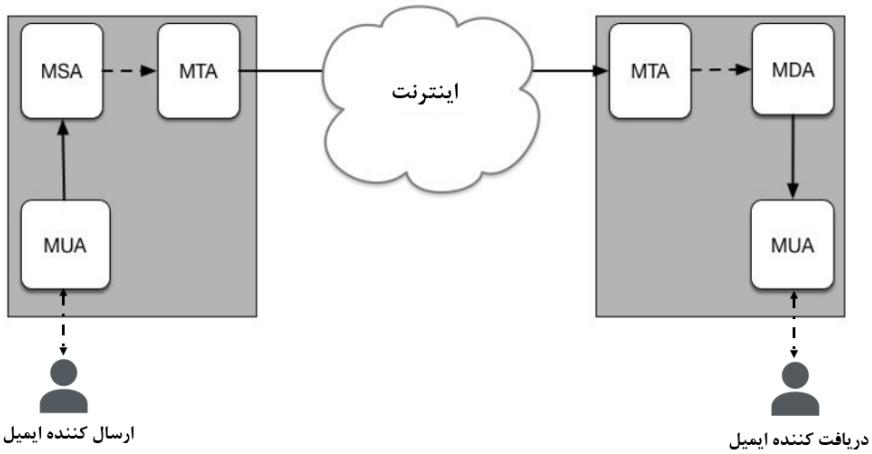
Abbreviation	Description
CC	Common Criteria
PP	Protection Profile
TOE	Target Of Evaluation
ST	Security Target
SFR	Security Functional Requirement
SAR	Security Assurane Requirement
SMTP	Simaple Mail Transfer Protocol
TLS	Transport Layer Security
DNS	Domain Name System
DNSSEC	Domain Name System Security 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 ۲- معرفی محصول مورد ارزیابی (TOE)

محصول مورد بررسی در این پروفایل حفاظتی یک برنامه‌ی سرویس‌گیرنده‌ی ایمیل یا Email Client Application است که بر روی کامپیوتر شخصی یا تجهیزاتِ همراه مانند گوشی موبایل نصب‌شده و وظیفه اصلی آن فراهم کردن مکانیزم‌هایی امن برای ارسال، دریافت، دسترسی و مدیریت ایمیل‌ها است.

۱-۲-مکانیزم کاری و مؤلفه‌های اصلی در سرویسِ ایمیل

شکل زیر مکانیزم کاری و مؤلفه‌های نرم‌افزاری درگیر در فرایند ایجاد، ارسال و دریافت ایمیل در بستر اینترنت را نشان می‌دهد. ضمن معرفی مؤلفه‌های درگیر در سرویسِ ایمیل[۱]، مخلفه‌ی موردبررسی در این پروفایل حفاظتی که نقش email client را ایفا می‌کند معرفی خواهد شد.



شکل .Error! No text of specified style in document-۱ مکانیزم کاری و مؤلفه‌های اصلی در سرویس ایمیل

وظیفه‌ی مؤلفه‌های نرم‌افزاری ذکرشده در تصویر از قرار زیر است:

مؤلفه MUA (Mail User Agent): این مخلفه‌ی 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 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 Error! No text

[۱] Email Service

.of specified style in document-۱ مشخص است، این مؤلفه برای دسترسی به ایمیل‌ها یا ارسال ایمیل جدید نیازمند ارتباط با سرورِ ایمیلِ مربوط به خود (مؤلفه MSA یا MDA از سرور) است. این اتصال با بهره‌گیری از پروتکل‌های مختلفی انجام می‌شود که جلوتر به آن‌ها اشاره خواهد شد. این مؤلفه نقش email client را ایفا می‌کند.

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.

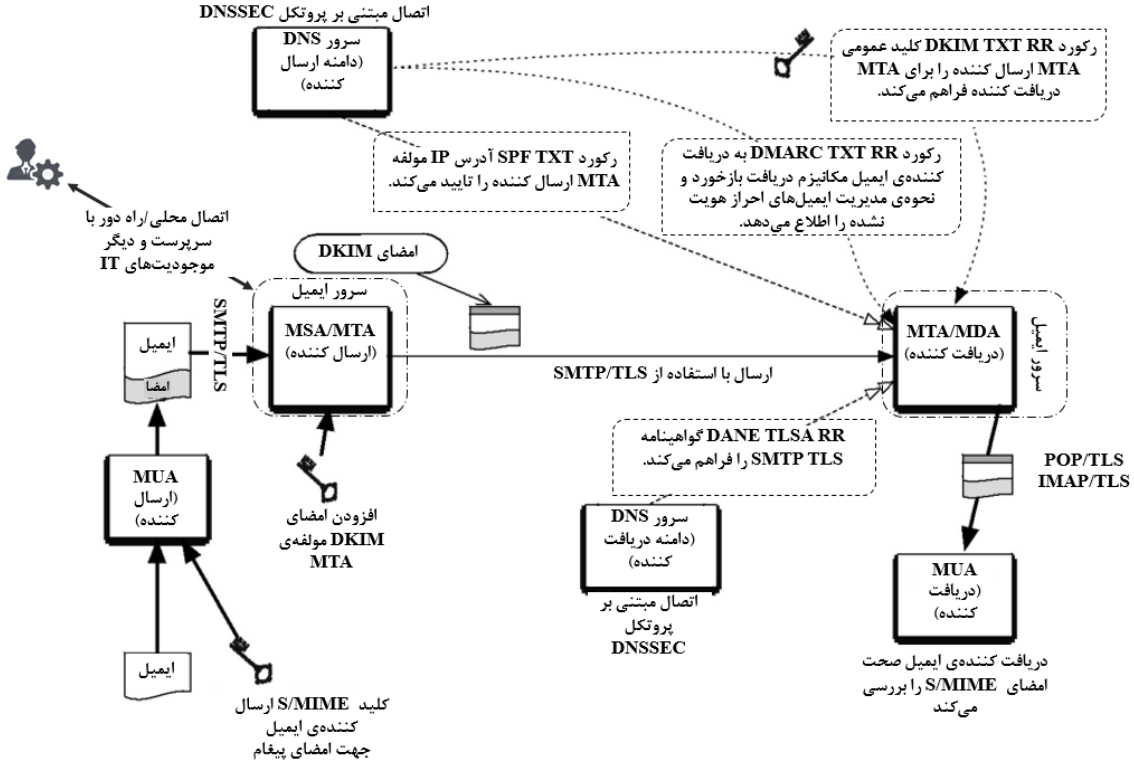
مؤلفه MDA (Mail Delivery Agent): این مؤلفه با تحویل ایمیل از مؤلفه‌ی MTA آن را در جعبه‌ی ایمیل مربوطه قرار می‌دهد و امکان دسترسی مؤلفه (های) MUA به ایمیل‌ها را فراهم می‌کند.

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، مؤلفه MUA در سمت کاربر قرارگرفته و نقش email client را ایفا می‌کند. سه مؤلفه‌ی MDA، MSA و MTA نیز نقش سرویس‌دهنده‌ی ایمیل را ایفا خواهند کرد. هدف اصلی این پروفایل حفاظتی تعیین مجموعه الزامات کارکردی-امنیتی موردنیاز برای مؤلفه MUA است (سرویس‌دهنده‌ی ایمیل در پروفایل حفاظتی جداگانه‌ای بررسی‌شده است).

۲-۲-معماری امنیتی و انواع اتصالات در یک سرویس‌گیرنده‌ی ایمیل

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



شکل .Error! No text of specified style in document-۲ چارچوب امنیتی یک سرویس ایمیل[3]

عمده‌ی مؤلفه‌ها و مکانیزم‌های تشریح شده در تصویر فوق به سرویس‌دهنده‌ی ایمیل مرتبط می‌شود که بحث در مورد آن خارج از تمرکز این سند است. اما آنچه که مرتبط با سرویس‌گیرنده ایمیل است از قرار زیر است:

- **اتصال MUA با سرویس‌دهنده‌ی ایمیل در سمت ارسال‌کننده:** در سمت ارسال‌کننده‌ی ایمیل، MUA از پروتکل SMTP برای تحویل ایمیل به سرویس‌دهنده استفاده می‌کند. پیشنهاد NIST برای تأمین امنیت این اتصال استفاده از پروتکل SMTP مبتنی بر TLS است.
- **اتصال سرویس‌دهنده‌ی ایمیل با MUA در سمت دریافت‌کننده:** در سمت دریافت‌کننده ایمیل، MUA باید از پروتکل‌های POP و IMAP مبتنی بر TLS برای دسترسی و برداشتن ایمیل استفاده کند.

- **تأمین امنیت محتوای ایمیل‌ها:** برای تأمین امنیت ایمیل‌ها به‌صورت «جعبه‌ی ایمیل-به-جعبه‌ی ایمیل»[1] دو پروتکل S/MIME و OpenPGP در این چارچوب پیشنهادشده است. در این حالت فقط محتوای ایمیل رمزنگاری‌شده و سرآیند دخیل نخواهد بود، زیرا برای تعیین مقصد ایمیل، سرور باید قادر به خواندن سرآیند ایمیل باشد.
- **توزیع و دسترسی به گواهینامه‌ها:** برای توزیع و نیز دسترسی به گواهی‌های TLS و S/MIME نیز این چارچوب استفاده از پروتکل DANE بر اساس DNS را پیشنهاد داده است. از روش‌های دیگر می‌توان به استفاده از یک Certificate Autority و یا پیکربندی اولیه Certificate Revocation List و به‌روزرسانی آن از سرورهای مرکزی اشاره کرد. (ازاین‌رو، الزامات مرتبط با پروتکل DANE در بخش الزامات اختیاری در نظر گرفته‌شده است.)

۳-۲-کارکرد محصول

کارکردهای اصلی یک برنامه‌ی سرویس‌گیرنده‌ی ایمیل عبارت از ارسال، دریافت، دسترسی، مدیریت و مشاهده‌ی ایمیل‌ها است. هدف این پروفایل حفاظتی کسب اطمینان از امن بودنِ روندِ ارائه‌ی این خدمات از طریقِ اجبار به رعایتِ مجموعه‌ای از الزامات کارکردی-امنیتی است.

فصل ۳- معیار مشترک CC[2] (ASE_CCL)

ادعای انطباق این پروفایل حفاظتی با سری استانداردهای ملی ایران به شماره ۱۵۴۰۸ به این شرح است:

- تطابق با سری استانداردهای ملی ایران به شماره ۱۵۴۰۸ نسخه ۵ (بازنگری اول)
- 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

انطباق محض[1] با این پروفایل حفاظتی (PP) در صورت ادعای انطباق آن با دیگر پروفایل‌های حفاظتی یا در هر سند هدف امنیتی (ST) الزامی است. برای یادآوری، میزان تطابق ST با هر PP به دو صورت ذیل می‌تواند باشد:

---

[1] MailBox to MailBox

[2] Common Criteria

- انطباق محض: ST شامل یا فراتر از PP است.
  - تعریف مسئله امنیت: ST باید به‌طور کامل حاوی تعریف مسئله امنیت موجود در PP باشد. فرضیات ST می‌تواند کمتر باشد و افزودن فرض اضافی، به‌شرط عدم ایجاد تهدید جدید، ممکن است.
  - 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-امنیتی اجباری و نیز الزامات تضمین امنیت است و علاوه بر آن، می‌تواند الزامات اضافی نیز داشته باشد.
- انطباق قابل‌اثبات[۲]: ST می‌تواند با ارائه دلایل منطقی، برخی موارد PP را تقلیل دهد یا مقید سازد.

همچنین قابل‌ذکر است که تمامی کلاس‌های ذکرشده در این سند مطابق با پروفایل‌های حفاظتیِ زیر بوده و هیچ کلاس یا الزام اختصاصی تعریف‌نشده است:

۱. "collaborative Protection Profile for Network Devices", Version 2.2e, 2020
۲. "PP-Module for Email Clients", Version 1.0, 2021
۳. "Protection Profile for Application Software", Version 1.3, 2019

این PP در انطباق با سطح یک تضمین ارزیابی یا EAL1 است. سطوح تضمین ارزیابی در شکل Error! No text of specified style in document.-۳ نشان داده‌شده است.

[۱] Strict Conformance

[۲] Demonstrable

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 .Error! No text of specified style in document-۳ سطح تضمین ارزیابی بر اساس کلاس‌های تضمین

فصل ۴– تعریف مسئله امنیت (ASE_SPD)

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

۱–۴–دارایی‌ها

۱. FIRMWARE/HARDWARE: سفت‌افزار/سخت‌افزاری که برنامه‌ی سرویس‌گیرنده ایمیل بر روی آن نصب‌شده است.

۲. USER_DATA: اطلاعات حساب کاربری و ایمیل‌های کاربر

۳. APP_DATA: اطلاعات پیکربندی و کنترلی برنامه‌ی سرویس‌گیرنده‌ی ایمیل

۴. SECURITY_DATA: کلیدهای رمزنگاری، گواهی‌های امنیتی، اطلاعات احراز هویتی، شناسه‌ها و ...

۲-۴-تهدیدات

در این بخش به بیان تهدیدات خواهیم پرداخت.

۱- T.FLAWED_ADDON: استفاده از افزونه‌های add-on یکی از روش‌های معمول برای توسعه‌ی عملگرهای برنامه‌ی سرویس‌گیرنده‌ی ایمیل است. اتصال و ارتباطِ تنگاتنگ میان یک افزونه با کد اصلیِ برنامه راه را برای تهدیدات مختلفی فراهم می‌کند. تزریق کدهای مخرب، دسترسی غیرمجاز به اطلاعات حساس (در سطح خودِ برنامه‌ی سرویس‌گیرنده ایمیل و یا سیستم-فایل) و تعدیل دسترسی‌های سیستمی به‌منظور دسترسی غیرمجاز به برنامه‌های دیگر و سیستم‌عامل ازجمله‌ی این تهدیدات هستند.

۲- T.UNAUTHORIZED_ADMINISTRATIVE_ACCESS: منظور از این تهدید، تلاش یک مهاجم یا عامل بیگانه برای نفوذ به برنامه و در اختیار گرفتن کنترل آن با سطح دسترسیِ کامل (سرپرست) است. استفاده از رمز عبور ساده و قابل حدس و یا اتصالات رمز نشده از عوامل وقوع این نوع تهدید هستند.

۳- T.CONNECTION_EAVESDROP_AND_MANIPULATION: این تهدید اشاره به‌قرار گرفتن یک مهاجم در میانه‌ی اتصالات با سرویس‌گیرنده‌ی ایمیل و یا دیگر موجودیت‌های IT و اقدام به استراق سمع، دست‌کاری و ایجاد اختلال در کانال تشکیل‌شده دارد.

۴- T.EMAIL_CONTENT_EAVESDROP_AND_MODIFICATION: این تهدید اشاره به شنود یا تغییر محتوای ایمیل‌ها در مسیر رسیدن به مقصد دارد.

۵- T.SECURITY_FUNCTIONALITY_FAILURE_EXPLOIT: این تهدید اشاره به کارکرد نادرست عملکردهای امنیتی و شناسایی شدن آن‌ها توسط مهاجم برای نفوذ به سیستم دارد.

۶- T.ATTACK_ON_STORED_CREDENTIALS: واضح است که اطلاعات پیکربندی و امنیتی مختلفی در حافظه ذخیره خواهند شد، اطلاعاتی چون نام کاربری و رمز عبور کاربر، کلیدهای رمزنگاری عمومی و خصوصی و گواهینامه‌های X.509. ذخیره‌ی این اطلاعات بر روی حافظه باید به‌صورت رمز شده و امن بوده و نحوه دسترسی به آن‌ها کنترل شود.

۷- T. UNAUTHORIZED_PLATFRORM_DATA_ACCESS: این تهدید اشاره به دسترسی غیرمجاز به داده‌های پلتفرم توسط سرویس‌گیرنده‌ی ایمیل دارد. منظور از پلتفرم، سیستم‌عامل و سکویی است که برنامه‌ی سرویس‌گیرنده ایمیل بر روی آن نصب می‌شود، به‌طور مثال سیستم‌عامل اندروید درگوشی‌های موبایل. دسترسی بدون محدودیت می‌تواند داده‌های کاربر را در معرض تهدید قرار دهد.

۸– T.MALICIOUS_UPDATE: این تهدید اشاره به آلوده شدن برنامه به‌واسطه به‌روزرسانی‌های نامعتبر آن دارد.

۹– T.UNDETECTED_ACTIVITIES: این تهدید یا آسیب‌پذیری اشاره به برجای نگذاشتن رد از خود توسط مهاجم دارد که نتیجه آن می‌تواند عدم توانایی در تشخیص آسیب‌های وارده و عامل آن باشد. ثبت رکوردهای ممیزی نقش مهمی در شناسایی تهدیدات و وقوع خرابی‌ها دارد.

*** قابل‌ذکر است که ارسال ایمیل با محتوای آلوده (مانند لینک‌ها یا ضمیمه‌های آلوده) نیز ازجمله‌ی تهدیدات برای سرویس ایمیل است اما این تهدید و مقابله با آن در سمتِ سرویس‌دهنده‌ی ایمیل پوشش داده می‌شود و از تکرار آن برای سرویس‌گیرنده ایمیل پرهیز شده است.

۴–۳–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 به برنامه برای سرپرست یا کاربر مربوطه نمایش داده‌شده و در صورت موافقت با موارد ذکرشده اجازه دسترسی به برنامه داده شود.

۱- OSP.ACCESS_BANNER: به هنگام لاگین کردن، برنامه باید قادر به نمایش بنری باشد که مجموعه قوانین و رویه‌های موردنظر جهت دسترسی به آن را نشان دهد. بدون اعلام موافقت با قوانین مربوطه نباید اجازه ورود داده شود.

الزام کارکردی امنیتی در نظر گرفته‌شده:

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

۴–۴–فرضیات

۱- A.PHYSICAL_PROTECTION: فرض بر این است که تجهیزی که برنامه بر روی آن نصب می‌شود به‌صورت فیزیکی محافظت‌شده و در معرض حملات فیزیکی و خسارت‌های ناشی از آن‌ها قرار ندارد. فرض می‌شود که این محافظت برای تأمین امنیت داده‌های آن کافی است. درنتیجه، این پروفایل حفاظتی شامل هیچ الزامی درزمینه حفاظت فیزیکی و ابزارهای لازم برای کاستن از خسارت‌های ناشی از حملات فیزیکی نیست.

۲– A.LIMITED_FUNCTIONALITY: فرض بر این است که برنامه تنها قرار است نقش یک سرویس‌گیرنده ایمیل را به‌عنوان کارکرد اصلی خود ارائه دهد و سرویس‌های همه‌منظوره و غیر مرتبط با این نقش را ارائه نمی‌دهد.

۳– A.REGULAR_UPDATES: فرض بر این است که در صورت منتشر شدن به‌روزرسانی‌های جدید در پاسخ به آسیب‌پذیری‌های شناسایی‌شده، برنامه به‌صورت منظم به‌روزرسانی می‌شود.

فصل ۵– اهداف امنیتی (ASE_OBJ)

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

۵–۱–اهداف امنیتی برای سرویس‌گیرنده ایمیل

اهداف امنیتی در نظر گرفته‌شده برای سرویس‌گیرنده‌ی ایمیل به شرح زیر است. قابل‌ذکر است که در ابتدای فصل ۶ به کمک یک جدول نگاشت، ارتباط میان این اهداف و الزامات در نظر گرفته‌شده برای تحقق آن‌ها ذکرشده است.

۱- O.ADDON_INTEGRITY: برای مقابله با افزونه‌های آلوده باید صحت و اصالت آن‌ها چه در زمان نصب و چه به‌روزرسانی بررسی و تضمین شود.

۲- O.ACCESS_CONTROL: سرویس‌گیرنده‌ی 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.

۳- 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 کانال استفاده شود.

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

۵- O.FUNTIONALITY_ASSURANCE: سرویس‌گیرنده ایمیل باید از سلامت کارکردهای امنیتی خود اطمینان حاصل کند.

۶- O.STORED_DATA_SECURITY: سرویس‌گیرنده باید قادر به محافظت از اطلاعات امنیتی ذخیره‌شده روی آن مانند نام کاربری و رمز عبور کاربر، کلیدهای رمزنگاری عمومی و خصوصی و گواهینامه‌های X.509 بوده و کاربر را مجبور به تعیین رمز عبورهای امن کند.

۷- O.PLATFRORM_DATA_ACCESS_CONTROL: سطح دسترسی برنامه‌ی سرویس‌دهنده ایمیل به داده‌های پلتفرم مربوطه باید کنترل‌شده و از دسترسی‌های غیرضروری تا حد امکان جلوگیری شود.

۸- O.UPDATE_SECURITY: برای حفظ آمادگی در جلوگیری از حملات جدید، برنامه‌ی سرویس‌گیرنده باید به‌صورت مرتب به‌روزرسانی شود. اما پیش از به‌روزرسانی باید اصالت محتوا و نیز مبدأ انجام گیرنده آن تأیید هویت شوند. در غیر این صورت احتمال آلوده شدن و نفوذ مهاجمین بالا خواهد بود.

۹- O.ACTION_MONITORING: تولید و ثبت رکوردهای ممیزی از فعالیت‌های انجام‌گرفته کمک شایانی در شناسایی خطاهای موجود و تولید گزارش می‌کند.

۵-۲-اهداف امنیتی برای محیط عملیاتی

۱- OE.PHYSICAL_PROTECTION: امنیت فیزیکی تجهیزی که برنامه بر روی آن نصب‌شده و داده‌هایی که در آن قرار دارند، توسط محیط باید تضمین شود.

۲- OE.NO_GENERAL_PURPOSE: به‌جز کارکرد اصلی که ارائه سرویس‌های ذکرشده برای سرویس‌گیرنده ایمیل است، سرویس جانبی دیگری ارائه نمی‌شود.

۳- OE.REGULAR_UPDATE_CHECKING: برنامه باید به‌طور منظم به‌روزرسانی شوند.

۵-۳-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.

۵-۳-۱-نگاشت اهداف امنیتی به مسئله امنیت

در **جدول** .Error! No text of specified style in document-۱، محور افقی اهداف امنیتی در نظر گرفته‌شده برای ... 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 .Error! No text of specified style in document-**۱ نگاشت تهدیدات/دارایی‌ها/سیاست‌های سازمان به اهداف امنیتی/محیط عملیات**

	O.ADDON_INTEGRITY	O.ACCESS_CONTROL	O.CONNECTION_SECURITY	O.EMAIL_CONTENT_SECURITY	O.FUNTIONALITY_ASSURANCE	O.STORED_DATA_SECURITY	O.PLATFRORM_DATA_ACCESS_CONTROL	O.UPDATE_SECURITY	O.ACTION_MONITORING	OE.PHYSICAL_DEVICE_PROTECTION	OE.NO_GENERAL_PURPOSE	OE.REGULAR_UPDATE_CHECKING
T.FLAWED_ADDON	✓											
T.UNAUTHORIZED_ADMINISTRATIVE_ACCESS		✓										
T.CHANNEL_EAVESDROP_AND_MANIPULATION			✓									
T.EMAIL_CONTENT_EAVESDROP_AND_MODIFICATION				✓								
T.SECURITY_FUNCTIONALITY_FAILURE_EXPLOIT					✓							
T.ATTACK_ON_STORED_CREDENTIALS						✓						
T. UNAUTHORIZED_PLATFRORM_DATA_ACCESS							✓					
T.MALICIOUS_UPDATE								✓				
T.UNDETECTED_ACTIVITIES									✓			
OSP.ACCESS_BANNER		✓										
A.PHYSICAL_PROTECTION										✓		
A.LIMITED_FUNCTIONALITY											✓	
A.REGULAR_UPDATES												✓

۲-۳-۵-استدلال نگاشت‌ها به اهداف امنیتی

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

۱-۲-۳-۵-نگاشت تهدیدات

همچنان که در جدول نگاشت نشان داده شد، برای مقابله با تهدیدات اهداف مختلفی در نظر گرفته‌شده است. هر تهدید یا حذف کامل می‌شود یا به‌وسیله کاهش انگیزه مهاجم یا ایجاد محدودیت برای او، به‌اندازه کافی تقلیل پیدا می‌کند. قابل‌ذکر است که رسیدن به اهداف امنیتی مربوطه نیز با رعایت الزامات کارکردی امنیتی محقق می‌شود که نگاشت آن در همان بخش اهداف برای هر یک ذکر شد و توضیحات کامل این الزامات کارکردی-امنیتی نیز در بخش بعد آورده شده است.

۱- T.FLAWED_ADDON:

این تهدید از طریق هدف O.ADDON_INTEGRITY و بررسی اصالت و صحت افزونه‌ها برطرف می‌شود.

۲- T.UNAUTHORIZED_ADMINISTRATIVE_ACCESS:

هدف O.ACCESS_CONTROL از طریق مجموعه الزامات مربوطه، راه را برای دسترسی غیرمجاز به برنامه می‌بندد.

۳- T.CONNECTION_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.

۴- T.EMAIL_CONTENT_EAVESDROP_AND_MODIFICATION:

هدف O.EMAIL_CONTENT_SECURITY از طریق الزام به استفاده از S/MIME و اجرای رمزنگاری اطمینان می‌دهد که محتوای ایمیل‌ها هرگز افشا نخواهد شد حتی اگر کانال‌های ارتباطی در مسیرِ ارسالِ ایمیل به مقصد شنود شوند.

۵- T. FUNTIONALITY_FAILURE_ EXPLOIT:

این تهدید با هدف نگاشت‌شده در جدول فوق از طریق انجام تست خودکار و اطمینان از کارکرد توابع امنیتی رفع می‌شود.

۶- T.ATTACK_ON_STORED_CREDENTIALS:

هدف STORED_DATA_SECURITY به ارائه سیاست‌ها و مکانیزم‌های امن برای ذخیره و نگهداری اطلاعات محرمانه اختصاص دارد.

۷- T. UNAUTHORIZED_PLATFRORM_DATA_ACCESS:

این تهدید به کمک هدف O.PLATFRORM_DATA_ACCESS_CONTROL رفع خواهد شد.

۸- T.MALICIOUS_UPDATE:

هدف UPDATE_SECURITY به تأییدِ صحتِ به‌روزرسانی‌ها ارتباط دارد.

۹- T.UNDETECTED_ACTIVITIES:

هدف ACTION_MONITORING به تهیه رکوردهای ممیزی از رخدادهای مهم ارتباط دارد.

۲-۲-۳-۵- نگاشت سیاست‌های امنیتی سازمان

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

۳-۲-۳-۵-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_ PROTECTION خواهد بود و فرض بر این است که امنیت فیزیکی توسط محیط تأمین خواهد شد.

۲- A.LIMITED_FUNCTIONALITY:

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

۳- A.REGULAR_UPDATES:

این فرض به هدف OE.REGULAR_UPDATE_CHECKING نگاشت شده و تضمین می‌دهد که سرویس‌گیرنده ایمیل به‌طور مرتب به‌روزرسانی خواهد شد.

فصل ۶- 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 سرویس‌گیرنده 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 سرویس‌گیرنده 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.

جدول ۶-۱ نگاشت میان الزامات کارکردی امنیتی و اهداف امنیتی ذکرشده را نشان می‌دهد. این الزامات تحقق اهداف مربوطه را تضمین خواهند کرد.

جدول .Error! No text of specified style in document-**۲ نگاشت میان الزامات و اهداف**

ردیف	الزام	هدف
۱	FAU_GEN.1.1	O.ACTION_MONITORING
۲	FAU_GEN.1.2	O.ACTION_MONITORING
۳	FAU_GEN.2	O.ACTION_MONITORING
۴	FCS_CKM_EXT.1.1	O.EMAIL_CONTENT_SECURITY O.CONNECTION_SECURITY O.UPDATE_SECURITY O.STORED_DATA_SECURITY
۵	FCS_CKM_EXT.3.1	O.EMAIL_CONTENT_SECURITY O.CONNECTION_SECURITY O.UPDATE_SECURITY O.STORED_DATA_SECURITY

ردیف	الزام	هدف
۶	FCS_CKM_EXT.4.1	O.EMAIL_CONTENT_SECURITY O.CONNECTION_SECURITY O.UPDATE_SECURITY O.STORED_DATA_SECURITY
۷	FCS_KYC_EXT.1.1	O.STORED_DATA_SECURITY
۸	FCS_RBG_EXT.3.1	O.EMAIL_CONTENT_SECURITY O.CONNECTION_SECURITY O.UPDATE_SECURITY O.STORED_DATA_SECURITY
۹	FCS_STO_EXT.1.1	O.STORED_DATA_SECURITY
۱۰	FCS_SMIME_EXT.1.1	O.EMAIL_CONTENT_SECURITY
۱۱	FCS_SMIME_EXT.1.2	O.EMAIL_CONTENT_SECURITY
۱۲	FCS_SMIME_EXT.1.3	O.EMAIL_CONTENT_SECURITY
۱۳	FCS_SMIME_EXT.1.4	O.EMAIL_CONTENT_SECURITY
۱۴	FCS_SMIME_EXT.1.5	O.EMAIL_CONTENT_SECURITY
۱۵	FCS_SMIME_EXT.1.6	O.EMAIL_CONTENT_SECURITY
۱۶	FCS_SMIME_EXT.1.7	O.EMAIL_CONTENT_SECURITY
۱۷	FIA_X509_EXT.3.1	O.EMAIL_CONTENT_SECURITY
۱۸	FIA_X509_EXT.3.2	O.EMAIL_CONTENT_SECURITY
۱۹	FIA_X509_EXT.3.3	O.EMAIL_CONTENT_SECURITY
۲۰	FIA_X509_EXT.3.4	O.EMAIL_CONTENT_SECURITY
۲۱	FIA_X509_EXT.3.5	O.EMAIL_CONTENT_SECURITY
۲۲	FMT_MOF.1/ManualUpdate	O.UPDATE_SECURITY
۲۳	FMT_MTD.1/CoreData	O.ACCESS_CONTROL
۲۴	FMT_SMF.1	مرتبط با تمامی اهداف
۲۵	FMT_SMR.2.1	O.ACCESS_CONTROL
۲۶	FMT_SMR.2.2	O.ACCESS_CONTROL
۲۷	FPR_ANO_EXT.1.1	O.STORED_DATA_SECURITY
۲۸	FDP_DEC_EXT.1.1	O.STORED_DATA_SECURITY O.ACCESS_CONTROL

ردیف	الزام	هدف
۲۹	FDP_DEC_EXT.1.2	O.STORED_DATA_SECURITY O.ACCESS_CONTROL
۳۰	FDP_NET_EXT.1.1	O.STORED_DATA_SECURITY O.ACCESS_CONTROL
۳۱	FDP_DAR_EXT.1.1	O.STORED_DATA_SECURITY O.ACCESS_CONTROL
۳۲	FDP_NOT_EXT.1.1	O.EMAIL_CONTENT_SECURITY
۳۳	FDP_SMIME_EXT.1.1	O.EMAIL_CONTENT_SECURITY
۳۴	FPT_AON_EXT.1.1	O.ADDON_INTEGRITY
۳۵	FPT_API_EXT.1.1	O.STORED_DATA_SECURITY O.ACCESS_CONTROL
۳۶	FPT_AEX_EXT.1.1	O.STORED_DATA_SECURITY O.ACCESS_CONTROL O.PLATFRORM_DATA_ACCESS_CONTROL
۳۷	FPT_AEX_EXT.1.2	O.STORED_DATA_SECURITY O.ACCESS_CONTROL O.PLATFRORM_DATA_ACCESS_CONTROL
۳۸	FPT_AEX_EXT.1.3	O.STORED_DATA_SECURITY O.ACCESS_CONTROL O.PLATFRORM_DATA_ACCESS_CONTROL
۳۹	FPT_AEX_EXT.1.4	O.STORED_DATA_SECURITY O.ACCESS_CONTROL O.PLATFRORM_DATA_ACCESS_CONTROL
۴۰	FPT_AEX_EXT.1.5	O.STORED_DATA_SECURITY O.ACCESS_CONTROL O.PLATFRORM_DATA_ACCESS_CONTROL
۴۱	FPT_LIB_EXT.1.1	O.STORED_DATA_SECURITY O.ACCESS_CONTROL O.PLATFRORM_DATA_ACCESS_CONTROL
۴۲	FPT_SKP_EXT.1.1	O.STORED_DATA_SECURITY
۴۳	FPT_APW_EXT.1.1	O.STORED_DATA_SECURITY
۴۴	FPT_APW_EXT.1.2	O.STORED_DATA_SECURITY

ردیف	الزام	هدف
۴۵	FPT_TST_EXT.1	O.FUNTIONALITY_ASSURANCE
۴۶	FPT_TUD_EXT.1.1	O.UPDATE_SECURITY
۴۷	FPT_TUD_EXT.1.2	O.UPDATE_SECURITY
۴۸	FPT_TUD_EXT.1.3	O.UPDATE_SECURITY
۴۹	FPT_TUD_EXT.1.4	O.UPDATE_SECURITY
۵۰	FPT_TUD_EXT.1.5	O.UPDATE_SECURITY
۵۱	FPT_IDV_EXT.1.1	O.ACCESS_CONTROL O.UPDATE_SECURITY
۵۲	FPT_STM_EXT.1.1	O.ACTION_MONITORING
۵۳	FPT_STM_EXT.1.2	O.ACTION_MONITORING
۵۴	FTP_ITC_EXT.1.1	O.CONNECTION_SECURITY
۵۵	FTP_ITC_EXT.1.2	O.CONNECTION_SECURITY
۵۶	FTP_ITC.1.1	O.CONNECTION_SECURITY
۵۷	FTP_ITC.1.2	O.CONNECTION_SECURITY
۵۸	FTP_ITC.1.3	O.CONNECTION_SECURITY
۵۹	FCS_TLSC_EXT.1.1	O.CONNECTION_SECURITY
۶۰	FCS_TLSC_EXT.1.2	O.CONNECTION_SECURITY
۶۱	FCS_TLSC_EXT.1.3	O.CONNECTION_SECURITY
۶۲	FCS_TLSC_EXT.1.4	O.CONNECTION_SECURITY
۶۳	FCS_TLSC_EXT.1.5	O.CONNECTION_SECURITY
۶۴	FCS_TLSS_EXT.1.1	O.CONNECTION_SECURITY
۶۵	FCS_TLSS_EXT.1.2	O.CONNECTION_SECURITY
۶۶	FCS_TLSS_EXT.1.3	O.CONNECTION_SECURITY
۶۷	FCS_TLSS_EXT.1.4	O.CONNECTION_SECURITY
۶۸	FCS_TLSS_EXT.1.5	O.CONNECTION_SECURITY
۶۹	FCS_TLSS_EXT.1.6	O.CONNECTION_SECURITY
۷۰	FIA_X509_EXT.1.1/Rev	O.EMAIL_CONTENT_SECURITY O.CONNECTION_SECURITY O.UPDATE_SECURITY

ردیف	الزام	هدف
		O.ADDON_INTEGRITY
۷۱	FIA_X509_EXT.1.2/Rev	O.EMAIL_CONTENT_SECURITY O.CONNECTION_SECURITY O.UPDATE_SECURITY O.ADDON_INTEGRITY
۷۲	FIA_X509_EXT.2.1	O.EMAIL_CONTENT_SECURITY O.CONNECTION_SECURITY O.UPDATE_SECURITY O.ADDON_INTEGRITY
۷۳	FIA_X509_EXT.2.2	O.EMAIL_CONTENT_SECURITY O.CONNECTION_SECURITY O.UPDATE_SECURITY O.ADDON_INTEGRITY
۷۴	FIA_X509_EXT.3.1	O.EMAIL_CONTENT_SECURITY O.CONNECTION_SECURITY O.UPDATE_SECURITY O.ADDON_INTEGRITY
۷۵	FIA_X509_EXT.3.2	O.EMAIL_CONTENT_SECURITY O.CONNECTION_SECURITY O.UPDATE_SECURITY O.ADDON_INTEGRITY

۱-۶-کلاس ثبت رکورد ممیزی

ثبت رکورد ممیزی از رویدادهای دارای اهمیت نقش مهمی در شناسایی و مقابله با تهدیدات مختلف دارد. پروفایل‌های حفاظتی مرجع برای سرویس‌گیرنده‌ی ایمیل از بیان الزامات برای ثبت رکورد ممیزی اجتناب کرده‌اند اما در این سند، با توجه به اهمیت این کلاس از بعد امنیتی، به‌صورت محدود به موارد قابل التفات اشاره‌شده است. به‌عبارتی‌دیگر، با اینکه برای کارکردِ سرویس‌گیرنده در سرویس ایمیل و محدودیت‌های آن در مقایسه با سرویس‌گیرنده‌ی ایمیل نمی‌توان انتظار ثبت رکورد ممیزی در مقیاس و جزییات متناظر را داشت ولی انتظار می‌رود تا برنامه‌ی سرویس‌گیرنده‌ی ایمیل قادر به ثبت آن در سطح خود باشد.

شماره الزام	نام الزام

۱	تولید داده ممیزی ۱,۱ (FAU_GEN.1.1)
سرویس‌گیرنده‌ی 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 اقدامات مدیریتی شامل موارد زیر: ▪ ورود و خروج مدیریتی به برنامه ▪ 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.	
۲	تولید داده ممیزی ۱,۲ (FAU_GEN.1.2)
در هر رکورد ممیزی دست‌کم اطلاعات زیر باید ذخیره شود: ❖ تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت انجام‌گیرنده رویداد و نتیجه رویداد (موفقیت یا شکست)	
۳	تولید داده ممیزی ۲ (FAU_GEN.2)
سرویس‌گیرنده‌ی ایمیل باید بتواند رویداد قابل ممیزی را با درج هویت انجام گیرنده آن ثبت کند.	

۲-۶-کلاس پشتیبانی از رمزنگاری

در این بخش الزامات پایه‌ای مرتبط با رمزنگاری به همراهِ الزامات پروتکل S/MIME شرح داده خواهند شد. بااین‌حال برای پیاده‌سازی الزامات پایه دو گزینه وجود دارد: ۱- برنامه‌ی سرویس‌گیرنده‌ی ایمیل خود این عملکردها را پیاده‌سازی می‌کند. ۲- پلتفرمی که برنامه بر روی آن نصب‌شده است این عملکردها

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

را پیاده‌سازی کرده و برنامه‌ی سرویس‌گیرنده‌ی ایمیل تنها از این سرویس‌ها استفاده می‌کند. لذا در عمده‌ی الزامات این بخش امکان انتخاب میان دو گزینه‌ی فوق فراهم است. در خصوص هر عملکرد، درصورتی‌که برنامه خود آن را پیاده‌سازی می‌کند، لازم است تا از بخش الزامات انتخابی، الزامات مربوطه نیز پیاده‌سازی شوند. به‌طور کل لازم است تا سازنده محصول زیر بخش «الزامات پایه رمزنگاری» از فصلِ الزامات انتخابی را چک کند تا از فراهم بودن یا پیاده‌سازی تمامی آن‌ها اطمینان حاصل شود.

الزامات پایه‌ای شامل تولید کلید و بیت تصادفی، روش‌های استقرار کلید[1]، از بین بردن کلید، روش‌های مختلف رمزنگاری برای پیاده‌سازی رمزنگاری/رمزگشایی AES، تأیید و تصدیق امضای دیجیتال و نیز روش‌های ساده یا مبتنی بر کلید برای درهم‌سازی است.

*** توجه شود که الزامات و الگوریتم‌های ذکرشده برای الزامات پایه با پروتکل‌های رمزنگاری مانند TLS و S/MIME مرتبط است و انتخاب‌های این بخش باید با مجموعه‌های رمز انتخابی برای پروتکل‌های مذکور متناسب باشند.

شماره الزام	نام الزام
۴	سرویس تولید کلید رمزنگاری ۱ (FCS_CKM_EXT.1.1)
برای تولید کلیدهای رمزنگاری، سرویس‌گیرنده ایمیل باید [انتخاب: از روش مبتنی بر رمزنگاری نامتقارن که توسط پلتفرم فراهم‌شده است استفاده کند، تولید کلید بر اساس رمزنگاری نامتقارن را پیاده‌سازی کند] نکات کاربردی: درصورتی‌که برنامه‌ی سرویس‌گیرنده ایمیل خود الگوریتم‌های تولید کلید را پیاده‌سازی کند، آنگاه باید الزام FCS_CKM.1 نیز از بخش الزامات انتخابی پیاده‌سازی شود.	
۵	محافظت از کلید و سازنده‌ی کلید ۱ (FCS_CKM_EXT.3.1)
سرویس‌گیرنده ایمیل باید: [انتخاب: • از ذخیره کلیدها در حافظه‌های غیرموقتی پرهیز کند، • تنها در صورتی یک کلید را در یک حافظه دائمی ذخیره کند که با رعایت الزامِ انتخابیِ FCS_COP_EXT.2 به لحاظ امنیتی آن را پوشش دهد، مگر اینکه کلید مربوطه حداقل یکی از	

[1] Key Establishment Methods

شرایط زیر را داشته باشد تا به‌صورت متن-ساده ذخیره گردد: [انتخاب:

- کلید مربوطه جزئی از زنجیره‌ی کلید که تعریف آن در الزام FCS_KYC_EXT.1 ارائه‌شده است نباشد،
- کلید مربوطه دیگر امکان دسترسی مجدد به داده‌ی رمز شده پس از رمزنگاری اولیه نمی‌دهد.
- کلید مربوطه یک‌نیمه از یک کلید بزرگ‌تر است که مطابق با الزام FCS_SMC_EXT.1 ساخته‌شده است و بخش دوم از کلید [انتخاب: مطابق با الزام FCS_COP_EXT.2 پوشش داده‌شده است، استخراج‌شده و در حافظه غیر-موقتی ذخیره نشده است]
- حافظه‌ی مربوطه یک حافظه خارجی امن هست که خود از کلیدها مراقبت می‌کند و دسترسی غیرِ امن به آن وجود ندارد.
- کلید مربوطه برای پوششِ بیشترِ کلید دیگری (مطابق با FCS_COP_EXT.2) استفاده می‌شود که خود قبلاً مطابق با رعایت الزام FCS_COP_EXT.2 پوشش داده‌شده است.
- کلید مربوطه جفتِ عمومی از جفت کلید عمومی/خصوصی است.

]

[

نکات کاربردی:

✓ بسته به انتخاب، الزامات FCS_COP_EXT.2 و FCS_SMC_EXT.1 باید رعایت شوند.

۶	سرویس نابودسازی کلید رمزنگاری ۱ (FCS_CKM_EXT.4.1)

سرویس‌گیرنده ایمیل باید: [انتخاب:

- از عملکردهای امنیتی پیاده‌سازی شده توسط پلتفرم برای نابودسازی کلیدهای رمزنگاری استفاده کند،
- روش‌ها و الگوریتم‌های لازم برای نابودسازی کلید را خود پیاده‌سازی کند.

]

نکات کاربردی:

✓ در صورت پیاده‌سازی باید الزام FCS_CKM.4.1 از بخش الزامات انتخابی پیاده‌سازی شود.

۷	زنجیره سازی از کلید ۱ (FCS_KYC_EXT.1.1)

سرویس‌گیرنده ایمیل باید یک زنجیره‌ی کلید از [انتخاب:

- یک،

- یک کلید ذخیره‌شده در platform key storage
- کلیدهای میانی نشأت گرفته از [انتخاب:
- یک رمز عبور (همچنان که در الزام انتخابی FCS_CKM_EXT.5 شرایط آن ذکرشده است)
- یک یا تعداد بیشتری از دیگر فاکتورهای مجوزدهی (authorization factor)
- Credentialهای ذخیره‌شده در platform key storage

[

به کلیدهای رمزنگاری/رمزگشایی با استفاده از روش(های) مقابل را نگهداری کند [انتخاب:

- استفاده از platform key storage
- استفاده از platform key storage که عملیات key wrap را با استفاده از یک کلید فراهم‌شده توسط محصول انجام می‌دهد.
- پیاده‌سازی عملکرد key wrap مطابق با الزام FCS_COP_EXT.2
- پیاده‌سازی عملکرد key combining مطابق با الزام FCS_SMC_EXT.1

[

و درعین‌حال، قدرت کلید در اندازه‌ی [انتخاب:۱۲۸ بیتی، ۲۵۶ بیتی] حفظ شود.

نکات کاربردی:

- ✓ بااینکه سند مرجع [5] توضیحات چندانی ارائه نکرده است، اما به نظر، مقصود از این الزام پیاده‌سازی سیستمی مشابه با Apple Key Chain است. چنین سیستمی درعین‌حال که امکان لاگینِ اتوماتیک در برنامه‌ی سرویس‌گیرنده ایمیل بعد از لاگین کردن در سیستم (کامپیوتر، گوشی و ...) را می‌دهد، امکان محافظت از رمز عبورها، گواهینامه‌های X.509 و دیگر رکوردهای مجوزدهی و لاگین کردن را با استفاده از تکنیک‌هایی چون key wrapping فراهم می‌کند.
- ✓ بسته به انتخاب‌های انجام‌گرفته، پیاده‌سازی الزاماتِ انتخابیِ FCS_CKM_EXT.5، FCS_COP_EXT.2 و FCS_SMC_EXT.1 نیاز خواهد بود.

۸	سرویس تولید بیت تصادفی ۳,۱ (FCS_RBG_EXT.3.1)

برای تولید بیت تصادفی جهت استفاده در عملیات رمزنگاری، سرویس‌گیرنده ایمیل باید [انتخاب: از تابع DRGB که توسط پلتفرم پیاده‌سازی شده است استفاده کند، الگوریتم DRGB را خود پیاده‌سازی کند]

نکات کاربردی:

درصورتی‌که برنامه‌ی سرویس‌گیرنده ایمیل خود الگوریتم DRGB را پیاده‌سازی می‌کند، آنگاه باید الزامات FCS_RBG_EXT.1&2 نیز از بخش الزامات انتخابی پیاده‌سازی شوند.

۹	ذخیره‌سازی مؤلفه‌های محرمانه ۱ (FCS_STO_EXT.1.1)
سرویس‌گیرنده ایمیل باید: [انتخاب: • هیچ مؤلفه‌ی محرمانه‌ای را ذخیره نکند، • از عملکردهای امنیتی پیاده‌سازی شده توسط پلتفرم برای ذخیره‌ی امنِ [اختصاص: لیستی از مؤلفه‌های محرمانه] استفاده کند. • عملکردهای امنیتی لازم برای ذخیره امنِ [اختصاص: لیستی از مؤلفه‌های محرمانه] را بر اساس الزامات FCS_COP.1 و FCS_CKM.1 پیاده‌سازی کند.] نکات کاربردی: ✓ منظور از مؤلفه‌های محرمانه در این الزام عبارت است از هرگونه کلید محرمانه/خصوصی و رمز عبور دائمی (و نه موقتی). ✓ برای قسمت [اختصاص]، نویسنده‌ی سند هدف امنیتی باید لیستی از مؤلفه‌های محرمانه که برای ذخیره‌سازی در نظر گرفته می‌شود را ذکر کند.	

۱-۲-۶-الزامات پروتکل S/MIME

۱۰	S/MIME ۱ (FCS_SMIME_EXT.1.1)
سرویس‌گیرنده ایمیل باید نسخه ۴ از S/MIME Agent را مطابق با RFC 8551 و برای هر دو نقشِ فرستنده و گیرنده پیاده‌سازی کند. بدین منظور باید از چارچوب CMS (Cryptographic Message Syntax) که در اسناد RFC با شماره‌های ۵۶۵۲، ۵۷۵۴ و ۳۵۶۵ تعریف‌شده است استفاده شود.	
۱۱	S/MIME 2 (FCS_SMIME_EXT.1.2)
برای رمزنگاری محتوا باید از الگوریتم‌های AES-256 CBC , AES-128 CBC و [انتخاب: AES-256 GCM , AES-128 GCM، هیچ الگوریتم دیگری] پشتیبانی شود و فیلد Content Encryption Algorithm Identifier همواره ست شده باشد. نکات کاربردی: ✓ RFC 3565 چگونگیِ استفاده از الگوریتم AES برای رمزنگاری در چارچوب CMS را شرح می-دهد.	
۱۲	S/MIME 3 (FCS_SMIME_EXT.1.3)

فیلد digest Algorithm از پروتکل S/MIME باید همواره به‌وسیله‌ی یکی از شناسه‌های مقابل برای تعیین الگوریتمِ محاسبه‌ی چکیده‌ی پیام: [انتخاب: id-sha256، id-sha384، id-sha512] مقداردهی شود.	
۱۳	(FCS_SMIME_EXT.1.4) 4 S/MIME
برای فیلد signature Algorithm پشتیبانی از sha256 with RSA Encryption الزامی است. همچنین علاوه بر آن امکان انتخاب از الگوریتم‌های زیر فراهم است: [انتخاب: sha384 With RSA Encryption، sha512 With RSA Encryption، ecdsa with sha256، ecdsa with sha384، ecdsa with sha512]	
۱۴	(FCS_SMIME_EXT.1.5) 5 S/MIME
سرویس‌گیرنده‌ی ایمیل باید از انواع کلیدهای محرمانه (private keys) و گواهینامه‌های متناظر (certificates) برای انجام امضا و رمزنگاری پشتیبانی کند.	
۱۵	(FCS_SMIME_EXT.1.6) 6 S/MIME
پذیرش امضا باید تنها منوط به ست بودنِ بیتِ digital Signature از گواهینامه باشد. نکات کاربردی: ✓ در حالتی که افزونه‌ی key Usage موجود نباشد، می‌توان ست بودنِ بیت digital Signature را به‌صورت فرضی پذیرفت.	
۱۶	(FCS_SMIME_EXT.1.7) 7 S/MIME
سرویس‌گیرنده‌ی ایمیل باید از مکانیزم مشخصی برای دسترسی به گواهینامه‌ها یا لیست certificate revocation استفاده کند. نکات کاربردی: ✓ دسترسی به گواهینامه‌ی طرف مقابل در پروتکل S/MIME یک امر ضروری و درعین‌حال چالش زا برای اجرای این پروتکل است. باوجود معرفی پروتکل DANE برای این کار، استفاده از آن هنوز فراگیر نشده و با چالش‌هایی همراه است. لذا در این سند پشتیبانی از آن اختیاری در نظر	

گرفته‌شده است. از روش‌های جایگزین می‌توان به استفاده از Online Certificate Status Protocol جهت دسترسی آنلاین به گواهینامه‌ها از طریق سرورهای مربوطه و یا استفاده از لیست certificate revocation و به‌روزرسانی دائمی آن اشاره کرد. به‌روزرسانی لیست به‌صورت دوره‌ای و اتوماتیک و هم در حالت ابتدایی‌تر به‌صورت دستی قابل انجام است.

۳-۶-کلاس شناسایی و احراز هویت

۱-۳-۶-الزامات گواهینامه‌های X.509 برای S/MIME

شماره الزام	نام الزام
۱۷	الزامات گواهینامه‌های S/MIME /X.509 (۱) (FIA_X509_EXT.3.1)
به‌منظور اجرای عملیات رمزنگاری و احراز هویت در پروتکل S/MIME، سرویس‌گیرنده‌ی ایمیل باید از گواهینامه‌های X.509v3 مطابق با RFC 5280 پشتیبانی کند.	
۱۸	الزامات گواهینامه‌های S/MIME /X.509 (۲) (FIA_X509_EXT.3.2)
در صورت نامعتبر تشخیص دادنِ گواهینامه‌ی طرف مقابل باید از تشکیل کانال و تلاش برای ارتباط پرهیز شود.	
۱۹	الزامات گواهینامه‌های S/MIME /X.509 (۳) (FIA_X509_EXT.3.3)
در صورت نامعتبر تشخیص دادنِ گواهینامه‌ی امضای کد[۱] باید از نصب کردن کد پرهیز شود[۲].	
۲۰	الزامات گواهینامه‌های S/MIME /X.509 (۴) (FIA_X509_EXT.3.4)
در صورت نامعتبر تشخیص دادنِ گواهینامه‌ی طرف مقابل باید از رمز کردن ایمیلِ ارسالی پرهیز شود.	
۲۱	الزامات گواهینامه‌های S/MIME /X.509 (۵) (FIA_X509_EXT.3.5)
در صورت نامعتبر تشخیص دادنِ گواهینامه‌ی طرف مقابل باید از امضا کردنِ ایمیلِ ارسالی پرهیز شود.	

۴-۶-کلاس مدیریت امنیت

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

[۱] Code signing certificate

[۲] Prevent the installation of code

- 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 سرپرست 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
۲۲	مدیریت کارکرد امنیتی ۱/ به‌روزرسانی دستی (FMT_MOF.1/ManualUpdate)
برنامه‌ی سرویس‌گیرنده ایمیل باید امکان استفاده از توابع به‌روزرسانی دستی را به سرپرست امنیتی محدود کند. نکات کاربردی: ✓ کارکرد این الزام از آنجایی است که سرویس‌گیرنده‌ی ایمیل می‌تواند امکان تعریف نقش‌های مختلف با دسترسی‌های متفاوت را فراهم کند. در چنین حالتی تنها نقش سرپرست یا administrator باید امکان پیکربندی و به‌روزرسانی دستی برنامه‌ی سرویس‌گیرنده را داشته باشد. ✓ این الزام امکان آغاز به‌روزرسانی دستی را به سرپرست سرویس‌گیرنده‌ی ایمیل محدود می‌کند.	
۲۳	مدیریت دسترسی به داده‌ها ۱ (FMT_MTD.1/CoreData)
سرویس‌گیرنده‌ی ایمیل باید امکان «مدیریت» داده‌های امنیتی، مانند اطلاعات پیکربندی را به سرپرست 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[1] رمز عبور کاربر به حالت پیش‌فرض توسط سرپرست سرویس‌گیرنده‌ی ایمیل است. ✓ عبارت"CoreData" در نام این الزام برای جداسازی آن با الزام ذکرشده در قسمت الزامات اختیاری با نام FMT_MTD.1/CryptoKeys است.
۲۴ | تعریف کارکردهای امنیتی ۱ (FMT_SMF.1)
سرویس‌گیرنده‌ی ایمیل باید امکانات و توابع مدیریتی زیر را ارائه کند: • فعال/غیرفعال کردنِ دانلودِ Object های تعبیه‌شده در ایمیل به‌صورت سراسری و بر اساس [انتخاب: دامنه، ارسال‌کننده، هیچ موردی] • فعال/غیرفعال کردنِ مد plaintext-only به‌صورت سراسری و بر اساس [انتخاب: دامنه، ارسال‌کننده، هیچ موردی] • فعال/غیرفعال کردنِ پردازش و اجرای ضمیمه‌ها به‌صورت سرا سری و بر اساس [انتخاب: دامنه، ارسال‌کننده، هیچ موردی] • فعال/غیرفعال کردنِ اعلان‌ها (email notifications) • پیکربندی کردنِ یک مرجعِ گواهینامه (certificate repository) برای رمزنگاری • فعال/غیرفعال کردنِ امکان تشکیل کانال زمانی که سرویس‌گیرنده ایمیل قادر به برقراری ارتباط جهت اعتبار سنجی گواهینامه نباشد. • فعال/غیرفعال کردنِ حالت استفاده از رمزنگاری S/MIME برای ایمیل‌های ورودی/خروجی • پیکربندی پارامترِ CRL retrieval frequency • فعال/غیرفعال کردنِ امکان پشتیبانی از افزونه‌ها • تغییر کلمه/عبارت ورود[2] • فعال/غیرفعال کردن امکان بازیابی کلید

[1] Reset

[2] Password/Passphrase authentication credential

• پیکربندی عملکردها و پارامترهای رمزنگاری • [اختصاص: لیستی از دیگر موارد قابل پیکربندی] نکات کاربردی: ✓ عملکردهای مذکور باید محدود به نقش سرپرست باشد.

۲۵	مدیریت نقش‌های امنیتی ۱ (FMT_SMR.2.1)
سرویس‌گیرنده ایمیل باید حداقل نقش امنیتی زیر را فراهم کند: • سرپرست امنیتی نکات کاربردی: ✓ مقصود از نقش سرپرست امنیتی، نقشی است که از تمامی دسترسی‌های لازم برخوردار باشد. ✓ در حالت پیشرفته می‌توان سطوح مختلف از دسترسی را برای سرپرستان و کاربران عادی تعریف کرد ولی این سند چنین امکانی را برای برنامه‌ی سرویس‌گیرنده‌ی ایمیل الزام نمی‌کند و این امر اختیاری است.	
۲۶	مدیریت نقش‌های امنیتی ۲ (FMT_SMR.2.2)
سرویس‌گیرنده‌ی ایمیل باید بتواند برای کاربران تعریف‌شده نقش تعیین کند.	

۵-۶-کلاس محرمانگی

شماره الزام	نام الزام
۲۷	رضایت کاربر برای انتقال اطلاعات قابل‌تشخیص هویتی (FPR_ANO_EXT.1.1)
برنامه‌ی سرویس‌گیرنده‌ی ایمیل باید: [انتخاب: • اجازه انتقال اطلاعات هویتی (PII[1]) در بستر شبکه را ندهد، • برای [اختصاص: لیست توابع و عملکردهایی که اطلاعات هویتی را در بستر شبکه انتقال می-دهند] درخواست تأییدیه از کاربر کند	

[1] Personal Identifiable Information

[

۶-۶-کلاس محافظت از داده‌های کاربر و پلتفرم

شماره الزام	نام الزام
۲۸	دسترسی به منابعِ پلتفرم ۱ (FDP_DEC_EXT.1.1)

دسترسی برنامه‌ی سرویس‌گیرنده‌ی ایمیل محدود به منابع زیر از پلتفرم است:

[انتخاب:

- هیچ منبع سخت‌افزاری
- اتصال شبکه
- دوربین
- میکروفن
- سرویس مکان‌یابی
- NFC
- USB
- Bluetooth
- [اختصاص: لیستی از دیگر منابع سخت‌افزاری]

]

نکات کاربردی:

✓ برنامه سرویس‌گیرنده‌ی ایمیل می‌تواند به هیچ، یک یا چند مورد از منابع سخت‌افزاری فوق دسترسی داشته باشد. ضمن مشخص کردن این موارد، علت دسترسی نیز باید شرح داده شود.

شماره الزام	نام الزام
۲۹	دسترسی به منابعِ پلتفرم ۲ (FDP_DEC_EXT.1.2)

دسترسی برنامه‌ی سرویس‌گیرنده‌ی ایمیل محدود به منابع اطلاعاتی زیر از پلتفرم است:

[انتخاب:

- هیچ منبعی از اطلاعات حساس
- Address book
- تقویم
- لیست تماس و مخاطبین
- لاگ‌های سیستمی

- [اختصاص: لیستی از دیگر منابع حاوی اطلاعات حساس]

]

نکات کاربردی:

✓ برنامه سرویس‌گیرنده‌ی ایمیل می‌تواند به هیچ، یک یا چند مورد از منابع فوق دسترسی داشته باشد. ضمن مشخص کردن این موارد، علت دسترسی نیز باید شرح داده شود.

۳۰	ارتباطات شبکه ۱ (FDP_NET_EXT.1.1)

دسترسی برنامه‌ی سرویس‌گیرنده‌ی ایمیل به ارتباطات شبکه محدود به موارد زیر است:

[انتخاب:

- هیچ ارتباط شبکه‌ای
- اتصالات آغازشده توسط کاربر برای [اختصاص: لیستی از توابع و عملکردها که کاربر می‌تواند برای آن‌ها ارتباط شبکه‌ای آغاز کند.]
- پاسخ به [اختصاص: لیستی از ارتباطات شبکه‌ای قابل شروع از سمت مقابل]
- [اختصاص: لیستی از ارتباطات شبکه‌ای قابلِ شروع توسط برنامه‌ی سرویس‌گیرنده‌ی ایمیل]

]

۳۱	رمزنگاری اطلاعات حساس برنامه سرویس‌گیرنده ایمیل ۱ (FDP_DAR_EXT.1.1)

این الزامِ عمومی برای برنامه‌های نرم‌افزاری توسط الزامات اختصاصی «ذخیره‌سازی مؤلفه‌های محرمانه ۱» و «محافظت از کلید و سازنده‌ی کلید» تأمین‌شده و در این سند، حذف شده است.

۳۲	اطلاع‌رسانی از وضعیت S/MIME ۱ (FDP_NOT_EXT.1.1)

سرویس‌گیرنده‌ی ایمیل باید با یک پیغام یا آیکونِ اعلامِ وضعیت[1] به ازای هر ایمیل دریافتی وضعیت S/MIME برای آن را نمایش دهد.

نکات کاربردی:

✓ مقصود از وضعیت S/MIME این است که آیا ایمیلِ مربوطه با استفاده از S/MIME امضا و رمز شده است یا امضای مربوطه و گواهینامه‌ی طرف مقابل تائید شده است یا نه.

[1] Notification

✓ این وضعیت باید حداقل در زمان مشاهده ایمیل توسط کاربر نشان داده شود، یا در نمایش ایمیل‌ها به‌صورت لیست در کنار هر ایمیل نشان داده شود.	
۳۳	استفاده از S/MIME ۱ (FDP_SMIME_EXT.1.1)
سرویس‌گیرنده‌ی ایمیل باید از پروتکل S/MIME برای امضا[۱]، تصدیق[۲]، رمزنگاری[۳] و رمزگشایی[۴] ایمیل‌ها، پشتیبانی کند. نکات کاربردی: ✓ مقصود از این الزام استفاده از S/MIME برای تمامی ایمیل‌های دریافتی و ارسالی نیست، بلکه مقصود الزام به پشتیبانی از آن است.	

۷-۶-کلاس محافظت از محصول

این کلاس شامل مجموعه‌ای از زیر کلاس‌ها برای محافظت از محصول است، مواردی چون پیشگیری از سوء استفاده از برنامه، محافظت از داده‌های امنیتی ذخیره‌شده مانند کلیدهای رمزنگاری و رمز عبورها، انجام خودآزمایی خودکار برای کسب اطمینان از کارکرد صحیح توابع امنیتی، فراهم کردن رویه‌های قابل‌اعتماد برای انجام به‌روزرسانی و غیره.

۱-۷-۶-پشتیبانی از افزونه‌های مورد اعتماد

شماره الزام	نام الزام
۳۴	پشتیبانی از افزونه‌های مورد اعتماد ۱ (FPT_AON_EXT.1.1)

[۱] Sign

[۲] Verify

[۳] Encrypt

[۴] Decrypt

برنامه‌ی سرویس‌گیرنده ایمیل باید قادر به بارگذاری[1] و نصب [انتخاب: افزونه‌های امن، هیچ افزونه‌ای] باشد. نکات کاربردی: ✓ هدف از این الزام این است که یا امکان نصب هیچ افزونه‌ای داده نشود و یا تنها به منابع امن اجازه داده شود. ✓ در صورتِ پشتیبانی از امکانِ نصب از منابع مورد اعتماد، الزام انتخابی FPT_AON_EXT.2. نیز باید رعایت شود.

۲-۷-۶-استفاده از سرویس‌ها و API های پشتیبانی شده

شماره الزام	نام الزام
۳۵	استفاده از سرویس‌ها و APIهای پشتیبانی شده (FPT_API_EXT.1.1)
برنامه‌ی سرویس‌گیرنده ایمیل تنها باید از سرویس‌ها و APIهای مستند و معتبر از پلتفرم استفاده کند. نکات کاربردی: ✓ مقصود از این الزام کسب اطمینان از این مسئله است که سرویس‌ها و APIهای مورداستفاده از پلتفرم، معتبر بوده و به محلی برای آسیب امنیتی تبدیل نخواهد شد. ✓ باید لیست انواع API های قابل پشتیبانی مشخص شود.	

۳-۷-۶-پیشگیری از سوء استفاده

۳۶	پیشگیری از سوءاستفاده ۱ (FPT_AEX_EXT.1.1)
جز در موارد استثنایی زیر، برنامه‌ی سرویس‌گیرنده‌ی ایمیل نباید درخواست نگاشت حافظه در یک آدرس صریح را ارائه کند[2]: [اختصاص: لیستی از موارد استثنایی] نکات کاربردی: ✓ این مسئله باعث به‌هم ریختن کارکرد ASLR (space layout randomization address) می‌شود.	

[1] Load

[2] The application shall not request to map memory at an explicit address

✓ ASLR تکنیکی برای جلوگیری از سوء استفاده مهاجمین جهتِ انتقال به محل مشخص از حافظه و اجرا یا تهدید عملکرد مورد هدف است.	
پیشگیری از سوء استفاده ۲ (FPT_AEX_EXT.1.2)	۳۷
برنامه سرویس‌گیرنده ایمیل باید: [انتخاب: • هیچ فضایی از حافظه را هم‌زمان با دو اجازه‌ی «نوشتن» و «اجرا» تخصیص ندهد، • تخصیص فضای حافظه با دو اجازه‌ی هم‌زمان «نوشتن» و «اجرا» را تنها به [اختصاص: لیستی از توابع که به ترجمه کردن[1] از نوع just-in-time نیاز دارند.] محدود کند. نکات کاربردی: ✓ تخصیص حافظه با دو اجازه‌ی «نوشتن» و «اجرا» عملکردِ مکانیزم DEP را مختل می‌کند. ✓ درصورتی‌که هیچ تابعی وجود ندارد که نیازمند just-in-time compiling باشد، آنگاه گزینه اول باید انتخاب شود.	
پیشگیری از سوءاستفاده ۳ (FPT_AEX_EXT.1.3)	۳۸
برنامه سرویس‌گیرنده ایمیل باید با امکانات امنیتی فراهم‌شده توسط پلتفرم سازگار باشد. نکات کاربردی: ✓ همچنان که پیش‌تر گفته‌شده است، مقصود از پلتفرم سیستم‌عامل یا محیطی است که برنامه‌ی سرویس‌گیرنده ایمیل بر روی آن نصب می‌شود. ازاین‌رو سازگاری با امکانات امنیتی فراهم‌شده توسط پلتفرم ضروری است.	
پیشگیری از سوءاستفاده ۴ (FPT_AEX_EXT.1.4)	۳۹
برنامه نباید فایل‌های قابل‌ویرایش توسط کاربر را در همان دایرکتوری‌هایی بنویسد که فایل‌های اجرایی خودش در آن‌ها قرار دارند مگر اینکه این مسئله صریحاً توسط کاربر اجبار شود.	
پیشگیری از سوءاستفاده ۵ (FPT_AEX_EXT.1.5)	۴۰
برنامه‌ی سرویس‌گیرنده‌ی ایمیل باید به همراه قابلیت stack-based buffer overflow protection و در	

[1] Compile

حالت enabled از آن ارائه شود.

۴-۷-۶-استفاده از کتابخانه‌های Third Party

۴۱	کتابخانه‌های Third Party ۱ (FPT_LIB_EXT.1.1)
در صورت استفاده از کتابخانه‌های third party، لیست مربوطه باید مشخص شود. نکات کاربردی: ✓ اهمیت این الزام ازاین‌جهت است که ممکن است کتابخانه‌های مربوطه خود به محلی برای حمله تبدیل شوند و یا آسیب‌پذیری جدیدی در آن‌ها شناسایی شود و نیاز به به‌روزرسانی داشته باشند. ✓ اطلاع از این کتابخانه‌ها برای فرایند ارزیابی نیز بسیار کمک‌کننده است.	

۵-۷-۶-محافظت از داده‌های امنیتی

شماره الزام	نام الزام
۴۲	محافظت از کلیدهای رمزنگاری۱ (FPT_SKP_EXT.1.1)
سرویس‌گیرنده ایمیل به‌هیچ‌وجه نباید اجازه خوانده شدن 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.	
۴۳	محافظت از رمز عبور ۱ (FPT_APW_EXT.1.1)
سرویس‌گیرنده ایمیل نباید رمز عبورها را به شکل متن ساده، ذخیره کند.	
۴۴	محافظت از رمز عبور ۲ (FPT_APW_EXT.1.2)
سرویس‌گیرنده ایمیل باید از خوانده شدن رمز عبورها جلوگیری کند. نکات کاربردی: ✓ هدف از دو الزام اخیر این است که داده‌های خام مربوط به احراز هویت از قبیل رمز عبور، به شکل واضح ذخیره نشوند و هیچ کاربر سرویس‌گیرنده ایمیل نیز نتواند این رمز عبورها را به‌صورت متن ساده از طریق واسط «عادی» بخواند.	

۶-۷-۶-خودآزمایی خودکار عملگرهای امنیتی

برای شناسایی وقوع مشکل در سازوکارهای امنیتی، سرویس‌گیرنده‌ی ایمیل باید از طریق خودآزمایی از صحت کارکرد آن‌ها اطمینان حاصل کند.

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

۷-۷-۶-به‌روزرسانی امن

این زیر کلاس به الزامات مرتبط با به‌روزرسانی نرم‌افزاری، چگونگی اعتبارسنجی فایل به‌روزرسانی و تأمین امنیت این فرایند می‌پردازد.

۴۶	به‌روزرسانی امن ۱ (FPT_TUD_EXT.1.1)
برنامه سرویس‌گیرنده ایمیل باید از طریق [انتخاب: فراهم کردن امکان لازم، استفاده از امکانات پلتفرم] وجود به‌روزرسانی‌های جدید (updates & patches) برای نرم‌افزار خود را چک کند. نکات کاربردی: ✓ هدف این الزام آگاهی یافتنِ به‌موقع از به‌روزرسانی‌های جدید برای برنامه سرویس‌گیرنده ایمیل است.	
۴۷	به‌روزرسانی امن ۲ (FPT_TUD_EXT.1.2)
برنامه سرویس‌گیرنده ایمیل باید از طریق [انتخاب: فراهم کردن امکان لازم، استفاده از امکانات پلتفرم] امکان اطلاع از نسخه نصب‌شده از نرم‌افزار خود را فراهم کند.	
۴۸	به‌روزرسانی امن ۳ (FPT_TUD_EXT.1.3)
برنامه نباید کدهای باینری اجرایی خود را به‌روزرسانی، تغییر، دانلود و جایگزین کند.	
۴۹	به‌روزرسانی امن ۴ (FPT_TUD_EXT.1.4)
برنامه سرویس‌گیرنده ایمیل باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری، 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 الزامِ انتخابی	

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 انتخابی FCS_COP.1/Hash باشد.

۵۰	به‌روزرسانی امن ۵ (FPT_TUD_EXT.1.5)
نحوه‌ی توزیع برنامه‌ی سرویس‌گیرنده‌ی ایمیل باید مشخص شود: [انتخاب: به همراه سیستم‌عامل، به‌صورت پکیج جداگانه] نکات کاربردی: ✓ در صورتی توزیع به‌صورت پکیج جداگانه باشد، آنگاه باید الزام FPT_TUD_EXT.2 نیز رعایت شود.	

۸-۷-۶-شناسه و نسخه نرم‌افزار

۵۱	شناسه و نسخه نرم‌افزار ۱ (FPT_IDV_EXT.1.1)
برنامه سرویس‌گیرنده ایمیل باید با استفاده از تکنیک تگ گذاری SWID[1] و با رعایت حداقل الزامات ISO/IEC 19770-2:2015 نسخه‌بندی شده و به‌صورت یکتا قابل‌تفکیک باشد.	

۹-۷-۶-مهرهای زمانی قابل‌اعتماد

۵۲	مهر زمانی امن ۱ (FPT_STM_EXT.1.1)
سرویس‌گیرنده‌ی ایمیل باید قابلیت ارائه مهرهای زمانی قابل‌اطمینان برای استفاده خودش را داشته باشد.	
۵۳	مهر زمانی امن ۲ (FPT_STM_EXT.1.2)
سرویس‌گیرنده‌ی ایمیل باید [انتخاب: به کاربر اجازه دهد که زمان را تنظیم کند، زمان را با منابع خارجی NTP همگام سازد]. نکات کاربردی:	

[1] Software Identification Tagging

✓ مهرهای زمانی قابل اطمینان جهت استفاده در دیگر توابع امنیتی سرویس‌گیرنده‌ی ایمیل، مورد نظر هستند. به‌عنوان‌مثال، برای ثبت زمان وقوع رخداد در رکوردهای ممیزی. ✓ این زمان می‌تواند به‌صورت دستی توسط کاربر 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.

۸-۶-کلاس کانال‌ها/مسیرهای مورد اعتماد

الزامات این کلاس اختصاص به چگونگی برقراری یک کانال امن میان سرویس‌گیرنده‌ی ایمیل و یک موجودیت خارجی مانند مؤلفه MDA/MSA در سمت سرویس‌گیرنده‌ی ایمیل و یا یک موجودیت خارجی دیگر دارد. این کانال امن هم باید داده‌های ارسالی را از شنود و تغییر حفظ کند و هم 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 که در این میان TLS از نقش پررنگ‌تری برخوردار است، زیرا امروزه پروتکل‌های مربوط به سرویس ایمیل چون SMTP، POP و IMAP نیز به کمک آن قادر به تشکیل کانال امن هستند.

شماره الزام	نام الزام
۵۴	کانال امن/ سرویس‌گیرنده ایمیل با سرویس‌دهنده‌ی ایمیل ۱ (FTP_ITC_EXT.1.1)
سرویس‌گیرنده ایمیل باید قادر به برقراری یا پذیرش اتصال از موجودیت‌های معتبر در سمت سرویس‌دهنده‌ی ایمیل باشد.	
۵۵	کانال امن/ سرویس‌گیرنده ایمیل با سرویس‌دهنده ایمیل ۲ (FTP_ITC_EXT.1.2)
سرویس‌گیرنده‌ی ایمیل باید قادر به استفاده از پروتکل TLS به‌منظور برقراری کانال امن برای پروتکل-های زیر باشد: • IMAP • SMTP • POP • افزونه‌های MAPI برای HTTP • MAPI/RPC • ActiveSync • [اختصاص: لیستی از پروتکل‌های دیگر] نکات کاربردی:	

✓توجه شود که در صورت انتخاب پروتکل‌های IMAP، SMTP یا POP، آنگاه الزامِ انتخابی FIA_SASL_EXT.1 نیز باید پیاده‌سازی شود. ✓درصورتی‌که امکان استفاده از پروتکل دیگری بجای TLS فراهم باشد، ضمنِ اشاره به استاندارد ارائه‌شده برای آن، الزامات مربوط به آن پروتکل نیز باید رعایت شود. ✓پروتکل مربوطه باید سازگاری و سطح تضمین فراهم‌شده به‌وسیله TLS را فراهم کند.	
۵۶	کانال امن/ سرویس‌گیرنده ایمیل با دیگر موجودیت‌های IT ۱ (FTP_ITC.1.1)
سرویس‌گیرنده‌ی ایمیل باید بتواند کانال ارتباطی امنی را با استفاده از پروتکل(های) [انتخاب: IPSEC، SSH، TLS، DTLS، HTTPS] میان خود و دیگر موجودیت‌های معتبر IT (در صورت وجود) شامل: [انتخاب: [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 نموده 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: ✓ کارکرد این الزام زمانی است که به‌جز سرویس‌گیرنده‌ی ایمیل نیاز به برقراری ارتباط و انتقال داده با موجودیت دیگری باشد.	
۵۷	کانال امن/ سرویس‌گیرنده ایمیل با دیگر موجودیت‌های IT ۲ (FTP_ITC.1.2)
سرویس‌گیرنده 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.	
۵۸	کانال امن/ سرویس‌گیرنده ایمیل با دیگر موجودیت‌های IT ۳ (FTP_ITC.1.3)
سرویس‌گیرنده ایمیل باید ارتباطات را از طریق کانال امن برای [اختصاص: لیست سرویس‌هایی که سرویس‌گیرنده ایمیل می‌تواند برای آن‌ها ارتباطات را آغاز کند] شروع کند.	

۹-۶-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 با سایر موجودیت-های IT 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 و تحویل ایمیل، مؤلفه MUA باید قادر به پیاده‌سازی هر یک از دو نقش client/server باشد.

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

جدول .Error! No text of specified style in document-۳ 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_SHAمطابق 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

شماره الزام	نام الزام
۵۹	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 را پیاده‌سازی کند: [انتخاب: یکی از مجموعه‌های رمزنگاری لیست شده در «لیست مجموعه‌های رمزنگاری برای پروتکل‌های TLS»]	
۶۰	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.	
۶۱	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 گواهینامه TLS server نامعتبر به نظر رسید، client باید [انتخاب: ارتباط را برقرار نسازد، برای برقراری ارتباط درخواست مجوز بدهد، [اختصاص: دیگر اقدامات.]].	
۶۲	الزامات پروتکل TLS Client (۴) (FCS_TLSC_EXT.1.4)
TLS Client باید [انتخاب: Supported Elliptic Curves Extension را ارائه نکند، Supported Elliptic Curves Extension را به همراه NIST curveهای [انتخاب: secp256r1, secp384r1, secp521r1] 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	

[۱] Identifier

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 "Elliptic Curves Extension Supported" 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.	
۶۳	الزامات پروتکل TLS Client (۵) (FCS_TLSC_EXT.1.5)
TLS Client باید از احراز هویت دوطرفه TLS server بر مبنای گواهینامه‌های X.509v3 پشتیبانی کند.	
۶۴	الزامات پروتکل TLS Server (۱) (FCS_TLSS_EXT.1.1)
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»]	
۶۵	الزامات پروتکل TLS Server (۲) (FCS_TLSS_EXT.1.2)
TLS server باید برای Client های 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.	
۶۶	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: 2048 بیت، 3072 بیت، 4096 بیت]، دیفی-هلمن با پارامترهایی با اندازه [۲۰۴۸ بیت، ۳۰۷۲بیت، ۴۰۹۶ بیت، ۶۱۴۴ بیت، ۸۱۹۲ بیت]، دیفی-هلمن با گروه‌های [انتخاب: ffdhe2048، ffdhe3072، ffdhe4096، ffdhe6144، ffdhe8192، هیچ گروه دیگری]، منحنی‌های ECDHE [انتخاب: secp256r1, secp384r1, secp521r1] و هیچ منحنی دیگری] انجام دهد.	

۶۷	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.	
۶۸	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]	
۶۹	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.	

۱۰-۶-الزامات گواهینامه‌های X.509

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

شماره الزام	نام الزام
۷۰	الزامات گواهینامه‌های X.509/ تأیید گواهینامه (۱) (FIA_X509_EXT.1.1/Rev)
سرویس‌گیرنده ایمیل باید گواهینامه‌ها را بر اساس قوانین زیر تأیید کند: • بر اساس RFC 5280 برای تأیید گواهینامه و مسیر آن‌که 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 بخش 6.3، لیست فسخ گواهینامه (CRL) مشخص‌شده در RFC 5759 بخش 5، 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 مورد استفاده 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.	
۷۱	الزامات گواهینامه‌های X.509/ تأیید گواهینامه (۲) (FIA_X509_EXT.1.2/Rev)
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.	
۷۲	الزامات گواهینامه‌های X.509/ احراز هویت (۱) (FIA_X509_EXT.2.1)
سرویس‌گیرنده ایمیل باید جهت پشتیبانی از احراز هویت در [انتخاب: DTLS, TLS, HTTPS, SSH ,IPsec] و [انتخاب: امضای کد[1] برای به‌روزرسانی‌های نرم‌افزاری سیستم، امضای کد برای تأیید یکپارچگی، [اختصاص: سایر کاربردها]، هیچ کاربرد دیگر] از گواهینامه‌های X.509v3 مطابق با 5280 RFC استفاده کند.	
۷۳	الزامات گواهینامه‌های X.509/ احراز هویت (۲) (FIA_X509_EXT.2.2)
زمانی که سرویس‌گیرنده ایمیل نمی‌تواند اتصال موردنیاز برای تأیید اعتبار یک گواهینامه را برقرار کند، باید [انتخاب: به سرپرست سرویس‌گیرنده ایمیل اجازه دهد که در این مورد تصمیم‌گیری کند، گواهینامه را بپذیرد، گواهینامه را نپذیرد.]	
۷۴	الزامات گواهینامه‌های X.509/ درخواست گواهینامه (۱)(FIA_X509_EXT.3.1)
سرویس‌گیرنده ایمیل باید مطابق با آنچه در RFC 2986 تشریح شده است، یک پیام Certificate Request تولید کند و بتواند اطلاعاتی شامل کلید عمومی و [انتخاب: اطلاعات مخصوص به سرویس‌گیرنده ایمیل، Common Name، Organization، Organization Unit، Country] را در	

[1] Code Signing

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 سرویس‌گیرنده ایمیل تولید می‌شود.	
۷۵	الزامات گواهینامه‌های X.509/ درخواست گواهینامه (۲)(FIA_X509_EXT.3.2)
با دریافت پاسخ CA Certificate Response، سرویس‌گیرنده ایمیل باید زنجیره گواهینامه‌ها را با شروع از Root CA اعتبارسنجی کند.	

فصل ۷– الزامات تضمین امنیت (ASE_REQ_SAR)

برای ارزیابی محصول، باید راهنمای محصول و چگونگی پیاده‌سازی و تحقق الزامات کارکردی-امنیتی در قالب سند «هدف امنیتی» و دیگر اسناد تکمیلی و راهنما ارائه شود. الزامات موجود در این بخش عملاً به فصل‌ها و بخش‌های موردنیاز در این اسناد اشاره دارند. همچنان که در فصل دوم اشاره شد سطح موردنظر برای تضمین امنیت در این پروفایل حفاظتی سطح 1 است.

۱–۷–کلاس هدف امنیتی

همچنان که پیش‌تر نیز گفته‌شده است، مهم‌ترین سندی که باید ارائه شود 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 ارائه‌شده در جدول زیر باشد:

شماره الزام	الزام	شرح الزام
(۱)	ادعای التزام به پروفایل(های) حفاظتی (ASE_CCL.1)	مطابق با این الزام باید لیست و نسخه پروفایل(های) حفاظتی که سرویس‌گیرنده ایمیل ادعای التزام و پیاده‌سازی آن‌ها را دارد، ذکر شود. لذا ضمن تصریح انطباق با این پروفایل حفاظتی، در صورت ادعای انطباق و پیاده‌سازی اسناد دیگر، موارد مربوطه نیز باید ذکر شوند.
(۲)	تعریف مؤلفه‌های توسعه‌یافته (ASE_ECD.1)	درصورتی‌که علاوه بر الزامات ذکرشده در این پروفایل حفاظتی، الزامات بیشتری نیز بنا به قابلیت‌های سرویس‌گیرنده 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 سرویس‌گیرنده ایمیل (ASE_INT.1)	مطابق با این الزام باید سرویس‌گیرنده ایمیل معرفی و مؤلفه‌ها و اجزای مختلف آن به همراه ویژگی‌ها، قابلیت‌ها 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 سرویس‌گیرنده 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 سرویس‌گیرنده 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 سرویس‌گیرنده ایمیل با جزئیات کامل به تشریح چگونگی پیاده‌سازی الزامات ذکرشده بپردازد.

اقدامات ارزیاب	
هدف امنیت (ASE)	مؤلفه: (ASE_CCL.1E) شرح مؤلفه: ارزیاب باید تأیید کند که توضیحات ارائه‌شده کامل بوده و مشخصات پروفایل‌های حفاظتی ذکرشده کامل بوده و پروفایل‌ها وجود خارجی دارند.
	مؤلفه: (ASE_ECD.1E) شرح مؤلفه: ارزیاب باید تأیید کند که هیچ مؤلفه توسعه‌یافته‌ای به‌وسیله مؤلفه‌های موجود به‌صورت 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 زیر بخش‌های 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 سرویس‌گیرنده

	ایمیل تمامی الزامات ذکرشده را پیاده‌سازی کرده و از جامعیت و شفافیت کامل در شرح مکانیزم برخوردار است.

۲-۷-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 کاربر 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 سرویس‌گیرنده 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.

۳-۷-کلاس اسناد راهنما

مستند(ات) راهنما همراه با سند هدف امنیتی ارائه خواهند شد. این اسناد باید مشخص کنند که چگونه می‌توان از سرویس‌گیرنده‌ی ایمیل و امکانات امنیتی آن استفاده کرد. 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 سرویس‌گیرنده ایمیل
- دستورالعمل‌های لازم برای مدیریت امنیت آن
- دستورالعمل‌ها و توصیه‌های مفید در اتخاذ استراتژی‌های امنیتی در شرایط مختلف با توجه به امکانات سرویس‌گیرنده 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 موردنیاز آن در اسناد دیگر گنجانده شود و یا به‌صورت آنلاین در اینترنت در دسترس باشد. این سند باید برای هر نوع نقش کاربری، کارکردها و واسط‌های در دسترس، به‌خصوص تمام پارامترهای امنیتی تحت کنترل را توصیف نموده و مقادیر امن را توصیه کند. باید برای هر نقش، رویدادهای امنیتی به کارکردهای در دسترس و قابل انجام توسط کاربر مرتبط شوند. سند راهنمای کاربر عملیاتی باید تمام مدهای عملیاتی سرویس‌گیرنده 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 کاربری، معیارهای امنیتی را که توسط کاربر باید تبعیت شوند توصیف کند تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده‌شده‌اند، به‌طور کامل اجرا گردند.
(۱۰)	راهنمای آماده‌سازی (AGD_PRE.1)	این سند باید همراه با محصول ارائه شود. مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن سرویس‌گیرنده‌ی 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 کاربر 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 سرویس‌گیرنده ایمیل می‌تواند به‌صورت امن برای عمل نمودن آماده شود.

۴-۷-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 کاربرِ سرویس‌گیرنده‌ی ایمیل قابل‌مشاهده باشد. این به آن معنی نیست که نحوه عمل توسعه گیرنده نقش کمرنگی در قابل‌اعتماد بودن سرویس‌گیرنده ایمیل دارد، بلکه در این سطح اطمینان تنها به این اطلاعات نیاز است.

شماره الزام	الزام	شرح الزام
(۱۱)	برچسب‌گذاری محصول CMC.1_ALC	توسعه گیرنده باید سرویس‌گیرنده ایمیل و مرجع آن را ارائه کند. به‌عبارتی‌دیگر محصول باید با یک مرجع نرم‌افزاری یکتا مشخص شود. این برچسب نرم‌افزاری محصول را به‌صورت یکتا در میان محصولات شرکت مربوطه معرفی می‌کند.
(۱۲)	پوشش پیکربندی محصول CMS.1_ALC	توسعه گیرنده باید لیست موارد قابل پیکربندی سرویس‌گیرنده 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.

۵-۷-کلاس آزمون

آزمون سرویس‌گیرنده ایمیل توسط ارزیاب و برای بررسی و تست کارکردهای سیستم و همچنین تست وجود حفره‌های امنیتی که در محصولات مشابه شناسایی شده‌اند، در نظر گرفته شده 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 سرویس‌گیرنده 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 سرویس‌گیرنده‌ی 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	توسعه گیرنده 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 مناسب برای ارزیابی هست یا نه.
	مؤلفه: (ATE_IND.1.2E) شرح مؤلفه: ارزیاب باید زیرمجموعه‌ای از توابع امنیتی سرویس‌گیرنده ایمیل را تست کند تا تأیید شود که توابع امنیتی به‌صورت مشخص‌شده عمل می‌کنند.

۶-۷-کلاس ارزیابی آسیب‌پذیری

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

شماره الزام	الزام	شرح الزام
(۱۴)	AVA_VAN.1	توسعه گیرنده 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 مناسب برای ارزیابی آسیب‌پذیری هست یا نه.
	مؤلفه: (AVA_VAN.1.2E) شرح مؤلفه: ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه و شناخته‌شده در سرویس‌گیرنده 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 سرویس‌گیرنده ایمیل را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص کند.

فصل ۸– 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.

۱–۸–کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱	تولید Initialization Vector (IV) (۱) (FCS_IVG_EXT.1.1)
تولید IV برای هر مد رمزنگاری باید به شکل مقابل باشد: [انتخاب: • CBC: باید به‌صورت غیر تکرارشونده (non-repeating) باشد. • CCM: باید به‌صورت غیر تکرارشونده (non-repeating) باشد. • XTS: فاقد IV. مقادیر پیچیده باید اعداد صحیح غیرمنفی، تخصیص‌یافته به‌صورت پشت سر هم و شروع‌شده از یک عدد صحیحِ غیرمنفیِ دلخواه باشد.[۱] • GCM: باید به‌صورت غیر تکرارشونده (non-repeating) باشد. تعداد دفعات فراخوانی[۲] GCM برای یک کلید محرمانه نباید بیشتر از 2^32 باشد.] نکات کاربردی: ✓ از میان ۴ مد ذکرشده، سه مدِ اول، سوم و چهارم برای رمزنگاری داده‌ها با AES و مد CCM برای AES-CCM جهتِ پوشاندن کلید کاربرد دارد.	
۲	تولید Cryptographic Nonce (۱) (FCS_NOG_EXT.1.1)
سرویس‌گیرنده ایمیل تنها باید از nonceهای یکتا با حداقل اندازه ۶۴ بیت استفاده کند.	

[۱] No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer.

[۲] Invocation

۳	تولید Cryptographic Salt (۱) (FCS_SAG_EXT.1.1)
سرویس‌گیرنده ایمیل تنها باید از saltهایی استفاده کند که به‌وسیله‌ی [انتخاب: • الگوریتم DRBG و مطابق با الزام‌های FCS_RBG_EXT.1&2 تولیدشده است. • الگوریتم DRGB که توسط پلتفرم فراهم می‌شود تولیدشده است.]	

۱-۱-۸-الزامات پروتکل DTLS

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 سرویس‌گیرنده ایمیل و موجودیت دوم مانند سرور خارجی رکوردهای ممیزی می‌توانند نقش کاربر DTLS یا سرور DTLS را بگیرند.

شماره الزام	نام الزام
۴	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.	
۵	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.	
۶	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.

۷	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.	
۸	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].	
۹	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.	

۲-۸-کلاس محافظت از داده‌های کاربر و پلتفرم

شماره الزام	نام الزام
۱۰	اعلانِ URI[۱] (۱) (FDP_NOT_EXT.2.1)
برنامه‌ی سرویس‌گیرنده‌ی ایمیل باید قادر به نمایش URI برای هر لینک تعبیه‌شده باشد.	

[۱] Notification of URI

نکات کاربردی:

- ✓مقصود از یک لینکِ تعبیه‌شده یک HTML URI است که ممکن است به‌وسیله‌ی یک عکس، عبارت یا آیکون پوشانده شده باشد. برنامه سرویس‌گیرنده‌ی ایمیل باید از این امر جلوگیری کند و URI همواره نمایش داده شود.

۱۱	ذخیره‌ی اطلاعات مانا (۱) (FDP_PST_EXT.1.1)

سرویس‌گیرنده‌ی ایمیل باید قادر به پردازش اطلاعاتِ مانا بدونِ ذخیره کردن آن‌ها بر روی پلتفرم کاربر باشد به‌جز موارد مقابل: [انتخاب: اطلاعات مرتبط با کلیدها و گواهینامه‌ها، اطلاعات مرتبط با پیکربندی‌های انجام‌شده توسط سرپرست (کاربر با نقش ادمین)، اطلاعات مرتبط با لیست certificate revocation، هیچ استثنایی]

نکات کاربردی:

- ✓مقصود از این الزام این است که تا حد امکان از ذخیره‌سازی اطلاعات (ایمیل‌ها و ...) بر روی پلتفرم کاربر پرهیز شود.
- ✓این الزام با بهره‌گیری از پروتکل‌های IMAP و MAPI قابل تحقق بوده و این امکان با POP فراهم نیست. IMAP امکان خوانش ایمیل‌ها بدون نیاز به دانلود یا امکانِ دسترسی به فولدرهای موجود بر روی سرویس‌دهنده ایمیل را می‌دهد، در حالیکه این امکانات در POP فراهم نیست و ایمیل‌ها حتماً باید ابتدا دانلود شوند.

۱۲	پردازش محتوای پیغام (۱) (FDP_REN_EXT.1.1)

سرویس‌گیرنده‌ی ایمیل باید از مدِ plaintext-only پشتیبانی کند که در آن امکان غیرفعال کردنِ پردازش و اجرای محتوای [انتخاب: HTMP، JavaScript، [اختصاص: انواع دیگر از محتوای تعبیه‌شده و قابل‌اجرا]] فراهم است.

نکات کاربردی:

- ✓ مدِ plaintext-only از دانلود، پردازش و اجرای اتوماتیک Image و انواع تعبیه‌شده مانند HTML و JavaScript جلوگیری می‌کند.

۳-۸-کلاس مدیریت امنیت

شماره الزام	نام الزام
۱۳	مدیریت کارکرد امنیتی ۱/سرویس‌ها (FMT_MOF.1/Services)

سرویس‌گیرنده ایمیل باید امکان فعال/غیرفعال کردن توابع و سرویس‌ها را به سرپرستان امنیتی محدود کند.

۱۴	مدیریت دسترسی به داده‌ها ۱/کلیدهای رمزنگاری (FMT_MTD.1/CryptoKeys)
سرویس‌گیرنده 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.	

۴-۸-الزامات پروتکل DANE

پروتکل DANE مکانیزمی امن و مطمئن برای ذخیره و دسترس‌پذیری گواهینامه‌های TLS و S/MIME فراهم می‌کند. همچنان که پیش‌تر گفته شد، الزامات این پروتکل در لیست الزامات اختیاری گنجانده‌شده است. قابل‌ذکر است که در صورت پشتیبانی از DANE پروتکل DNSSEC نیز باید پیاده‌سازی شود.

شماره الزام	نام الزام
۱۵	الزامات پروتکل DANE (۱) (FCS_DANE_EXT.1.1)
سرویس‌گیرنده 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.	
۱۶	الزامات پروتکل DANE (۳) (FCS_DANE_EXT.1.3)
سرویس‌گیرنده 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.	
۱۷	الزامات پروتکل DANE (۴) (FCS_DANE_EXT.1.4)
سرویس‌گیرنده 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.	
۱۸	الزامات پروتکل DANE (۵) (FCS_DANE_EXT.1.5)
هرگونه اتصال با سرور DNS برای ثبت و خوانش رکوردهای DANE باید با استفاده از پروتکل DNSSEC باشد.	

۵-۸-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، سرویس‌گیرنده ایمیل مطمئن خواهد شد که پاسخ دریافتی از سرویس‌دهنده DNS معتبر است.

شماره الزام	نام الزام
۱۹	الزامات پروتکل DNSSEC (۱) (FCS_DNSSEC_EXT.1.1)

سرویس‌گیرنده ایمیل باید پروتکل DNSSEC (RFC 4033) را با توجه به لیست مجموعه رمز زیر برای انجام DNSSEC Validation پیاده‌سازی کند. مطابق با این پروتکل، سرویس‌گیرنده باید قادر به انجام احراز هویت زنجیره‌ای برای تائید امضای موجود در جواب‌های دریافتی از سرویس‌دهنده DNS باشد.

ستون «نیازمندی» الزام به پیاده‌سازی هر مجموعه را مشخص کرده و ستون مرجع نیز الگو و استاندارد موردنیاز در پیاده‌سازی را مشخص می‌کند.

جدول .Error! No text of specified style in document-**۴ مجموعه رمز برای انجام DNSSEC Validation**

الگوریتم	مرجع	نیازمندی
RSA/SHA-1	RFC 3110	لازم

[1] Domain Name System Security Extensions

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

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

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

نکات کاربردی:

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

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

به‌منظور دریافت کردن[1] رکوردهای DNS در حافظه محلی، سرویس‌گیرنده ایمیل باید طول عمر امضای رکوردها را نیز در نظر بگیرد.

نکات کاربردی:

[1] Cash

✓ عموماً هدف از دریافت کردن رکوردهای DNS در حافظه محلی صرفه جوبی در زمان و نیز کمک به کاهش بار کاری سرویس‌گیرنده 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)	۲۲
درصورتی‌که از موجودیت مجزایی برای ارسال درخواست‌های DNS و دریافت و تائید اصالت پاسخ‌ها استفاده شود، کانال ارتباطی میان سرویس‌گیرنده 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 پراکسی 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 سرویس‌گیرنده ایمیل برقرار باشد.	
الزامات پروتکل DNSSEC (۵) (FCS_DNSSEC_EXT.1.5)	۲۳
در صورت استفاده از یک موجودیت مجزا، سرویس‌گیرنده ایمیل باید اطمینان حاصل کند که موجودیت مربوطه اصالت امضا در پاسخ دریافتی از سرویس‌دهنده DNS را به‌طور کامل احراز کرده است. نکات کاربردی: ✓ سرویس‌گیرنده می‌تواند با چک کردن بیت AD (Authenticated Data) در هدر پیغام دریافتی از موجودیت مربوطه این کار را انجام دهد.	

فصل ۹– پیوست دو: الزامات انتخابی

این پیوست به بیان الزامات مبتنی بر انتخاب می‌پردازد. پیاده‌سازی الزامات این بخش بسته به انتخاب‌های انجام‌شده در فصل ۶ است. به‌طور مثال در صورت انتخاب پروتکل SSH برای امن کردن کانال ارتباطی، باید الزامات مربوط به SSH از این بخش پیاده‌سازی شود.

۱–۹–کلاس پشتیبانی از رمزنگاری

۱–۱–۹–الزامات پایه رمزنگاری

الزامات ذکرشده با این عنوان، همچنان که مشخص است، پایه و مبنا برای اجرای عملیات دیگری چون تشکیل کانال امن هستند. لذا فراهم بودن آن‌ها الزامی است. اما ازآنجایی‌که ممکن است این عملکردها توسط پلتفرم فراهم شود، لذا به‌عنوان الزامات انتخابی در نظر گرفته‌شده‌اند. اما درصورتی‌که سرویس‌گیرنده‌ی ایمیل خود آن‌ها را پیاده می‌کند، رعایت این الزامات نیز اجباری خواهد بود.

شماره الزام	نام الزام
۱	مدیریت کلید رمزنگاری ۱ (FCS_CKM.1)

سرویس‌گیرنده ایمیل باید تولید کلیدهای رمزنگاری نامتقارن را با انتخاب یکی از روش‌های 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 سرویس‌گیرنده ایمیل به‌عنوان یک دریافت‌کننده در الگوهای استقرار کلید عمل کند و برای پشتیبانی از احراز هویت دوطرفه پیکربندی نشده باشد، سرویس‌گیرنده ایمیل نیاز به پیاده‌سازی تولید کلید ندارد.	
۲	مدیریت کلید رمزنگاری ۲ (FCS_CKM.2.1)
سرویس‌گیرنده ایمیل باید استقرار کلید[1] 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 کند. ❖ 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.]	
۳	نابودسازی کلید رمزنگاری (FCS_CKM.4.1)
سرویس‌گیرنده 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	

[1] Key Establishment

[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 (به‌طور مستقیم 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 سرویس‌گیرنده 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 سرویس‌گیرنده ایمیل»، بخش خلاصه مشخصات محصول باید این «بخش» و واسط مرتبط با آن را مشخص و معرفی کند. واسط اشاره‌شده می‌تواند در سرویس‌گیرنده ایمیل‌های مختلف، اشکال متفاوتی داشته باشد. شاید مشهودترین شکل آن‌یک 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 سرویس‌گیرنده ایمیل از برخی داده‌های خاص استفاده کند

[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

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. در واقع 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.

۴	عملیات رمزنگاری/ رمزنگاری داده‌ها (FCS_COP.1/DataEncryption)

سرویس‌گیرنده 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 ۳-۱۸۰۳۳ ISO تعریف شده است و استاندارد [انتخاب: CBC که در ۱۰۱۱۶ ISOتعریف‌شده است، GCM که در ۱۹۷۷۲ ISO تعریف شده است، CTR که در ۱۰۱۱۶ ISO تعریف شده 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.

۵	عملیات رمزنگاری/ تولید و تأیید امضا (FCS_COP.1/SigGen)

سرویس‌گیرنده 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، مخصوصاً زمانی که از Elliptic Curve استفاده شود.	
۶	عملیات رمزنگاری/الگوریتم درهم‌ساز (FCS_COP.1/Hash)
سرویس‌گیرنده 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 به‌روزرسانی 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 (برای مثال SHA-256 برای کلیدهای ۱۲۸ بیتی).	
۷	عملیات رمزنگاری/الگوریتم درهم‌ساز مبتنی بر کلید (FCS_COP.1/KeyedHash)
سرویس‌گیرنده 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 اندازه کلید رمزنگاری [اختصاص: اندازه کلید به بیت که در HMAC استفاده شده] 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 استاندارد ISO/IEC 10118 مربوط به توابع درهم‌ساز). به‌طور مثال در مورد SHA-256 داریم: L2<=k<=L1 که L1=512, L2=256

۸	عملیات رمزنگاری/تولید بیت تصادفی ۱ (FCS_RBG_EXT.1)

سرویس‌گیرنده 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.

۹	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 اندازه آنتروپی [انتخاب: ۱۲۸، ۱۹۲، ۲۵۶] بیتی گردآوری کند. همچنین اندازه آنتروپی باید معادل یا بزرگ‌تر از طولانی‌ترین یا قوی‌ترین کلیدی باشد که در سرویس‌گیرنده 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 مورد استفاده است. برای مثال دو منبع نرم‌افزاری برای تولید آنتروپی.

۲-۱-۹-الزامات پوشش کلید

۱۰	عملیات رمزنگاری/پوشش کلید (FCS_COP_EXT.2.1/KeyWrapping)

برای انجام عملیات پوشش کلید، سرویس‌گیرنده‌ی ایمیل از

[انتخاب:

- از روش فراهم‌شده توسط پلتفرم استفاده می‌کند،
- عملکرد پوشش کلید را خود پیاده‌سازی می‌کند

]

و این پیاده‌سازی مبتنی بر تکنیکِ رمزنگاریِ

[انتخاب:

- AES Key Wrap,
- AES Key Wrap همراه با Padding ,
- RSA با استفاده از مدلِ KTS-OAEP-basic ,
- RSA با استفاده از مدلِ KTS-OAEP-receiver-confirmation ,
- ECC CDH

]

و اندازه کلیدِ

[انتخاب:

- ۱۲۸ بیت (AES),
- ۲۵۶ بیت (AES),
- ۲۰۴۸ بیت (RSA),
- ۴۰۹۶ بیت (RSA),
- 256-bit prime,
- (ECC CDH) modulus,
- 384-bit prime modulus (ECC CDH)

]

و با رعایتِ

[انتخاب:

- section 6.2 از NIST SP 800-38F در صورتِ انتخابِ "Key Wrap" و section 6.3 از آن در

صورتِ انتخابِ "Key Wrap همراه با Padding "

- section 9.2.3 از NIST SP 800-56B در صورت انتخابِ «RSA با استفاده از مدلِ KTS-OAEP-basic» و section 9.2.4 از آن در صورتِ انتخابِ «RSA با استفاده از مدلِ KTS-OAEP-receiver-confirmation» و section 5.6.1.2 & 6.2.2.2 در صورت انتخابِ " ECC CDH"

[

است.

نکات کاربردی:

- ✓ پیاده‌سازی این الزام وابسته به انتخاب انجام‌گرفته در الزامات FCS_CKM_EXT.3.1 و FCS_KYC_EXT.1.1 است.
- ✓ در صورت استفاده از روش‌های فراهم‌شده توسط پلتفرم نیازی به انتخاب‌های بعدی نیست، اما درصورتی‌که برنامه‌ی سرویس‌گیرنده‌ی ایمیل خود عملکرد مربوطه را پیاده‌سازی می‌کند باید الگوریتم مورداستفاده و اندازه کلید مشخص‌شده و استاندارد مربوطه از NIST نیز به‌دقت رعایت شود.

۳-۱-۹-الزامات ترکیب کلید

۱۱	عملیات رمزنگاری/ترکیب کلید (FCS_SMC_EXT.1.1/KeyCombining)
سرویس‌گیرنده‌ی ایمیل از [انتخاب: XOR، SHA-256، SHA-512] برای ترکیب کلید و تولید کلید جدید استفاده می‌کند. نکات کاربردی: پیاده‌سازی این الزام بسته به انتخاب انجام‌گرفته در الزامات FCS_CKM_EXT.3.1 و FCS_KYC_EXT.1.1 است.	

۴-۱-۹-الزامات رمز عبور و استخراج کلید به روش رمزنگاری

الزامات این بخش در صورت انتخاب شدنِ FCS_CKM_EXT.5 در الزام FCS_KYC_EXT.1.1. باید پیاده‌سازی شوند.

۱۲	رمز عبور و استخراج کلید به روش رمزنگاری (۱) (FCS_CKM_EXT.5.1)
حداکثر طول رمز عبور باید [انتخاب: [اختصاص: حداکثر طول رمز عبور به انتخاب سرپرست]، ۶۴ یا بیشتر] کاراکتر باشد. نکات کاربردی:	

✓ مقصود از ۶۴ در الزام فوق این است که حداقل باید این تعداد کاراکتر برای حداکثر طول رمز عبور پشتیبانی شود.	
۱۳	رمز عبور و استخراج کلید به روش رمزنگاری (۲) (FCS_CKM_EXT.5.2)
رمز عبور را باید بتوان با هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای ویژه‌ی مقابل ساخت: ")","(","*","&","^","%","$","#","@","!"،[اختصاص: سایر کاراکترها]	
۱۴	رمز عبور و استخراج کلید به روش رمزنگاری (۳) (FCS_CKM_EXT.5.3)
سرویس‌گیرنده ایمیل باید عملکرد Password-based Key Derivation را با استفاده از الگوریتمِ [انتخاب: HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512] و با تعداد تکرارِ (iteration) [اختصاص: ۴۰۹۶ یا یک عدد مثبت بزرگ‌تر] انجام داده و اندازه کلید خروجی باید: [انتخاب: ۱۲۸، ۲۵۶] بیت و مطابق با استاندارد NIST SP 800-132 باشد.	
۱۵	رمز عبور و استخراج کلید به روش رمزنگاری (۴) (FCS_CKM_EXT.5.4)
برنامه‌ی سرویس‌گیرنده‌ی ایمیل نباید رمز عبور با طول کمتر از [انتخاب: یک عددِ پیکربندی‌شده توسط سرپرست، مقدار پیش‌فرض محصول (که باید 1=< باشد)] و طول بیشتر از عددِ تعیین‌شده در الزام FCS_CKM_EXT.5.1 را بپذیرد.	

۵-۱-۹-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 **.No text of specified style in document** !Error-۵ آورده شده و در خلال الزامات DTLS به آن مراجعه خواهیم کرد.

جدول .No text of specified style in document !Error-۵ 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_SHAمطابق 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 این 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 سرویس‌گیرنده ایمیل و موجودیت دوم مانند سرور خارجی رکوردهای ممیزی می‌توانند نقش کاربر DTLS یا سرورDTLS را بگیرند.

شماره الزام	نام الزام

۱۶	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]	
۱۷	الزامات پروتکل DTLS Client بدون احراز هویت دوطرفه (۲) (FCS_DTLSC_EXT.1.2)
DTLS client باید مطابقت شناسه 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.	
۱۸	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.]].	
۱۹	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، Supported Elliptic Curves Extension را به همراه NIST curveهای [انتخاب: secp256r1, secp384r1, secp521r1] 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 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 DTLS Server بدون احراز هویت دوطرفه (۱) (FCS_DTLSS_EXT.1.1)	۲۰
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]	
الزامات پروتکل DTLS Server بدون احراز هویت دوطرفه (۲) (FCS_DTLSS_EXT.1.2)	۲۱
DTLS server نباید برای کلاینت‌هایی که درخواست هیچ دارند، ارتباطات را ایجاد کند.	
الزامات پروتکل DTLS Server بدون احراز هویت دوطرفه (۳) (FCS_DTLSS_EXT.1.3)	۲۲
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. سرویس‌گیرنده 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.	
الزامات پروتکل DTLS Server بدون احراز هویت دوطرفه (۴) (FCS_DTLSS_EXT.1.4)	۲۳
DTLS server باید استقرار کلید را با استفاده از [انتخاب: RSA با اندازه کلید [انتخاب: 2048 بیت، 3072 بیت، 4096 بیت]، دیفی-هلمن با پارامترهایی با اندازه [۲۰۴۸ بیت، ۳۰۷۲بیت، ۴۰۹۶ بیت،	

۶۱۴۴ بیت، ۸۱۹۲ بیت]، دیفی-هلمن با گروه‌های [انتخاب: ffdhe2048، ffdhe3072،ffdhe4096 ، ffdhe6144، ffdhe8192، هیچ گروه دیگری]، منحنی‌های ECDHE [انتخاب: secp521r1, secp384r1, secp256r1,] و هیچ منحنی دیگری] انجام دهد.	
۲۴	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.	
۲۵	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: ۲. رکوردهای DTLS که قبلاً دریافت شده‌اند (یعنی شماره ترتیب آن تکراری هست). ۳. رکوردهای DTLS بسیار قدیمی که شماره ترتیب آن‌ها در sliding receive window قرار نمی‌گیرد. را به‌صورت خاموش نادیده بگیرد.	

۶-۱-۹-الزامات پروتکل IPSEC

شماره الزام	نام الزام
۲۶	الزامات پروتکلIPSEC (۱) (FCS_IPSEC_EXT.1.1)
سرویس‌گیرنده 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[1] در مسیریاب‌ها، مجموعه قوانین فیلترینگ بسته(packet filtering rule set) در فایروال‌ها و مواردی شبیه به آن را 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.

۲۷	الزامات پروتکلIPSEC (۲) (FCS_IPSEC_EXT.1.2)
سرویس‌گیرنده 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.	
۲۸	الزامات پروتکلIPSEC (۳) (FCS_IPSEC_EXT.1.3)
سرویس‌گیرنده 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.	
۲۹	الزامات پروتکلIPSEC (۴) (FCS_IPSEC_EXT.1.4)
سرویس‌گیرنده 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	

[1] Access Control Lists

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.

۳۰	الزامات پروتکل IPSEC (۵) (FCS_IPSEC_EXT.1.5)

سرویس‌گیرنده 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 سرویس‌گیرنده 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 سرویس‌گیرنده ایمیل از HMACهای مبتنی بر SHA، کوتاه شده مطابق با RFC 4868 استفاده کند، باید در خلاصه مشخصات محصول، مشخص گردد.

۳۱	الزامات پروتکل IPSEC (۶) (FCS_IPSEC_EXT.1.6)

[۱] Extended Sequence Numbers

سرویس‌گیرنده ایمیل باید اطمینان حاصل کند که برای پایه‌بار[1] 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.	
۳۲	الزامات پروتکلIPSEC (۷) (FCS_IPSEC_EXT.1.7)
سرویس‌گیرنده ایمیل باید اطمینان حاصل کند که [انتخاب: سرپرست سرویس‌گیرنده ایمیل می‌تواند طول عمر SA[2] 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 سرویس‌گیرنده 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.] نکات کاربردی: ✓ تعیین طول عمر برای SAهای فاز اول به مدیر سرویس‌گیرنده 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.	

[1] Payload

[2] Security Association

۳۳	الزامات پروتکلIPSEC (۸) (FCS_IPSEC_EXT.1.8)

سرویس‌گیرنده ایمیل باید اطمینان حاصل کند که [انتخاب:

سرپرست سرویس‌گیرنده 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 سرویس‌گیرنده 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 سرویس‌گیرنده 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.

۳۴	الزامات پروتکلIPSEC (۹) (FCS_IPSEC_EXT.1.9)

سرویس‌گیرنده 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.

۳۵	الزامات پروتکلIPSEC (۱۰) (FCS_IPSEC_EXT.1.10)

سرویس‌گیرنده 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[1] 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 تک‌شمار انتخاب کند. نویسنده سند هدف امنیتی مجاز است هر یک از گزینه‌ها را برای IKEv1 انتخاب کند.	
الزامات پروتکل IPSEC (۱۱) (FCS_IPSEC_EXT.1.11)	۳۶
سرویس‌گیرنده 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 پشتیبانی شده است، بکار می‌رود. این الزام برای هر دو IKEv1 و IKEv2 اعمال می‌گردد.	
الزامات پروتکل IPSEC (۱۲) (FCS_IPSEC_EXT.1.12)	۳۷
سرویس‌گیرنده ایمیل باید به‌صورت پیش‌فرض بتواند اطمینان حاصل کند که قدرت الگوریتم متقارنی (از نظر 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)	۳۸
سرویس‌گیرنده 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.	

[1] Sudo Random Function

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.

شماره الزام	نام الزام
۳۹	الزامات پروتکل IPSEC (۱۴) (FCS_IPSEC_EXT.1.14)
سرویس‌گیرنده 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]].	

۷-۱-۹-الزامات پروتکل SSH

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

شماره الزام	نام الزام
۴۰	الزامات پروتکل Client SSH (۱) (FCS_SSHC_EXT.1.1)
سرویس‌گیرنده 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	
۴۱	الزامات پروتکل SSH Client (۲) (FCS_SSHC_EXT.1.2)
سرویس‌گیرنده 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].	
۴۲	الزامات پروتکل SSH Client (۳) (FCS_SSHC_EXT.1.3)
همان‌طور که در RFC 4253 توضیح داده‌شده است، سرویس‌گیرنده 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 سرویس‌گیرنده ایمیل تعریف شود.	
۴۳	الزامات پروتکل SSH Client (۴) (FCS_SSHC_EXT.1.4)
سرویس‌گیرنده 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.	
۴۴	الزامات پروتکل SSH Client (۵) (FCS_SSHC_EXT.1.5)
سرویس‌گیرنده 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).	

۴۵	الزامات پروتکل SSH Client (۶) (FCS_SSHC_EXT.1.6)
سرویس‌گیرنده 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.	

۴۶	الزامات پروتکل SSH Client (۷) (FCS_SSHC_EXT.1.7)
سرویس‌گیرنده 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.	

۴۷	الزامات پروتکل SSH Client (۸) (FCS_SSHC_EXT.1.8)
سرویس‌گیرنده 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 گیگا بایت 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 سرویس‌گیرنده ایمیل وارد و از سرویس‌گیرنده 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.

- ✓ سرویس‌گیرنده ایمیل همچنین می‌تواند مقادیری کمتر از مقادیر حد آستانه ذکرشده در این الزام را پیاده‌سازی کند. سند راهنمای سرویس‌گیرنده 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.

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

سرویس‌گیرنده 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.

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

سرویس‌گیرنده 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	
۵۰	الزامات پروتکل Server SSH (۲) (FCS_SSHS_EXT.1.2)
سرویس‌گیرنده ایمیل باید اطمینان حاصل کند که در پیاده‌سازی پروتکل SSH، همان‌طور که در 4252 RFC توضیح داده‌شده است، روش‌های احراز هویت مقابل پشتیبانی می‌شوند: احراز هویت مبتنی بر کلید عمومی، احراز هویت مبتنی بر رمز عبور.	
۵۱	الزامات پروتکلServer SSH (۳) (FCS_SSHS_EXT.1.3)
همان‌طور که در RFC 4253 توضیح داده‌شده است، سرویس‌گیرنده 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 سرویس‌گیرنده ایمیل تعریف شود.	
۵۲	الزامات پروتکلServer SSH (۴) (FCS_SSHS_EXT.1.4)
سرویس‌گیرنده 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.	
۵۳	الزامات پروتکل Server SSH (۵) (FCS_SSHS_EXT.1.5)
سرویس‌گیرنده 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).	

۵۴	الزامات پروتکل Server SSH (۶) (FCS_SSHS_EXT.1.6)
سرویس‌گیرنده 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.	

۵۵	الزامات پروتکل Server SSH (۷) (FCS_SSHS_EXT.1.7)
سرویس‌گیرنده 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.	

۵۶	الزامات پروتکل Server SSH (۸) (FCS_SSHS_EXT.1.8)
سرویس‌گیرنده 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 گیگا بایت 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 سرویس‌گیرنده ایمیل وارد و از سرویس‌گیرنده 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.	

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

۸-۱-۹-الزامات پروتکل HTTPS

شماره الزام	نام الزام
۵۷	الزامات پروتکل HTTPS (۱) (FCS_HTTPS_EXT.1.1)
سرویس‌گیرنده 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.	
۵۸	الزامات پروتکل HTTPS (۲) (FCS_HTTPS_EXT.1.2)
سرویس گیرند ایمیل باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	
۵۹	الزامات پروتکل HTTPS (۳) (FCS_HTTPS_EXT.1.3)
درصورتی‌که گواهینامه همتا ارائه‌شده باشد و نامعتبر باشد، سرویس‌گیرنده 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

۲-۹-کلاس شناسایی و احراز هویت

پیاده‌سازی الزامات SASL زمانی لازم است که در الزام FTP_ITC_EXT.1.2 هریک از سه پروتکل SNMP، POP یا IMAP انتخاب شود که با توجه به کاربرد گسترده و متداول این سه پروتکل، طبعاً نیاز به پیاده‌سازی الزامات این بخش اجتناب‌ناپذیر به نظر می‌رسد. لزوم این پیاده‌سازی در پشتیبانی از گواهینامه‌های PKI X.509 در این سه پروتکل است.

شماره الزام	نام الزام
۶۰	مکانیزم SASL (۱) (FIA_SASL_EXT.1.1/SASL)
مکانیزم SASL[۱] باید مطابق با RFC 4422 پیاده‌سازی شود.	
۶۱	مکانیزم SASL (۲) (FIA_SASL_EXT.1.2/SASL)
سرویس‌گیرنده ایمیل باید از افزونه‌های POP3 CAPA و AUTH مطابق با RFC 5034 برای مکانیزم SASL پشتیبانی کند. نکات کاربردی: ✓ پیاده‌سازی این الزام زمانی لازم است که از POP استفاده شود.	
۶۲	مکانیزم SASL (۳) (FIA_SASL_EXT.1.3/SASL)
سرویس‌گیرنده ایمیل باید از افزونه‌های IMAP CAPABILITY و AUTHENTICATE مطابق با RFC 4959 برای مکانیزم SASL پشتیبانی کند. نکات کاربردی: ✓ پیاده‌سازی این الزام زمانی لازم است که از IMAP استفاده شود.	
۶۳	مکانیزم SASL (۴) (FIA_SASL_EXT.1.4/SASL)
سرویس‌گیرنده ایمیل باید از افزونه‌های SMTP AUTH مطابق با RFC 4954 برای مکانیزم SASL پشتیبانی کند. نکات کاربردی:	

[۱] Simple Authentication and Security Layer

✓ پیاده‌سازی این الزام زمانی لازم است که از SNMP استفاده شود.

۳-۹-کلاس محافظت از محصول

۱-۳-۹-خودآزمایی خودکار عملگرهای امنیتی

شماره الزام	نام الزام
۶۴	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.	

۲-۳-۹-به‌روزرسانی امن محصول

شماره الزام	نام الزام
۶۵	به‌روزرسانی امن بر اساس گواهینامه (۱) (FPT_TUD_EXT.2.1)
درصورتی‌که کد امضای گواهینامه‌ی یک به‌روزرسانی نامعتبر باشد سرویس‌گیرنده ایمیل نباید آن را نصب کند.	
۶۶	به‌روزرسانی امن بر اساس گواهینامه (۲) (FPT_TUD_EXT.2.2)
هنگامی‌که گواهینامه به علت انقضای آن، غیر معتبر اعلام شده است، سرویس‌گیرنده ایمیل باید [انتخاب: اجازه بدهد که در این موارد سرپرست سرویس‌گیرنده ایمیل در مورد پذیرش گواهی تصمیم‌گیری کند، گواهی را بپذیرد، گواهی را نپذیرد.]	
۶۷	به‌روزرسانی امنِ افزونه (۱) (FPT_AON_EXT.2.1)
سرویس‌گیرنده ایمیل باید [انتخاب: با بهره‌گیری از قابلیت‌های پلتفرم، مبتنی بر پیاده‌سازی خودش] از یک روش تائید اصالتِ مبتنی بر رمزنگاری با اتکا بر مکانیزم امضای دیجیتال و [انتخاب: هشِ توزیع‌شده[1]، هیچ روش دیگری] برای چک کردنِ فایل نصب یا به‌روزرسانی افزونه‌ها، استفاده کند.	

[1] Published hash

نکات کاربردی: ✓ پیاده‌سازی سری الزام FPT_AON_EXT.2.x به انتخابِ انجام گرفته در الزام FPT_AON_EXT.1.1 وابسته است.	
۶۸	به‌روزرسانی امنِ افزونه (۲) (FPT_AON_EXT.2.2)
سرویس‌گیرنده ایمیل باید [انتخاب: با بهره‌گیری از قابلیت‌های پلتفرم، با اتکا به پیاده‌سازی خودش] قادر به پرس‌وجو و تعیین نسخه‌ی فعلی از افزونه فراهم کند.	
۶۹	به‌روزرسانی امنِ افزونه (۳) (FPT_AON_EXT.2.3)
سرویس‌گیرنده ایمیل باید از نصب خودکار افزونه‌ها جلوگیری کند.	

۴-۹-مراجع

1. "Common Criteria for Information Technology Security Evaluation", CC:2022
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
5. "PP-Module for Email Clients", Version 1.0, 2021
6. "Application Software Extended Package for Email Clients", Version 2.0, 2015
7. "Protection Profile for Email Clients", Version 1.0, 2014
8. "Protection Profile for Application Software", Version 1.3, 2019