به نام خدا

بسته الحاقی پروفایل حفاظتی نرم‌افزار کاربردی برای سرویس‌گیرنده‌های ایمیل

بهمن ۹۴

نسخه ۱,۰

فهرست

۱- مقدمه ۴
۲- فرهنگ اصطلاحات ۴
۲-۱- اصطلاحات معیار مشترک ۴
۲-۲- اصطلاحات فناوری ۷
۳- شرح محصول ۹
۳-۱- سازگاری محصول ۱۰
۳-۲- حالت‌های استفاده ۱۱
۴- مسائل امنیتی ۱۱
۴-۱- تهدیدها ۱۲
۵- اهداف امنیتی ۱۴
۶- الزامات کارکرد امنیتی ۱۴
۶-۱- کلاس پشتیبانی رمزنگاری ۱۷
۶-۲- کلاس حفاظت از داده کاربری ۳۲
۶-۳- کلاس شناسایی و احراز هویت ۳۴
۶-۴- کلاس مدیریت امنیت ۳۶
کلاس محافظت از محصول ۴۰
۶-۵- کلاس کانال‌ها/مسیر امن ۴۱

7- پیوست یک ۴۴
۷-۱- کلاس پشتیبانی رمزنگاری ۴۴
۷-۲- کلاس حفاظت از داده کاربر ۵۰
8- پیوست دو ۵۵
۸-۱- کلاس پشتیبانی رمزنگاری ۵۵
۸-۲- کلاس شناسایی و احراز هویت ۵۹
۸-۳- کلاس حفاظت از محصول ۶۱
۹- نمادها و اختصارات ۶۳
۱۰- منابع و مآخذ ۶۶

۱- مقدمه

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی که در این سند برای برآورده نمودن الزامات ارائه شده‌اند را در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد نمود. مرکز افتا با مشارکت سازمان فناوری اطلاعات این سند را بر اساس سند طرح ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 در راستای این هدف تهیه نموده است. این پروفایل حفاظتی بسته الحاقی[۱] نرم‌افزارهای کاربردی و ارائه‌دهنده مجموعه پایه الزامات کارکرد امنیتی[۲] برای ایمیل کلاینت[۳] بوده و بدون توجه به پلتفرم مورد استفاده[۴]، روی هر سیستم‌عاملی قابل‌اجرا است.

پیچیدگی و مجموعه‌ای از ویژگی‌های غنی انواع پیشرفته ایمیل کلاینت‌ها، آن‌ها را به یک هدف برای مهاجمان تبدیل کرده و باعث ایجاد نگرانی‌های امنیتی شده است. این سند به‌منظور تسهیل در بهبود امنیت ایمیل کلاینت‌ها با نیاز به استفاده از سرویس‌های امنیتی سیستم‌عامل‌ها، استانداردهای رمزنگاری و کاهش خطرات محیطی در نظر گرفته‌شده است. بعلاوه الزامات موجود در این سند، رفتار قابل‌قبول یک ایمیل کلاینت بدون توجه به ویژگی‌های امنیتی فراهم‌شده توسط سیستم‌عامل را تعریف می‌کند.

۲- فرهنگ اصطلاحات

۲-۱- اصطلاحات معیار مشترک

[۱] Extended Package (EP)

[۲] Security Functional Requirements (SFRs)

[۳] Email clients

[۴] underlying platform

مستند: به هر سندی که حاوی اطلاعات برای اجرا و پشتیبانی عملیات ها و فعالیت های سازمانی مورد استفاده قرار می گیرند، مستند گفته می شود.

رکورد: مستندی که اطلاعات فعالیت‌ها، رویدادها و نتایج حاصله را نگهداری می‌کند. به عبارت دیگر یک رکورد مستندی است که مدرک انجام یک فعالیت مشخص است. یک رکورد می‌تواند شامل دو یا چند مستند باشد.

رکورد ممیزی: رکوردی که حاوی اطلاعات رویدادهایی است که برای ممیزی سامانه مورد نیاز است و در محل ذخیره‌سازی ممیزی، ذخیره می‌شود.

داده‌های کاربری ذخیره شده: فایل‌های داده و اطلاعاتی هستند که توسط کاربر ایجاد و ذخیره می‌شوند. این داده‌ها می‌تواند شامل مستندات تولید شده با استفاده از برنامه کاربردی Microsoft Office، نامه های ارجاع کار و پاسخ الکترونیکی و اسکن تصاویر باشد.

موجودیت فعال: موجودیتی در محصول که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون مدیر، کاربر نهایی و غیره.

موجودیت غیرفعال: موجودیتی در محصول، که حاوی اطلاعات است و یا اطلاعات را دریافت می‌نماید و توسط موجودیت‌های فعال، عملیاتی بر روی آن انجام می‌گیرد. همانند لیست کردن رکوردها توسط مدیر سیستم، حذف فایل‌ها توسط مهاجم (رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.)

مشخصه‌های موجودیت فعال: مشخصه‌های هر موجودیت فعال از قبیل نام کاربری، کلمه عبور، آدرس IP کاربر می‌تواند باشد.

مشخصه‌های موجودیت غیرفعال: مشخصه‌های هر موجودیت غیرفعال از قبیل نوع، نام و اندازه مستند می‌تواند باشد.

انتخاب: «انتخاب» یکی از عملیاتی است که در الزامات پروفایل جهت منعطف شدن پروفایل به منظور تدوین سند هدف امنیتی توسط تولید کننده آمده است. در الزاماتی با این عملیات نویسنده باتوجه به کارکرد امنیتی محصول یک یا چند مورد از موارد ذکر شده در الزام را انتخاب می نماید و به عنوان ادعا در بخش الزامات کارکردی سند هدف امنیتی ذکر می نماید.

اختصاص: «اختصاص» یکی از عملیاتی است که در الزامات پروفایل جهت منعطف شدن پروفایل به منظور تدوین سند هدف امنیتی توسط تولید کننده آمده است. در الزاماتی با این عملیات نویسنده باتوجه به کارکرد امنیتی محصول، مقدار یا پارامتر مشخصی را اختصاص می‌دهد.

- **معیار مشترک**[۱] (CC)

معیاری مشترک برای ارزیابی امنیت فناوری اطلاعات

- **بسته الحاقی**[۲] **(EP)**

مجموعه‌ای از الزامات امنیتی وابسته به پیاده‌سازی برای رده‌ای از محصولاتی که آن‌ها را در یک پروفایل حفاظتی توسعه می‌دهند.

- **هدف ارزیابی(محصول)**[۳] **(TOE)**

محصول مورد ارزیابی و مجموعه‌ای از نرم‌افزارها، سخت‌افزارها و میان‌افزارهای[۴] تحت ارزیابی که ممکن است همراه با راهنماهایی باشند.

- **پروفایل حفاظتی**[۵] **(PP)**

مجموعه‌ای از الزامات امنیتی برای دسته‌ای از محصولات می‌باشد که مستقل از پیاده‌سازی است.

- **هدف امنیتی**[۶] **(ST)**

---

[۱] Common Criteria

[۲] Extended Package

[۳] Target of Evaluation

[۴] firmware

[۵] Protection Profile

[۶] Security Target

بیان وابستگی‌های پیاده‌سازی نیازهای امنیتی برای محصول خاص شناسایی شده.

- **الزام کارکرد امنیتی[۱] (SFR)**

الزامات اجرای امنیت توسط محصول است.

- **الزام تضمین امنیتی[۲] (SAR)**

الزامات تضمین امنیت محصول است.

- **خلاصه مشخصه محصول[۳] (TSS)**

مستندی است توصیفی درباره پیاده‌سازی الزامات کارکرد امنیتی محصول که به ارزیاب کنندگان ارائه می‌گردد.

۲-۲- اصطلاحات فناوری

- **همگام‌سازی فعال[۴]**

پروتکل مایکروسافت به منظور همگام‌سازی ارسال/ دریافت پیغام‌ها و داده‌های‌تقویم بین کلاینت‌های سیار و سرورهای ایمیل.

[۱] Security Functional Requirement

[۲] Security Assurance Requirement

[۳] TOE Summary Specification

[۴] ActiveSync

- **افزونه[۱]**

توانایی‌ها یا کارکردهای اضافه‌شده به یک اپلیکیشن شامل پلاگین‌ها۲، پسوندها و یا کنترل‌های دیگر.

- **ایمیل کلاینت[۳]**

نرم‌افزار مورداستفاده برای ارسال، دریافت، دسترسی و مدیریت ایمیل که توسط یک سرور ایمیل ارائه می‌شود.

- **پروتکل دسترسی به پیام اینترنتی[۴] (IMAP)**

پروتکلی برای یک ایمیل کلاینت برای بازیابی ایمیل از یک سرور از طریق TCP/IP; IMAP4 که در RFC 3501 تعریف‌شده است.

- **رابط برنامه‌نویسی برنامه پیام‌رسانی[۵] (MAPI)**

مشخصه باز استفاده‌شده توسط ایمیل کلاینت شامل Microsoft Outlook و Thunderbird که در [MSOXCMAPIHTTP] تعریف‌شده [MSOXCMAPIHTTP].

- **پروتکل ایمیل[۶] (POP)**

---

[۱] Add-on

[۲] Plug-ins

[۳] EmailClient

[۴] Internet Message Access Protocol

[۵] Messaging Application Programming Interface

[۶] Post Office Protocol (POP)

پروتکلی برای یک ایمیل کلاینت جهت بازیابی ایمیل از یک سرور ایمیل بر روی TCP/IP است. تعریف POP3 در RFC 1939 آمده است.

- **پروتکل فرایند تماس از راه دور[۱] (RPC)**

توسط Microsoft Exchange برای ارسال/دریافت فرمان‌های رابط برنامه‌نویسی کاربردی پیغام، که در MSOXCRPC تعریف‌شده است.

- **ضمیمه‌های چندمنظوره امنیت/پست الکترونیک[۲] (S/MIME)**

برای ثبت‌نام یا پیام رمزگذاری در درخواست یک کاربر هنگام ارسال ایمیل و به‌منظور بررسی امضای دیجیتال از یک پیام امضاشده‌ی پس از دریافت استفاده می‌شود.

- **پروتکل انتقال ایمیل ساده[۳] (SMTP)**

پروتکلی برای یک ایمیل کلاینت جهت ارسال ایمیل به یک سرور ایمیل بر روی TCP/IP. پروتکل انتقال ایمیل ساده در RFC 5321 تعریف‌شده است.

۳- شرح محصول

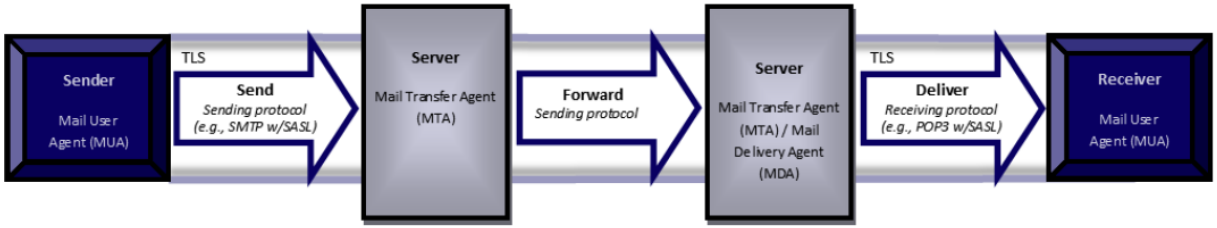
ایمیل کلاینت‌ها برنامه‌های کاربردی هستند که ارائه‌کننده کارکردهایی برای ارسال، دریافت، دسترسی و مدیریت ایمیل می‌باشند. پیچیدگی محتوای ایمیل و ایمیل کلاینت‌ها در طول زمان رشد کرده است. انواع پیشرفته ایمیل کلاینت‌ها می‌توانند فایل HTML را مانند متن خام ارائه دهند که ممکن است شامل

[۱] Remote Procedure Call

[۲] Secure/Multipurpose Internet Mail Extensions

[۳] Simple Mail Transfer Protocol

قابلیت‌هایی برای نمایش فرمت‌های پیو ست م شترک از قبیل نرم‌افزار Adobe PDF و مدارک Microsoft Word با شد. کارکردهای برخی از انواع ایمیل کلاینت اجازه می‌دهند قابلیت‌هایشان توسط کاربرانی که به افزونه اضافه‌شده‌اند، اصلاح شود. پروتکل‌هایی نیز برای برقراری ارتباط بین مشتریان و سرورها تعریف‌شده‌اند. برخی از انواع ایمیل کلاینت‌ها، پشتیبان چندین پروتکل برای انجام کارهای مشابه هستند، که به آن‌ها اجازه می‌دهند تا بر طبق مشخصات سرور ایمیل پیکربندی شوند (شکل ۱).



شکل ۱- ارسال و تحویل ایمیل بر روی TLS

۳-۱- سازگاری محصول

محصول در این بسته تکمیلی، پیاده‌سازی کاربردی یک ایمیل کلاینت روی یک میز کار[۱] یا سیستم‌عامل سیار است. این بسته الحاقی توصیف‌کننده کارکرد گسترده امنیتی یک ایمیل کلاینت در قالب معیار مشترک است. به‌عنوان الحاقی بر پروفایل حفاظتی برنامه کاربردی، انتظار می‌رود که محتوای این بسته الحاقی به‌طور مناسبی با پروفایل حفاظتی برنامه کاربردی ترکیب شود که شامل الزامات انتخاب[۲] در تطابق با انتخاب‌ها و/یا اختصاص‌های ایجادشده و/یا هر مؤلفه اجباری و یا اختیاری برای در برگرفتن موارد ذیل باشد:

۱ Desktop

۲Selection-based

FCS_CKM.2.1, FCS_COP.1.1 (*), FCS_RBG_EXT.2.*, FCS_TLSC_EXT.1.*, FIA_X509_EXT.1.*, FIA_X509_EXT.2.*

یک هدف امنیتی باید یک نسخه قابل اجرا از پروفایل حفاظتی برنامه کاربردی و این بسته الحاقی را در ادعاهای انطباقی‌اش[۱] تشخیص دهد.

۳-۲- حالت‌های استفاده

موارد استفاده: ارسال، دریافت، دسترسی، مدیریت و نمایش ایمیل

ایمیل کلاینت‌ها برای ارسال، دریافت، دسترسی، مدیریت و نمایش ایمیل در هماهنگی با یک سرور ایمیل استفاده می‌شوند. ایمیل کلاینت‌ها می‌توانند فایل HTML را مانند متن خام ارائه دهند و می‌توانند قالب‌های پیوست متداول را نمایش دهند.

۴- مسائل امنیتی

مسائل امنیتی در قالب تهدیدهایی بیان می‌شوند که انتظار می‌رود ایمیل کلاینت مشخص کند، فرضیات در مورد محیط عملیاتی و هر نوع سیاست امنیتی سازمانی که انتظار اجرای آن وجود دارد. این بسته امنیتی تکرارکننده تهدیدها، فرضیات و سیاست‌های امنیتی سازمانی نیست که در برنامه پروفایل حفاظتی تعریف‌شده؛ حتی اگر آن‌ها در انطباق داده‌شده صدق کنند و ازاین رو وابسته به بسته تکمیلی موجود در آن باشند.

تهدیدها، فرضیات و سیاست‌های امنیتی سازمانی برنامه پروفایل حفاظتی و تعاریفی که در این بسته تکمیلی بیان شدند، بیانگر این هستند که ایمیل کلاینت به‌عنوان محصول مشخص شود.

[۱] conformance claims

قابل‌ذکر است که ایمیل کلاینت‌ها منحصراً در معرض خطر تهدید حمله شبکه[۱] که در برنامه پروفایل حفاظتی مشخص شده، می‌باشند. مهاجمان می‌توانند پیام‌های مخرب را مستقیماً به ایمیل کاربران ارسال کنند و ایمیل کلاینت به ارائه آن پرداخته و در غیر این صورت این محتوای غیرقابل اطمینان را پردازش کند.

۴-۱- تهدیدها

تهدید زیر مختص ایمیل کلاینت بوده و مکمل آن چیزی است که در برنامه پروفایل حفاظتی تعریف شده است:

[۱] Network Attack

تهدیدات	توضیحات
T.FLAWED_ADDON	کارکرد ایمیل کلاینت می‌تواند توسط نرم‌افزارهای سودمند و ابزارهای شخص ثالث[۱] توسعه یابد. این مجموعه گسترده از کارکردهای ایمیل کلاینت از طریق استفاده از افزونه‌ها ایجاد شده است. ترکیب[۲] کد اصلی ایمیل کلاینت و قابلیت‌های جدیدی که افزونه فراهم کرده، خطر تزریق نقص‌های جدی از سوی خرابکار[۳] را، چه مغرضانه از طریق یک مهاجم و چه به‌صورت تصادفی توسط یک توسعه‌دهنده[۴] به ایمیل کلاینت افزایش می‌دهد. این نقص‌ها باعث ایجاد رفتارهایی نامطلوب شامل موارد ذیل است (و فقط به این موارد محدود نمی‌شود): امکان دسترسی غیرمجاز به اطلاعات حساس موجود در ایمیل کلاینت، دسترسی غیرمجاز به افزاره سامانه فایل۵، یا حتی تشدید امتیازاتی که دسترسی غیرمجاز را در دسترسی به سایر برنامه‌های کاربردی یا سیستم عملیاتی ممکن می‌سازد.

[۱] Third-party

[۲] tight integration

[۳] Malefactor

[۴] developer

[۵] device's file system

۵- اهداف امنیتی

هدف امنیتی	توضیحات
O.MANAGEMENT	این هدف امنیتی موردتوجه الزامات کارکرد امنیتی زیر قرارگرفته است: FDP_NOT_EXT.1،FDP_NOT_EXT.2 ،FMT_MOF_EXT.1
O.PROTECTED_STORAGE	این هدف امنیتی موردتوجه الزامات کارکرد امنیتی زیر قرارگرفته است: FCS_CKM_EXT.3 ،FCS_CKM_EXT.4، FCS_CKM_EXT.5 ،FCS_COP_EXT.2, FCS_IVG_EXT.1, FCS_KYC_EXT.1, FCS_NOG_EXT.1 FCS_SAG_EXT.1, FCS_SMC_EXT.1
O.PROTECTED_COMMS	این هدف امنیتی موردتوجه الزامات کارکرد امنیتی زیر قرارگرفته است: FCS_SMIME_EXT.1,FDP_SMIME_EXT.1, FIA_SASL_EXT.1, FIA_X509_EXT.3, FTP_ITC_EXT.1
O.ADDON_INTEGRITY	برای معرفی مسائل مربوط به نقص‌ها یا افزونه‌های معیوب یا توسعه‌ها، برنامه‌های ایمیل کلاینت به تطبیق سازوکارهایی برای اطمینان از یکپارچگی آن‌ها می‌پردازند که شامل تائید در زمان نصب و به‌روزرسانی است. این هدف امنیتی موردتوجه الزامات کارکرد امنیتی زیر قرارگرفته است: FPT_AON_EXT.1 ،FPT_AON_EXT.2

۶- الزامات کارکرد امنیتی

الزامات کارکرد امنیتی Email Client، با توجه به الزاماتی که در استاندارد ارزیابی معیار مشترک مطرح گردیده، به صورت خلاصه در زیر آورده شده است:

جدول ۱- الزامات کارکرد امنیتی

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**پشتیبانی رمزنگاری پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۱**	FCS_SMIME_EXT.1.1
۲	**پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۲**	FCS_SMIME_EXT.1.2
۳	**پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۳**	FCS_SMIME_EXT.1.3
۴	**پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۴**	FCS_SMIME_EXT.1.4
۵	**پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۵**	FCS_SMIME_EXT.1.5
۶	**پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۶**	FCS_SMIME_EXT.1.6
۷	**پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۷**	FCS_SMIME_EXT.1.7
۸	**حفاظت از کلید و اجزای کلید توسعه‌یافته ۱**	FCS_CKM_EXT.3.1
۹	**تخریب کلید رمزنگاری توسعه‌یافته ۱**	FCS_CKM_EXT.4.1
۱۰	**زنجیره‌ای کردن کلید توسعه‌یافته ۱**	FCS_KYC_EXT.1.1
۱۱	**تولید بردار مقداردهی اولیه توسعه‌یافته ۱**	FCS_IVG_EXT.1.1
۱۲	**اعلان وضعیت S/MIME توسعه‌یافته ۱**	FDP_NOT_EXT.1.1
۱۳	**حفاظت از داده کاربری پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۱**	FDP_SMIME_EXT.1.1
۱۴	**احراز هویت و رمزنگاری X509 ۱**	FIA_X509_EXT.3.1
۱۵	**احراز هویت و رمزنگاری X509 ۲**	FIA_X509_EXT.3.2
۱۶	**احراز هویت و رمزنگاری X509 ۳**	FIA_X509_EXT.3.3
۱۷	**احراز هویت و رمزنگاری X509 ۴**	FIA_X509_EXT.3.4

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۸	**احراز هویت و رمزنگاری X509 ۵**	FIA_X509_EXT.3.5
۱۹	**مدیریت کارکرد در محصول توسعه‌یافته ۱**	FMT_MOF_EXT.1.1
۲۰	**پشتیبانی افزونه‌های مورد اعتماد توسعه‌یافته ۱**	FPT_AON_EXT.1.1
۲۱	**کانال امن توسعه‌یافته ۱**	FTP_ITC_EXT.1.1
۲۲	**کانال امن توسعه‌یافته ۲**	FTP_ITC_EXT.1.2

جدول ۲- الزامات پیوست یک

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**اشتقاق کلید رمزنگاری (اصلاح[1] کلمه‌عبور/عبارت عبور) ۱**	FCS_CKM_EXT.5.1
۲	**تولید داده تصادفی (Salt) رمزنگاری ۱**	FCS_SAG_EXT.1.1
۳	**ایجاد رمزنگاری مقطعی ۱**	FCS_NOG_EXT.1.1
۴	**اعلان URI ۱**	FDP_NOT_EXT.2.1
۵	**انبارش اطلاعات دائمی ۱**	FDP_PST_EXT.1.1
۶	**پردازش محتوای پیام ۱**	FDP_REN_EXT.1.1

جدول ۳- الزامات پیوست دو

1 - Conditioning

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**پوشاندن کلید ۱**	FCS_COP_EXT.2.1
۲	**ترکیب کلید ۱**	FCS_SMC_EXT.1.1
۳	**لایه امنیت و احراز هویت ساده ۱**	FIA_SASL_EXT.1.1
۴	**لایه امنیت و احراز هویت ساده ۲**	FIA_SASL_EXT.1.2
۵	**لایه امنیت و احراز هویت ساده ۳**	FIA_SASL_EXT.1.3
۶	**لایه امنیت و احراز هویت ساده ۴**	FIA_SASL_EXT.1.4
۷	**نصب و به‌روزرسانی امن برای افزونه‌ها ۱**	FPT_AON_EXT.2.1
۸	**نصب و به‌روزرسانی امن برای افزونه‌ها ۲**	FPT_AON_EXT.2.2
۹	**نصب و به‌روزرسانی امن برای افزونه‌ها ۳**	FPT_AON_EXT.2.3

۶-۱- کلاس پشتیبانی رمزنگاری[۱]

شماره الزام	نام الزام
۱	**پشتیبانی رمزنگاری** **پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۱**
ایمیل کلاینت باید ارسال و دریافت Agent S/MIME نسخه ۳,۲ را که در پروتکل RFC 5751 تعریف‌شده با استفاده از CMS که در پروتکل RFCs 5652، RFCs 5754 و RFCs 3565 پیاده‌سازی نماید.	

[۱] Cryptographic Support (FCS)

نکته کاربردی ۱: RFCها برای یک عامل ارسال، دریافت و یا به‌کارگیری هردو قابلیت را فراهم می‌نماید.. هدف از این الزام تضمین این است که ایمیل کلاینت، توانایی ارسال و دریافت پیام‌های S/MIME نسخه ۳,۲ را داشته باشد.	
پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۲	**۲**
ایمیل کلاینت باید انتقال‌دهنده شناسه الگوریتم رمزنگاری محتوا[۱] برای AES-128 CBC و AES-256 CBC به‌عنوان بخشی از پروتکل S/MIME باشد. **نکته کاربردی:** همانطورکه در RFC 3565 تعریف شد، AES به CMS اضافه شد.	
پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۳	**۳**
ایمیل کلاینت ارائه‌کننده رشته الگوریتم چکیده[۲] با شناسه الگوریتم چکیده‌پیام[۳] انتخاب:[id-sha256, id-sha384, id-sha512] زیر به‌عنوان بخشی از پروتکلS/MIME است و هیچ الگوریتم دیگری قابل‌قبول نیست.	
پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۴	**۴**
ایمیل کلاینت باید رشته شناسه الگوریتم را پیرو sha256withRSAEncryption بازنمایی نماید: [انتخاب: sha384WithRSAEncryption, sha512WithRSAEncryption, ecdsawithSHA256,	

[۱] Content Encryption Algorithm Identifier(CEAI)

[۲] Digest Algorithm

[۳] Message Digest Algorithm identifiers

ecdsawithsha384, ecdsawithsha512] به‌عنوان بخشی از پروتکل S/MIME نباید هیچ الگوریتم دیگری بازنمایی شود. **نکته کاربردی**: در RFC 5751 عامل‌های ارسال و دریافت مجبور به پشتیبانی از RSA با SHA256 هستند. الگوریتم‌هایی که در پیکربندی ارزیابی‌شده مورد آزمون قرار می‌گیرند، محدود به الگوریتم‌های مشخص شده در انتخاب FCS_SMIME_EXT.1.4 هستند. هر الگوریتم اجرا شده دیگری با این الزامات مطابق نباشد، نباید در ارزیابی ایمیل کلاینت مورداستفاده قرار بگیرد.
۵ پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۵
ایمیل کلاینت باید به‌کارگیری کلیدهای خصوصی مختلف (و گواهی‌های مرتبط) برای امضاء جهت رمزنگاری خواهد بود، که بخشی از پروتکل S/MIME است را پشتیبانی نماید.
۶ پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۶
ایمیل کلاینت باید فقط یک امضاء از یک گواهی را با مجموعه بیت[۱] امضای دیجیتال به‌عنوان بخشی از پروتکل S/MIME بپذیرد. **نکته کاربردی:** این فرض مورد قبول است که مجموعه بیت امضای دیجیتال در مواردی استفاده شده است که پسوند KeyUsage در آن وجود ندارد.
۷ پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۷
ایمیل کلاینت باید سازوکارهایی را به عنوان بخشی از پروتکل S/MIME برای بازیابی گواهی[۲] و اطلاعات ابطال گواهی[۳] [انتخاب: برای هر پیام رمزگذاری‌شده/امضا شده ارسال / دریافت‌شده، [اختصاص: فراوانی]] اجرا نماید.

[۱] Bit Set

[۲] retrieve certificates

[۳] certificate revocation information

نکته کاربردی: در انطباق با FIA_X509_EXT.1.1 بازیابی گواهی ممکن است از فهرست بازیابی گواهی[۱] یا پروتکل وضعیت گواهی آنلاین[۲] استفاده کند. ایمیل کلاینت می‌تواند تعریف کند که این سازوکار چگونه باشد؛ از جمله، آیا از سیستم‌عامل مورد استفاده کمک بگیرداین نیازمند وجود یک سازوکاری است که در آن وضعیت ابطال[۳]، پشتیبانی شده و به نحوی با شد که گواهی‌ها برای ار سال و تحویل ایمیل قابل بازیابی با شند. تکرار[۴] در FMT_MOF_EXT.1.1 قابل تنظیم ا ست. در این الزام می‌توان تکرار را به‌عنوان یک بار تکرار[۵] با ذخیره محلی تفسیر کرد؛ به‌عنوان یک بازیابی زمان‌بندی‌شده منظم، یا به‌عنوان یک سازوکاری که نیاز به بازیابی دستی دارد. اگر سازوکار بازیابی ماهیتاً تکرارپذیر با شد، نویسنده مجموعه الزامات، به گنجاندن یک تکرار از FCS برای ذخیره اطلاعات ابطال نیاز خواهد دا شت؛ ذخیره گواهی‌ها در FCS_CKM پوشش داده شده است. اهمیت گواهی‌ها و زنجیره‌های گواهی در این الزام نیامده است اما در FIA_X509 و FMT_MOF پوشش داده‌شده است.

اقدامات تضمین:

- **بخش خلاصه مشخصات محصول[۶]**

باید در محصول بررسی شود که نسخه اجراشده S/MIME توسط ایمیل کلاینت، در خلاصه مشخصه محصول موجود باشد. همچنین باید تحقیق شود که الگوریتم‌های پشتیبانی شده مشخص‌شده‌اند و الگوریتم‌های مشخص‌شده آن‌هایی باشند که در این مؤلفه، ذکرشده‌اند.

در محصول باید تحقیق شود که خلاصه مشخصه محصول، توصیف‌کننده شناسه الگوریتم رمزنگاری محتوا باشد و رفتار موردنیاز به‌صورت پیش‌فرض انجام‌شده یا در صورت امکان، پیکربندی‌شده باشد.

---

[۱] Certificate Revocation List (CRL)

[۲] Online Certificate Status Protocol (OCSP)

[۳] revocation status

[۴] Frequency

[۵] One-time

[۶] TOE Summory Specification (TSS)

در محصول باید تحقیق شود که خلاصه مشخصه محصول توصیف‌کننده الگوریتم چکیده باشد و رفتار موردنیاز به‌صورت پیش‌فرض انجام‌شده یا در صورت امکان، پیکربندی‌شده باشد.

در محصول باید تحقیق شود که خلاصه مشخصه محصول توصیف‌کننده شناسه الگوریتم باشد و رفتار موردنیاز به‌صورت پیش‌فرض انجام‌شده یا در صورت امکان، پیکربندی‌شده باشد.

در محصول باید تحقیق شود که خلاصه مشخصه محصول توصیف‌کننده سازوکارهای بازیابی برای گواهی‌ها و ابطال گواهی باشد و همچنین مشخص‌کننده تعداد دفعاتی باشند که این گواهی‌ها اجرا می‌شوند.

راهنما

همچنین باید با بررسی راهنمای عملیاتی[۱] اطمینان یابند که این راهنما در محصول شامل دستورالعمل‌هایی برای تنظیم ایمیل کلاینت باشد به‌طوری که با توضیحات مندرج در خلاصه مشخصه محصول مطابقت داشته باشد.

اگر خلاصه مشخصه محصول دلالت کند که باید الگوریتم‌های موجود در FCS_SMIME_EXT.1.2 برای مطابقت با الزام، پیکربندی‌شده باشند، محصول باید تحقیق کنند که راهنمای AGD شامل پیکربندی این ID است.

اگر خلاصه مشخصه محصول دلالت کند که الگوریتم‌های موجود در FCS_SMIME_EXT.1.3 باید برای مطابقت با الزام، پیکربندی‌شده باشد، محصول باید تحقیق کنند که راهنمای AGD شامل پیکربندی این ID است.

اگر خلاصه مشخصه محصول دلالت کند که الگوریتم‌های موجود در FCS_SMIME_EXT.1.4 باید برای مطابقت با الزام، پیکربندی‌شده باشد، محصول باید تحقیق کند که راهنمای AGD شامل پیکربندی این ID است.

[۱] Operational Guidance

اگر خلاصه مشخصه محصول دلالت کند که سازوکارهای موجود در FCS_SMIME_EXT.1.7 قابل پیکربندی هستند، محصول باید تحقیق کنند که راهنمای AGD شامل پیکربندی این سازوکارها است.

آزمون‌ها

ارزیاب باید آزمون‌های زیر را برای هر کدام از انواع رویدادها انجام دهد:

این آزمون‌ها باید از طریق ارتباط پیوسته با آزمون تعریف‌شده در FIA_X509 برای تائید گواهی/زنجیره گواهی و FDP_NOT_EXT.1 انجام شوند.

- آزمون ۱: محصول باید یک پیام بدون محافظت (بدون امضا یا رمزنگاری) ارسال و دریافت کرده و بررسی کند که پیام به‌درستی منتقل‌شده و می‌تواند در عامل دریافت[۱] مشاهده شود. این انتقال می‌تواند به‌عنوان بخشی از تعدادی سازوکار انجام شود. کافی است مشاهده شود که پیام با محتوایی مشابه با آنچه در هنگام ارسال داشته، به گیرنده مدنظر رسیده است.
- آزمون ۲: محصول باید یک پیام امضاءشده را با استفاده از هریک از الگوریتم‌های مشخص‌شده در مجموعه الزامات متناظر، ارسال و دریافت کنند و تائید نمایند که امضاء برای هردو پیام دریافت شده و ارسال‌شده معتبر است. پس‌ازاینکه اعتبار امضاءها بررسی شد، محصول باید یک پیام امضاءشده با استفاده از هریک از الگوریتم‌های مشخص‌شده در مجموعه الزامات، ارسال کنند و یک ابزار حمله استراق سمع[۲] برای اصلاح حداقل یک بایت از پیام استفاده کنند؛ طوری که باعث شود امضاء اعتبار نداشته باشد. این کار می‌تواند با اصلاح محتوای پیام‌بر آنچه امضا محاسبه‌شده یا اصلاح امضاء به‌تنهایی، انجام شود. محصول باید تحقیق کنند که پیام دریافت شده در بررسی اعتبار امضاء رد می‌شود.

[۱] receiving agent

[۲] man-in-the-middle

- آزمون ۳: محصول باید یک پیام رمزنگاری با استفاده از هر یک از الگوریتم‌های مشخص‌شده در مجموعه الزامات ارسال و دریافت کنند. محصول باید بررسی کنند که محتویات در انتقالات رمزنگاری‌شده‌اند و پیام دریافت شده رمزگشایی‌شده باشد. پس‌ازاینکه رمزگشایی پیام ارزیابی شد، محصول باید یک پیام رمزنگاری‌شده را با استفاده از الگوریتم‌های مشخص‌شده در مجموعه الزامات، ارسال کنند و ابزار حمله استراق سمع برای اصلاح حداقل یک بایت از پیام را استفاده نمایند بطوریکه رمزنگاری اعتبار خود را از دست دهد. محصول باید بررسی کنند که پیام دریافت شده در رمزگشایی ناموفق باشد.
- آزمون ۴: محصول باید یک پیام که امضاء و رمزنگاری‌شده را ارسال و دریافت کنند. بعلاوه، محصول باید یک ابزار حمله استراق سمع برای اصلاح حداقل یک بایت از پیام استفاده کنند؛ طوری که باعث شود امضاء و رمزنگاری اعتبار خود را از دست دهند. محصول باید بررسی کنند که پیام دریافت شده در رمزگشایی ناموفق بوده، در بررسی اعتبار امضاء ناموفق بوده و یا در هردو ناموفق باشد.
- آزمون ۵: محصول باید یک پیام امضاءشده با استفاده از الگوریتم امضاء[۱] به ایمیل کلاینت ارسال کنند که طبق الگوریتم شناساگر امضاء دیجیتال پشتیبانی نمی‌شود (به‌عنوان‌مثال، SHA1). محصول باید تحقیق کنند که ایمیل کلاینت اعلانی مبنی بر اینکه محتویات نمی‌توانند بررسی شوند، ارائه کند؛ زیرا الگوریتم امضاء پشتیبانی نشده است.
- آزمون ۶: محصول باید یک پیام رمزنگاری‌شده با استفاده از الگوریتم رمزنگاری به ایمیل کلاینت ارسال کنند که طبق حوزه شناساگر الگوریتم پشتیبانی نمی‌شود. محصول باید بررسی کنند که ایمیل کلاینت محتویات پیام را نمایش/رمزگشایی نمی‌کند.
- آزمون ۷: محصول باید یک پیام امضاءشده توسط گواهی را بدون نشاندن بیت امضاء دیجیتال به ایمیل کلاینت ارسال کنند. محصول باید تحقیق کنند که ایمیل کلاینت به کاربر اعلام کند که امضاء نامعتبر است.

[۱] signature algorithm

• آزمون ۸: محصول باید یک پیام امضاءشده توسط گواهی را بدون هدف حفاظت ایمیل[۱] در کلید کاربری پیوست، ارسال کنند. محصول باید بررسی نماید که ایمیل کلاینت کاربر را از فاقد اعتبار بودن امضاء آگاه می‌کند. • آزمون ۹: محصول باید تائید کنند که ایمیل کلاینت از پروتکل وضعیت گواهی آنلاین استفاده می‌کند یا CRL را در تکرار اختصاص‌یافته، بارگیری کرده است.	
حفاظت از کلید و اجزای کلید توسعه‌یافته ۱	**۸**
ایمیل کلاینت باید [انتخاب: هنگام پیروی از الزام FCS_COP_EXT.2 مشخص‌شده، نباید کلیدها را در حافظه غیر فرار ذخیره نماید؛ مگر اینکه کلیدها با یکی از معیارهای زیر مطابقت داشته باشند: [انتخاب: کلید متن آشکار نباید بخشی از زنجیره کلیدی مشخص‌شده در FCS_KYC_EXT.1 باشد، کلید متن آشکار بعد از تأمین اولیه، دیگر قادر به دسترسی به داده‌های رمزنگاری‌شده نباشد، کلید متن آشکار یک کلید تقسیم است که مطابق با مشخصه‌های FCS_SMC_EXT.1 ترکیب یافته و نیم دیگر از کلید تقسیم نیز [انتخاب: طبق پوشش FCS_COP_EXT.2 مشخص‌شده، برگرفته شده و در حافظه غیر فرار ذخیره نشده است]، کلید متن آشکار بر روی یک حافظه خارجی ذخیره‌شده که برای استفاده به‌عنوان یک عامل اعطای مجوز به کار می‌رود، کلید متن آشکار برای محافظت از یک کلید مشخص‌شده در FCS_COP_EXT.2 استفاده شود که در حال حاضر مطابق با مشخصات FCS_COP_EXT.2 است، کلید متن آشکار یک بخش عمومی از جفت کلید است.]].	

[۱] Email Protection

نکته کاربردی: ذخیره سازی کلید متن آ شکار در حافظه غیر فرار به چند دلیل مجاز ا ست: اگر کلیدها داخل حافظه‌ی محافظت شده با شند، که برای کاربر بر روی ایمیل کلاینت یا محیط عملیاتی قابل دسترس‌پذیر نیست، تنها، روش‌هایی که اجازه می‌دهند که آن یک نقش امنیتی ایفا کند که یک کلید تقسیم باشد یا فراهم‌کننده لایه‌های اضافی پوشش یا رمزنگاری روی کلیدهایی که تاکنون حفاظت‌شده‌اند.

اقدامات تضمین:

- **خلاصه مشخصه محصول**

در محصول باید بررسی شود که خلاصه مشخصه محصول، برای توصیفی سطح بالا از کلیدهای حفاظت مورداستفاده است که در حافظه غیر فرار ذخیره‌شده‌اند.

در محصول باید بررسی شود که خلاصه مشخصه محصول تضمینی بر توصیف فضای ذخیره‌شده همه کلیدها است و حفاظت از همه کلیدها، در یک حافظه غیرفرار ذخیره‌شده است. توصیف زنجیره کلید باید بررسی شود تا اطمینان حاصل شود که FCS_COP_EXT.2 برای ذخیره کلیدهای پوشش داده‌شده یا رمزنگاری‌شده در یک حافظه غیر فرار پیگیری شده و کلید متنی در حافظه غیر فرار یکی از معیارهای ذخیره‌سازی را رعایت می‌کند.

راهنما

کاربرد ندارد

۹	**تخریب کلید رمزنگاری توسعه‌یافته ۱**

ایمیل کلاینت باید

[انتخاب: فراخوانی بستر فراهم‌کننده تخریب کلیدی، اجرای کلید تخریب با استفاده از [انتخاب:برای حافظه فرار، پاک سازی[۱] حافظه باید توسط یک بازنویسی مستقیم اجرا شود [انتخاب:

[۱] erasure

متشکل از یک الگوی شبه‌تصادفی[۱] با استفاده از RBG ایمیل کلاینت.

متشکل از یک الگوی شبه‌تصادفی با استفاده از RBG بستر میزبان.

متشکل از صفرها.]

برای حافظه غیر فرار، باید پاک سازی حافظه توسط:

[انتخاب:

یک

سه، یا دفعات بیشتر]

بازنویسی از محل ذخیره داده‌های کلیدی شامل [انتخاب:

یک الگوی شبه تصادفی با استفاده از RBG ایمیل کلاینت، همان‌طور که در FCS_RBG_EXT.1 توصیف شده است.

یک الگوی شبه تصادفی با استفاده از پلتفرم میزبان یک الگوی ثابت]]]

که متناسب با [انتخاب: NIST SP80088،بدون استاندارد] برای از بین بردن همه اجزای کلید[۲] و پارامترهای امنیتی رمزنگاری در موقعی انجام می‌گیرد که دیگر مورد نیاز نمی‌باشند.

- **اقدامات تضمین**

خلاصه مشخصه محصول

[۱] pseudorandom

[۲] keying material

اگر بستر، تخریب کلید را فراهم کند، محصول باید خلاصه مشخصه محصول را آزمایش کنند تا تعیین شود که قابلیت تخریب کلی چگونه فراخوانی می‌شود.

اگر نرم‌افزار، تخریب کلید را فراخوانی می‌کند، محصول باید از اینکه خلاصه مشخصه محصول توصیفگر هریک از کلیدهای راز[۱](کلیدهای استفاده‌شده برای رمزنگاری متقارن و/یا احراز هویت داده‌ها)، کلیدهای اختصاصی[۲] و CSPهای استفاده‌شده در ایجاد کلید است، اطمینان حاصل کنند؛

زمان حذف داده‌های کلیدی[۳] (برای مثال، بلافاصله پس از استفاده، در هنگام خاموش کردن سیستم و غیره.) و نوع رویه‌ای که در حذف داده‌های کلیدی مورداستفاده قرار می‌گیرد (بازنویسی با صفر، بازنویسی سه مرتبه‌ای با الگوی تصادفی و غیره.) اگر برای ذخیره موادی که باید مورد محافظت قرار گیرند، از حافظه‌های مختلفی استفاده شود، محصول باید اطمینان یابند که خلاصه مشخصه محصول، توصیفگر رویه حذف داده‌های کلیدی از قالب حافظه‌ای است که داده‌ها بر آن ذخیره‌شده‌اند. (برای مثال، "کلیدهای مخفی ذخیره‌شده روی درایو[۴] با یک‌بار بازنویسی با چندین صفر حذف می‌شود درحالی‌که کلیدهای ذخیره‌شده روی هارد[۵] داخلی توسط سه مرتبه نوشتار با الگوی تصادفی که قبل از هر بار نوشتن تغییر می‌کند، حذف می‌شود").

راهنما

کاربرد ندارد

آزمون‌ها

آزمون زیر فقط برای تخریب کلید است که توسط ایمیل کلاینت فراهم‌شده است:

---

[۱] secret

[۲] private

[۳] zeroized

[۴] drive

[۵] Hard

آزمون ۱: برای هر نوع خدمت صدور مجوز، مود رمزنگاری و عملیات رمزنگاری، یک عامل صدور مجوز شناخته‌شده و زنجیره‌ای از کلیدهایی که باید با مجموعه داده‌های رمزگزاری‌شده مرتبط[۱] برای محصول فراهم شوند. (برای مثال اگر یک کلمه عبور برای ایجاد یک کلید واسطه استفاده شود، متن رمز شده دربردارنده کلید رمزنگاری باشد همچنین کلید واسطه باید برای محصول فراهم شود.) محصول باید بر طبق خلاصه مشخصه محصول مشخص کنند که تعریف فروشنده[۲] از "دیگر موردنیاز نیست" چیست و توالی اقداماتی را که در این زمینه از سوی ایمیل کلاینت برای فراخوانی طی شده، اجرا نماید. در این رابطه، محصول باید یک روگرفت[۳] از حافظه فرار ایجاد کرده و روگرفت بازیابی شده را برای صدور مجوز اعتبارنامه‌ها یا کلیدها جستجو کنند (برای مثال اگر کلمه‌عبور "PaSSw0rd" بوده یک جستجوی رشته‌ای برای"PaSSw0rd" ایجاد کند). محصول باید هر دستور، برنامه یا اقدام صورت گرفته در طی این فرایند را مستندسازی کنند، و باید تائید کنند که هیچ پارامتر کلید متن آشکار در حافظه فرار مستقر نیست. محصول باید این آزمون را سه بار برای اطمینان از تکرارپذیری انجام دهند. اگر در طی این دوره آزمایشی محصول تائید کنند که مواد کلیدی در حافظه فرار باقی‌مانده‌اند، باید قابلیت مشخص کردن علل آن‌ها وجود داشته باشد (برای مثال اجرای فرمان grep برای "PaSSw0rd" باعث ایجاد یک مثبت کاذب می‌شود) و علت نقص در تطابق با الزام را مستند نماید. ارزیاب باید این همین آزمون را برای جستجوی پارامترهای کلید در حافظه غیرفرار تکرار کند. **نکته کاربردی:** به‌منظور این الزام، مواد کلید، اشاره به داده‌های احراز هویت، کلمه‌عبورها، کلیدهای متقارن، داده‌های استفاده‌شده برای استخراج کلید و غیره دارد. الزام تخریب ذکرشده در بالا، برای هر حوزه ذخیره‌سازی میانه، برای پارامترهای مهم امنیتی رمزنگاری/کلید (مثل هرگونه ذخیره‌سازی، از قبیل بافرهای حافظه که در مسیر چنین داده‌هایی قرار داده شده‌اند) هنگام انتقال پارامترهای امنیتی مهم رمزنگاری/کلید به مکان حافظه دیگر بکار می‌رود.	
زنجیره‌ای کردن کلید توسعه‌یافته ۱	**۱۰**

[۱] associated ciphertext data set

[۲] vendor

[۳] dump

ایمیل کلاینت باید یک زنجیره کلید (از موارد ذیل) نگهداری کند:

[انتخاب: یک، یک کلید ذخیره شده در محل ذخیره‌سازی کلید پلت فرم [۱]، کلیدهای میانی ناشی از [انتخاب: یک کلمه‌عبور که در FCS_CKM_EXT.5.1 مشخص‌شده، یک یا چند عامل صدور گواهی، گواهی‌های ذخیره‌شده در محل ذخیره‌سازی کلید برای کلیدهای رمزگشایی/رمزنگاری داده‌ها با استفاده از روش‌های زیر استفاده شود:

[انتخاب:

استفاده از محل ذخیره‌سازی کلید پلت فرم،

به‌کارگیری محل ذخیره‌سازی کلید پلت فرم که حفاظت[۲] کلید با یک کلید فراهم‌شده TSF انجام می‌شود،

پیاده‌سازی حفاظت از کلید مطابق با آنچه که در FCS_COP_EXT.2 مشخص‌شده است،

پیاده‌سازی ترکیب کلید مطابق با آنچه که در FCS_SMC_EXT.1 مشخص‌شده است]

در حای که قدرت مؤثر با استفاده از موارد زیر حفظ شده باشد

[انتخاب:۱۲۸ بیت، ۲۵۶ بیت]]

نکته کاربردی: زنجیره‌ای کردن کلید، روشی است با استفاده از چندین لایه از کلیدهای رمزنگاری برای امن نمودن کلید رمزنگاری داده‌ها است. تعداد کلیدهای میانی(واسطه) متفاوت خواهد بود. این امر برای تمام کلیدهایی که در محافظت نهایی یا استنتاج داده‌های کلید رمزنگاری مشارکت دارند، دلالت می‌کند؛ ازجمله آن‌هایی که در حوزه‌های حفظ‌شده هستند. این الزام همچنین توصیف می‌کند که کلیدها چگونه ذخیره می‌شوند.

- **اقدامات تضمین**

[۱] storage

[۲] Wrap

خلاصه مشخصه محصول

برای محصول باید بررسی کنند که خلاصه مشخصه محصول* توصیف سطح بالایی از سلسله‌مراتب کلید برای همه روش‌های صدور گواهی است که برای حفاظت از کلیدهای رمزنگاری استفاده می‌شود. برای محصول باید خلاصه مشخصه محصول را امتحان کنند تا اطمینان یابند که زنجیره کلید به‌تفصیل توصیف‌شده. این توصیف باید مرور شود تا اطمینان حاصل شود که نگه‌دارنده‌ی زنجیره‌ای از کلیدهایی است که برای حفاظت کلیدها مطابق با FCS_COP_EXT.2 است. برای محصول باید تحقیق کنند که خلاصه مشخصه محصول* تضمین‌کننده توصیفی بر چگونگی فعالیت‌های رویه زنجیره کلیدی باشد، بطوریکه هیچ یک از اجزایی را که ممکن است با هر کلیدی در زنجیره مطابقت داشته باشد نمایش ن‌دهد. یک توصیف سطح بالا باید دربردارنده نموداری باشد که شرح دهنده سلسله‌مراتب اجرای کلید و جزییات مکانی که همه کلیدها و موادکلیدزنی یا نتایج حاصل از آن در آن ذخیره‌شده‌اند. برای محصول باید بررسی شود که اطمینان حاصل شود سلسله‌مراتب کلید، تضمینی است که هیچ نقطه‌ای از زنجیره نمی‌تواند بدون یک جستجوی کامل[۱] رمزگشایی شکسته شود یا دانش کلید درون زنجیره و قدرت مؤثر رمزنگاری داده‌ها از طریق زنجیره کلید حفظ‌شده.

* در صورت لزوم، این اطلاعات می‌تواند در یک سند اختصاصی مندرج شود و در خلاصه مشخصه محصول وارد نشود.

اگر بستر فراهم‌کننده تولید بردار مقداردهی اولیه [۲] باشد، ارزیاب باید بررسی کند که خلاصه مشخصه محصول توصیف‌کننده چگونگی فراخوانی تولید IV است.

راهنما

کاربرد ندارد

۱۱	**تولید بردار مقداردهی اولیه توسعه‌یافته ۱**

[۱] exhaust

[۲] Initialization Vector (IV)

ایمیل کلاینت باید بردارهای مقداردهی اولیه را مطابق ذیل تولید نماید:

[انتخاب:

CBC: بردارهای مقداردهی اولیه باید غیرتکراری[۱] باشند،

CCM: بردار مقداردهی اولیه باید غیرتکراری باشد،

XTS: مقادیر No IV. Tweak باید اعداد صحیح نامنفی بوده، متوالی اختصاص داده شده باشند و با یک عدد صحیح نامنفی دلخواه شروع شوند،

GCM: بردار مقداردهی اولیه (IV) باید غیرتکراری باشد. برای یک کلید مخفی نباید تعداد GCM از 2^{32} بیشتر باشد.

نکته کاربردی:

الزام کارکرد امنیتی FCS_IVG_EXT.1.1 مشخص می‌کند که چگونه باید برای هر مود رمزنگاری، بردار مقداردهی اولیه ساماندهی شود. CBC، XTS و GCM برای رمزنگاری AES داده‌ها مجاز می‌باشند. AES-CCM مود مجاز برای محافظت از کلید است.

- **اقدامات تضمین**

خلاصه مشخصه محصول

برای محصول باید اطمینان حاصل شود که خلاصه مشخصه محصول، توصیف‌کننده چگونگی ساماندهی بردارهای مقداردهی اولیه و تنظیم‌ها[۲] است (بر اساس سبک AES). در محصول باید بردارهای مقداردهی اولیه و تنظیم‌های الزامات ذکرشده رعایت می‌شود.

راهنما

[۱] Nonrepeating

[۲] Tweaks

کاربرد ندارد

۶-۲- کلاس حفاظت از داده کاربری

۱۲	اعلان وضعیت S/MIME توسعه‌یافته ۱

ایمیل کلاینت باید نشان‌دهنده یک اعلان از وضعیت S/MIME از ایمیل‌های مشاهده شده باشد.

نکته کاربردی: وضعیت S/MIME نشان می‌دهد که آیا ایمیل امضاء یا رمزنگاری‌شده است و آیا امضاء تائید شده و گواهی‌های تائید مربوطه صادر شده است. این اعلان باید حداقل پس از مشاهده محتوی ایمیل، صادر شود. همچنین این پیاده‌سازی‌ها زمانی وضعیت S/MIME هر ایمیلی را نمایش می‌دهند که همه ایمیل‌ها به‌عنوان یک لیست مشاهده شوند.

- **اقدامات تضمین**

خلاصه مشخصه محصول

محصول باید اطمینان یابند که خلاصه مشخصه محصول توصیف‌کننده اعلان‌های وضعیت S/MIME است، ازجمله اینکه وضعیت S/MIME دلالت بر مشاهده یک فهرست از ایمیل‌ها است.

راهنما

محصول باید تائید کنند که راهنمای AGD (با تصاویر مناسب) فراهم‌کننده توصیفی از اعلان‌های وضعیت S/MIME است، ازجمله اینکه هریک از موارد زیر چگونه نشان داده‌شده‌اند: رمزنگاری، امضاهای معتبر و تائید شده، امضاهای نامعتبر و تائید نشده.

آزمون‌ها:

محصول باید آزمون‌های زیر را انجام دهند و یا لازم باشد این آزمون‌ها در رابطه با FCS_SMIME_EXT.1 انجام شوند:

آزمون ۱: محصول باید یک ایمیل امضاء نشده و نامعتبر برای کلاینت ارسال کنند و تائید کنند که پس از خواندن آن هیچ اعلانی مشاهده نشد.

آزمون ۲: محصول باید یک ایمیل معتبر برای کلاینت ارسال کنند و تائید کنند که پس از خواندن آن‌یک اعلان رمزنگاری‌شده مشاهده شد.

آزمون ۳: محصول باید یک ایمیل امضاءشده برای کلاینت ارسال کنند و تائید کنند که پس از خواندن آن‌یک اعلان امضاءشده مشاهده شد.

آزمون ۴: محصول باید یک ایمیل با امضاء نامعتبر برای کلاینت ارسال کنند (برای مثال، استفاده از گواهی که شامل آدرس ایمیل صحیح نیست یا یک گواهی که به ریشه ذخیره متصل نیست) و بررسی کند که پس از خواندن ایمیل، اعلان امضاء نامعتبر مشاهده شد.

۱۳	**حفاظت از داده کاربری، پست الکترونیک اینترنتی چندمنظوره/ امن توسعه‌یافته(S/MIME) ۱**

ایمیل کلاینت باید برای امضاء، بررسی، رمزنگاری و رمزگشایی ایمیل از S/MIME استفاده کند.

نکته کاربردی: توجه کنید که این الزام اجباری وجود ندارد که S/MIME برای همه پیام‌های ورودی/خروجی استفاده شود یا اینکه ایمیل کلاینت به صورت خودکار رمزنگاری و یا امضاء/ بررسی همه پیام‌های دریافت شده را انجام دهد.این الزام فقط مشخص می‌کند که سازوکار امضاء دیجیتال و رمزنگاری باید S/MIME باشد.

- **اقدامات تضمین**

خلاصه مشخصه محصول

برای محصول باید اطمینان حاصل شود که خلاصه مشخصه محصول شامل توصیفی از اجرای S/MIME و کاربرد آن در محافظت از ایمیل در مقابل اصلاح قابل‌تشخیص با استفاده از امضاء دیجیتال و افشای غیرمجاز با استفاده از رمزنگاری است.

برای محصول باید تائید شود که خلاصه مشخصه محصول توصیف کند آیا رمزگشایی و تائید امضاء در دریافت یا مشاهده محتویات پیام انجام می‌شود و آیا پیام‌ها با پاکت‌های S/MIME خود ذخیره می‌شوند. **راهنما** برای محصول باید اطمینان حاصل شود که راهنمای AGD شامل دستورالعمل‌هایی برای پیکربندی یک گواهی برای استفاده S/MIME و دستورالعمل‌هایی برای امضاء و رمزنگاری ایمیل است. **آزمون‌ها:** برای محصول باید این جزء در رابطه با آزمون‌هایی برای FCS_SMIME_EXT.1 و FDP_NOT_EXT.1 انجام شود.

۶-۳- کلاس شناسایی و احراز هویت

۱۴	**احراز هویت و رمزنگاری X509 ۱**
ایمیل کلاینت باید گواهی X.509v3 را همان‌طور که در RFC 5280 تعریف‌شده استفاده کند تا پشتیبانی از احراز هویت و رمزنگاری برای S/MIME صورت پذیرد.	
۱۵	**احراز هویت و رمزنگاری X509 ۲**
ایمیل کلاینت باید هنگامی‌که گواهی متناظر نامعتبر تلقی شده، از ایجاد یک کانال ارتباطی قابل‌اعتماد جلوگیری نماید. **نکته کاربردی:** کانال ارتباطی مورد اعتماد شامل هر TLS انجام شده توسط ایمیل کلاینت است. اعتبار توسط مسیر گواهی مشخص می‌شود، تاریخ انقضاء[۱] و وضعیت لغو مطابق با RFC 5280 است.	

[۱] expiration date

۱۶	**احراز هویت و رمزنگاری X509 ۳**
اگر گواهی امضاء کد نامعتبر تلقی شده، ایمیل کلاینت باید مانع از نصب کد شود.	
۱۷	**احراز هویت و رمزنگاری X509 ۴**
اگر گواهی حفاظت ایمیل نامعتبر تلقی شده، ایمیل کلاینت باید مانع از رمزنگاری ایمیل شود.	
۱۸	**احراز هویت و رمزنگاری X509 ۵**
اگر گواهی حفاظت ایمیل نامعتبر تلقی شده، ایمیل کلاینت باید مانع از امضاء ایمیل شود. • **اقدامات تضمین** در محصول باید با بررسی خلاصه مشخصه محصول اطمینان حاصل شود که برای استفاده از گواهی‌های موجود، توصیف چگونگی انتخاب‌های ایمیل کلاینت درباره انتخاب اینکه کدام گواهی استفاده شود، ذکرشده. در محصول باید خلاصه مشخصه محصول را به‌منظور بررسی توصیف رفتار ایمیل کلاینت درزمانی که یک ارتباط نمی‌تواند در طی بررسی اعتبار استفاده از یک گواهی در ایجاد یک کانال مورد اعتماد و حفاظت از ایمیل ایجاد شود، بررسی شود. **راهنما** در محصول باید بررسی شود که راهنمای مدیریتی شامل هر دستورالعمل لازم برای محیط عملیاتی است طوری که ایمیل کلاینت بتواند از گواهی‌ها استفاده کند. **آزمون‌ها** برای محصول باید آزمون‌های زیر انجام شوند:	

- آزمون ۱:برای محصول باید آزمون ۱ برای هر عملیات ذکرشده در FIA_X509_EXT.2.1 که نیازمند استفاده از گواهی‌ها است انجام شود. برای محصول باید ثابت شود که استفاده از یک گواهی بدون یک مسیر گواهی معتبر، نتیجه خود را به‌صورت نقص در کارکرد عملیات نشان می‌دهد. سپس باید هر گواهی موردنیاز برای اعتبار دهی گواهی مورداستفاده در عملیات را به محل ذخیره ریشه بستر منتقل کرده و نشان دهند که عملیات موفق بوده است.

آزمون ۲: برای محصول باید نشان داده شود که استفاده از یک گواهی موردنیاز که نیازمند اعتبارسنجی است، برای انجام حداقل برخی بخش‌های مرتبط با یک موجودیت non-TOE IT لازم است. سپس باید طوری محیط را دست‌کاری نمایند که ایمیل کلاینت قادر به بررسی اعتبار گواهی نباشد و مشاهده نمایند که اقدام انتخاب‌شده در FIA_X509_EXT.2.2 صورت پذیرفته است. اگر اقدام انتخاب‌شده قابل تنظیم-مدیریتی باشد، محصول باید راهنمای عملیاتی را پیگیری کرده تا مشخص کنند که همه گزینه‌های قابل تنظیم-مدیریتی پشتیبانی شده، به روش مستند شده خود رفتار می‌کنند.

۶-۴- کلاس مدیریت امنیت

۱۹	مدیریت کارکرد در محصول توسعه‌یافته ۱

ایمیل کلاینت باید قادر به انجام قابلیت‌های مدیریتی زیر باشد این قابلیت‌ها توسط کاربر یا مدیر سیستم به‌صورت زیر نشان داده می‌شوند:

X: اجباری

O: اختیاری

کارکرد مدیریتی	مدیر	کاربر
فعال/غیرفعال کردن دانلود اشیاء تعبیه شده و توسط [انتخاب: دامنه، فرستنده، نه دیگر روشی]	O	O
فعال/غیرفعال کردن متن آشکار فقط در مد کلی و توسط [انتخاب: دامنه، فرستنده، نه دیگر روشی]	O	O
فعال/غیرفعال کردن ارائه و اجرای ضمائم و توسط [انتخاب: دامنه، فرستنده، نه روش دیگر]	O	O

فعال/غیرفعال کردن اعلان‌های ایمیل	0	0
پیکربندی یک مخزن گواهی برای رمزنگاری	0	0
پیکربندی اجازه یا عدم اجازه ایجاد کانال قابل‌اطمینان درصورتی‌که ایمیل کلاینت نتواند یک ارتباط برای تعریف اعتبار یک گواهی ایجاد کند.	0	0
پیکربندی ارسال/دریافت پیام فقط برای استفاده از الگوریتم‌های رمزگشایی که در FCS_SMIME_EXT.1 تعریف شده است.	0	0
پیکربندی فرکانس بازیابی CRL	0	0
فعال/غیرفعال کردن پشتیبانی از افزونه	0	0
تغییر کلمه‌عبور/عبارت عبور اعتبارنامه احراز هویت	0	0
غیرفعال کردن کلید قابلیت بازیابی	0	0
پیکربندی قابلیت رمزگشایی	0	0
[اختصاص : سایر قابلیت‌های مدیریتی]	0	0

نکته کاربردی: برای قابلیت‌های مدیریتی، اصطلاح "مدیر سیستم" اشاره به وسیله غیرقابل تحرک یا صاحب دستگاهی از یک دستگاه سیار دارد. مدیر، در قبال فعالیت‌های مدیریتی شامل تنظیم خط‌مشی که در ایمیل کلاینت بکار می‌رود، مسئول است.

مدیر سیستم می‌تواند فعالیت از راه دور داشته باشد و می‌تواند مدیر MTA بوده و از طریق یک کنسول[۱] یا داشبورد مدیریت متمرکز فعالیت داشته باشد. برنامه‌هایکاربردی استفاده شده برای پیکربندی خط‌مش باید شناسه‌های خود، مجوز و الزامات امنیتی تکمیلی را برای اطمینان از مورد اعتماد بودن مدیر داشته باشند.

هدف از این الزام این است که مدیر مجاز به پیکربندی ایمیل کلاینت با یک خط‌مش باشد که ممکن است توسط کاربر قابل لغو نیست. اگر مدیر برای قابلیت مشخصی، سیاست‌گذاری نکرده باشد، ممکن است همچنان کاربر این قابلیت را بکار بگیرد. اعمال سیاست توسط خود ایمیل کلاینت صورت می‌گیرد، یا از طریق هماهنگی دوطرفه ایمیل کلاینت و پلت‌فرم ایمیل کلاینت سیاست اعمال می‌شود.

[۱] console

قابلیت پیکربندی برای ایجاد یک کانال ارتباطی مورد اعتماد برای قابلیت شرح داده‌شده در FIA_X509_EXT.2.2. مدیر اختیار پذیرش یا رد همه گواهی‌هایی که نمی‌توانند اعتبار دهی شوند را دارد، همچنین اختیار پذیرش یک گواهی دریافت شده که امکان تائید اعتبار آن وجود ندارد و همچنین عدم پذیرش یک گواهی داده‌شده که امکان تائید اعتبار آن وجود ندارد. بسته به انتخابی که مدیر در FIA_X509_EXT.2.2 داشته، ارتباط مورد اعتماد، می‌تواند برای همه گواهی‌هایی که نمی‌توانند اعتبار دهی شوند مجاز باشد، برای همه گواهی‌هایی که نمی‌تواند اعتباردهی شوند غیرمجاز باشد یا برای یک گواهی که نمی‌تواند اعتبار دهی شود مجاز باشد؛ یا برای یک گواهی داده شده که نمی‌تواند اعتباردهی شود، غیرمجاز باشد.

اگر عوامل صدور مجوز کلمه‌عبور یا عبارت عبور توسط ایمیل کلاینت مورداستفاده قرار بگیرد، باید انتخاب مناسب «تغییر» صورت پذیرد.

اگر ایمیل کلاینت فراهم‌کننده کارکرد رمزنگاری باشد (برای مثال، اندازه کلید) حتی اگر پیکربندی به صورت پارامترهایی باشد که ممکن است برای به‌کارگیری کارکرد رمزنگاری بر روی پلت‌فرم ایمیل کلاینت مورد استفاده قرار بگیرد، بنابراین باید «پیکربندی کارکرد رمزنگاری» را در برگیرد. مشخصات قابلیت پیشنهاد شده می‌تواند به عنوان bullet points در الزامات نوشته شود یا در TSS ذکر شود.

اگر ایمیل کلاینت شامل کارکرد ازیابی کلید نباشدباید فراهم‌کننده قابلیتی برای کاربر باشد که این قابلیت را خاموش کرده تا کلید بازیابی ایجاد نشود و هیچ کلیدی مجوز صدور نداشته باشد.

- **اقدامات تضمین**

فعالیت‌های تضمین برای این مؤلفه با انتخاب‌هایی اخذشده از طریق نویسنده هدف امنیتی صورت می‌گیرد. اگر یک قابلیت در هدف امنیتی انتخاب‌نشده باشد، اجرای فعالیت تضمین ذکرشده لازم نیست.

خلاصه مشخصه محصول

محصول باید تحقیق کنند که خلاصه مشخصه محصول توصیف‌کننده کارکردهای مدیریتی است که ممکن است فقط با مدیر بستر ایمیل کلاینت پیکربندی شود و هنگام مطابقت دادن باسیاست، نمی‌تواند توسط کاربر بازنویسی شود.

تغییر کلمه‌عبور: محصول باید راهنمای عملیاتی را بررسی کنند تا اطمینان یابند که این راهنما توصیف می‌کند که چگونه فاکتور مجوز دهی رمز عبور/کلمه عبور تغییریافته است.

غیرفعال کردن کلید بازیابی: اگر ایمیل کلاینت فراهم‌کننده کلید بازیابی باشد، باید این موضوع در خلاصه مشخصه محصول ذکر شود. همچنین خلاصه مشخصه محصول توصیف‌کننده چگونگی غیرفعال کردن این قابلیت باشد. این کار شامل توصیفی از چگونگی بازیابی موادی است که برای نگه‌دارنده بازیابی[۱] فراهم‌شده است.

پیکربندی رمزنگاری: محصول باید برای سایر الزامات(*_FCS) بر اساس خلاصه مشخصه محصول تعیین کنند که چه سهمی از عملکرد رمزنگاری قابل پیکربندی است.

راهنما

محصول باید راهنمای عملیاتی را بررسی کنند که شامل دستورالعمل‌هایی برای یک مدیر بستر ایمیل کلاینت برای پیکربندی توابع موجود در FMT_MOF_EXT.1.1 باشد.

غیرفعال کردن بازیابی کلید: اگر ایمیل کلاینت پشتیبان بازیابی کلید باشد، راهنمای غیرفعال کردن این قابلیت باید در اسناد AGD توصیف شود.

پیکربندی رمزنگاری: محصول باید اسناد AGD را بررسی نمایند تا مشخص شود که دستورالعمل‌هایی برای همه سازوکارهای ادعاشده وجود دارد.

آزمون‌ها

محصول باید آزمون‌های زیر را انجام دهند:

آزمون ۱: محصول باید بررسی کنند که توابع فعال‌سازی، غیر فعال‌سازی و پیکربندی همان‌گونه که در نظر گرفته‌شده، عمل می‌کنند.

[۱] recovery holder

آزمون ۲: محصول باید کارکردهای مدیریتی تنظیم کنند که توسط مدیر(شرکت) کنترل می‌شود و نمی‌تواند توسط کاربر بازنویسی شود. محصول باید این توابع را برای کلاینت اعمال کنند، در جایگاه یک کاربر، تلاش در بازنویسی هریک از این مجموعه‌ها نموده و تضمین کنند که ایمیل کلاینت این اجازه را ندارد. آزمون ۳: غیرفعال کردن بازیابی کلید: اگر ایمیل کلاینت، ایجادکننده توانایی بازیابی کلید با شد، محصول باید آزمونی تدبیر نمایند که اطمینان دهنده این با شد که قابلیت بازیابی کلید پس از پیگیری راهنمایی‌های فراهم‌شده توسط عرضه‌کننده، غیرفعال یا می‌تواند غیرفعال شود.

کلاس محافظت از محصول[۱]

۲۰	پشتیبانی افزونه‌های مورد اعتماد توسعه‌یافته ۱
ایمیل کلاینت باید قابلیت بارگذاری[انتخاب: افزونه‌های مورد اعتماد، هیچ افزونه‌ای] فراهم کند. **نکته کاربردی:** الزام کارکرد امنیتی FPT_AON_EXT.2 وابسته به انتخاب‌هایی است که در این قسمت صورت گرفته‌اند. اگر ایمیل کلاینت فقط پشتیبانی از نصب افزونه‌های مورد اعتماد را الزام نکند، باید پشتیبانی تمام افزونه‌هایی که در الزام کارکرد امنیتی FMT_MOF_EXT.1 ذکر شد را غیرفعال نماید. تائید رمزنگاری(مثلاً، مورد اعتماد) افزونه‌ها، در الزام کارکرد امنیتی FPT_AON_EXT.2.1 مورد آزمون قرار می‌گیرد. **خلاصه مشخصه محصول** محصول باید بررسی کنند که خلاصه مشخصه محصول توصیفگر آن است که ایمیل کلاینت توانایی بارگذاری افزونه‌های مورد اعتماد را دارد. **راهنما** محصول باید راهنمای عملیاتی را به‌منظور ارزیابی اینکه شامل دستورالعمل‌هایی درباره بارگیری منابع افزونه‌های قابل‌اعتماد است، بررسی نمایند.	

[۱] Protection of the TSF

آزمون‌ها
برای محصول باید این آزمون انجام شود: آزمون ۱: برای محصول باید به ایجاد محصول یک افزونه مورد اعتماد پرداخته و سعی در بارگیری آن شود. برای محصول باید تحقیق کنند که افزونه نامعتبر رد شده و قابلیت بارگیری ندارد.

۶-۵- کلاس کانال‌ها/مسیر امن[۱]

۲۱	**کانال امن توسعه‌یافته ۱**
ایمیل کلاینت باید ارتباطات را از کانال‌های مورد اعتماد دریافت یا آغاز نماید.	
۲۲	**کانال امن توسعه‌یافته ۲**
ایمیل کلاینت باید برای موارد زیر با استفاده از کانال‌های مورد اعتماد ارتباط [انتخاب: IMAP، SMTP، POP، پیوست‌های MAPI برای HTTP، MAPI/RPC، ActiveSync [اختصاص: پروتکل دیگر(مرجع RFC یا مشخص‌سازی[۲])]]برقرار کند. **نکته کاربردی:** الزام کارکرد امنیتی FIA_SASL_EXT.1 وابسته به انتخاب‌هایی است که در این بخش انجام می‌شود. برای مثال اگر POP انتخاب شود باید FIA_SASL_EXT.1.2 در هدف امنیتی گنجانده شود. انتخاب‌ها باید شامل حداقل یک پروتکل ارسال و یک پروتکل دریافت باشند. اگر اختصاص مورداستفاده قرار بگیرد، مجوز دهنده هدف امنیتی همچنین باید یک مرجع برای پروتکل قرار دهد (برای مثال، یک عدد RFC).	

[۱] Trusted Path/Channels (FTP)

[۲] specification

- **اقدامات تضمین**

خلاصه مشخصه محصول

برای محصول باید بررسی شود که خلاصه مشخصه محصول مشخص‌کننده جزییاتی تفصیلی از ارتباط ایمیل کلاینت با یک Mail Transfer Agent در قالب ارتباط معتبری است(مثلاً، TLS) که مطابق با FTP_DIT_EXT.1 و همراه با مشخصه‌ها و رویه‌های خاص ایمیل کلاینت باشد، که ممکن است این خصیصه‌ها را منعکس نکنند.

راهنما

برای محصول باید تائید شود که راهنمای عملیاتی شامل دستورالعمل‌هایی برای ایجاد ارتباط با عامل انتقال ایمیل است.

آزمون‌ها

همچنین برای محصول باید آزمون‌هایی انجام دهند:

• آزمون ۱: برای محصول باید اطمینان حاصل شود که ایمیل کلاینت قادر به برقراری ارتباطاتی با استفاده از هر پروتکل منتخب یا اختصاص‌یافته‌ای است که در الزامات TLS مشخص‌شده؛ راه‌اندازی ارتباطاتی که در راهنمای عملیاتی ذکر شد و اطمینان از اینکه این ارتباطات موفقیت‌آمیز بوده است.

• آزمون ۲: برای محصول باید اطمینان حاصل شود که ایمیل کلاینت برای استفاده از SMTP و هر پروتکل اختصاص‌یافته که الزامات آن درTLS مشخص‌شده، قادر به برقراری ارتباطاتی با عامل انتقال ایمیل بوده، مطمئن شوند که راه‌اندازی ارتباطات، همان‌گونه که در راهنمای عملیاتی بیان‌شده، انجام‌شده باشد و این ارتباط موفقیت‌آمیز بوده است.

• آزمون ۳: برای محصول باید اطمینان پیدا شود که برای هر کانال ارتباطی با یک موجودیت فناوری اطلاعات در آزمون‌های ۱ و ۲، کانال داده‌ها در متن ارسال نشده است. برای انجام این آزمون، محصول باید یک sniffer و یک تحلیل‌گر بسته‌ها استفاده کنند. تحلیل‌گر بسته‌ها باید تائید کند که پروتکل مورداستفاده، TLS است.

۷- پیوست یک

الزامات انتخابی

الزامات پایه (که باید برای محصول انجام شوند) در بدنه این بسته الحاقی موجود است. بعلاوه دو نوع دیگر از الزامات مشخص‌شده در پیوست یک و پیوست دو. نوع اول (در این پیوست) الزاماتی هستند که می‌توانند در هدف امنیتی ذکر شوند، اما برای ایمیل کلاینت به منظور مطابقت با ادعای انطباق با این بسته تکمیل‌شده، موردنیاز نیستند. نوع دوم (در پیوست دو) الزاماتی مبتنی بر انتخاب در بدنه بسته تکمیلی می‌باشند. اگر انتخاب‌های قطعی صورت گرفته باشد، باید الزامات اضافی در این پیوست آورده شود. توجه کنید که نویسنده هدف امنیتی مسئول کسب این اطمینان است که الزاماتی که مربوط به پیوست یک، پیوست دو می‌باشند ولی در فهرست نیامده‌اند (مانند، الزامات نوع FMT) نیز باید در هدف امنیتی آورده شود.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**اشتقاق کلید رمزنگاری (اصلاح[1] کلمه‌عبور/عبارت عبور) ۱**	FCS_CKM_EXT.5.1
۲	**تولید داده تصادفی (Salt) رمزنگاری ۱**	FCS_SAG_EXT.1.1
۳	**ایجاد رمزنگاری فعلی ۱**	FCS_NOG_EXT.1.1
۴	**اعلان URI ۱**	FDP_NOT_EXT.2.1
۵	**انبارش اطلاعات دائمی ۱**	FDP_PST_EXT.1.1
۶	**پردازش محتوای پیام ۱**	FDP_REN_EXT.1.1

۷-۱- کلاس پشتیبانی رمزنگاری

1 - Conditioning

۱	**اشتقاق کلید رمزنگاری (اصلاح کلمه‌عبور/عبارت عبور) ۱**

یک کلمه‌عبور/عبارت عبور که برای ایجاد یک مؤلفه مجوزدهی استفاده می‌شود، باید قابلیت زیر را داشته باشد: [انتخاب:

[اختصاص: عدد صحیح مثبت از ۶۴ یا بیشتر] کاراکترهایی در این مجموعه [انتخاب:

کاراکترهای حرف بزرگ

کاراکترهای حرف کوچک

اعداد

کاراکترهای خاص: !، @، #، $، ٪، ^، &، *،)، (

[اختصاص: سایر کاراکترهای خاص پشتیبانی‌شده]

] و باید توانایی اجرای [کارکردهای استخراج کلید مبتنی بر کلمه‌عبور] مطابق با یک الگوریتم رمزنگاری مشخص‌شده

[انتخاب:

HMACSHA256,

HMACSHA384
HMACSHA512

] با [انتخاب: [اختصاص: عدد صحیح مثبت بیشتر یا مساوی ۴۰۹۶]] تکرارو خروجی اندازه کلید رمزنگاری از [انتخاب:

۱۲۸ بیت

۲۵۶ بیت

] که مطابق با NIST SP 800132 است.

نکته کاربردی: کلمه‌عبور/عبارت عبور در سیستم میزبان به‌صورت کاراکترهای متوالی نمایش داده می‌شود که کدگذاری آن‌ها به ایمیل کلاینت و سیستم عملیاتی زیرین آن وابسته است. ا

این کلمه‌عبور/عبارت عبور باید مشروط بر رشته‌ای از بیت‌هایی باشد که تشکیل‌دهنده submask بوده تا به‌عنوان ورودی در یک کلید مورداستفاده قرار گیرند.

تایید صلاحیت می‌تواند با استفاده از یکی از کارکردهای hash شناخته‌شده یا فرایند توصیف‌شده در NIST SP ۸۰۰۱۳۲ صورت گیرد. روش مورداستفاده توسط نویسنده هدف امنیتی انتخاب می‌شود.

SP ۸۰۰۱۳۲ نیز نیاز به استفاده از یک کارکرد شبه تصادفی (PRF) شامل HMAC با یک تابع درهم‌سازی مناسب است

نویسنده هدف امنیتی تابع درهم‌سازی مورداستفاده را انتخاب می‌کند، همچنین الزامات مناسب برای HMAC و تابع درهم‌سازی را مشخص می‌کند.

پیوست A از SP ۸۰۰۱۳۲ توصیه به ایجاد تعداد تکرار داشته تا به افزایش محاسبات موردنیاز برای استخراج کلید از یک کلمه‌عبور منجر شده و بنابراین بارکاری عملکرد یک حمله بازیابی کلمه‌عبور را افزایش دهد. با این حال برای این بسته تکمیلی، حداقل تعداد تکرار ۴۰۹۶ مورد نیاز است تا تضمین دهد که ۱۲بیت امنیتی به مقدار کلمه‌عبور/عبارت عبور اضافه شده است یک مقدار مشخص قابل ملاحظه‌ای، برای اطمینان از امنیت بهینه توصیه‌شده است.

دو جنبه از این مؤلفه وجود دارد که نیازمند به ارزیابی است: کلمه‌عبور/عبارت عبور طول مشخص‌شده در الزامات پشتیبانی شود(حداقل ۶۴ کاراکتر) و کاراکترهای ورودی عاملی برای کارکرد شرطی منتخب باشند. این فعالیت بطور مجزا در آزمون‌های زیر بیان شده‌اند.

- **اقدامات تضمین**

خلاصه مشخصه محصول

برای محصول باید بررسی شود که خلاصه مشخصه محصول، مشخص‌کننده این خصوصیات است که یک کارکرد با حداقل تعداد کاراکترهای مشخص‌شده در هدف امنیتی، برای پذیرش کلمه‌عبور/عبارت عبور در این بیانیه اختصاص وجود دارد. محصول باید بررسی نماید که سلسله مراتب کلمه‌عبور خلاصه مشخصه محصول[۱] تضمین می‌کند که اطلاعات همه کلیدها توصیف‌شده و اندازه‌های کلید با آنچه که مجوزدهنده مشخص کرده، مطابقت دارد. محصول باید بررسی نماید که خلاصه مشخصه محصول توصیف‌کننده روشی است که توسط آن ابتدا کلمه‌عبور/عبارت عبور کدگذاری شده است و سپس با استفاده از الگوریتم SHA رمزگذاری می‌شود. تنظیمات الگوریتم (افزودن، مسدود کردن و غیره) باید توصیف‌شده باشد و باید برای محصول بررسی شود که این موارد با انتخاب‌های این مؤلفه همانند انتخاب‌های تابع درهم‌سازبه‌تنهایی انجام شود. برای محصول باید بررسی شود که خلاصه مشخصه محصول شامل توصیفی از چگونگی خروجی تابع درهم‌ساز است که برای ایجاد *submask* مورداستفاده قرار می‌گیرد. .

برای NIST SP 800132 مبتنی بر اصلاح کلمه‌عبور/عبارت عبور فعالیت‌های تضمین موردنیاز زمانی صورت می‌گیرد که فعالیت‌های تضمین برای الزامات مناسب[۲] (FCS_COP.1.1(4) [AppPP]) انجام‌شده باشد. اگر هرگونه دست‌کاری کلید در ایجاد submask برای استفاده کلید انجام شود، این فرایند باید در خلاصه مشخصه محصول توصیف شود. ارزیابی صریح اطلاعات submask از کلمه‌عبور ورودی موردنیاز نیست.

راهنما

ارزیاب باید راهنمای عملیاتی را بررسی نماید تا تعیین شود که چگونه کلمه‌عبور/عبارت عبور بزرگ بیرون از ایمیل کلاینت تولید می‌شود و روش‌هایی درباره چگونگی پیکربندی طول کلمه‌عبور/عبارت عبور و تنظیمات پیچیدگی اختیاری۳ (به بخش مدیریت توجه کنید) وجود دارد. این مسئله از این لحاظ اهمیت دارد که بسیاری از تنظیمات پیش‌فرض برای کلمه‌عبور/عبارت عبور آنتروپی موردنیاز مشخص‌شده برای این بسته تکمیلی را رعایت نمی‌کنند.

[۱] password hierarchy TSS

[۲] appropriate

[۳] optional complexity settings

آزمون‌ها

برای محصول باید آزمون‌های زیر انجام شوند:

- آزمون ۱: اطمینان از اینکه ایمیل کلاینت پشتیبان کلمه‌عبور/عبارت عبوری با ۶۴ کاراکتر است.
- آزمون ۲: تلاش برای واردکردن کلمه‌عبور/عبارت عبوری که تعداد کاراکترهای آن کمتر از ۶۴ است.
- آزمون ۳: اگر ایمیل کلاینت پشتیبان یک کلمه‌عبور/عبارت عبور با حداکثر تعداد کاراکتر ممکن n (بیش از ۶۴ کاراکتر) بود، اطمینان یابند که ایمیل کلاینت بیشتر از n کاراکتر را نمی‌پذیرد.

شرط‌گذاری: آزمون صریحی از شکل‌گیری عامل مجوز دهی از ورودی کلمه‌عبور/عبارت عبور گرفته نمی‌شود.

برای محصول باید بررسی شود که تعداد تکرار برای PBKDFs توسط ایمیل کلاینت که مطابق با NIST SP800-132 انجام‌شده اطمینان می‌دهد که خلاصه مشخصه محصول شامل توصیفی از زمان تخمینی موردنیاز برای استخراج مواد کلید از کلمه‌عبور بوده همچنین چگونه ایمیل کلاینت زمان محاسبه برای استخراج کلید مبتنی بر کلمه‌عبور را افزایش می‌دهد (که شامل افزایش تعداد تکرار بوده ولی به آن محدود نمی‌شود.)

۲	**تولید داده تصادفی (Salt) رمزنگاری ۱**

ایمیل کلاینت باید فقط Saltهایی را استفاده کند که ایجادشده توسط یک

] انتخاب:

RNG همان‌طور که در FCS_RBG_EXT.1 مشخص‌شده

RNG فراهم‌شده توسط بستر میزبان

نکته کاربردی: عدد salt باید تصادفی باشد.

- **اقدامات تضمین**

خلاصه مشخصه محصول

محصول باید بررسی کنند که خلاصه مشخصه محصول، مشخص‌کننده این است که چگونه salt ایجاد می‌شود. همچنین باید تائید کنند که salt با استفاده از روش ذکرشده در.FCS_RBG_EXT یا توسط محیط عملیاتی ایجادشده است. اگر کارکرد خروجی برای این هدف استفاده شود، خلاصه مشخصه محصول باید شامل API مشخصی باشد که با ورودی‌ها فراخوانی می‌شود.

اگر ایمیل کلاینت وابسته به ایجاد بیت تصادفی از بستر میزبان باشد، محصولمحصول باید تحقیق کنند که خلاصه مشخصه محصول شامل نام/سازنده RBG خروجی بوده و توصیف‌کننده فراخوانی تابع بوده و پارامترها هنگام فراخوانی خروجی تابع DRBG مورداستفاده قرار می‌گیرند.

اگر DRBGهای خروجی متفاوتی، برای بسترهای مختلف مورداستفاده قرار گیرد، خلاصه مشخصه محصول مشخص‌کننده هر RBG برای هر بستری است. همچنین خلاصه مشخصه محصول شامل توصیف کوتاهی از فرضیات عرضه‌کنندگان برای مقدار آنتروپی ایجادکننده DRBG خروجی است.

راهنما

N/A

۳	**ایجاد رمزنگاری فعلی ۱**

ایمیل کلاینت باید فقط شماره‌های فعلی را با حداقل اندازه ۶۴ بیت استفاده کند.

نکته کاربردی: شماره فعلی باید یکتا باشد.

- **اقدامات تضمین**

خلاصه مشخصه محصول

محصول باید اطمینان پیدا کنند که خلاصه مشخصه محصول توصیف‌کننده چگونگی ایجاد شماره‌های فعلی یکتا باشد. **راهنما** N/A

۷-۲- کلاس حفاظت از داده کاربر

ایجاد رمزنگاری فعلی ۱	۴
ایمیل کلاینت باید فقط شماره‌های فعلی را با حداقل اندازه ۶۴ بیت استفاده کند. **نکته کاربردی:** شماره فعلی باید یکتا باشد. • **اقدامات تضمین** **خلاصه مشخصه محصول** محصول باید اطمینان پیدا کنند که خلاصه مشخصه محصول توصیف‌کننده چگونگی ایجاد شماره‌های فعلی یکتا باشد. **راهنما** N/A	
اعلان URI ۱	۵
ایمیل کلاینت باید نشان‌دهنده کامل شناسه منبع یکتا (URI)[۱] هر پیوند تعبیه‌شده‌ای باشد.	

[۱] Uniform Resource Identifier (URI)

نکته کاربردی: پیوندهای تعبیه‌شده اشیاء شناسه منبع یکتا به‌صورت HTML هستند که ممکن است یک برچسب(مثل یک کلمه، عبارت، شمایل[۱] یا تصویر) داشته باشند که باعث مبهم شدن شناسه منبع یکتا پیوند شود. هدف از این الزام مبهم کردن پیوند است. شناسه منبع یکتا ممکن است به‌عنوان یک رویداد "خلاصه" نشان داده شود یا ممکن است در کنار برچسب ترجمه شده باشد.

- **اقدامات تضمین**

خلاصه مشخصه محصول

برای محصول باید بررسی شود که خلاصه مشخصه محصول شامل توصیفی از چگونگی تعبیه پیوندها و روشی باشد که توسط آن شناسه منبع یکتا پیوند نمایش داده می‌شود.

راهنما

برای محصول باید تضمین شود که راهنمای AGD شامل دستورالعمل‌هایی (به هر شکل دیداری مناسبی) برای مرور شناسه منبع یکتا برای یک پیوند تعبیه‌شده است.

آزمون‌ها

برای محصول باید آزمون زیر انجام شود:

آزمون ۱: محصول باید یک پیام HTML به همراه یک لینک تعبیه‌شده که در آن برچسب فقط شناسه منبع یکتا نیست (مثلاً، "اینجا کلیک کنید") به کلاینت ارسال کند. محصول باید پیام را مشاهده نموده و دستورالعمل‌های موجود در راهنمای AGD را دنبال و تائید کنند که شناسه منبع یکتا کامل که در پیوند تعبیه‌شده است، نمایش داده می‌شود.

۶	**انبارش اطلاعات دائمی ۱**

[۱] icon

ایمیل کلاینت باید قادر به عملیاتی بدون ذخیره‌سازی اطلاعات ماندگار در پلت فرم کلاینت باشد این کار از طریق استثناهای زیر انجام می‌شود: [انتخاب: اطلاعات اعتبارنامه، اطلاعات پیکربندی فراهم‌شده مدیریت، اطلاعات ابطال گواهی، بدون استثناها[۱]]

نکته کاربردی: هر داده‌ای که بعد از بستن ایمیل کلاینت همچنان موجود باشد، از قبیل، فایل‌های موقت، به عنوان داده ماندگار تلقی می‌شود. تائید این الزام نیازمند استفاده از پروتکلی از قبیل IMAP یا MAPI است. همچنین با پروتکل POP سازگار نمی‌باشد.

- **اقدامات تضمین**

خلاصه مشخصه محصول

باید برای محصول بررسی شود که خلاصه مشخصه محصول توصیف‌کننده اطلاعات ماندگاری است که در پلت‌فرم ذخیره‌شده و همچنین مکان‌هایی که این اطلاعات در پلت‌فرم ذخیره‌شده‌اند نیز باید مشخص شود. باید برای محصول تائید شود که داده‌های ماندگار توصیف‌شده، محدود به شناسه داده‌ها در این انتخاب می‌باشند.

راهنما

N/A

آزمون‌ها

برای محصول باید آزمون زیر انجام شود:

آزمون ۱: محصول باید طوری با ایمیل کلاینت فعالیت نماید که چندین پیام، امضاء، رمزگشایی و فاقد امضاء پردازش شوند. همچنین باید کارکردهایی از قبیل جابجایی پیام‌ها به فولدرها، پیام‌های پیش‌نویس ارسال نشده، و غیره همان‌طور که توسط کلاینت ارائه‌شده، تمرین شوند. سپس محصول باید پلت‌فرم کلاینت را به منظور تعیین تنها اطلاعات ماندگار ذخیره شده که در خلاصه مشخصه محصول تعیین‌شده، بررسی نمایند.

[۱] no exceptions

۷	پردازش محتوای پیام ۱

ایمیل کلاینت باید یک حالت فقط متنی داشته باشد که ترجمه و اجرای مواردی را غیرفعال نماید: [انتخاب:

HTML

جاوا اسکریپت

[اختصاص: انواع دیگر محتویات تعبیه‌شده]

هیچ نوع محتوی تعبیه‌شده

]

نکته کاربردی: مود فقط متنی از دانلود خودکار، ترجمه و نمایش تصاویر، و اشیا تعبیه‌شده مانند اشیا HTML یا جاوا اسکریپت جلوگیری می‌کند. پیکربندی این حالت در FMT_MOF_EXT.1.1 آمده است. نویسنده هدف امنیتی باید همه انواع محتویاتی که توسط ایمیل کلاینت و از طریق انتخاب‌ها یا اختصاص‌ها پشتیبانی می‌شود را مشخص کند. اگر ایمیل کلاینت فقط پشتیبان مود فقط متنی باشد، باید نوع هیچ محتوای تعبیه‌شده انتخاب شود.

- **اقدامات تضمین**

خلاصه مشخصه محصول

باید برای محصول تائید شود که خلاصه مشخصه محصول توصیف‌کننده مود فقط متنی برای ارسال و دریافت پیام‌ها است. همچنین باید بررسی شود که ایمیل کلاینت قادر به ترجمه و اجرای HTML و جاوا اسکریپت است. اگر ایمیل کلاینت قادر به ترجمه و اجرای HTML و جاوا اسکریپت باشد، این توصیف باید نشان دهد که چگونه ایمیل کلاینت پیام‌های دریافت شده را که شامل HTML یا جاوا اسکریپت را در مود فقط متنی بکار می‌گیرد. محصول باید اطمینان یابد که این توصیفات تائید می‌کنند که این انواع اشیا تعبیه‌شده ترجمه و اجرا نشده‌اند و منابع خارجی/تصویری به‌صورت خودکار دانلود نشده‌اند.

راهنما

برای محصول باید بررسی شود که راهنمای AGD شامل دستورالعمل‌هایی برای فعال‌سازی مود فقط متنی باشد.

آزمون‌ها

برای محصول باید آزمون‌های زیر انجام شوند:

- آزمون ۱: اگر در FDP_REN_EXT.1.1 مورد HTML انتخاب‌شده باشد، محصول باید به کلاینت یک پیام شامل اشیاء تعبیه‌شده HTML ارسال کرده و ترجمه HTML را بررسی نمایند. سپس باید مد فقط متنی را فعال کنند و تائید کنند که HTML را ترجمه نمی‌کند.
- آزمون ۲: اگر در FDP_REN_EXT.1.1 مورد جاوا اسکریپت انتخاب‌شده باشد، محصول باید به کلاینت یک پیام شامل اشیاء تعبیه‌شده جاوا اسکریپت ارسال کرده و ترجمه جاوا اسکریپت را بررسی نماید. سپس محصول باید مود فقط متنی را فعال کرده و تائید کنند که جاوا اسکریپت را ترجمه نمی‌کند.

۸- پیوست دو

الزامات مبتنی بر انتخاب

همان‌طور که در مقدمه این بسته الحاقی ذکر شد، الزامات پایه در پیوست پروفایل حفاظتی و در بدنه این بسته تکمیلی بیان‌شده‌اند. الزامات مکمل، بر مبنای انتخاب‌های پیوست پروفایل حفاظتی و یا در بدنه بسته تکمیلی وجود دارند: اگر انتخاب‌ها قطعی باشند، لازم است که الزامات مکمل زیر لحاظ شوند.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**پوشاندن کلید ۱**	FCS_COP_EXT.2.1
۲	**ترکیب کلید ۱**	FCS_SMC_EXT.1.1
۳	**لایه امنیت و احراز هویت ساده ۱**	FIA_SASL_EXT.1.1
۴	**لایه امنیت و احراز هویت ساده ۲**	FIA_SASL_EXT.1.2
۵	**لایه امنیت و احراز هویت ساده ۳**	FIA_SASL_EXT.1.3
۶	**لایه امنیت و احراز هویت ساده ۴**	FIA_SASL_EXT.1.4
۷	**نصب و به‌روزرسانی امن برای افزونه‌ها ۱**	FPT_AON_EXT.2.1
۸	**نصب و به‌روزرسانی امن برای افزونه‌ها ۲**	FPT_AON_EXT.2.2
۹	**نصب و به‌روزرسانی امن برای افزونه‌ها ۳**	FPT_AON_EXT.2.3

۸-۱- کلاس پشتیبانی رمزنگاری

۱	**پوشاندن کلید ۱**
ایمیل کلاینت باید [انتخاب:	

از کارکرد فراهم‌شده پلت فرم برای محافظت از کلید استفاده کند، پیاده‌سازی کارکرد را برای محافظت از کلید] در تطابق با یک الگوریتم رمزنگاری مشخص‌شده[اختصاص: محافظت از کلید AES محافظت از کلید AES با لایه‌گذاری[۱] RSA با استفاده از طرح KTS-OAEP-basic RSA با استفاده از طرح KTSO-AEP-receiver-confirmation ECC CDH] و اندازه کلید رمزنگاری [اختصاص: 128 bits (AES), 256 bits (AES), 2048 (RSA), 4096 (RSA), 256bit prime, modulus (ECC CDH), 384-bit prime modulus (ECC CDH)]مطابق با: [اختصاص:

[۱] padding

"NIST SP 80038F" برای محافظت از کلید (بخش ۶,۲) و برای محافظت از کلید با افزودن(بخش ۶,۳)

"NIST SP 80056A" بخش (۹,۲,۴)، KTS-OAEP-receiver-confirmation (بخش ۹,۲,۳) و طرح KTS-OAEP-basic از RSA برای استفاده "NIST SP 80056B" rev 2" برای ECC CDH (بخش ۵,۶,۱,۲ و ۶,۲,۲,۲)

].

این الزام وابسته به انتخاب موجود در FCS_KYC_EXT.1.1 و FCS_CKM_EXT.3.1 است.

نکته کاربردی: در اولین انتخاب، نویسنده هدف امنیتی موجودیتی را انتخاب می‌کند که عمل رمزنگاری/رمزگشایی را انجام می‌دهد. در دومین انتخاب، روش مورداستفاده برای رمزگشایی انتخاب می‌شود:

استفاده از یکی از دو روش محافظت از کلید مبتنی بر AES که در NIST SP 800-38F مشخص‌شده

استفاده از یکی از دو طرح KTS-OAEP برای RSA به‌نحوی‌که در NIST SP 800-56B توصیف‌شده (KTSOAEP-basic در بخش ۹,۲,۳ توصیف‌شده)

استفاده از ECC CDH به‌نحوی‌که در بخش ۶,۲,۲,۲ در NIST SP 80056A توصیف‌شده.

سومین انتخاب باید برای منعکس کردن اندازه کلید صورت گیرد. ۲۰۴۸/۴۰۹۶ برای طرح‌های مبتنی بر RSA مورداستفاده قرار می‌گیرد درحالی‌که اندازه اولیه ماژول‌ها برای طرح‌های مبتنی بر ECC استفاده می‌شود. پشتیبانی از اندازه‌های کلید 256 بیت AES برای ارزیابی ورودی محصولات بعد از سومین فصل سال ۲۰۱۵موردنیاز است. بر اساس روش(های) انتخاب‌شده، باید آخرین انتخاب برای استفاده در انتخاب مرجع(های) مناسب صورت بگیرد.

- **اقدامات تضمین**

خلاصه مشخصه محصول

محصول باید خلاصه مشخصه محصول را برای اطمینان از وجود یک توصیف سطح بالا از چگونگی حفاظت از کلید و برآورده سازی خصوصیات مناسب بررسی نماید. **راهنما** N/A	
ترکیب کلید ۱	۲
ایمیل کلاینت باید submasks ها را با استفاده از روش‌های زیر ترکیب نماید تا کلید دیگری ایجاد کند [انتخاب: exclusive OR (XOR), SHA256, SHA512] ***این الزام وابسته به الزام موجود در FCS_KYC_EXT.1.1 و FCS_CKM_EXT.3.1 است.*** **نکته کاربردی:** این الزام مشخص‌کننده روشی است که ممکن است یک محصول با استفاده از یک XOR یا یک SHA-hash تائید شده به ترکیب چندین ubmaskها بپردازد. • **اقدامات تضمین** **خلاصه مشخصه محصول** اگر کلیدها برای ایجاد یک کلید واسطه باهم XOR شده باشند، بخش خلاصه مشخصه محصول باید تعیین‌کننده چگونگی این مطلب باشد(مثلاً آیا الزامات سفارش دهی موجود است، بررسی‌ها انجام‌شده و غیره). همچنین محصول باید تائید کنند که خلاصه مشخصه محصول توصیف‌کننده این است که چطور اندازه خروجی ایجادشده حداقل برابر با کلید رمزگشایی داده‌ها است. **راهنما**	

N/A

۸-۲- کلاس شناسایی و احراز هویت

۳	**لایه امنیت و احراز هویت ساده ۱**
ایمیل کلاینت باید پشتیبان احراز هویت ساده و امنیت لایه باشد که مطابق با RFC 4422 است. ***این الزام وابسته به الزام موجود در FTP_ITC_EXT.1.2 است.*** **نکته کاربردی:** اگر ایمیل SMTP را برای ارسال پیام بکار گیرد، احراز هویت ساده و امنیت لایه موردنیاز است. کلاینت‌هایی که SMTP را مورداستفاده قرار نمی‌دهند،(مثل ActiveSync یا MAPI) نیازی به پشتیبانی برای احراز هویت ساده و امنیت لایه ندارند.	
۴	**لایه امنیت و احراز هویت ساده ۲**
ایمیل کلاینت باید پشتیبان POP3 CAPA و ضمایم AUTH برای سازوکار احراز هویت ساده و امنیت لایه باشد. ***این الزام وابسته به الزام موجود در FTP_ITC_EXT.1.2 است.***	
۵	**لایه امنیت و احراز هویت ساده ۳**
ایمیل کلاینت باید پشتیبان IMAP CAPABILITY و ضمایم AUTHENTICATE برای سازوکار احراز هویت ساده و امنیت لایه باشد. ***این الزام وابسته به الزام موجود در FTP_ITC_EXT.1.2 است.***	

۶	**لایه امنیت و احراز هویت ساده ۴**

ایمیل کلاینت باید پشتیبان ضمایم SMTP AUTH برای سازوکار احراز هویت ساده و امنیت لایه باشد.

این الزام وابسته به الزام موجود در FTP_ITC_EXT.1.2 است.

نکته کاربردی: برای پشتیبانی ایمیل کلاینت از گواهی‌های PKI X.509 برای POP3، IMAP و SMTP که در این سند موردنیاز است، ایمیل کلاینت باید روش اعتبار دهی احراز هویت ساده و امنیت لایه را که در RFC 4422 توصیف شد، پیوست‌های AUTH و CAPA برای POP3 که در5034 RFC توصیف شد، پیوست‌های AUTHENTICATION و CAPABILITY برای IMAP که در RFC 4959 توصیف شد، پیوست AUTH برای SMTP که در RFC 4954 توصیف شد را پشتیبانی نماید.

- **اقدامات تضمین**

خلاصه مشخصه محصول

باید برای محصول بررسی شود که خلاصه مشخصه محصول توصیف‌کننده جزییات ارتباط ایمیل کلاینت به یک عامل انتقال ایمیل در قالب اتصال احراز هویت ساده و امنیت لایه باشد که همراه با گزینه‌های مشخص یا رویه‌هایی است که ممکن است در این خصوصیات منعکس نشده باشند.

راهنما

محصول باید بررسی کنند که راهنمای عملیاتی شامل دستورالعمل‌هایی برای ایجاد ارتباط با عامل انتقال ایمیل است.

آزمون‌ها

باید برای محصول آزمون‌های زیر انجام شود:

• آزمون ۱: برای محصول باید اطمینان حاصل شود که ایمیل کلاینت قادر به شروع ارتباطاتی با استفاده از POP ، IMAP ، SMTP و الزامات احراز هویت ساده و امنیت لایه باشد؛ همچنین قادر به تنظیم ارتباطاتی باشد که در راهنمای عملیاتی توصیف شد و اطمینان از ارتباطات موفقیت‌آمیز حاصل شود. • آزمون ۲: برای محصول باید اطمینان حاصل شود که هر کانال ارتباطی با یک موجودیت مجاز فناوری اطلاعات در آزمون ۱، که یک دست‌داد احراز هویت ساده و امنیت لایه است، انجام‌شده است.

۸-۳- کلاس حفاظت از محصول

۱	**نصب و به‌روزرسانی امن برای افزونه‌ها ۱**
ایمیل کلاینت باید [انتخاب: قابلیت، قدرت نفوذ پلت فرم] برای فراهم کردن ابزاری برای تائید رمزنگاری افزونه با استفاده از یک سازوکار امضاء دیجیتال و [انتخاب: درهم‌ساز منتشر شده، هیچ توابع دیگری] قبل از نصب و به‌روزرسانی فراهم نماید. ***این الزام وابسته به الزام موجود در FPT_AON_EXT.1.1 است.***	
۲	**نصب و به‌روزرسانی امن برای افزونه‌ها ۱**
ایمیل کلاینت باید برای جستجوی نسخه فعلی افزونه، [انتخاب: ارائه توانایی، قدرت نفوذ پلت فرم] را فراهم نماید. ***این الزام وابسته به الزام موجود در FPT_AON_EXT.1.1 است.***	
۳	**نصب و به‌روزرسانی امن برای افزونه‌ها ۱**
ایمیل کلاینت باید از نصب خودکار افزونه جلوگیری نماید.	

این الزام وابسته به الزام موجود در FPT_AON_EXT.1.1 است.

- **اقدامات تضمین**

خلاصه مشخصه محصول

برای محصول باید بررسی شود که خلاصه مشخصه محصول بیانگر این باشد که ایمیل کلاینت افزونه‌هایی را که از منابع نامعتبر هستند رد می‌کند.

راهنما

باید برای محصول راهنمای عملیاتی به‌منظور تائید اینکه شامل دستورالعمل چگونگی پیکربندی ایمیل کلاینت با افزونه‌های منابع معتبر است بررسی شود.

آزمون‌ها:

باید برای محصول آزمون‌های زیر بررسی شوند:

آزمون ۱: باید برای محصول یک افزونه امضاءشده توسط یک منبع معتبر ایجاد شده و سعی در نصب آن شود. برای محصول باید بررسی شود که امضاء افزونه معتبر است و این افزونه قابلیت نصب دارد.

آزمون ۲: برای محصول باید یک افزونه امضاءشده با یک گواهی نامعتبر ایجاد شده و اقدام به نصب آن شود و بررسی شود که این افزونه امضاءشده رد شده و قابل‌نصب نیست.

آزمون ۳: برای محصول باید یک افزونه امضاشده با یک منبع معتبر ایجادکننده بدون امضاء مجدد آن را اصلاح نموده و اقدام به نصب آن شود. برای محصول باید بررسی شود که افزونه امضاءشده رد شده و قابل‌نصب نیست.

۹- نمادها و اختصارات

نماد	معادل انگلیسی	معادل فارسی
AES	Advanced Encryption Standard	استاندارد رمزگذاری پیشرفته
CBC	Cipher Block Chaining	زنجیره‌ای کردن قالب رمز
CC	Common Criteria	معیار مشترک
CRL	Certificate Revocation List	فهرست ابطال گواهی
CSP	Cryptographic Service Provider	تامین‌کننده خدمات رمزنگاری
DHE	Diffie-Hellman Ephemeral	موقت دایف - هلمن
DRBG	Deterministic Random Bit Generator	تولید کننده بیت تصادفی قطعی
DN	Distinguished Name	نام برجسته
DSA	Digital Signature Algorithm	الگوریتم امضای دیجیتال
ECC	Elliptic Curve Cryptography	رمزنگاری منحنی بیضوی
ECDSA	Elliptic Curve Digital Signature Algorithm	الگوریتم امضای دیجیتال منحنی بیضوی
FFC	Finite-Field Cryptography	رمزنگاری رشته متناهی
FIPS	Federal Information Processing Standards	استانداردهای پردازش اطلاعات فدرال
GCM	Galois/Counter Mode	مد شمارنده گالیوس

HMAC	Keyed Hash Message Authentication Code	کد احراز هویت پیام مبتنی بر چکیده‌ساز
HTML	HyperText Markup Language	زبان علامت‌گذاری فرا متنی
HTML5	HyperText Markup Language version 5	زبان علامت‌گذاری فرا متنی نسخه ۵
HTTP	HyperText Transfer Protocol	پروتکل انتقال فرامتن
HTTPS	HyperText Transfer Protocol Secure	پروتکل انتقال فرامتن امن
IETF	Internet Engineering Task Force	نیروی اجرای عملیات مهندسی اینترنت
IV	Initialization Vector	بردار اولیه
KAT	Known Answer Test	آزمون پاسخ معلوم
KDF	Key Derivation Function	تابع اشتقاق کلید
MTA	Mail Transportation Agent	عامل انتقال ایمیل
NIST	National Institute of Standards and Technology	مؤسسه ملی استاندارد و فناوری
OCSP	Online Certificate Status Protocol	پروتکل وضعیت گواهی آنلاین
OID	Object Identifier	شناسه موجودیت غیرفعال
PBKDF	Password-Based Key Derivation Function	تابع اشتقاق کلید مبتنی بر کلمه‌عبور
PDF	Portable Document Format	قالب سند قابل‌حمل
PP	Protection Profile	پروفایل حفاظتی
RBG	Random Bit Generator	تولید کننده بیت تصادفی
RFC	Request for Comment	درخواست برای تفسیر

RSA	Rivest-Shamir-Adleman cryptosystem	سیستم رمزنگاری رایوست، شامیر، ادلمن
SAR	Security Assurance Requirement	الزام تضمین امنیتی
SFP	Security Function Policy	خط‌مشی کارکرد امنیتی
SFR	Security Functional Requirement	الزام کارکرد امنیتی
SHA	Secure Hash Algorithm	الگوریتم درهم‌ساز امن
ST	Security Target	هدف امنیتی
S/MIME	Secure/Multipurpose Internet Mail Extensions	توسعه‌های پست اینترنتی چند منظوره یا امن
TLS	Transport Layer Security	امنیت لایه انتقال
TOE	Target of Evaluation	محصول
TSF	TOE Security Functionality	توابع امنیتی محصول
TSS	TOE Summary Specification	خلاصه مشخصه محصول

۱۰- منابع و مآخذ

شناسه	عنوان
[CC]	Common Criteria for Information Technology Security Evaluation
	Part1: Introduction and General Model, CCMB201209001, Version 3.1 Revision 4, September 2012.
	Part 2: Security Functional Components, CCMB201209002, Version 3.1 Revision 4, September 2012.
	Part 3: Security Assurance Components, CCMB201209003, Version 3.1 Revision 4, September 2012.
[AppPP]	Protection Profile for Application Software
[MSOXCMAPIHTTP]	Messaging Application Programming Interface (MAPI) Extensions for HTTP