به نام خدا

سند هدف امنیتی برنامه کاربردی اندروید

سامانه یکپارچه خدمات الکترونیک آرشام

نسخه ۱.۱۹.۰

مهندسی فناوری اطلاعات داده گستر آشام

اردیبهشت ماه ۱۴۰۲

نسخه ۱.۷

فهرست

۱ معرفی سند هدف امنیتی

۱/۱ مرجع سند هدف امنیتی و محصول

عنوان سند هدف امنیتی	سند هدف امنیتی برنامه کاربردی سامانه یکپارچه خدمات الکترونیک آرشام
نسخه	۱.۷
تاریخ	۱۴۰۲/۰۲/۱۸
نویسندگان	حامد رضازاد باری

نام تولید کننده (شرکت)	مهندسی فناوری اطلاعات داده گستر آرشام
نام محصول	برنامه کاربردی اندروید سامانه یکپارچه خدمات الکترونیک آرشام
نوع محصول	برنامه کاربردی اندروید
نسخه	۱.۱۹.۰

نوع محصول

برنامه کاربردی موبایل که بر روی سیستم عامل اندروید اجرا می شود.

نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز محصول

در جدول زیر سخت‌افزار، نرم افزار و میان افزارهای لازم برای کارکرد محصول بیان شده است:

کامپونت‌ها	حداقل الزامات
سخت افزار	گوشی تلفن همراه
پردازنده	Quad-core 1.8 GHz
حافظه	۴ گیگ
فضای آزاد مموری	32 گیگ
شبکه	GSM / HSPA / LTE

نرم افزار	سیستم عامل اندروید، API 26 به بالا

۲٫۱ شرح محصول

محصول مورد ارزیابی، یک برنامه کاربری تحت سیستم عامل اندروید می باشد. این محصول بستر و امکانات لازم برای برقراری ارتباط امن مورد نیاز به منظور انتقال اطلاعات ما بین برنامه کاربردی تحت وب و اکیپ های عملیاتی با استفاده از بستر شبکه اینترنت و یا APN سیم کارت موجود بر روی موبایل را فراهم می کند. این محصول به زبان برنامه نویسی جاوا پیاده سازی شده است.

ویزگی های اصلی این محصول عبارت است از:

کنترل احزار هویت کاربر

پروفایل کاربر

تحویل شیفت

درخواست مرخصی

مدیریت پیام ها(مشاهده لیست پیام ها، ارسال پیام جدید)

تشکیل و ارسال پرونده به سامانه

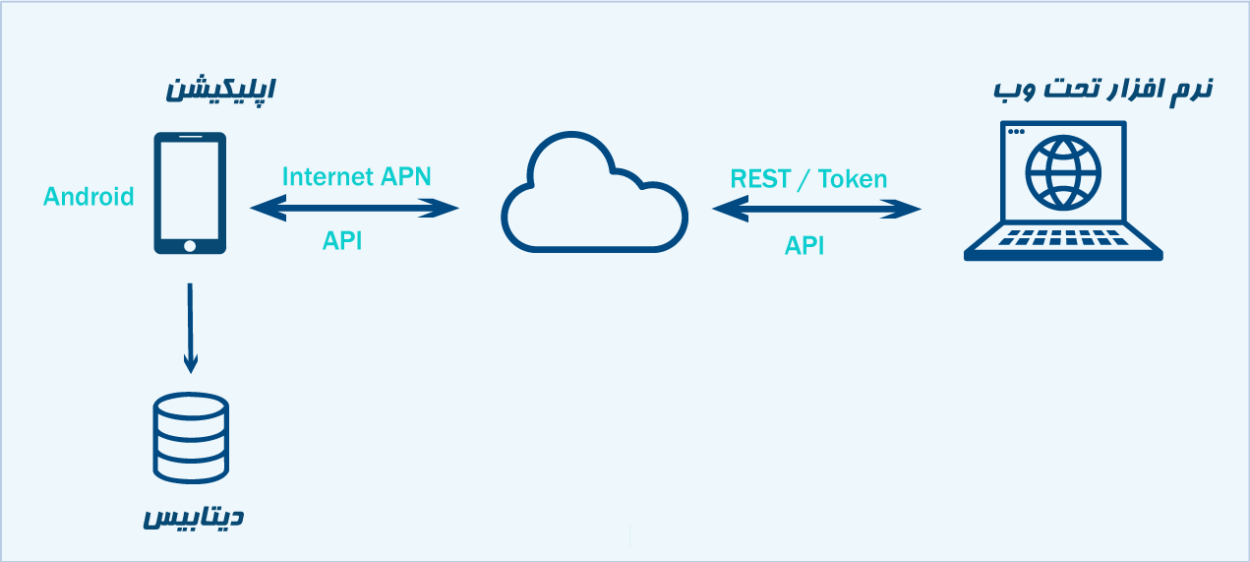
دریافت و بازدید از ایستگاه ها

ثبت انواع گزارشات به ازای پرونده

حوزه فیزیکی

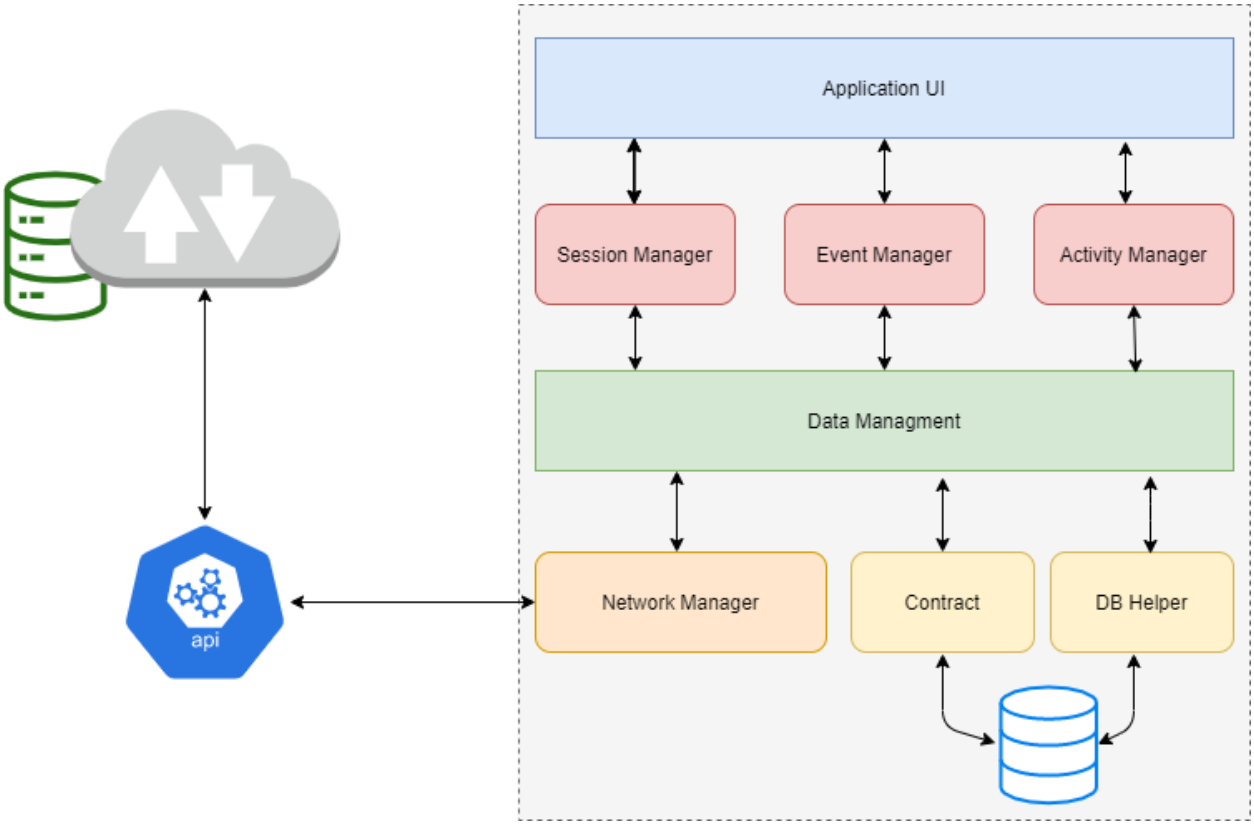
عناصر سخت‌افزاری و نرم‌افزاری مورد استفاده با توجه به پیکربندی ارزیابی در جدول زیر معرفی می‌شود:

عناصر محصول	شماره مدل یا نسخه
گوشی تلفن همراه	گوشی هوشمند
سیستم عامل اندروید	به بالا API 26



حوزه منطقی

کارکردهای امنیتی هدف ارزیابی تحت عنوان حوزه منطقی شناخته می‌شود که باید به صورت مشخص هریک از کارکردها و شرح آنها در این قسمت مطرح شود.



کارکردها	توصیف
شناسایی و احراز هویت	تمامی اکیپ های عملیاتی (کاربران) پیش از دسترسی به بخش های مختلف نرم افزار، باید براساس نام کاربری و رمز عبور خود لاگین کرده تا مجوز فعالیت آنها صادر گردد. لازم به ذکر می باشد، اطلاعات کاربران و مجوزها از طریق API موجود با نرم افزار تحت وب بررسی می شود. همچنین شناسه دستگاه (اندروید) به ازای هر کاربر تعریف شده در نرم افزار تحت وب بررسی و صحت سنجی می شود.
ارتباطات امن	محصول مورد ارزیابی از کانال SSL جهت ارتباط با سرور استفاده می کند
ثبت رویدادها	تمامی فعالیت کاربران ثبت و به سرور ارسال می شود.

۲ ادعای انطباق

۱/۲ انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	Common Criteria Version 3.1 Revision 4
نام پروفایل حفاظتی	PP-APP Software-V1.0
سطح تضمین امنیتی	EAL1

۳ تعریف مسائل امنیتی

۱/۳ خطمشی

خطمشی‌ها	توصیف
ممیزی کامل	تمامی رخدادهای محصول به سرور انتقال داده می شوند.

۲/۳ تهدیدات

تهدید	توصیف
T.NETWORK_ATTACK	فرد مهاجم روی یک کانال ارتباطی یا هر جای دیگری از زیرساخت شبکه قرار می‌گیرد. مهاجمان ممکن است سعی در برقراری ارتباط با برنامه کاربردی نمایند یا در ارتباطات میان

	نرم‌افزار برنامه کاربردی و دیگر نقاط پایانی دست ببرند تا بتوانند به آن نفوذ کنند.
T.NETWORK_EAVESDROP	فرد مهاجم روی یک کانال ارتباطی یا هر جای دیگری از زیرساخت شبکه قرار می‌گیرد. مهاجمان ممکن است داده‌های انتقالی بین برنامه کاربردی و دیگر نقاط پایانی را مشاهده کنند یا به آن‌ها دسترسی یابند.
T.LOCAL_ATTACK	فرد مهاجم ممکن است از طریق نرم‌افزارهای عادی (نرم‌افزارهایی که امتیاز دسترسی ویژه ندارند) موجود روی پلت‌فرمی که برنامه کاربردی روی آن اجرا می‌شود، وارد عمل شود. مهاجمان ممکن است ورودی‌های آلوده را در قالب فایل یا ارتباطات محلی، وارد برنامه کاربردی کنند.
T.PHYSICAL_ACCESS	مهاجم ممکن است به اطلاعات حساس بایگانی‌شده، دسترسی پیدا کند.

۳/۳ فرضیات

فرضیات	***توصیف***
A.PLATFORM	اجرای محصول منوط به یک پلتفرم رایانشی قابل‌اعتماد است و شامل پلتفرم زیرین و هرگونه محیط زمان اجرا که پلت فرم برای محصول فراهم کرده است، است.
A.PROPER_USER	کاربر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، به کار می‌گیرد.
A.PROPER_ADMIN	راهبر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند، بی‌دقت نیست و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، راهبری می‌نماید.

٤ اهداف امنیتی

۱/۴ اهداف امنیتی برای هدف ارزیابی

هدف امنیتی	توصیف
O.INTEGIRITY	محصولات انطباق‌پذیر، صحت نصب خود و بسته‌های به‌روزرسانی را تضمین می‌کنند و همچنین اقدامات اجرایی محیط محور را در جهت کاهش تهدیدات، تسهیل می‌نمایند. نرم‌افزارهای خیلی کمی، اگر نگوییم هیچ، عاری از خطا هستند؛ بنابراین، توانایی نصب بسته‌های تعمیر و عیب‌یابی و به‌روزرسانی نرم‌افزارهای نصب‌شده به‌صورت منسجم، اقدامی ضروری برای امنیت شبکه‌های سازمانی است. سازندگان پردازشگرها، برنامه‌نویسان کامپایلر، فروشندگان محیط‌های اجرا و فروشندگان سیستم‌عامل‌ها، اقدامات اجرایی محیط‌محوری را در جهت کاهش تهدیدات ایجاد کرده‌اند که با پیچیده‌تر کردن وظایف سیستم‌ها، کار نفوذ به آن‌ها را برای مهاجمان، دشوارتر و پرهزینه‌تر می‌کند. نرم‌افزارهای برنامه کاربردی اغلب می‌توانند از این سازوکارها بهره ببرند. این کار با استفاده از APIهایی انجام می‌شود که در زمان اجرا فراهم‌شده است؛ یا توسط فعال‌سازی این سازوکارها از طریق کامپایلر یا لینکر.
O.QUALITY	برای تضمین کیفیت پیاده‌سازی، محصولات انطباق‌پذیر به‌جای پیاده‌سازی سرویس‌ها و APIهای خود، سرویس‌ها و APIهایی را به کار می‌گیرند که توسط محیط زمان اجرا تأمین‌شده است. اهمیت این کار به‌طور خاص برای سرویس‌های رمزنگاری و دیگر عملیات پیچیده‌ای مثل تجزیه فایل و رسانه، بیشتر است. بهره‌گیری از این قابلیت پلتفرم، فقط منوط به استفاده از APIهای مستند و پشتیبانی شده است.
O.MANAGEMENT	برای تسهیل روند مدیریت توسط کاربران و سازمان، محصولات انطباق‌پذیر، واسط‌های منسجم و پشتیبانی‌شده‌ای را برای نگهداری و پیکربندی امنیتی خود فراهم می‌کنند. این کار شامل پیاده‌سازی و به‌روزرسانی برنامه کاربردی با استفاده از قالب‌ها و سازوکار

	پیاده‌سازی پشتیبانی شده توسط پلتفرم و همچنین فراهم کردن سازوکاری برای پیکربندی است.
O.PROTECTED_STORAGE	برای جلوگیری از افشای اطلاعات محرمانه‌ی کاربر در نتیجه‌ی حوادثی که منجر به از دست رفتن کنترل فیزیکی ابزارهای ذخیره‌سازی می‌شوند، محصولات انطباق‌پذیر از شیوه‌های حفاظت داده‌های بایگانی‌شده استفاده می‌کنند. این کار شامل رمزگذاری داده‌ها و ذخیره کلیدها توسط محصول است تا از دسترسی غیرمجاز به این داده‌ها جلوگیری شود.
O.PROTECTED_COMMS	برای جلوگیری از حملات تهدیدآمیز فعال (دست‌کاری بسته‌های داده) و غیرفعال (استراق سمع)، محصولات انطباق‌پذیر از یک کانال مورد اعتماد برای انتقال داده‌های حساس استفاده می‌کنند. داده‌های حساس شامل کلیدهای رمزنگاری، گذرواژه‌ها و هرگونه داده‌های دیگری است که مربوط به برنامه کاربردی بوده و نباید خارج از برنامه کاربردی، در معرض دید باشند.

۲٫۴ اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توصیف
OE.PLATFORM	اجرای محصول متکی به یک پلتفرم رایانشی مورد اعتماد است. این شامل سیستم‌عامل زیرین و هرگونه محیط اجرایی دیگری نیز می‌شود که در اختیار محصول قرارگرفته است.
OE.PROPER_USER	کاربر برنامه کاربردی از روی عمد دست به اشتباه یا خرابکاری نمی‌زند و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، به کار می‌گیرد.
OE.PROPER_ADMIN	راهبر برنامه کاربردی بی‌دقت نیست و از روی عمد دست به اشتباه یا خرابکاری نمی‌زند و نرم‌افزار را در تبعیت از سیاست‌های امنیتی سازمانی که از آن استفاده می‌کند، راهبری می‌نماید.

۵ الزامات کارکرد امنیتی

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	تولید بیت تصادفی ۱	FCS_RBG_EXT.1.1
۲	ذخیره‌سازی اسرار ۱	FCS_STO_EXT.1.1
۳	دسترسی به منابع پلتفرم ۱	FDP_DEC_EXT.1.1
۴	دسترسی به منابع پلتفرم ۲	FDP_DEC_EXT.1.2
۵	ارتباطات شبکه‌ای۱	FDP_NET_EXT.1.1
۶	رمزگذاری داده‌های حساس برنامه کاربردی ۱	FDP_DAR_EXT.1.1
۷	استفاده کاربر از یک سرویس بدون افشاء هویت ۴	FPR_ANO_EXT.1.1
۸	سازوکار پیکربندی پشتیبان‌شده ۱	FMT_MEC_EXT.1.1
۹	تأمین امنیت با پیکربندی پیش‌فرض۱	FMT_CFG_EXT.1.1
۱۰	تأمین امنیت با پیکربندی پیش‌فرض ۲	FMT_CFG_EXT.1.2
۱۱	کارکرد مدیریتی محصول ۱	FMT_SMF.1.1
۱۲	استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱	FPT_API_EXT.1.1
۱۳	قابلیت‌های ضد اکسپلویت ۱	FPT_AEX_EXT.1.1
۱۴	قابلیت‌های ضد اکسپلویت ۲	FPT_AEX_EXT.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۵	قابلیت‌های ضد اکسپلویت ۳	FPT_AEX_EXT.1.3
۱۶	قابلیت‌های ضد اکسپلویت ۴	FPT_AEX_EXT.1.4
۱۷	قابلیت‌های ضد اکسپلویت ۵	FPT_AEX_EXT.1.5
۱۸	به‌روزرسانی امن ۱	FPT_TUD_EXT.1.1
۱۹	به‌روزرسانی امن ۲	FPT_TUD_EXT.1.2
۲۰	به‌روزرسانی امن ۳	FPT_TUD_EXT.1.3
۲۱	به‌روزرسانی امن ۴	FPT_TUD_EXT.1.4
۲۲	به‌روزرسانی امن ۵	FPT_TUD_EXT.1.5
۲۳	به‌روزرسانی امن ۶	FPT_TUD_EXT.1.6
۲۴	استفاده از کتابخانه‌های شخص ثالث ۱	FPT_LIB_EXT.1.1
۲۵	حفاظت از تبادل داده‌ها ۱	FTP_DIT_EXT.1.1
الزامات پیوست یک		
۲۶	مدیریت کلید رمزنگاری ۳	FCS_CKM.1.1(2)
۲۷	الزامات پروتکلTLS Client/ احراز هویت دستی ۵	FCS_TLSC_EXT.2.1
الزامات پیوست دو		
۲۸	تولید بیت تصادفی ۳	FCS_RBG_EXT.2.1
۲۹	تولید بیت تصادفی ۴	FCS_RBG_EXT.2.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۳۰	مدیریت کلید رمزنگاری ۵	FCS_CKM_EXT.1.1
۳۱	مدیریت کلید رمزنگاری ۱	FCS_CKM.1.1(1)
۳۲	مدیریت کلید رمزنگاری ۲	FCS_CKM.2.1
۳۳	عملیات رمزنگاری – رمزنگاری/رمزگشایی ۱ (۱)	FCS_COP.1.1(1)
۳۴	عملیات رمزنگاری – درهم‌سازی ۱ (۲)	FCS_COP.1.1(2)
۳۵	عملیات رمزنگاری – امضاء ۱ (۳)	FCS_COP.1.1(3)
۳۶	عملیات رمزنگاری – امضاء ۲ (۴)	FCS_COP.1.1(4)
۳۷	پروتکل TLSC(۱)	FCS_TLSC_EXT.1.1
۳۸	پروتکل TLSC (۲)	FCS_TLSC_EXT.1.2
۳۹	پروتکل TLSC(۳)	FCS_TLSC_EXT.1.3
۴۰	پروتکل TLSC (۷)	FCS_TLSC_EXT.4.1
۴۱	الزامات پروتکلTLS Server/ احراز هویت ۱	FCS_TLSS_EXT.1.1
۴۲	الزامات پروتکلTLS Server/ احراز هویت ۲	FCS_TLSS_EXT.1.2
۴۳	الزامات پروتکلTLS Server/ احراز هویت ۳	FCS_TLSS_EXT.1.3
۴۴	الزامات پروتکلTLS Server/ احراز هویت ۴	FCS_TLSS_EXT.1.4
۴۵	الزامات پروتکلTLS Server/ احراز هویت ۵	FCS_TLSS_EXT.1.5
۴۶	الزامات پروتکلTLS Server/ احراز هویت ۶	FCS_TLSS_EXT.1.6

شماره الزام	نام الزام	تطابق الزام با استاندارد
۴۷	پروتکل DTLS(۱)	FCS_DTLS_EXT.1.1
۴۸	پروتکل DTLS(۲)	FCS_DTLS_EXT.1.2
۴۹	پروتکل DTLS(۳)	FCS_DTLS_EXT.1.3
۵۰	پروتکل HTTPS(۱)	FCS_HTTPS_EXT.1.1
۵۱	پروتکل HTTPS(۲)	FCS_HTTPS_EXT.1.2
۵۲	پروتکل HTTPS(۳)	FCS_HTTPS_EXT.1.3
۵۳	الزامات پروتکل X509 (۱)	FIA_X509_EXT.1.1
۵۴	الزامات پروتکل X509 (۲)	FIA_X509_EXT.1.2
۵۵	الزامات پروتکل X509 (۳)	FIA_X509_EXT.2.1
۵۶	الزامات پروتکل X509 (۴)	FIA_X509_EXT.2.2
	الزامات پیوست سه	
۵۷	پروتکل TLSS(۶)	FCS_TLSC_EXT.3.1
۵۸	استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۲	FPT_API_EXT.2.1
۵۹	شناسایی نرم‌افزار و نسخه‌ها ۱	FPT_IDV_EXT.1.1

۱/۵ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام

۱	**تولید بیت تصادفی ۱**
برنامه‌ی کاربردی برای عملیات رمزنگاری باید [از عملکرد تولید بیت تصادفی قطعی که توسط پلتفرم ارائه‌شده است کمک بگیرد،]	
۲	**ذخیره‌سازی اسرار ۱**
برنامه‌ی کاربردی در فضای حافظه‌ی غیر فرّار باید [هیچ‌گونه اطلاعات کاربری را ذخیره نکند،]	

۲٫۵ کلاس حفاظت از داده‌ها

شماره الزام	عنصر امنیتی
۳	**دسترسی به منابع پلتفرم ۱**
برنامه کاربردی باید کاربر را از قصد خود برای دسترسی به این منابع، آگاه کند: **]** • اتصال شبکه، • حافظه داخلی، • دوربین، • سرویس‌های موقعیت‌یاب، • بلوتوث،].	
۴	**دسترسی به منابع پلتفرم ۲**
برنامه کاربردی باید کاربر را از قصد خود برای دسترسی به این منابع، آگاه کند:] • هیچ نوع از منابع اطلاعات حساس، .[	
۵	**ارتباطات شبکه‌ای۱**
برنامه کاربردی باید ارتباطات شبکه‌ای خود را محدود کند به **]** • ارتباط‌هایی که به درخواست کاربر یا برنامه برای ارتباط با سرور برقرار می‌شود. • ارتباطات شبکه که برنامه کاربردی به منظور ▪ احراز هویت کاربران	

▪ ارسال اطلاعات ثبتی و جمع آوری شده توسط کاربران به سامانه ایجاد کرده است.]

۶	**رمزگذاری داده‌های حساس برنامه کاربردی ۱**
برنامه کاربردی باید **]** • هیچ‌گونه داده‌های حساسی را در حافظه غیر فرار ذخیره نکند. [	

۳/۵ کلاس محرمانگی

شماره الزام	عنصر امنیتی
۷	**استفاده کاربر از یک سرویس بدون افشاء هویت4**
برنامه کاربردی باید **]** اطلاعات شناسایی شخصی (PII) را در شبکه انتقال ندهد، [	

۴/۵ کلاس مدیریت امنیت

شماره الزام	عنصر امنیتی
۸	**سازوکار پیکربندی پشتیبان‌شده ۱**
برنامه کاربردی باید سازوکار توصیه‌شده توسط تولیدکننده‌ی پلتفرم را برای ذخیره‌سازی و تنظیم گزینه‌های پیکربندی، استفاده نماید.	
۹	**تأمین امنیت با پیکربندی پیش‌فرض ۱**
هنگامی که برنامه کاربردی بدون اعتبارنامه یا با اعتبارنامه پیش‌فرض پیکربندی‌شده است، برنامه کاربردی باید اقدامات لازم برای ایجاد اعتبارنامه جدید را فراهم آورد.	
۱۰	**تأمین امنیت با پیکربندی پیش‌فرض ۲**
برنامه کاربردی باید به‌طور پیش‌فرض طوری پیکربندی شود که با قرار دادن مجوزهای دسترسی به فایل مناسب، خود برنامه کاربردی و داده‌های آن را از دسترسی‌های غیرمجاز محافظت کند.	

۱۱	**کارکرد مدیریتی محصول ۱**
محصول باید قابلیت اجرای کارکردهای امنیتی زیر را داشته باشد: **]** • بدون کارکرد مدیریتی، .[	

۵٫۵ کلاس حفاظت از محصول

شماره الزام	عنصر امنیتی
۱۲	**استفاده از واسط برنامه‌نویسی کاربردی و سرویس‌های پشتیبانی شده ۱**
برنامه کاربردی باید تنها از واسط برنامه‌نویسی کاربردی‌های (API) پلتفرم پشتیبانی شده استفاده کند.	
۱۳	**قابلیت‌های ضد اکسپلویت ۱**
برنامه کاربردی نباید درخواست نگاشت حافظه به آدرس مشخصی نماید.	
۱۴	**قابلیت‌های ضد اکسپلویت ۲**
برنامه کاربردی باید **]** • هیچ بخشی از حافظه را همزمان هم به نوشتن اطلاعات و هم اجرای مجوزها اختصاص ندهد، [	
15	**قابلیت‌های ضد اکسپلویت ۳**
برنامه کاربردی باید با امکانات امنیتی که توسط تولیدکننده‌ی پلتفرم ارائه‌شده است، سازگار باشد.	
16	**قابلیت‌های ضد اکسپلویت ۴**
برنامه کاربردی نباید فایل‌هایی را که توسط کاربر قابل‌تغییر هستند در دایرکتوری‌هایی بنویسد که حاوی فایل‌های اجرایی‌اند، مگر این‌که کاربر به‌طور مستقیم چنین دایرکتوری‌ها را انتخاب نماید.	
17	**قابلیت‌های ضد اکسپلویت ۵**
برنامه کاربردی باید با قابلیت محافظت از سرریز بافر مبتنی بر پشته کامپایل شود.	
18	**به‌روزرسانی امن ۱**
برنامه کاربردی باید [انتخاب: این قابلیت را ارائه کند،] که به‌روزرسانی‌ها و وصله‌های برنامه‌های کاربردی را بررسی نماید.	

19	**به‌روزرسانی امن ۲**
برنامه کاربردی باید با استفاده از قالب مدیریت بسته که توسط آن پلتفرم پشتیبانی می‌شود، توزیع و منتشر شود. **نکته کاربردی ۱۷:** برای سیستم‌عامل ویندوز دارای فرمت فایل‌های " msi" و یا " appx" باشد.	
20	**به‌روزرسانی امن ۳**
برنامه کاربردی باید طوری بسته‌بندی[1] شود که حذف آن، منجر به پاک شدن تمامی آثار برنامه کاربردی شود؛ به‌استثناء تنظیمات پیکربندی، فایل‌های خروجی و ثبت وقایع/ ممیزی.	
21	**به‌روزرسانی امن ۴**
برنامه کاربردی نباید کد باینری خود را دانلود، اصلاح، جایگزین یا به‌روزرسانی کند.	
22	**به‌روزرسانی امن ۵**
برنامه کاربردی باید [حداقل یا این قابلیت را ارائه کند، یا این قابلیت را برای پلتفرم فراهم نماید] تا نسخه فعلی برنامه کاربردی را بازیابی کند.	
23	**به‌روزرسانی امن ۶**
بسته‌ی نصب برنامه کاربردی و نسخه‌های به‌روزرسانی آن باید به‌طور دیجیتالی امضا شوند به‌طوری‌که پلتفرم بتواند رمزنگاری آنان را قبل از نصب برنامه کاربردی، چک کند.	
24	**استفاده از کتابخانه‌های شخص ثالث ۱**
هدف از این الزام آن است که ارزیاب کتابخانه‌های شخص ثالث غیرضروری یا پیش‌بینی‌نشده در برنامه کاربردی را تشخیص و ثبت نماید. این شامل کتابخانه‌هایی که جهت امور تبلیغاتی ایجادشده‌اند نیز می‌شود که می‌تواند تهدیدی برای حریم خصوصی به شمار رود. همچنین شامل تضمین مستندسازی این کتابخانه‌ها برای مواقعی که آسیب‌پذیری‌هایی در آینده کشف شوند نیز است.	

۶٫۵ کلاس کانال‌ها و مسیرهای مورد اعتماد

شماره الزام	عنصر امنیتی
25	**حفاظت از تبادل داده‌ها ۱**
برنامه کاربردی باید بین خود و دیگر محصولات مورد اعتماد IT	

[1] Packaged

]
تمامی داده‌های مورد تبادل را با استفاده از[HTTPS،] رمزگذاری کند
.[

٦ الزامات تضمین امنیتی

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی هدف ارزیابی است. در این بخش الزامات EAL1 آورده می‌شود که لیست الزامات آن در جدول زیر آمده است.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب گذاری هدف ارزیابی
	ALC_CMS.1	پوشش پیکربندی هدف ارزیابی

۶/۱ کلاس توسعه

اطلاعات محصول، از طریق «مستندات راهنمای کاربر» و بخش «مشخصات امنیتی محصول» از سند هدف امنیتی در اختیار کاربر نهایی قرار می‌گیرد. الزامی بر وجود بخش «مشخصات امنیتی محصول» در سند هدف امنیتی نیست، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه‌دهندگان محصول باشد.

مشخصات کارکردی:

مشخصات کارکردی، واسطهای کارکرد امنیتی محصول را توصیف می‌نماید اما نیازی به شرح مفصل و کاملی از این واسطها نیست. فعالیت‌های این خانواده باید بر روی شناخت واسطهای معرفی‌شده در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و «مستندات راهنما» متمرکز گردد.

شماره الزام	نام الزام
۱	**مشخصات کارکرد ابتدایی۱**
توسعه‌دهنده باید مشخصات کارکردی را ارائه نماید.	
۲	**مشخصات کارکرد ابتدایی۲**
توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید.	
۳	**مشخصات کارکرد ابتدایی۳**
مشخصات کارکردی باید اهداف و متدهای مورداستفاده برای هر واسط اجراکننده کارکرد امنیتی [۲] و پشتیبان کننده‌ی الزام کارکرد امنیتی[3] توصیف نماید.	
٤	**مشخصات کارکرد ابتدایی۴**
مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجراکننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.	
٥	**مشخصات کارکرد ابتدایی۵**
مشخصات کارکردی باید برای دسته‌بندی ضمنی واسطهای غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.	

[2]-SFR-enforcing TSFI
[3]-SFR-supporting TSFI

شماره الزام	نام الزام
٦	**مشخصات کارکرد ابتدایی۶**
ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسطهای کارکرد امنیتی در سند مشخصات کارکردی باشد.	
۷	**مشخصات کارکرد ابتدایی۷**
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.	
۸	**مشخصات کارکرد ابتدایی۸**
ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.	

مستندات «مشخصات کارکردی» جهت پشتیبانی از ارزیابی الزامات کارکردی و اقدامات لازم در کلاس‌های «راهنما»، «آزمون» و «آسیب‌پذیری» ارائه‌شده است.

6.2 کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل سرپرستی و نحوه بررسی محیط عملیاتی توسط سرپرست (تا مشخص گردد که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می‌شود.

برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد. این راهنما شامل:

- دستورالعمل نصب موفقیت‌آمیز محصول در محیط
- دستورالعمل مدیریت امنیت محصول به‌عنوان یک محصول و به‌عنوان بخشی از یک محیط عملیاتی بزرگ‌تر

- دستورالعمل‌هایی که ارائه‌دهنده قابلیت سرپرستی محافظت‌شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو است.

6.2.1 راهنمای کاربردی

شماره الزام	نام الزام
۹	**راهنمای کاربردی ۱**
توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.	
۱۰	**راهنمای کاربردی ۲**
سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.	
۱۱	**راهنمای کاربردی ۳**
سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسطهای در دسترس ارائه‌شده توسط محصول به‌صورت امن استفاده می‌گردد.	
۱۲	**راهنمای کاربردی ۴**
سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسطهای در دسترس، به‌خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به‌صورت مناسبی تعیین نماید.	
۱۳	**راهنمای کاربردی ۵**
سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت‌های تحت کنترل محصول.	

شماره الزام	نام الزام
۱٤	**راهنمای کاربردی ۶**
سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آن‌ها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.	
۱۵	**راهنمای کاربردی ۷**
سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده‌اند، کاملاً اجرا گردند.	
۱٦	**راهنمای کاربردی ۸**
سند راهنمای کاربردی باید واضح و قابل‌فهم باشد	
۱۷	**راهنمای کاربردی ۹**
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌نماید.	

6.2.2 راهنمای آماده‌سازی

شماره الزام	نام الزام
۱۸	**راهنمای آماده‌سازی ۱**
توسعه‌دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.	

شماره الزام	نام الزام
۱۹	**راهنمای آماده‌سازی ۲**
مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه‌دهنده شرح دهند.	
۲۰	**راهنمای آماده‌سازی ۳**
مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکرشده در سند هدف امنیتی، شرح دهند.	
۲۱	**راهنمای آماده‌سازی ۴**
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.	
۲۲	**راهنمای آماده‌سازی ۵**
ارزیاب باید رویه‌های آماده‌سازی شرح داده‌شده در سند را بکار ببرد تا تائید نماید، محصول می‌تواند به‌صورت امن برای عمل نمودن آماده شود.	

6.3 کلاس آزمون

آزمون محصول برای بررسی بخش‌های کارکردی سیستم و همچنین بخش‌هایی که طراحی و پیاده‌سازی آن‌ها برای سیستم دارای آسیب‌های امنیتی است، در نظر گرفته می‌شود. آزمون بخش‌های کارکردی سیستم از طریق خانواده ATE_IND؛ و آزمون بخش‌هایی که طراحی و پیاده‌سازی آسیب‌زایی دارند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) آزمون بر اساس کارکردی که برای

محصول در نظر گرفته‌شده و واسط‌هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌گردد. نتایج آزمون و تحلیل آسیب‌پذیری باید در گزارش آزمون لحاظ شوند این مسئله در الزامات زیر در نظر گرفته‌شده است.

6.3.1 آزمون مستقل

«آزمون مستقل» برای تائید عملکرد محصول که در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و مستندات «راهنمای سرپرست» ارائه‌شده، صورت می‌گیرند. هدف اصلی آزمون اطمینان از برآورده شدن الزامات کارکردی مشخص‌شده در سند هدف امنیتی است. ارزیاب باید در سند «گزارش آزمون»، طرح آزمون و نتایج آن را مستند نماید.

شماره الزام	نام الزام
۲۳	آزمون مستقل ۱
توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.	
۲٤	آزمون مستقل ۲
محصول باید مناسب آزمودن باشد.	
۲٥	آزمون مستقل ۳
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، مؤلفه‌های محتوایی را برآورده می‌نماید.	

۶/۴ کلاس آسیب‌پذیری

٦,٤,١ تحلیل آسیب‌پذیری

شماره الزام	نام الزام
۲۸	آسیب‌پذیری ۲

شماره الزام	نام الزام
محصول باید مناسب آزمودن باشد.	
۲۹	آسیب‌پذیری ۳
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، تمام مؤلفه‌های محتوایی را برآورده می‌نماید.	
۳۰	آسیب‌پذیری ۴
ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.	
۳۱	آسیب‌پذیری ۵
ارزیاب باید بر اساس آسیب‌پذیری‌های بالقوه شناسایی‌شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.	

۶/۵ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه‌شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی-هایی از چرخه حیات محدود می‌گردد که توسط کاربر نهایی قابل‌مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه‌دهنده نقش کمرنگی در قابل‌اعتماد بودن محصول دارد، بلکه در این سطح اطمینان (EAL1) تنها به این اطلاعات نیاز است.

۶/۵/۱ قابلیت‌های پیکربندی

این مؤلفه جهت معرفی محصول به‌صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه‌شده، است (بدین معنی که جدا از برچسب‌گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به‌تنهایی، برچسب‌گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصول که توسط مرکز گواهی تائید شده است را به‌آسانی تشخیص دهد.

شماره الزام	نام الزام
۳۲	**برچسب‌گذاری محصول ۱**
توسعه‌دهنده باید محصول و مرجع محصول را ارائه نماید.	
۳۳	**برچسب‌گذاری محصول ۲**
محصول باید با یک مرجع یکتا برچسب زده شود.	
۳٤	**برچسب‌گذاری محصول ۳**
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.	

۶/۵/۲ حوزه پیکربندی

شماره الزام	نام الزام
۳۵	**پوشش پیکربندی محصول ۱**
ارزیاب باید لیست پیکربندی محصول را ارائه نماید.	
۳٦	**پوشش پیکربندی محصول ۲**
لیست پیکربندی باید شامل خود محصول و مدارک موردنیاز توسط الزامات تضمین امنیتی باشد.	
۳۷	**پوشش پیکربندی محصول ۳**
لیست پیکربندی باید موارد پیکربندی را به‌صورت یکتا معرفی نماید.	
۳۸	**پوشش پیکربندی محصول ۴**

شماره الزام	نام الزام
ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.	

۷ پیوست یک: الزامات اختیاری

شماره الزام	نام الزام
۲۶	**مدیریت کلید رمزنگاری 3**
برنامه کاربردی باید قادر به تولید کلیدهای رمزنگاری متقارن با استفاده از تولیدکننده بیت تصادفی که در الزام شماره ۱ «تولید بیت تصادفی ۱» تعریف‌شده است باشد و اندازه کلید رمزنگاری مشخص‌شده **[**انتخاب: ۱۲۸ بیت، ۲۵۶ بیت**]** است.	

۸ پیوست دوم: الزامات بر اساس انتخاب

شماره الزام	نام الزام
۲۸	**تولید بیت تصادفی ۳**
برنامه کاربردی باید تمام خدمات تولید بیت تصادفی قطعی را مطابق با استانداردهای زیر انجام دهد: [انتخاب: NIST Special Publication 800-90A با استفاده از [انتخاب: Hash_DRBG(any)،]	
۲۹	**تولید بیت تصادفی ۴**

تولید بیت تصادفی قطعی باید توسط یک منبع آنتروپی که آنتروپی‌های یک مولد بیت تصادفی قطعی وابسته به پلتفرم را تجمیع می‌کند و [انتخاب: یک منبع نرم‌افزاری نویز هیچ منبع نویز دیگری با [انتخاب: ۲۵۶ بیت] از آنتروپی، حداقل برابر با بالاترین قدرت امنیت (بر اساس NIST SP 800-57) از کلیدها و هش‌هایی که تولید می‌کند، پر شود.	
شماره الزام	**نام الزام**
۳۰	**مدیریت کلید رمزنگاری ۵**
برنامه کاربردی باید برای تولید کلید رمزنگاری یکی از اقدامات زیر را انجام دهد: فراخوانی کارکردهای ارائه‌شده توسط پلتفرم برای تولید کلید نامتقارن،	
۳۱	**مدیریت کلید رمزنگاری ۱**
برنامه کاربردی باید کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم زیر تولید نماید:] طرح RSA با استفاده از اندازه کلید رمزنگاری [۲۰۴۸ بیت یا بیشتر] که استانداردهای زیر را برآورده می‌نماید:] استاندارد FIPS PUB 186-4، «استاندارد امضای دیجیتال»، پیوست B.3	

]،	
طرح ECC با استفاده از [منحنی‌های P-256، P-384 و [هیچ منحنی دیگر]] که استانداردهای زیر را برآورده می‌نماید:	
[استاندارد FIPS PUB 186-4، «استاندارد امضای دیجیتال»، پیوست B.4]	
طرح FFC با استفاده از اندازه کلیدهای [۲۰۴۸ بیت یا بیشتر] که استانداردهای زیر را برآورده می‌کند:	
[استاندارد FIPS PUB 186-4، «استاندارد امضای دیجیتال»، پیوست B.1]	
۳۲	**مدیریت کلید رمزنگاری ۲**
برنامه کاربردی باید [درخواست نمودن کارکردی که پلتفرم ارائه می‌دهد،]برای استقرار کلید رمزنگاری مطابق با طرح‌های استقرار کلید مبتنی بر RSA که استانداردهای زیر را برآورده می‌نماید:	
NIST SP 800-56B و]	
طرح برقراری کلید مبتنی بر منحنی بیضوی که برآورده کننده استاندارد NIST SP 800-56A،	
طرح برقراری کلید مبتنی بر میدان متناهی که برآورده کننده استاندارد NIST SP 800-56A،	
هیچ طرح دیگر]	
۳۳	**عملیات رمزنگاری – رمزنگاری/رمزگشایی ۱ (۱)**
برنامه کاربردی باید رمزنگاری/رمزگشایی را مطابق با الگوریتم‌های رمزنگاری زیر انجام دهد:	
AES-CBC mode(به صورتی که در NIST SP 800-38A تعریف‌شده)،	
و [انتخاب:	
AES-GCM(به صورتی که در NIST SP 800-38D تعریف‌شده)،	
و [هیچ مد دیگر]	

و اندازه کلید رمزنگاری ۱۲۸ بیت و [۲۵۶ بیت، هیچ اندازه دیگر]	
عملیات رمزنگاری – درهم‌سازی ۱ (۲)	۳۴
برنامه کاربردی باید خدمات درهم‌سازی رمزنگاری را مطابق با الگوریتم درهم‌سازی SHA-1 و [انتخاب: SHA-256، SHA-384] و اندازه چکیده پیام ۱۶۰ و [انتخاب: ۲۵۶، ۳۸۴،] بیت انجام دهد که استاندارد FIPS Pub 180-4 را برآورده می‌نماید.	
عملیات رمزنگاری – امضاء ۱ (۳)	۳۵
برنامه کاربردی باید خدمات امضاء رمزنگاری (تولید و وارسی) را مطابق با الگوریتم رمزنگاری زیر انجام دهد:] طرح RSA با استفاده از اندازه کلید رمزنگاری ۲۰۴۸ بیت یا بزرگ‌تر که برآورده‌کننده‌ی استاندارد FIPS PUB 186-4 «استاندارد امضای دیجیتال DSS»، بخش چهارم است، طرح ECDSA با استفاده از «منحنی NIST»P-256، P-384 و [انتخاب: P-521، هیچ منحنی دیگر] که برآورده‌کننده‌ی استاندارد FIPS PUB 186-4 «استاندارد امضای دیجیتال DSS»، بخش پنجم است]	
عملیات رمزنگاری – امضاء ۱ (۴)	۳۶
برنامه کاربردی باید کد اصالت‌سنجی پیام بر پایه درهم‌سازی (HMAC) مطابق با الگوریتم رمزنگاری HMAC-SHA-256 و [هیچ الگوریتم دیگر] با اندازه کلید [اختصاص: اندازه کلید استفاده شده در HMAC] و اندازه خلاصه پیام ۲۵۶ بیت و [هیچ اندازه دیگر] انجام دهد که استاندارد FIPS Pub 198-1 «کد اصالت‌سنجی پیام بر پایه درهم‌سازی» و استاندارد FIPS Pub 180-4 «استاندارد درهم‌سازی امن» را برآورده می‌نماید.	
پروتکل TLSC(۱)	۳۷

برنامه کاربردی باید با پشتیبانی از مجموعه رمز[4] لیست شده در زیر، [TLS 1.2 ارائه‌شده توسط پلتفرم را درخواست نماید]

مجموعه رمز الزامی:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA به‌صورت تعریف‌شده در RFC 5246

مجموعه رمز اختیاری:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA به‌صورت تعریف‌شده در RFC 5246،

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246،

TLS_DHE_RSA_WITH_AES_256_CBC_SHA به‌صورت تعریف‌شده در RFC 5246،

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246،

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA به‌صورت تعریف‌شده در RFC 4492،

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5289،

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 به‌صورت تعریف‌شده در RFC 5289،

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA به‌صورت تعریف‌شده در RFC 4492،

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 به‌صورت تعریف‌شده در RFC 5289،

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 به‌صورت تعریف‌شده در RFC 5289،

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA به‌صورت تعریف‌شده در RFC 4492،

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 به‌صورت تعریف‌شده در RFC 5289،

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA به‌صورت تعریف‌شده در RFC 4492،

[4] CipherSuite

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 به‌صورت تعریف‌شده در RFC 5289، TLS_RSA_WITH_AES_128_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246، TLS_RSA_WITH_AES_256_CBC_SHA به‌صورت تعریف‌شده در RFC 5246، TLS_RSA_WITH_AES_256_CBC_SHA256 به‌صورت تعریف‌شده در RFC 5246،]	
پروتکل TLSC(۲)	۳۸
برنامه کاربردی باید منطبق بودن شناسه ارائه‌شده با شناسه مرجع را بر طبق RFC 6125 وارسی نماید.	
پروتکل TLSC(۳)	۳۹
برنامه کاربردی باید در صورت معتبر بودن گواهی همتا، تنها یک کانال امن برقرار نماید.	
پروتکل TLSC(۷)	۴۰
برنامه کاربردی باید بسطهای منحنی بیضوی پشتیبانی شده در مرحله Hello کلاینت را بر اساس منحنی-های NIST [انتخاب: secp256r1 ، secp521r1، secp384r1] ارائه دهد.	
پروتکل HTTPS(۱)	۵۰
برنامه کاربردی باید پروتکل HTTPS را مطابق با RFC 2818 پیاده‌سازی نماید.	
پروتکل HTTPS(۲)	۵۱
برنامه کاربردی باید پروتکل HTTPS را با استفاده از TLS، الزام شماره ۳۷ «پروتکل TLSC(۱)» پیاده‌سازی نماید.	

۵۲	**پروتکل HTTPS(۳)**
برنامه کاربردی باید درصورتی‌که گواهی همتا به نظر نامعتبر آید به کاربر اطلاع دهد و [اتصال را برقرار ننماید].	
۵۳	**الزامات پروتکل X509 (۱)**

برنامه کاربردی باید [کارکرد ارائه‌شده توسط پلتفرم را درخواست نماید] تا مطابق با قوانین زیر، گواهی‌ها را معتبر نماید:

- اعتبارسنجی گواهی و مسیر گواهی RFC 5280
- مسیر گواهی باید با یک گواهی CA امن خاتمه یابد.
- برنامه کاربردی باید مسیر گواهی را اعتبارسنجی نماید با تضمین نمودن وجود آیتم basicConstraints و اینکه پرچم CA برای تمامی گواهینامه‌ها وضعیت TRUE داشته باشد.
- برنامه کاربردی باید وضعیت لغو گواهی را با استفاده از [پروتکل وضعیت گواهی آنلاین (OCSP[5]) به‌صورت مشخص‌شده در RFC 2560]
- برنامه کاربردی باید فیلد extendedKeyUsage را مطابق با قوانین زیر اعتبارسنجی نماید:
  - گواهی استفاده شده برای به‌روزرسانی امن و بررسی صحت کد اجرایی باید در فیلد extendedKeyUsage دارای هدف Code Signing باشد (id-kp 3 با OID 1.3.6.1.5.5.7.3.3)
  - گواهی‌های سرور ارائه‌شده برای TLS باید در فیلد extendedKeyUsage دارای هدف احراز هویت سرور باشد (id-kp 1 با OID 1.3.6.1.5.5.7.3.1)
  - گواهی‌های کلاینت ارائه‌شده برای TLS باید در فیلد extendedKeyUsage دارای هدف احراز هویت کلاینت باشد (id-kp 2 با OID 1.3.6.1.5.5.7.3.2)
  - گواهی‌های S/MIME ارائه‌شده برای امضاء و رمزنگاری ایمیل باید در فیلد extendedKeyUsage دارای هدف حفاظت از ایمیل باشد (id-kp 4 با OID 1.3.6.1.5.5.7.3.4)
  - گواهی‌های OCSP ارائه شده برای پاسخ‌های OCSP باید در فیلد extendedKeyUsage دارای هدف امضای OCSP باشد (id-kp 9 با OID 1.3.6.1.5.5.7.3.9)
  - گواهی‌های سرور ارائه شده برای EST باید در فیلد extendedKeyUsage دارای هدف مرکز ثبت گواهی CMC باشد (id-kp-cmcRA با OID 1.3.6.1.5.5.7.3.28)

[5] Online Certificate Status Protocol

۵۴	**الزامات پروتکل X509 (۲)**
برنامه کاربردی باید در صورت وجود basicConstraints extension و true بودن CA Flag، گواهی را به‌عنوان گواهی CA تلقی نماید.	
۵۵	**الزامات پروتکل X509 (۳)**
برنامه کاربردی باید از گواهی X.509v3 به‌صورت تعریف‌شده توسط RFC 5280 استفاده نماید تا از احراز هویت برای [HTTPS، TLS،] پشتیبانی نماید.	
۵۶	**الزامات پروتکل X509 (۴)**
زمانی که برنامه کاربردی نمی‌تواند جهت تعیین اعتبار گواهی، اتصالی را برقرار نماید؛ برنامه کاربردی باید [گواهی پذیرفته نمی‌شود].	

۹ پیوست سوم: الزامات اضافی

این پیوست شامل الزامات کارکرد امنیتی است که باعث کاهش تهدیدات محصول می‌گردد. در حال حاضر استفاده از این الزامات در پروفایل حفاظتی به اجباری نیست. با این حال این الزامات می‌تواند در سند هدف امنیتی آورده شود که با الزامات پروفایل حفاظتی سازگار است.

شماره الزام	نام الزام

۷ شرح خلاصه‌ای از محصول

این محصول به منظور ارائه بستری امن به منظور برقراری ارتباط سامانه تحت وب با اکلیپ های عملیاتی پیاده سازی شده است. هر یک از کاربران(اکیپ ها) قبل از دسترسی یه پروفایل کاربری و بخش های مختلف نرم افزار باید عمل احراز هویت آنها با موفقیت انجام شده باشد. حساب کاربری تمامی اکیپ های عملیاتی وابسته به شناسه یکتا دستگاه اندروید تعریف شده در سامانه تحت وب می باشد. تمامی اطلاعات ارسالی و دریافت شده فی ما بین برنامه کاربردی و سرور با استفاده از الگوریتم رمزگذاری AES-128 می شوند. اطلاعات پایه (برای مثال ابزارآلات، آیتم های تحویل شیفت) مربوط به محصول، هر بار پس از احزار هویت موفق کاربر از سرور بارگیری شده و در دیتابیس محلی ذخیره می شوند. همچنین فعالیت های کاربر در قالب مشخص به عنوان اطلاعات ممیزی به سرور ارسال می شوند.