به نام خدا

سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه

فناوری اطلاعات بهپایا

سامانه مانیتورینگ معین

نسخه‌ی ۲

مهر ۱۴۰۲

نسخه ۱.۳

پیشگفتار

در نظام ارزیابی امنیتی محصولات فتا، یکی از اسناد مورد نیاز برای انجام آزمون امنیتی، سند هدف امنیتی است. بر اساس استاندارد معیار مشترک (CC) سند هدف امنیتی مبتنی بر اسنادی که پروفایل حفاظتی نام دارند، تهیه و تدوین می‌گردد. پروفایل‌های حفاظتی حاوی الزامات امنیتی هستند که در یک محصول افتایی می‌بایست رعایت گردد. از آنجا که متن این پروفایل‌ها پیچیده بوده، تهیه سند هدف امنیتی برای تولیدکننده کاری زمان‌بر است، ساده‌سازی الزامات امنیتی موجود در پروفایل‌های حفاظتی به نحوی که برای تولیدکننده مشخص شود که چه مواردی امنیتی باید در یک محصول خاص رعایت شود، بسیار مفید خواهد بود.

در این راستا مرکز افتا و سازمان فناوری اطلاعات ایران با همکاری آزمایشگاه‌های ارزیابی امنیتی، به منظور چابک‌سازی فرآیند ارزیابی امنیتی، «سند الزامات امنیتی» را جایگزین پروفایل‌های حفاظتی نموده است. هدف از سند الزامات امنیتی، ساده‌سازی مفاهیم الزامات مطرح شده در پروفایل‌های حفاظتی و نیز کمک به تولیدکننده در جهت سرعت بخشیدن به تدوین سند هدف امنیتی است.

سند پیشرو حاوی الزامات امنیتی «پروفایل حفاظتی برنامه‌های کاربردی تحت شبکه» که سعی شده است تا حد ممکن ساده و قابل فهم گردد، است. این سند دو هدف را دنبال می‌کند. اول آنکه موارد امنیتی را که باید در محصول رعایت شود (تا منجر به دریافت گواهی امنیتی گردد) برای تولیدکننده مشخص نماید و ثانیاً، تدوین سند هدف امنیتی را که کاری زمان‌بر است را برای تولیدکننده سریع و آسان نماید.

فهرست

۱- معرفی محصول

سامانه مانیتورینگ عملیات یکپارچه نوین، به اختصار سامانه معین، راهکاری جامع برای مانیتورینگ هوشمند خدمات است که امکان افزایش هوش عملیاتی و کسب وکاری(تجاری) را برای ارائه دهندگان خدمات برخط فراهم می کند.

۱-۱- مانیتورینگ عملیات و کسب و کار

هدف در عملیات، استمرار در ارائه خدمات با کیفیت است. استمرار در ارائه یک خدمت با کیفیت، نیازمند پایداری، دسترس پذیری مطلوب و عملکرد کارای همه اجزای موثر در ارائه آن خدمت است. به بیان دیگر کیفیت و کارایی خدمات بر بستر فناوری اطلاعات به کارایی همه اجزا و فناوری های موثر در ارائه آن خدمات اعم از زیرساخت های رایانش، زیرساخت های کاربرد و در نهایت کاربردهای کسب و کاری ارائه دهنده آن خدمات، وابسته است. لذا تضمین کیفیت و کارایی یک خدمت مستلزم پایش و مانیتورینگ مستمر اجزای تاثیر گذار در آن خدمت می باشد. سامانه معین، از یک سو، امکان مانیتورینگ همه اجزای موثر در یک خدمت را بطور مستقل فراهم می نماید و از سوی دیگر، مانیتورینگ یکپارچه یک خدمت را با ترسیم گرافی از اجزای موثر در آن خدمت و ارتباطات آنها ممکن ساخته است. به کمک این گراف، در سامانه معین، تحلیل ریشه خطا در خدمات فراهم شده است.

عملکرد مطلوب و کارای این اجزاء می تواند منجر به افزایش دسترس پذیری و کیفیت خدمات و در نهایت بهبود شاخص های کسب وکاری گردد. به عبارتی در کسب وکارهای برخط بین شاخص های کسب وکاری و شاخص های عملیاتی وابستگی وجود دارد. لذا مانیتورینگ توامان و یکپارچه شاخص های عملیاتی و شاخص های کسب وکاری اطلاعات بهتری از وضعیت خدمات یا کسب وکار و علل و عوامل تغییرات در آنها ارائه می دهد و بر هوش عملیاتی و کسب وکاری ارائه دهندگان خدمات برخط می افزاید. در سامانه معین شاخص های کسب وکاری با انواع روش ها، استخراج، جمع آوری و تحلیل می شوند.

در جهت نیل به این اهداف، در سامانه معین، مانیتورینگ در سه سطح زیر فراهم شده است:

۱. زیرساخت های رایانش
۲. زیرساخت های کاربرد
۳. کاربردهای کسب‌وکار

که در ادامه به اختصار به هر یک از این سطوح می‌پردازیم.

۱-۲- مانیتورینگ زیرساخت های رایانش

در سامانه معین در سطح زیرساخت های رایانش، تجهیزات شبکه، تجهیزات امنیتی، سرورهای فیزیکی، ذخیره سازها، سیستم عامل ها، ابزارهای مجازی ساز، تجهیزات محیطی و سایر تجهیزات سخت افزاری مانیتور می‌شوند. زیرساخت مورد استفاده در خدمات یک کسب وکار، از حیاتی ترین بخشهای فناوری اطلاعات آن کسب وکار است. این سطح از نظر فناوری و برند بسیار متنوع است. سامانه معین به منظور یکپارچه سازی در مانیتورینگ، طیف وسیعی از انواع و برندهای این سطح را پوشش می دهد و به ازای هر نوع از آنها، شاخص های متنوعی را استخراج و ارائه می کند. در سامانه معین به طور مستمر، نوع و برندهای پوشش داده شده، بر اساس نیاز مشتریان در حال توسعه می باشد.

۱-۳- مانیتورینگ زیرساخت های کاربرد

در سامانه معین در سطح زیرساخت های کاربرد، انواع پایگاه های داده، وب سرورها، سرورهای کاربردی، سیستم های صف پیام، ابزارهای تدارک سرویس، ابزارهای تحلیل داده، ابزارهای ارکستراسیون، نرم افزارهای امنیتی و شبکه، ابزارهای سازمانی، محیط های اجرا و ... مانیتور می شوند. به طور عام، خدمات بر بستر فناوری اطلاعات با استفاده از تعدادی از این کاربردها توسعه داده می شوند. لذا ارائه یک خدمت همیشه مستلزم استفاده از تعدادی از کاربردهای این سطح است و ارائه با کیفیت آن خدمت هم مستلزم عملکرد مطلوب آنها

است. سامانه معین، مانیتورینگ بسیاری از نرم افزارها و ابزارهای برندهای معتبر و رایج را پوشش می دهد و شاخص های متنوعی از آنها را با استفاده از واسط های استاندارد استخراج می نماید. در سطح زیرساخت های کاربرد برخلاف سطح زیرساخت های رایانش، شاخص ها و شیوه استخراج آنها بسیار متفاوت از یکدیگر می باشد و گاه ممکن است این تفاوت در نسخ یک ابزار هم وجود داشته باشد. در سامانه معین به طور مستمر، بر تعداد کاربردها و برندهای تحت پوشش در این سطح افزوده می شود. همچنین بر اساس نیاز مشتریان، بصورت سفارشی نیز، امکان توسعه فراهم می باشد.

۴-۱- مانیتورینگ کاربردهای کسب‌وکار

در سامانه معین، در سطح کاربردهای کسب‌وکار، مانیتورینگ عملیاتی و کسب وکاری کاربردها و خدمات توسعه داده شده برای یک کسب‌وکار فراهم شده است. در این سطح، شما می توانید برای مانیتورینگ یک خدمت کسب وکاری، خدمت کسب وکاری متناظر در سامانه معین بسازید و با استفاده از انواع واسط ها، شاخص های کسب وکاری و عملیاتی آن خدمت را استخراج نموده و داشبوردهای متنوعی برای نمایش آنها ایجاد نمایید.

همچنین در این سطح، قابلیت مانیتورینگ یک کاربرد بصورت یک سامانه یکپارچه هم فراهم شده است که می توانید به کمک آن، سامانه توزیع شده ای در محیط عملیات که یک کاربرد یا خدمات یک کسب و کار را محقق می سازد را بصورت گرافی از اجزای (از هر سطح) موثر در آن کاربرد، ترسیم نمایید و تابع سلامت آن را بر اساس وضعیت اجزای موثر اضافه شده در گراف تعریف نمایید.

در سامانه معین علاوه بر شاخص ها، امکان جمع آوری لاگ های رخداد و لاگ های ردیابی هم فراهم می باشد. لاگ های رخداد لاگ‌های رایجی هستند که ممکن است تجهیزات سطح زیرساخت رایانش، ابزارهای سطح زیرساخت کاربرد و یا کاربردهای کسب و کاری پس از وقوع یک تغییر یا رخداد، تولید نمایند که در سامانه معین امکان جمع آوری آنها به طرق مختلف فراهم می باشد. همچنین امکان جمع آوری لاگهای ردیابی کاربردهای کسب و کاری که حاوی اطلاعاتی از تراکنش‌های توزیع شده خدمات هستند نیز در سامانه معین مهیا می باشد.

امکاناتی چون استخراج شاخص های عملیاتی، استخراج شاخص های کسب وکاری، تعریف گرافی از اجزای موثر و نحوه اثر گذاری آنها، جمع آوری لاگ های رخداد و لاگ های ردیابی یک کاربرد کسب و کاری و خدمات آن، از جمله امکانات سامانه معین در این سطح می باشد.

۱-۵- ویژگی‌های فنی محصول

نسخه‌ی نرم‌افزار /میان‌افزار	۲
مدل و نسخه سیستم‌عامل	سیستم عامل ubuntu 22.04 پیشنهاد می‌شود اما معمولاً توسط کارفرما تعیین و نگهداری می‌شود و از نظر ما لزومی بر انتخاب توزیع خاصی نیست و هر سیستم‌عامل برپایه‌ی linux که قابلیت نصب داکر بر روی آن وجود داشته باشد، قابل استفاده خواهد بود.
مدل و نسخه وب‌سرور	Apache web server 2.4.41 Apache Tomcat 9.0.30
مدل و نسخه پایگاه داده	Postgres v11.5, Redis v5.0.6
زبان برنامه‌نویسی	Java, Typescript

۱-۶- معماری محصول

همانطور که در معماری سامانه معین در شکل ۱ آمده است، سامانه معین از سه ماژول اصلی Moein Core، Moein Portal و Moein UI تشکیل شده است. گردش اطلاعات در سامانه معین به دلیل ارتباطات داخلی، ارتباط با سامانه خارجی، ارتباط با اشیاء و ارتباط با کاربران در چهار حوزه قابل بررسی می باشد:

۱. گردش اطلاعات بین Moein Core و اشیای در حال مانیتورینگ جهت دریافت اطلاعات

ماژول Moein Core جهت اتصال به اشیاء (تجهیزات نرم افزاری و سخت افزاری مختلف) که در حال مانیتورینگ می باشند، از پروتکل‌ها و استانداردهای ارائه شده از سوی شرکت‌های سازنده‌ی آن تجهیزات استفاده می‌کند. معین گاه برای استخراج اطلاعات از عامل (agent) هم استفاده می کند که بسیار محدود است.

۲. گردش اطلاعات بین Moein Portal و سامانه‌های خارجی جهت ارسال تیکت، اعلان و احراز هویت

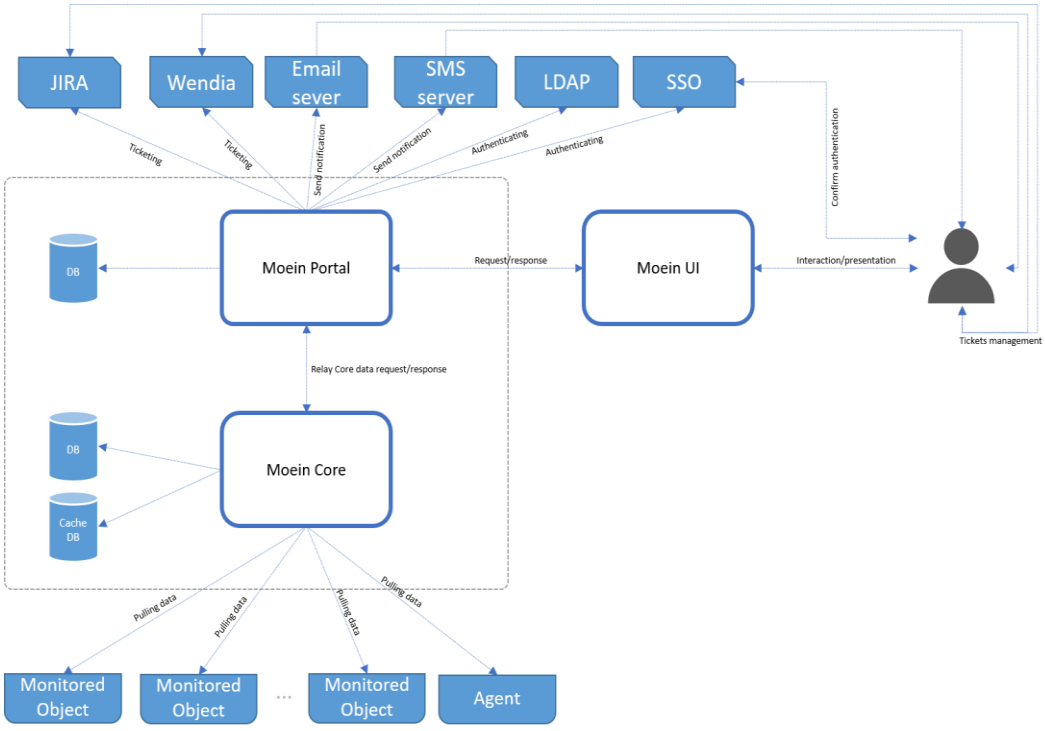
در سامانه‌ی معین علاوه بر پیاده‌سازی مدیریت کاربران داخلی برای احراز هویت و تیکتینگ داخلی، امکان اتصال به سامانه‌های احراز هویت متمرکز مانند LDAP و SSO و سامانه‌های تیکتینگ خارجی مانند JIRA و Wendia وجود دارد. همچنین برای ارسال اعلان از سرویس های ایمیل و پیامک هم استفاده می شود.

۳. گردش اطلاعات بین Moein Portal و Moein UI با کنترل دسترسی‌ها

ماژول Moein UI درخواست‌های کاربران را به ماژول Moein Portal می فرستد. تمامی اطلاعات (فرم‌ها، اکشن ها، اشیاء) در سامانه‌ی معین دارای مجوز دسترسی هستند و کنترل دسترسی از طریق اعطای مجموعه‌ای از مجوزها به نقش‌ها فراهم می‌گردد. لذا همه درخواست های کاربران قبل از اجرا از نظر داشتن مجوزهای لازم بررسی می شوند.

۴. گردش اطلاعات بین Moein Portal و Moein Core

ماژول Moein Portal در پاسخ به درخواست‌های کاربر، پس از کنترل دسترسی، داده های درخواست شده را از Moein Core درخواست می‌نماید و برای کاربر ارسال می نماید. ماژول Moein Core هم پس از دریافت اطلاعات از اشیا و تحلیل آنها، در صورتی که وقوع رخدادی را تشخیص دهد، آن را برای Moein Portal ارسال می کند تا برای کاربران اعلان ارسال شود.



شکل ۱ نمای کلی از معماری سامانه‌ی معین

۲- الزامات امنیتی

الزامات امنیتی این سند بر اساس نسخه ۱.۱ نمایه[1] حفاظتی «برنامه‌های کاربردی تحت شبکه» تهیه شده است. ساختار این سند بدین صورت است که برای هر رده در پروفایل حفاظتی مربوطه، یک دسته الزام بیان شده است.

۲-۱- ممیزی امنیت (Log)

در این رده توانایی‌های محصول از نظر امکان تولید داده ممیزی (Log) مناسب برای فعالیت‌های مختلفی که در محصول صورت می‌گیرد، در شرایط مختلف سنجیده می‌شود.

شماره الزام	رده ممیزی امنیت (Log)				توضیحات
۱	**محصول باید برای موارد مشخص‌شده که در زیر آمده است، ثبت‌نشان[2] تولید کند (Log ثبت نماید).**			☑	
	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.	شروع و اتمام توابع	☑		
		تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها	☑		
		خواندن اطلاعات از ثبت‌نشان‌ها	☑		
		تمامی تغییرات در پیکربندی ثبت‌نشان‌ها	☑		
		عملیات انجام‌شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه	☑		
		عملیات انجام‌شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها	☑		
		تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.	☑		
		تمام کاربردهای سازوکار احراز هویت	☑		
		نتایج نهایی عملیات احراز هویت	☑		
		تلاش موفق و ناموفق هر گذرواژه بررسی‌شده توسط محصول	☑		

[1] Profile
[2] Log

		شکست و موفقیت انتساب ویژگی‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)	☑		
		تمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی	☑		
		تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	☑		
		تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه ویژگی‌های امنیتی)	☑		
		همه تلاش‌ها برای خارج کردن اطلاعات از محصول	☑		
		تمامی تغییرات در رفتارهای توابع کارکردی محصول	☑		
		استفاده از کارکردهای مدیریتی	☑		
		تغییرات در گروه کاربران	☑		
		شکست در کارکردهای امنیتی محصول	☐		با تنظیمات سرویس داکر بعد از کار افتادن هر ماژول از محصول معین، عمل راه‌اندازی مجدد به صورت خودکار اجرا شده و جلوی شکست گرفته می‌شود. به همین دلیل در هیچ حالت فعالی از محصول ماژولی وجود نخواهد داشت که دچار شکست در عملکردش شود. در نتیجه ثبت‌نشانی مشابه سایر رویدادها برای این بخش نیاز نداشتیم. البته لاگ‌های چارچوب در ترمینال چاپ می‌شوند.
		تمامی قابلیت‌هایی از محصول که به دلیل شکست (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند.	☐		مشابه توضیح بالا، لاگی برای این بخش نیز نیاز نبوده است.
		تلاش موفق یا ناموفق برای برقراری نشست.	☑		
		ایجاد نشدن نشست به دلیل محدودیت نشست‌های همزمان (حداقل)	☑		
		خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست	☑		
		خاتمه به نشست غیرفعال توسط مدیر سیستم	☑		
		سایر موارد	☐		
۲	**محصول باید برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید.**			☑	
		تاریخ و زمان رویداد	☑		

	ویژگی‌هایی که در ثبت‌نشان‌ها وجود دارد مشخص شود.	☑	نوع رویداد		
		☑	هویت ایجادکننده رویداد		
		☑	نتیجه رویداد		
		☑	آدرس IP ایجادکننده رویداد		
		☐	سایر موارد		
۳	**محصول باید ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید.**			☑	دسترسی به ثبت‌نشان‌ها، تنها برای مدیران امنیتی فراهم است.
۴	**ثبت‌نشان‌هایی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند.**			☑	
	موارادی که در ثبت‌نشان‌ها وجود دارند، مشخص شوند.	☑	نبود داده نامفهوم در رکوردها		
		☑	نبود بخش‌های نامرتبط		
		☑	وجود داده معتبر و مناسب در هر بخش		
۵	**محصول باید امکان انتخاب و مرتب‌سازی برای ثبت‌نشان‌های تولیدشده را بر اساس بخش‌ها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.**			☑	
	مواردی که بر اساس آنها مرتب‌سازی وجود دارد، مشخص شود.	☑	هویت موجودیت فعال		
		☐	نوع حساب کاربری		
		☑	تاریخ/زمان		
		☐	روش اتصال کاربر		
		☑	نوع رخداد		
		☑	مکان رویداد		
		☑	سایر موارد		واحد مانیتورینگ
۶	**محصول باید هرگونه حذف و تغییر غیرمجاز در ثبت‌نشان‌ها را تشخیص دهد و در صورت امکان جلوگیری نماید.**			☑	
		☐	استفاده از درهم‌سازی (Hash) برای تشخیص تغییرات		

	روش‌های تشخیص مشخص شود. (وجود یک مورد لازم و کافی است)	پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	☐		
		فقط خواندنی کردن ثبت‌نشان‌ها در محصول	☑		
		سایر موارد	☑		امکان حذف لاگ از یک تاریخی به قبل توسط مدیر امنیتی
۷	**محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.**		☐		به دلیل اینکه، در صورت رسیدن به حد آستانه، سیاست بازنویسی بر روی قدیمی‌ترین ثبت‌نشان‌های ذخیره‌شده در محصول معین اتخاذ شده است و مدیریت فضای ذخیره‌سازی از این طریق انجام می‌گیرد، نیازی به مطلع کردن کاربر در این باره وجود نداشته است.
	روش‌های اطلاع‌رسانی مشخص شود (وجود یک مورد لازم و کافی است)	استفاده از یک کانال ارتباطی	☐		
		ارسال پیام	☐		
		از طریق واسط کاربر مجاز	☐		
		سایر موارد	☐		
۸	**محصول باید توانایی تولید ثبت‌نشان (ثبت Log) هنگام از کار افتادن محصول و/یا پر شدن حافظه ثبت‌نشان‌ها را داشته باشد و برای این کار از رویکردهای بیان‌شده استفاده نماید.**		☑		
	رویکردهای مورد استفاده در محصول مشخص گردد (وجود یک مورد لازم و کافی است)	نادیده گرفتن ثبت‌نشان‌ها	☐		
		ذخیره‌سازی محدود ثبت‌نشان‌ها (آنهایی که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند)	☐		
		بازنویسی روی قدیمی‌ترین ثبت‌نشان‌های ذخیره‌شده	☑		
		سایر موارد	☐		

۲-۲- رمزنگاری

در این رده، توانایی محصول در پیاده‌سازی یا به‌کارگیری ماژولهای رمزنگاری، بررسی می‌گردد. برای حفظ محرمانگی داده از رمزنگاری استفاده می‌گردد و این رمزنگاری‌ها می‌تواند به صورت متقارن و نامتقارن صورت گیرد. در رمزنگاری متقارن از یک کلید مشترک برای رمزگذاری و رمزگشایی، استفاده می‌شود ولی در رمزنگاری نامتقارن این کار با استفاده از یک زوج کلید (کلید عمومی و کلید خصوصی) صورت می‌گیرد. الگوریتمها میتوانند با طول کلیدهای مختلف و به روشهای مختلفی (مد عملیاتی) به رمزگذاری و رمزگشایی داده بپردازند که در این رده، توانایی محصول از این حیث مورد بررسی قرار گرفته است. در رده رمزنگاری همچنین از الگوریتمهای درهم‌سازی (هش) برای برقراری جامعیت داده استفاده می‌گردد.

شماره الزام	رده رمزنگاری			توضیحات
۱	**محصول باید قابلیت رمزنگاری یا واحد [3] رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ISO 18033-3) با توجه به موارد زیر انجام دهد.**		☑	در حال حاضر سامانه‌ی معین برای گذرواژه‌های کاربران از الگوریتم BCrypt استفاده می‌کند که برای این کاربرد مناسب‌تر از الگوریتم‌های AES است.
	مد عملیاتی که الگوریتم از آن استفاده می‌کند را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	مد عملیاتی CBC و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در NIST SP 800-38A)	☐	
		مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در NIST SP 800-38D)	☑	طول کلید مورد استفاده برای این مدل عملیاتی ۱۲۸ و ۲۵۶ است.
		مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در ISO10116)	☑	برای سایر بخش‌های معین مانند تعیین رمز در تنظیمات عمومی (بخش ایمیل و sms) و همچنین credential ها از الگوریتم‌های مبتنی برای AES و مد عملیاتی CTR با طول کلید ۲۵۶ بیت استفاده کرده‌ایم.
۲	**محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (Hash) را داشته باشد؛ بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده نماید.**		☑	
	الگوریتم و اندازه خلاصه پیام مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	الگوریتم SHA-1 با اندازه خلاصه پیام ۱۶۰ بیت	☐	
		الگوریتم SHA-256 با اندازه خلاصه پیام ۲۵۶ بیت	☑	
		الگوریتم SHA-384 با اندازه خلاصه پیام ۳۸۴ بیت	☑	
		الگوریتم SHA-512 با اندازه خلاصه پیام ۵۱۲ بیت	☐	
۳	**در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری)**		☑	

[3] Module

	روش نابودی کلید مشخص گردد. (وجود یک مورد لازم و کافی است)	نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یک‌ها، مقدار تصادفی، مقدار جدیدی از کلید)	☐		
		نابودی با استفاده از یک واسط مشخص	☐		
		از طریق توابع امنیتی محصول	☑		
		سایر موارد	☐		
۴	**در صورتی که امضای دیجیتال در محصول پشتیبانی می‌شود، نیاز است که سرویس‌های امضای رمزنگاری (تولید و تأیید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری)**			☑	
	الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است)	الگوریتم‌های امضای دیجیتال RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS) بخش ۵.۵، الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال ۲ و یا الگوی امضای دیجیتال ۳)	☑		
		الگوریتم‌های امضای دیجیتال ECDSA با کلیدهای رمزنگاری ۲۵۶ بیت یا بزرگتر (بر اساس ISO/IEC 14888-3 بخش ۶.۴، استاندارد امضای دیجیتال (DSS) بخش ۶ و پیوست D، با استفاده از منحنی P-256 یا P-384 یا P-521)	☑		

۲-۳- شناسایی و احراز هویت

در این رده توانایی‌های محصول از نظر امکان شناسایی و احراز هویت کاربر در حالت‌های مختلف و اقدامات متقابل در راستای عدم برقراری آنها، بررسی می‌گردد.

شماره الزام	رده شناسایی و احراز هویت				توضیحات
۱	**محصول باید بتواند تعداد تلاش‌های ناموفقی را که برای احراز هویت صورت گرفته است (در هر بخش یا قسمتی که نیاز به احراز هویت وجود دارد)، بر اساس موارد زیر مشخص نماید.**			☑	سامانه‌ی معین قادر است تا از ورود غیر مجاز اشخاص و یا نفوذ سیستماتیک که از طریق حملات brute-force بر روی رمز عبور صورت می‌گیرد جلوگیری نماید.
	مقدار یا یازه‌ی مورد استفاده در هریک باید مشخص گردد. (وجود یک مورد لازم و کافی است)	یک عدد مثبت ثابت	☐		
		یک عدد مثبت قابل تنظیم توسط مدیر	☑		مدیر محصول می‌تواند سقف تعداد تلاش‌های ناموفق برای احراز هویت را از طریق واسط کاربری تنظیم کرده، تا در صورت عبور از این سقف، سامانه به صورت خودکار اقدامات لازم را جهت جلوگیری از اقدامات کاربر خاطی انجام دهد.
۲	**محصول باید هنگامی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین‌شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید.**			☑	
	روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب نمایید. (وجود یک مورد لازم و کافی است.) لازم به ذکر است روش‌های فوق با توجه به نوع کاربرد می‌تواند از حالت انتخابی به حالت الزامی تغییر یابد.	غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)	☑		
		غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)	☑		
		استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت «توضیحات» بیان شود)	☐		

	برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست.	سایر موارد	☐		
۳	**محصول باید برای هر کاربر، ویژگی‌های امنیتی را که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت می‌باشند، نگهداری نماید.**		☑	☑	
	ویژگی‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.	شناسه کاربر	☑		
		روش احراز هویت مورد استفاده	☑		با توجه به اینکه سامانه‌ی معین علاوه بر سیستم احراز هویت داخلی خود، امکان اتصال به سیستم‌های احراز هویت خارجی مانند LDAP و SSO را نیز دارد، ارزیابی اطلاعات وارد شده بر اساس سیستم احراز هویت انتخابی مدیر سیستم نیز ذخیره می‌شود.
		داده احراز هویت	☑		
		وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)	☑		
		نقش کاربر	☑		
		سایر موارد	☑		علاوه بر موارد بالا، واحد مانیتورینگ کاربران نیز به عنوان یک ویژگی امنیتی در سامانه‌ی معین ذخیره می‌شود.
۴	**محصول باید قابلیت مدیریت گذرواژه را فراهم آورد.**		☑	☑	امکان انتخاب «اجباری بودن» وجود هر گزینه در گذرواژه ایجاد شده است.
	موارد نیاز که باید در تعریف گذرواژه استفاده شوند.	استفاده از حروف کوچک	☑		
		استفاده از حروف بزرگ	☑		
		استفاده از اعداد	☑		
		استفاده از کاراکترهای خاص («@»، «#»، «$»، «٪»، «^»، «!»، «&»، «*»، «(» , «)» و ...)	☑		
		حداقل طول ۸ یا بیشتر (قابل تنظیم)	☑		
		سایر موارد	☐		

۵	**محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.**			☑	
	اقدامات عمومی که کاربر می‌تواند قبل از احراز هویت انجام دهد، انتخاب شود.	مشاهده راهنمای نحوه ورود به سیستم	☐		
		بازیابی گذرواژه	☐		
		هیچ اقدامی	☐		
		سایر موارد	☑		تغییر زبان سامانه
۶	**محصول باید از سازوکار احراز هویت پشتیبانی نماید (برای احراز هویت کاربران راه‌دور، باید بیش از یک سازوکار احراز هویت در محصول به کار رفته باشد).**			☑	
	سازوکارهای احراز هویت موجود در محصول مشخص شوند.	نام کاربری و گذرواژه	☑		
		امضای دیجیتال	☐		
		سامانه‌های احراز هویت مرکزی (مانند Active Directory و ...)	☑		Microsoft Active Directory Open LDAP
		OTP یا توکن	☐		
		احراز هویت دو فاکتوری	☐		
		سایر موارد	☑		SSO (SAML)
۷	**محصول باید برای هر کاربر فعال، ویژگی‌های امنیتی را نگهداری نماید.**			☑	
	ویژگی‌هایی امنیتی که محصول برای هر کاربر نگهداری می‌کند، مشخص گردد (در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین	شناسه کاربر	☑		
		نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمتهای مختلف برنامه	☑		
		جزئیات واسط کلاینت	☑		جزئیات واسط به عنوان بخشی از اطلاعات پیشینه‌ی احراز هویت نگهداری می‌شود.
		پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)	☑		

	در «سایر موارد» بیان می‌شوند).	سایر موارد	☐		
۸	**محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.**		☑		
	در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند).	از بین رفتن اعتبار نشستهای قبلی هنگام برقراری یک نشست جدید (به جز مواردی که فعال بودن همزمان چندین نشست مورد نیاز کارکردی برنامه باشد. در این موارد، هنگام فعال شدن نشست‌های جدید، باید به صفحه کاربر اصلی (نشست اول) اطلاع داده شود.)	☑	محصول معین امکان برقراری چندین نشست همزمان را برای کاربران فراهم می‌کند و از طرفی در صورت رسیدن به محدودیت‌های تعداد نشست‌های موازی، از برقراری نشست جدید جلوگیری می‌کند.	
		بروزرسانی اطلاعات پیشینه احراز هویت	☑		
		سایر موارد	☐		
۹	**محصول باید بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید.**		☑		
	قوانینی که در صورت تغییر ویژگی‌های امنیتی کاربر فعال، اعمال می‌شود، مشخص گردد.	غیرمجاز بودن هرگونه تغییر در طول نشست فعال	☑		
		سایر موارد	☐		

۲-٤- حفاظت از داده‌ی کاربری

داده کاربری در واقع هر نوع داده‌ای است که کاربر تولید می‌کند یا مالک آن است. توضیح کامل داده کاربری در سند «*راهنمای سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه*» در قسمت اصطلاحات بیان گردیده است. در این رده، توانایی محصول در حفاظت از این داده‌ها مورد بررسی قرار می‌گیرد.

شماره الزام	رده حفاظت از داده‌ی کاربری				توضیحات
۱	**محصول باید برای موجودیت‌ها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید.**			☑	
	موجودیت‌های فعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می‌شوند، مشخص گردد.	مدیر سیستم	☑		
		کاربر عادی	☑		
		سایر موارد	☑		سامانه‌ی معین با اعطای نقش‌های مختلف به یک کاربر سطوح دسترسی او را به موجودیت‌های غیرفعال کم یا زیاد می‌کند.
	موجودیت‌های غیرفعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می‌شوند، مشخص گردد.	سوابق، مستندات و فراداده	☑		
		داده متعلق به کاربران	☑		
		داده احراز هویت	☑		
		سایر موارد	☐		
	عملیاتی که خط‌مشی‌های کنترل دسترسی در رابطه با	ایجاد موجودیت غیرفعال جدید	☑		
		حذف موجودیت غیرفعال	☑		
		تغییر دسترسی‌ها به موجودیت غیرفعال	☑		
		عملیات بر روی فراداده وابسته به موجودیت غیرفعال	☑		

	آنها اعمال می‌شوند، مشخص گردد.	سایر موارد	☐		
۲	**محصول باید بر اساس ویژگی‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.**		☑	با توجه به اینکه در هنگام ارسال درخواست توسط کاربر، نشست برقرار شده است، هویت کاربر از طریق نشست مذکور دردسترس خواهد بود که با توجه به این موضوع سامانه با در نظر گرفتن نقش‌های کاربر دسترسی او را کنترل خواهد کرد.	
	ویژگی‌هایی که بر اساس آن خط‌مشی‌ها تعریف می‌شوند، انتخاب گردد.	نقش‌ها و مجوزهای کاربر مجاز	☑		
		اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.	☑		
		سایر موارد	☐		
۳	**محصول باید بر اساس قاعده‌ای عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل‌شده را مجاز نماید (این قاعده می‌تواند بدین شکل باشد که در لیست کنترل دسترسی، سابقه (رکوردی) وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف‌شده حق دسترسی به موجودیت غیرفعال را بدهد.)**		☑	در سامانه‌ی معین دسترسی کاربران با استفاده از اعطای نقش(ها)، کنترل می‌شود. به این ترتیب سطح دسترسی یک کاربر از اجتماع کل نقش‌های اعطایی به او حاصل خواهد شد. مدیر سامانه با تعریف دقیق نقش و میزان دسترسی به هر یک از موجودیت‌های غیرفعال در واحد مانیتورینگ مشخص شده، سطح دسترسی کاربر موردنظر را کنترل می‌کند.	
۴	**محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.**		☑		
	قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).	عبور تعداد نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف‌شده	☑	با توجه به ممانعت از برقراری نشست پس از عبور از حد آستانه، که یکی از نیازمندی‌های مطرح شده در بخش ۲-۸ است، این الزام نیز رعایت می‌شود.	
		سایر موارد	☐		
۵	**محصول باید تضمین نماید تمام اطلاعات قبلی منابع یا در هنگام تخصیص و یا در هنگام آزادسازی آنها، غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.**		☑	در سامانه‌ی معین تمامی اطلاعات از جمله فایل‌ها داخل پایگاه‌داده ذخیره و از آن حذف می‌گردند و هیچ اطلاعی بر روی فایل سیستم ذخیره نمی‌گردد. بر روی پایگاه‌داده نام کاربری و رمز عبور تنظیم می‌شود. از همین رو تضمین می‌شود که تمامی اطلاعات همواره برای کاربر غیرمجاز غیرقابل دسترس خواهد بود.	

					همچنین با توجه به اینکه محصول بر روی یک سیستم عامل اجرا می‌شود سایر تخصیص‌ها و آزادسازی‌ها توسط سیستم عامل انجام و تضمین می‌شود.
۶	**محصول باید هنگام دریافت داده کاربری خطمشی کنترل دسترسی را اعمال و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.**			☑	
	ویژگی‌های امنیتی مرتبط با داده کاربری که در هنگام ورود آن به محصول استفاده می‌شوند، مشخص شود (در صورتی که کنترل دسترسی برای موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد» بیان گردد).	نوع داده	☑		
		حجم و اندازه	☑		**تصاویر**: تصویر پس‌زمینه‌ی داشبوردها در ابعاد حداکثر 2K (۲۰۴۸ در ۱۰۸۰) و سایر تصاویر مانند تصویر پروفایل کاربر و سامانه‌های در ابعاد حداکثر ۵۱۲ در ۵۱۲ قابل ذخیره‌سازی است. در صورتی که تصویر بزرگتر از ابعاد مذکور ارسال شود. سامانه به صورت خودکار آن را به ابعاد یادشده تغییر اندازه خواهد داد. سایر تصاویری که از طریق فیلد تصویر در فرم‌های نمونه‌ی سامانه برای اشیاء بارگذاری می‌شوند می‌بایست حجمی کمتر از حجم تعیین‌شده در فایل پیکربندی داشته باشند. این حد آستانه در فایل پیکربندی محصول قابل تنظیم است که به صورت پیشفرض مقدار آن ۲ مگابایت است. **فایل‌های باینری**: فایل‌هایی که از طریق فیلد فایل در فرم‌های نمونه‌ی سامانه برای اشیاء بارگذاری می‌شوند می‌بایست حجمی کمتر از حجم تعیین‌شده در فایل پیکربندی داشته باشند. این حد آستانه در فایل پیکربندی محصول قابل تنظیم است که به صورت پیشفرض مقدار آن ۱۰ مگابایت است.
		فرمت	☑		تنها عکس‌هایی که MediaType آن‌ها یکی از انواع ««image/png، image/jpeg»» باشد، قابل بارگذاری هستند. تنها فایل‌هایی با پسوند «.png»، «.jpg»، «.jpeg»، «.gif»، «.bmp»، «.pdf»، «.json»، «.zip»، «.rar»، «.tar»، «.doc»، «.docx»، «.ppt»، «.pptx»، «.xls»، «.xlsx»، «.txt»، «.html»، «.xml»، «.mp4»، «.wmv»، «.mov»، «.mp3»، «.wma»، «.aac» که mediaType آن‌ها یکی از انواع «image/png»، «image/jpeg»، «image/gif»، «image/bmp»،

					«application/pdf»، «application/json»، «application/zip»، «application/x-tika-ooxml» (مربوط به برخی نسخه‌های قدیمی پاورپوینت و اکسل)، «application/x-tika-msoffice» (مربوط به نسخه‌های قدیمی ورد)، «text/plain»، «text/html»، «application/xml»، «video/mp4»، «video/quicktime»، «audio/vnd.wave»، «audio/mpeg»، باشد، قابل بارگذاری هستند. به این صورت از بارگذاری فایل‌های اجرایی مانند exe. و سایر اسکریپت‌ها ممانعت شده است.
		تعداد دفعات Import	☐		
		سایر موارد	☐		
۷	**محصول باید از یک پروتکل امن برای انتقال داده استفاده نماید. این پروتکل ارتباط و همبستگی شفافی را بین داده کاربری دریافت‌شده و ویژگی‌های امنیتی آن فراهم و همچنین از شنود و گم‌شدن داده حین انتقال جلوگیری می‌کند.**		☑		تمامی ارتباطات سرور با کلاینت‌ها مبتنی بر پروتکل Https می‌باشد که امکان شنود را از بین می‌برد.
۸	**محصول باید هنگام انتقال داده به بیرون از محصول، خط‌مشی کنترل دسترسی اعمال نماید و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.**		☑		در سامانه‌ی معین امکان خروجی گرفتن از گزارشات (تولید در سمت سرور)، نمودارها و جداول رخدادها و راهنمای سامانه (تولید در سمت کلاینت) وجود دارد. هر کاربری که بتواند اصل محتوای مذکور را در سامانه مشاهده کند به انواع خروجی‌های پیاده‌سازی شده برای آن محتوا نیز دسترسی خواهد داشت.
	ویژگی‌های امنیتی مرتبط با داده کاربری که در هنگام خروج آن از محصول استفاده می‌شوند، مشخص شوند	نوع داده	☐		
		حجم و اندازه	☐		
		فرمت	☑		گزارشات: pdf و csv نمودارها: png، jpeg، svg، pdf و csv جدول رخدادها: csv راهنمای سامانه: pdf

		سایر موارد	☐		
۹	**محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.**		☑		
	قوانینی که در هنگام خروج داده از محصول اعمال می‌شوند، مشخص شوند	مدیر سیستم باید خروج داده‌ها را محدود نماید، به طوریکه کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند.	☑		در سامانه‌ی معین، خروجی داده‌ی کاربری تنها در یک مورد وجود دارد که مربوط به فایل‌های meta-data بارگذاری شده توسط خود کاربران در فرم‌های اشیاء است. با توجه به اینکه دسترسی به اشیاء توسط خط مشی کنترل دسترسی برای کاربران مجاز محدود شده است، تنها کاربران دارای مجوز دسترسی به شی مورد نظر توانایی بارگیری فایل مذکور را خواهند داشت.
		سایر موارد	☐		
۱۰	**محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره‌شده در محصول تشخیص دهد.**		☑		
	چگونگی تشخیص تغییر در داده‌های کاربری حساس، مشخص شود.	مقدار درهم‌سازی‌شده داده‌های کاربری ذخیره‌شده، نگهداری می‌شود.	☑		
		سایر موارد	☐		
۱۱	**محصول باید در صورت تشخیص خطای صحت در داده‌ها، اقدامات مقابله‌ای زیر را انجام دهد.**		☑		
	اقدام مقابله‌ای در صورت تشخیص خطا، مشخص شود (وجود یک مورد لازم و کافی است)	ایجاد هشدار/اخطار برای نقش‌های مجاز	☑		
		تصحیح داده بر اساس مقادیر قبل	☐		
		سایر موارد	☐		

۲-۵- مدیریت امنیت

در این رده توانایی‌های محصول در مدیریت (حذف، تغییر، فعال کردن و ...) کارکردهای امنیتی (جمع‌آوری داده‌های سیستم، پیکربندی‌ها و ...) مورد بررسی قرار می‌گیرد. همچنین توانایی محصول در مدیریت نقش‌ها و دسترسی آنها برای اعمال مدیریت بر روی کارکردهای امنیتی سنجیده می‌شود.

شماره الزام	رده مدیریت امنیت				توضیحات
۱	**محصول باید برای مدیر سیستم و هر کاربری که مجوز لازم را دارد، امکان فعالیت‌های مدیریتی زیر را بر روی توابع و تمام کارکردهای مربوط به مدیریت محصول فراهم آورد.**			☑	
	فعالیت‌های مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند.	تعیین و تغییر رفتار	☑		
		غیرفعال نمودن	☑		
		فعال نمودن	☑		
		سایر موارد	☐		
۲	**محصول باید با اعمال خط‌مشی کنترل دسترسی، امکان تغییر پیش‌فرض و عملیات زیر را بر روی ویژگی‌های امنیتی الزام ۷ از رده (Class) شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.**			☑	
	عملیات بر روی ویژگی‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد.	پرس‌وجو	☑		
		تغییر	☑		
		حذف	☑		
		تغییر پیش‌فرض	☑		
		سایر موارد	☐		
۳	**محصول باید برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.**			☑	
	عملیات بر روی داده‌های محصول که	تغییر پیش‌فرض	☑		
		حذف نمودن	☑		

	در محصول پشتیبانی می‌شوند، مشخص شود.	پرس‌وجو	☑		
		مقداردهی	☑		
		ایجاد	☑		
		مشاهده	☑		
		سایر موارد	☐		
۴	**محصول باید توانایی انجام کارکردهای زیر را داشته باشد.**			☑	
	در صورتی که هرکدام از موارد مطرح‌شده، توسط محصول قابل اجرا نیست، در قسمت توضیحات باید دلایل مطرح گردد.	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشان‌ها	☑		کاربرانی که به عنوان مدیر امنیتی در سامانه معرفی شوند می‌توانند به ثبت‌نشان‌ها دسترسی داشته باشند.
		پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشان‌ها	☑		
		پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشان‌ها	☑		با توجه به اینکه در معین، سیاست بازنویسی روی ثبت‌نشان‌های قدیمی اتخاذ شده است، خرابی‌ای از این بابت رخ نخواهد داد. با این حال مدیران امنیتی این امکان را دارند که در هر زمان دلخواه، لاگ‌های ماقبل تاریخ انتخابی‌شان را حذف نمایند.
		مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول	☑		
		انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده که می‌تواند در محصول قابل پیکربندی باشد. (برای مثال، زمان تخصیص و یا زمان آزادسازی منابع)	☐		با توجه به توضیحات ارائه شده در بند ۵ بخش ۲-۴ (حفاظت داده‌ی کاربری) با توجه به اینکه هیچ داده‌ای از کاربر از جمله فایل‌ها در فایل سیستم ذخیره نمی‌شود و همگی داخل پایگاه داده قرار دارند، آزادسازی آن‌ها مساوی با حذف کامل از پایگاه داده خواهد بود، لذا پیاده‌سازی چنین تنظیماتی به جهت حفاظت از داده‌های روی فایل سیستم برای سامانه معین موردنیاز نبوده است.
		ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول	☑		قوانین مورد نظر از طریق فایل پیکربندی توسط مدیر محصول قابل تنظیم خواهد بود.
		در نظر گرفتن یک عملیات از پیش تعیین‌شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد.	☑		
		۱. مدیریت حد آستانه برای تلاش‌های ناموفق ۲. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد.	☑		حد آستانه از طریق تنظیم مقدار مذکور توسط مدیر قابل تنظیم است.

		مدیریت معیارها برای تنظیم گذرواژه‌ها	☑		مدیریت هر کدام از معیارها به صورت جداگانه قابل انتخاب و اعمال توسط مدیر خواهد بود.
		۱. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه ۲. مدیریت یک‌سری عملیاتی که قبل از احراز شدن هویت کاربر انجام می‌شوند.	☑		در سامانه‌ی معین پیش از احراز هویت یک کاربر، مدیر می‌تواند گذرواژه‌ی یک کاربر، وضعیت فعال بودن حساب کاربری او را از طریق سامانه و روش‌های احراز هویت (مانند استفاده از LDAP یا SSO یا لاگین با نام کاربری و رمز عبور داخلی) را از طریق پیکربندی هنگام راه‌اندازی سامانه تنظیم کند.
		۱. مدیریت سازوکارهای احراز هویت ۲. مدیریت قوانین مرتبط با احراز هویت	☑		قابلیت انتخاب سیستم احراز هویت داخلی یا خارجی مانند LDAP در هنگام راه‌اندازی سیستم و پیش از عملیات احراز هویت کاربران وجود دارد.
		مدیریت تغییرات و فرآیندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.	☑		مدیر می‌تواند تمام IPهای مجاز را جهت اتصال کلاینت‌ها برای سامانه تعریف کند.
		مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.	☑		
		مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول	☑		
		مدیریت نقش‌ها در محصول	☑		
		مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر	☑		
		مدیریت شرایط آغاز نشست توسط مدیر مجاز	☑		
		۱. تعیین زمان غیرفعال بودن برای یک کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد. ۲. تعیین زمان پیش‌فرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.	☑		در سامانه‌ی معین مدیر می‌تواند مدت زمان منقضی شدن یک نشست غیرفعال را مشخص کند. مقدار جدید آن برای تمامی نشست‌های جدید قابل اعمال خواهد بود.
۵	**محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد.**		☑		
	نقش‌هایی که در محصول پشتیبانی	مدیر سیستم	☑		
		کاربر پیشرفته	☑		
		کاربر عادی	☑		

	می‌شـــوند، مشـــخص گردد.	سایر موارد	☐	
۶	**محصول باید قادر باشد کاربران را به نقش‌های تعریف‌شده یا قابل تعریف مرتبط نماید، همچنین لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد، اما ممکن است نقش‌ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.**		☑	در سامانه‌ی معین با توجه به نیازمندی مشتریان، امکان تخصیص نقش‌های مختلف به یک کاربر وجود دارد. در صورت تخصیص بیش از یک نقش یه یک کاربر، اجتماع نقش‌ها به عنوان نقش‌های نهایی کاربر موردنظر در نظر گرفته می‌شود.

۲-۶- حفاظت از توابع امنیتی محصول

در این رده، توانایی محصول در حفظ وضعیت امن در زمان رخ دادن شکست و همچنین حفاظت از داده‌ها هنگام تبادل بین اجزای محصول یا تبادل با موجودیت‌های دیگر، مورد بررسی قرار گرفته است.

شماره الزام	رده حفاظت از توابع امنیتی محصول				توضیحات
۱	**محصول باید هنگام رخ دادن هرگونه خرابی، اشکال یا شکست مانند از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول، در وضعیت امنی قرار گرفته، صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید.**			☑	
	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول حفظ می‌شود، مشخص گردد.	خرابی‌های نرم‌افزاری	☑		خرابی‌های نرم‌افزاری از طریق اعلان و به صورت مفهوم به اطلاع کاربر می‌رسد. کاربر هیچگاه کد خطا یا صفحه‌ی خطای چارچوب را مشاهده نخواهد کرد. مانند خطای ارتباط با سرور، یا timeout شدن یک درخواست ارسالی از سمت کاربر.
		خرابی‌های سخت‌افزاری	☑		هیچ خطای سخت‌افزاری باعث از کار افتادن سطوح دسترسی در سامانه نخواهد شد و امنیت داده‌های کاربر به خطر نخواهد افتاد. کاربر غیرمجاز قادر به دسترسی به داده‌ها در چنین حالتی را نخواهد داشت.
۲	**محصول باید از طریق فراهم نمودن بستر و زیرساخت امن، توانایی جلوگیری از افشاء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد.**			☑	بین core و portal از routing mesh/ingress network سرویس داکر استفاده می‌شود.
۳	**در صورتی که محصول از محصولات امن IT استفاده می‌کند، باید تفسیر سازگار و یکسانی را از داده امنیتی در زمان اشتراک‌گذاری آن بین خود و دیگر محصولات امن IT، فراهم آورد.**			☑	
	داده امنیتی قابل اشتراک‌گذاری که در محصول پشتیبانی می‌شوند، مشخص گردد.	داده‌های احراز هویت	☑		داده‌های دریافتی کاربران از LDAP و SSO به مدل‌های سازگار با ماژول احراز هویت داخلی تفسیر و ذخیره‌سازی می‌شوند.
		کلید	☐		
		امضای دیجیتال	☐		
		ثبت‌نشان‌ها (داده‌های ممیزی)	☐		

		سایر موارد	☐		
۴	**محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی[۴] معتبر را تولید یا از آن‌ها استفاده نماید.**			☑	
	روش‌های ایجاد مهرهای زمانی معتبر انتخاب شود. (دیگر روشهای موجود در محصول، در قسمت «سایر موارد» بیان شود).	گرفتن مهرهای زمانی از سرور NTP	☐		
		تنظیم مهرهای زمانی از طریق اینترنت	☐		
		تنظیم مهرهای زمانی به صورت پیش‌فرض (معتبر و عدم امکان دستکاری غیرمجاز)	☑		
		سایر موارد	☐		
۵	**محصول باید امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید.**			☑	
	روش بروزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).	بروزرسانی دستی	☑		
		جستجوی خودکار بروزرسانی‌ها	☐		
		بروزرسانی‌های خودکار	☐		
		بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی	☐		
۶	**در صورت استفاده از بروزرسانی به روش خودکار، محصول باید پیش از نصب بروزرسانی‌های نرم‌افزاری و میان‌افزاری، امکان احراز اصالت میان‌افزار یا نرم‌افزار را فراهم نماید.**			☐	
	سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی) به‌روزرسانی‌ها انتخاب گردد.	امضای دیجیتال	☐		
		درهم‌ساز منتشرشده	☐		

[4] Time stamp

۲-۷- تخصیص منابع

در این رده، به بررسی وضعیت عملکردهای محصول و منابع مورد استفاده توسط آن در زمانهای مختلف از جمله زمان شکست پرداخته می‌شود.

شماره الزام	رده تخصیص منابع		توضیحات
۱	محصول باید در زمان رخداد هرگونه اشکال و خرابی (شکست) نرم‌افزاری، از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.	☑	در سامانه‌ی معین از مکانیزم راه‌اندازی مجدد به صورت خودکار (ریستارت) استفاده شده است و وضعیت‌ها در این حالت‌ها لاگ می‌شوند.

۲-۸- دسترسی به محصول

در این رده توانایی محصول در مدیریت نشست‌های صورت گرفته شده توسط کاربر، ارزیابی می‌شود.

شماره الزام	رده دسترسی به محصول				توضیحات
۱	**محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.**			☑	با توجه به نیاز مشتریان جهت استفاده‌ی همزمان یک کاربر از سامانه‌ی معین بر روی دستگاه‌های مختلف مانند video wallها، رایانه‌ی شخصی، لپ تاپ و مرورگر تلفن همراه، به صورت پیشفرض هر کاربر در سامانه، مجاز به برقراری ۱۰ نشست همزمان خواهد بود که توسط مدیر قابل تغییر است.
۲	**محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمانی که غیرفعال هستند (و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.**			☑	
۳	**محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.**			☑	
۴	**در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد.**			☑	
	انتخاب یک مورد لازم و کافی است.	روز	☑		
		زمان	☑		
		سایر موارد	☑		جزئیات واسط کلاینت مانند نوع و نسخه‌ی مرورگر و سیستم عامل، آدرس IP
۵	**در صورت برقراری نشست به طور موفقیت آمیز، محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس موارد زیر و تعداد تلاش‌های ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز باشد.**			☑	
	انتخاب یک مورد لازم و کافی است.	روز	☑		
		زمان	☑		

		سایر موارد	☑		جزئیات واسط کلاینت مانند نوع و نسخه‌ی مرورگر و سیستم عامل، آدرس IP
۶	**محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.**			☑	
۷	**محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.**			☑	
	پارامترهای موجود برای جلوگیری از نشست، مشخص شوند (وجود یک مورد لازم و کافی است).	مکان	☑		
		شماره پورت	☐		
		روز	☐		
		زمان	☐		
		سایر موارد	☐		

۲-۹- کانال‌ها/مسیرهای مورد اعتماد

در این رده به بررسی پروتکل‌های امنی که برای برقراری کانال/مسیر مورد اعتماد، بین محصول و موجودیت‌های IT خارجی، یا بین اجزای محصول، استفاده می‌شوند، پرداخته می‌شود.

شماره الزام	رده کانال‌ها/مسیرهای مورد اعتماد			توضیحات
۱	**محصول باید قادر باشد مسیر ارتباطی امنی بین خود، کاربران و دیگر محصولات IT فراهم نماید که به طور منطقی از دیگر کانال‌ها متمایز باشد. سپس از طریق این کانال احراز هویت را انجام دهد و از تغییر و افشای داده تبادلی حفاظت نماید و تغییرات را تشخیص دهد.** در صورت انتخاب مورد HTTPS، رعایت الزام ۱-۳- و ۳-۳- و در صورت انتخاب TLS، رعایت الزامات ۳-۲- تا ۴-۳- که در بخش ۳- بیان گردیده است، الزامی است.		☑	
	پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.	HTTPS	☑	
		TLS	☑	از این پروتکل برای اتصال به سرورهای ایمیل (SMTP over TLS) استفاده می‌شود.
		SSH	☑	
۲	**محصول باید به کاربر /دیگر محصول IT معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.**		☑	تمامی APIهای ارائه شده بر اساس HTTPS می‌باشند.
۳	**محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.**		☑	تمامی اتصالات http به نوع امن https ری دایرکت می‌شوند و بر روی http هیچ سرویسی ارائه نمی‌شود.

۳-الزامات امنیتی مبتنی بر انتخاب

این بخش به بیان الزاماتی می‌پردازد که رعایت آنها وابسته به برخی از الزاماتی است که در بخش‌های پیشین بیان شده است. برای مثال اگر در الزامات مربوط به رده کانال امن، پروتکل HTTPS انتخاب شود، آنگاه رعایت الزامات HTTPS که در این بخش بیان شده است، اجباری می‌گردد.

۳-۱- پروتکل HTTPS

شماره الزام	پروتکل HTTPS				توضیحات
۱	**محصول باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند.**			☑	
۲	**محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند.**			☑	
۳	**در صورتی که گواهی‌نامه ارائه شده از سمت دیگر محصولات IT (درهنگام برقراری ارتباط) نامعتبر باشد، محصول باید بر اساس موارد زیر عمل نماید.** اعتبارسنجی گواهی‌نامه بر اساس الزامات بخش ۵-۳- انجام می‌شود که در این صورت الزامات بخش ۵-۳- الزامی است.			☑	
	محصول تنها از موارد بیان‌شده می‌تواند استفاده نماید.	اتصال را برقرار نکند.	☑		رفتار پیشفرض محصول برقرار نکردن ارتباط است.
		برای برقراری اتصال درخواست مجوز کند.	☑		در سامانه‌ی معین گزینه‌ی «صرف نظر کردن از خطاهای SSL» نیز وجود دارد که کاربر در صورت اصرار بر برقراری ارتباط ناامن با محصولات دارای گواهی‌های نامعتبر، مجوز را به صورت صریح به سامانه می‌دهد.

۳-۲- پروتکل TLS Client

شماره الزام	پروتکل TLS Client				توضیحات
۱	**محصول باید TLS 1.2 (RFC 5246) و/یا TLS 1.1 (RFC 4346) را پیاده‌سازی و دیگر نسخه‌های TLS و SSL را رد کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.**			☑	
	مجموعه رمز مورد استفاده و پیاده‌سازی‌شـــــــده محصول، انتخاب گردد.	☑	TLS_AES_256_GCM_SHA384 0x1302 مطابق با RFC 8446		
		☑	TLS_AES_128_GCM_SHA256 0x1301 مطابق با RFC 8446		
		☑	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 0x009F مطابق با RFC 5288		
		☑	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 0x009E مطابق با RFC 5288		
		☑	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xC02F مطابق با RFC 5289		
		☑	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xC030 مطابق با RFC 5289		
		☑	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 0xC02C		

				مطابق با RFC 5289		
			☑	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 0xC02B مطابق با RFC 5289		
			☑	TLS_RSA_WITH_AES_256_GCM_SHA384 0x009D مطابق با RFC 5288		
			☑	TLS_RSA_WITH_AES_128_GCM_SHA256 0x009C مطابق با RFC 5288		
			☑	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 0xC02E مطابق با RFC 5288		
			☑	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 0xC02D مطابق با RFC 5289		
			☑	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 0xC032 مطابق با RFC 5289		
			☑	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 0xC031 مطابق با RFC 5289		
			☐	TLS_DH_RSA_WITH_AES_256_GCM_SHA384 0x00A1 مطابق با RFC 5288		
			☐	TLS_DH_RSA_WITH_AES_128_GCM_SHA256 0x00A0 مطابق با RFC 5288		

۲	**محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تأیید نماید.**			☑	
۳	**محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد؛ بنابراین اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید بر اساس موارد زیر رفتار نماید.**			☑	
	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.	ارتباط را برقرار نکند	☑		رفتار پیشفرض محصول برقرار نکردن ارتباط است.
		برای برقراری ارتباط درخواست مجوز کند	☑		در سامانه‌ی معین گزینه‌ی «صرف نظر کردن از خطاهای SSL» نیز وجود دارد که کاربر در صورت اصرار بر برقراری ارتباط ناامن با محصولات دارای گواهی‌های نامعتبر، مجوز را به صورت صریح به سامانه می‌دهد.
		سایر موارد	☐		
۴	**محصول باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید.**			☑	لیست خم‌های ارائه شده: secp256r1 (0x0017) secp384r1 (0x0018) secp521r1 (0x0019) ffdhe2048 (0x0100) ffdhe3072 (0x0101) ffdhe4096 (0x0102) ffdhe6144 (0x0103) ffdhe8192 (0x0104)
	در صورت که محصول از منحنی استفاده می‌نماید، طول کلید باید مشخص گردد.	Supported Elliptic Curves Extension را ارائه نکند.	☐		
		Supported Elliptic Curves Extension را به همراه NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 ارائه نماید.	☑		

۳-۳- پروتکل TLS Server

شماره الزام	پروتکل TLS Server				توضیحات
۱	**محصول باید TLS 1.2 (RFC 5246) را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.**			☑	
	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.	☑	TLS_AES_256_GCM_SHA384 0x1302 مطابق با RFC 8446		
		☑	TLS_AES_128_GCM_SHA256 0x1301 مطابق با RFC 8446		
		☑	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 0x009F مطابق با RFC 5288		
		☑	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 0x009E مطابق با RFC 5288		
		☑	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xC02F مطابق با RFC 5289		
		☑	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xC030 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 0xC02C مطابق با RFC 5289		

		☐	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 0xC02B مطابق با RFC 5289			
		☑	TLS_RSA_WITH_AES_256_GCM_SHA384 0x009D مطابق با RFC 5288			
		☑	TLS_RSA_WITH_AES_128_GCM_SHA256 0x009C مطابق با RFC 5288			
		☐	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 0xC02E مطابق با RFC 5288			
		☐	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 0xC02D مطابق با RFC 5289			
		☐	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 0xC032 مطابق با RFC 5289			
		☐	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 0xC031 مطابق با RFC 5289			
		☐	TLS_DH_RSA_WITH_AES_256_GCM_SHA384 0x00A1 مطابق با RFC 5288			
		☐	TLS_DH_RSA_WITH_AES_128_GCM_SHA256 0x00A0 مطابق با RFC 5288			
		☑	TLS_CHACHA20_POLY1305_SHA256			

۲	**محصول باید اتصال‌های کاربرانی که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و TLS1.1 دارند را رد نماید.**			☑	
۳	**محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.**			☑	
	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.	استفاده از RSA با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ یا ۴۰۹۶ بیت	☑		اندازه‌ی کلید در مجموعه رمزهای…TLS_RSA مقدار ۲۰۴۸ بیت است.
		پارامترهای ECDH با استفاده از NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگر	☑		خم مورد استفاده در مجموعه رمزهای …TLS_ECDH(E) مقادیر زیر است: Prime256v1 Secp384r1 Secp521r1 X25519 X448
		پارامترهای دیفی-هلمن با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ بیت	☑		اندازه‌ی کلید مورد استفاده در مجموعه مرزهای …TLS_(DHE مقدار ۲۰۴۸ است.

۳-٤- پروتکل TLS مشترک کلاینت و سرور

لازم به ذکر است که الزاماتی که با عنوان پروتکل‌های TLS Server و TLS Client مطرح شده است، برای مباحث مرتبط به احراز هویت TLS Server و TLS Client نیز مطرح می‌گردد. در این بخش چند الزام که برای احراز هویت این پروتکل‌ها مطرح می‌گردد و برای هر دوی کلاینت و سرور نیز یکسان است و باید برای هر کدام مورد بررسی قرار گیرد، آورده شده است.

شماره الزام	پروتکل TLS مشترک کلاینت و سرور		توضیحات
۱	**محصول باید احراز هویت دوطرفه کلاینت‌ها/سرورهای TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.**	☑	
۲	**در صورت مطابقت نداشتن نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه از شناساننده کلاینت مورد انتظار بوده است، محصول نباید کانال امن را برقرار سازد.**	☐	با توجه به اینکه سازوکار احراز هویت کلاینت‌ها در سامانه‌ی معین از طریق گواهی‌نامه نیست، نیازی به پیاده‌سازی این بخش نبوده است.

۳-۵- اعتبارسنجی گواهی‌نامه

شماره الزام	اعتبارسنجی گواهی‌نامه				توضیحات
۱	**محصول باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند.**			☑	
		تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.	☑		با توجه به نیاز مشتری، لازم است تا در صورتی که کاربر دارای گواهی‌نامه‌های self-signed نیز باشد، سرور بتواند آن‌ها را تأیید کند. با توجه به نیاز مشتری، مدیر سیستم که به کل سرور دسترسی دارد، می‌تواند Cert های مورد اعتماد خود را داخل پوشه‌ی certs قرار دهد و به این ترتیب سامانه‌ی معین هر cert ای که در این پوشه قرار داشته باشد را معتبر می‌داند زیرا با اختیار خود مدیر در آنجا قرار داده شده‌اند.
		مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.	☑		با توجه به نیاز مشتری، مدیر سیستم که به کل سرور دسترسی دارد، می‌تواند Cert های مورد اعتماد خود را داخل پوشه‌ی certs قرار دهد و به این ترتیب سامانه‌ی معین همه‌ی آن‌ها را به عنوان Root CA معتبر در نظر می‌گیرد.
		محصول باید برای تأیید مسیر یک گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم شده است.	☑		
	روش‌های تأیید وضعیت فسخ گواهی‌نامه	پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص‌شده در RFC 696	☐		
		لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۶.۳	☐		
		لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵	☐		
		هیچ روش فسخ دیگری	☑		
	قوانین تأیید بخش extendedKeyUsage	گواهی‌نامه‌های مورد استفاده برای تأیید بروزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی باید هدف «Code Signing» (id-kp3 با OID 1.3.6.1.5.5.7.3.1) را در بخش extendedKeyUsage خود داشته باشند.	☐		با توجه به اینکه محصول معین از روش بروزرسانی دستی (مورد اول از بند ۵ جدول ۲-۶) استفاده می‌کند. نیازی به پیاده‌سازی این بخش نداشته‌ایم.

		گواهی‌نامه‌های سرور ارائه شده برای TLS باید هدف « Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در بخش extendedKeyUsage خود داشته باشند.	☑		
		گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف « Client Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در بخش extendedKeyUsage خود داشته باشند.	☑		
		گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ OCSP باید « OCSP Signing» (id-pk9 با OID 1.3.6.1.5.5.7.3.9) را در بخش extendedKeyUsage خود داشته باشند.	☐		
۲		**محصول باید تنها در صورتی که افزونه مربوط به basicConstraints از پیش تنظیم شده باشد و همچنین، پرچم CA به حالت «TRUE» تنظیم شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA بپذیرد.**	☑		
۳		**محصول باید برای پشتیبانی از احراز هویت برای موارد زیر، از گواهی‌نامه‌های X509v3 تعریف‌شده در RFC 5280 استفاده کند.**	☑		
	در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.	HTTPS	☑		
		TLS	☑		
		SSH	☐		
		امضای کد برای بروزرسانی‌های نرم‌افزار سیستم	☐		
		امضای کد برای تأیید یکپارچگی	☐		
		سایر موارد	☐		

۶-۳- پروتکل SSH

شماره الزام	پروتکل SSH		توضیحات
۱	**محصول باید پروتکل SSH را مطابق با RFCهای ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۵۶۵۶ و ۶۶۶۸ پیاده‌سازی نماید.**	☑	محصول از ابزار OpenSSH نسخه‌ی 8.9p1 استفاده می‌کند که مطابق بر RFCهای خواسته شده پیاده‌سازی شده است.
۲	**محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4252، از روش‌های احراز هویت زیر پشتیبانی نماید.**	☑	
	احراز هویت مبتنی بر کلید عمومی	☑	
	احراز هویت مبتنی بر گذرواژه	☑	
۳	**محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4253، بسته‌های بزرگتر از مقدار مشخصی (در بخش «توضیحات» ذکر شود) را کنار بگذارد.**	☑	در این بخش از پیشفرض بیشینه‌ی حجم بسته‌ی تعیین شده در ابزار OpenSSH یعنی 256KB استفاده می‌شود.
۴	**محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های رمزنگاری زیر استفاده نماید.**	☑	
	AES128-CBC	☐	
	AES192-CBC	☐	
	AES256-CBC	☐	
	AES128-CTR	☑	
	AES192-CTR	☑	
	AES256-CTR	☑	
	AEAD_AES_128_GCM	☐	
	AEAD_AES_256_GCM	☐	

۵	**محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های کلید عمومی زیر استفاده نماید.**		☑	
	ssh-ed25519	☑		
	ssh-ed448	☐		
	rsa-sha2-512	☑		
	rsa-sha2-256	☑		
	ecdsa-sha2-nistp521	☐		
	ecdsa-sha2-nistp384	☐		
	ecdsa-sha2-nistp256	☐		
	x509v3-ecdsa-sha2-nistp521	☐		
	x509v3-ecdsa-sha2-nistp384	☐		
	x509v3-ecdsa-sha2-nistp256	☐		
	x509v3-rsa2048-sha256	☐		
	ssh-rsa	☐		
	x509v3-ssh-rsa	☐		
۶	**محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های MAC صحت داده‌های زیر استفاده نماید.**		☑	
	AEAD_AES_256_GCM	☐		
	AEAD_AES_128_GCM	☐		
	hmac-sha2-512	☑		
	hmac-sha2-256	☑		
	hmac-sha1-96	☑		
	hmac-sha1	☑		
۷	**محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های تبادل کلید زیر استفاده نماید.**		☑	
	curve25519-sha256	☑		
	curve448-sha512	☐		

		☑	diffie-hellman-group-exchange-sha256		
		☑	diffie-hellman-group18-sha512		
		☐	diffie-hellman-group17-sha512		
		☑	diffie-hellman-group16-sha512		
		☐	diffie-hellman-group15-sha512		
		☑	ecdh-sha2-nistp521		
		☑	ecdh-sha2-nistp384		
		☑	ecdh-sha2-nistp256		
		☐	rsa2048-sha256		
		☐	diffie-hellman-group-exchange-sha1		
		☐	diffie-hellman-group14-sha256		
۸	**محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه (طول نشست بیشتر از یک ساعت و حجم داده مبادله شده بیشتر از ۱ گیگابایت نباشد) استفاده گردد. در صورت پر شدن حد آستانه برای هر کدام از موارد ذکر شده، باید تجدید کلید صورت بگیرد.**		☑		
۹	**محصول باید اطمینان حاصل نماید که کلاینت SSH، سرور SSH را احراز هویت می‌کند. سرور SSH از یک پایگاه داده محلی که نام هر میزبان را با کلید عمومی متناظر آن (تشریح‌شده در RFC 4251 بخش ۱.۷) همراه می‌کند، استفاده می‌نماید.**		☑		