به نام خدا

لطفا نام فایل پرسشنامه را به صورت «Quest.{SoftwareName}.{CompanyName}.v{QuestVersion}» اصلاح نمایید.
بخش «نسخه»، به «نسخه‌ی پرسشنامه» اشاره دارد. اگر مایل به درج «نسخه‌ی محصول» در نام فایل هستنید، آن را پس از نام محصول به صورت زیر درج نمایید. «Quest.{SoftwareName}.v{ProductVersion}.{CompanyName}.v{QuestVersion}»
لطفا علامت‌های «{» و «}» را حذف نمایید. این علامت‌ها صرفا جهت معرفی بخش‌هایی است که لازم است تکمیل شوند.

سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه

<نام شرکت>
<نام محصول>
<نسخه محصول>

لطفا علامت‌های «<» و «>» را حذف نمایید.
این علامت‌ها صرفا جهت معرفی بخش‌هایی است که لازم است تکمیل شوند.

<لوگوی شرکت>

<ماه><سال>
نسخه <۱,۰>

آزمایشگاه آزمون و ارزیابی تجهیزات شبکه و امنیت
دانشگاه صنعتی شریف

راهنمای تکمیل «پرسشنامه»
نسخه‌ی ۱,۱

هرگونه نسخه‌برداری بدون مجوز آزمایشگاه آزمون و ارزیابی تجهیزات شبکه و امنیت دانشگاه صنعتی شریف ممنوع ولی استناد به مطالب این راهنما با ذکر مرجع مجاز است.

Commented [SE1]: این «نسخه»، نسخه‌ی «پرسشنامه» است که در نام فایل نیز باید ذکر شود.
(بدیهی است «نسخه‌ی محصول» و «نسخه‌ی پرسشنامه» با یکدیگر تفاوت دارند.)

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.

با توجه به ماهیت «پرسشنامه»، لطفا از انجام موارد زیر خودداری نمایید:

۱. ضربدر زدن مواردی که در محصول وجود ندارند
   انتخاب نکردن هر الزام یا گزینه، به معنی نداشتن آن ویژگی است
۲. نوشتن توضیح‌های اضافی مانند «پیاده‌سازی شده است»، «پشتیبانی نمی‌شود» و ...
   انتخاب کردن یا نکردن الزام‌ها یا گزینه‌ها همین معنی را دارند.
۳. نوشتن توضیح‌هایی مانند «در حال پیاده‌سازی» و ...
   هنگام ارزیابی محصول، این موارد باید در محصول وجود داشته باشند، بنابراین نوشتن این عبارت‌ه اضافی است.
۴. تکرار و تأیید متن الزام در بخش «توضیحات»
   انتخاب الزام به معنی رعایت آن است و نیازی نیست دوباره در بخش «توضیحات» تکرار شود.
۵. در بخش «توضیحات» تنها مواردی را درج نمایید که نوع پیاده‌سازی مهم است یا توضیحی مورد نیاز است.

لطفا برای انتخاب گزینه‌ها از علامت‌ها مناسب موجود در Word استفاده نمایید. (✓ ☑ ☒)

راهنمایی: علامت‌های یاد شده، با انتخاب فونت Wingdings 2 و حروف P (✓)، Q (☒)، R (☑)، S (☒) و T (☒) قابل استفاده هستند. همچنین از برگه (Tab) Insert و بخش Symbol نیز می‌توانید این علامت‌ها را پیدا نمایید.

این «پرسشنامه» برای محصول‌های تحت‌وب و نرم‌افزارهای ویندوزی که با سرور ارتباط دارند است.

در صورتی که محصول نرم‌افزار موبایل (Android یا iOS) دارد، لازم است «پروفایل حفاظتی برنامه کاربردی» تکمیل شود.

تاریخ تکمیل «پرسشنامه» را در پانویس صفحه‌ها اصلاح نمایید.
(این تاریخ مطابق تاریخ درج شده در صفحه‌ی اول خواهد بود.)

نسخه‌ی «پرسشنامه» را پس از هر بروزرسانی اصلاح نمایید.
(این عدد، با مقدار درج شده در صفحه‌ی اول و نام فایل مطابقت خواهد داشت.)

[SE] Commented [۲]: پس از تکمیل «پرسشنامه»، لطفا این جدول را نیز بروزرسانی نمایید.

فهرست

فهرست ۳
۱- معرفی محصول ۴
۱-۱- ویژگی‌های فنی محصول ۴
۱-۲- معماری محصول ۴
۲- الزامات امنیتی ۵
۲-۱- ممیزی امنیت (Log) ۵
۲-۲- رمزنگاری ۹
۲-۳- شناسایی و احراز هویت ۱۲
۲-۴- حفاظت از داده‌ی کاربری ۱۶
۲-۵- مدیریت امنیت ۲۰
۲-۶- حفاظت از توابع امنیتی محصول ۲۴
۲-۷- تخصیص منابع ۲۶
۲-۸- دسترسی به محصول ۲۷
۲-۹- کانال‌ها/مسیرهای مورد اعتماد ۲۹
۳- الزامات امنیتی مبتنی بر انتخاب ۳۰
۳-۱- پروتکل HTTPS ۳۰
۳-۲- پروتکل TLS Client ۳۱
۳-۳- پروتکل TLS Server ۳۴
۳-۴- پروتکل TLS مشترک کلاینت و سرور ۳۷
۳-۵- اعتبارسنجی گواهی‌نامه ۳۸
۳-۶- پروتکل SSH ۴۰

۱- معرفی محصول

توضیحات خود را جایگزین این متن نمایید.

[SE] Commented [۳]: به صورت مختصر و در حد چند عنوان عملکرد کلی محصول را تشریح نمایید

<معرفی عملکرد محصول> {لطفا در این بخش به اختصار و در حد چند عنوان عملکرد محصول را مشخص نمایید}

۱-۱- ویژگی‌های فنی محصول

نسخه‌ی نرم‌افزار/میان‌افزار	
مدل و نسخه سیستم‌عامل	
مدل و نسخه وب‌سرور	
مدل و نسخه پایگاه داده	
زبان برنامه‌نویسی	

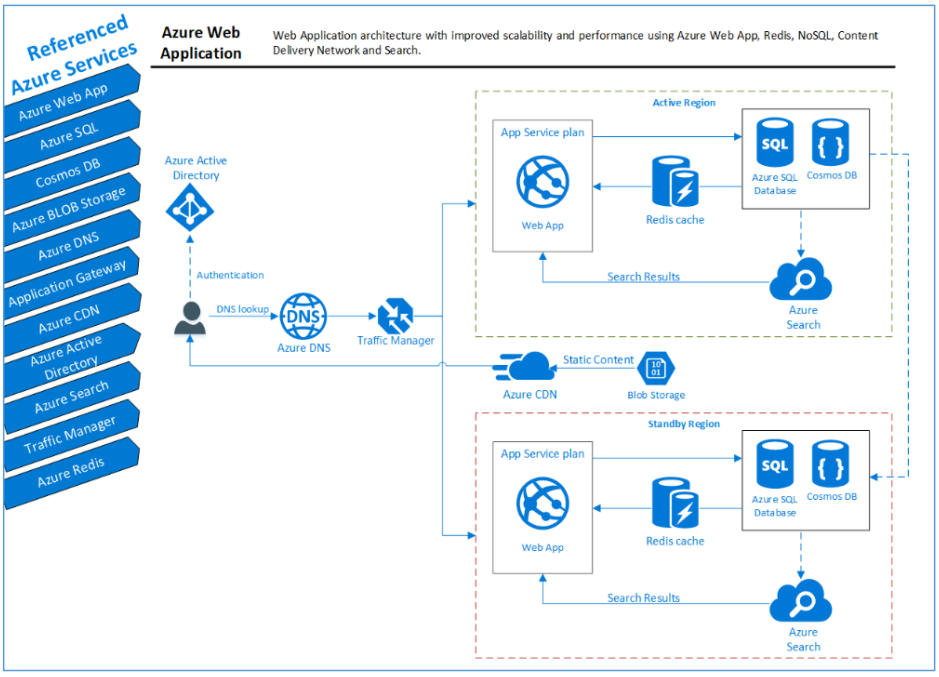
۱-۲- معماری محصول

توضیحات خود را جایگزین این متن نمایید.

[SE] Commented [٤]: ضمن تشریح معماری محصول و توضیح ارتباط‌های بین بخش‌های مختلف، تصویری از این معماری که شامل جریان اطلاعات (Data Flow) است نیز ارائه نمایید

<این نمودار چگونگی انجام رویدادها در یک گردش اطلاعات را نشان می دهد. این نمودارنرم‌افزارها، سخت‌افزارها و زیرسیستم‌ها و مؤلفه هایی که درگیر این گردش اطلاعات می‌شوند را در قالب ماژولها و مؤلفه‌های اصلی، مؤلفه‌های امنیتی، مؤلفه‌های سمت کلاینت (درصورت وجود)، مؤلفه یکپارچگی با سامانه خارجی (در صورت وجود) و اینکه چه اطلاعاتی جابه‌جا می‌شود؟ چه مؤلفه‌هایی این اطلاعات را دریافت می‌کنند؟ چه فرآیندهای عمومی‌ای رخ می‌دهد؟ و ... را در سیستم مشخص می‌کند.>

مثالی از نمای کلی معماری یک برنامه کاربردی تحت شبکه {لطفا این متن و تصویر را با معماری محصول خود جایگزین نمایید.}



۲- الزامات امنیتی

الزامات امنیتی این سند بر اساس نسخه ۱,۱ نمایه[۱] حفاظتی «برنامه‌های کاربردی تحت شبکه» تهیه شده است. ساختار این سند بدین صورت است که برای هر رده در نمایه‌ی حفاظتی مربوطه، یک دسته الزام بیان شده است.

لطفا گزینه‌های جلوی الزام‌ها را نیز انتخاب نمایید.

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[۲] تولید کند (Log ثبت نماید).**			✓	انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است. توجه نمایید که این الزام به تولید ثبت‌نشان (ثبت Log) برای موارد زیر اشاره دارد. عملیات یا رفتار ذکر شده، در الزام‌های دیگری (که روبروی هر گزینه نوشته شده است) بررسی می‌شود.
	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.	☑	شروع و اتمام توابع		این گزینه به شروع و پایان توابع عملکردی محصول به ویژه توابع ممیزی اشاره دارد.
		☑	تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها		این گزینه مربوط به بند ۳ جدول ۲-۱ (ممیزی امنیت (Log) است.
		☑	خواندن اطلاعات از ثبت‌نشان‌ها		این گزینه مربوط به بند ۳ جدول ۲-۱ (ممیزی امنیت (Log) است.
		☑	تمامی تغییرات در پیکربندی ثبت‌نشان‌ها		این گزینه، به تولید ثبت‌نشان برای تغییر در پیکربندی توابع ممیزی اشاره دارد.
		☑	عملیات انجام‌شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه		این گزینه مربوط به بند ۷ جدول ۲-۱ (ممیزی امنیت (Log) است.
		☑	عملیات انجام‌شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها		این گزینه مربوط به بند ۸ جدول ۲-۱ (ممیزی امنیت (Log) است.
		☑	تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.		این گزینه مربوط به بند ۱۱ جدول ۲-۴ (حفاظت از داده‌ی کاربری) است.
		☑	تمام کاربردهای سازوکار احراز هویت		این گزینه مربوط به بندهای ۱، ۲ و ۶ جدول ۲-۳ (شناسایی و احراز هویت) است.

[SECommented [SE۵]: انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است.

تنها در موارد خاصی که به دلایل منطقی، موردی پیاده‌سازی نشده است، حتما در بخش «توضیحات» و مقابل گزینه‌ی مورد نظر، علت آن درج شود.
(برای نمونه، چنانچه مدیر سیستم توانایی خاتمه نشست کاربرها را ندارد، تولید ثبت‌نشان (ثبت Log) برای «خاتمه به نشست غیرفعال توسط مدیر سیستم» امکان‌پذیر نخواهد بود. (با توجه به اجباری نبودن وجود این ویژگی که مدیر بتواند نشست کاربرها را خاتمه دهد، پیاده‌سازی چنین امکانی اختیاری و بسته به شرایط محصول و صلاحدید شرکت توسعه‌دهنده خواهد بود)

[۱] Profile
[۲] Log

	نتایج نهایی عملیات احراز هویت	☑		این گزینه مربوط به بند ۶ جدول ۲-۳ (شناسایی و احراز هویت) است.
	تلاش موفق و ناموفق هر گذرواژه بررسی‌شده توسط محصول	☑		این گزینه مربوط به بند ۴ جدول ۲-۳ (شناسایی و احراز هویت) است.
	شکست و موفقیت انتساب ویژگی‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)	☑		این گزینه مربوط به بند ۷ جدول ۲-۳ (شناسایی و احراز هویت) است.
	تمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی	☑		این گزینه مربوط به بندهای ۷ و ۹ جدول ۲-۳ (شناسایی و احراز هویت) است.
	تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	☑		این گزینه مربوط به بند ۲ جدول ۲-۴ (حفاظت از داده‌ی کاربری) است.
	تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه ویژگی‌های امنیتی)	☑		این گزینه مربوط به بند ۶ جدول ۲-۴ (حفاظت از داده‌ی کاربری) است.
	همه تلاش‌ها برای خارج کردن اطلاعات از محصول	☑		این گزینه مربوط به بند ۸ جدول ۲-۴ (حفاظت از داده‌ی کاربری) است.
	تمامی تغییرات در رفتارهای توابع کارکردی محصول	☑		این گزینه مربوط به بند ۱ جدول ۲-۵ (مدیریت امنیت) است.
	استفاده از کارکردهای مدیریتی	☑		این گزینه مربوط به بند ۴ جدول ۲-۵ (مدیریت امنیت) است.
	تغییرات در گروه کاربران	☑		این گزینه مربوط به بند ۱ جدول ۲-۴ (حفاظت از داده‌ی کاربری) است.
	شکست در کارکردهای امنیتی محصول	☑		این گزینه مربوط به بند ۱ جدول ۲-۶ (حفاظت از توابع امنیتی محصول) است.
	تمامی قابلیت‌هایی از محصول که به دلیل شکست (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند.	☑		این گزینه مربوط به بند ۱ جدول ۲-۷ (تخصیص منابع) است.
	تلاش موفق یا ناموفق برای برقراری نشست.	☑		این گزینه مربوط به بند ۷ جدول ۲-۸ (دسترسی به محصول) و بند ۸ جدول ۲-۳ (شناسایی و احراز هویت) است.
	ایجاد نشدن نشست به دلیل محدودیت نشست‌های همزمان (حداقل)	☑		این گزینه مربوط به بند ۱ جدول ۲-۸ (دسترسی به محصول) است.
	خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست	☑		این گزینه مربوط به بند ۲ جدول ۲-۸ (دسترسی به محصول) است.
	خاتمه به نشست غیرفعال توسط مدیر سیستم	☑		این گزینه مربوط به بند ۲ جدول ۲-۸ (دسترسی به محصول) است.
	سایر موارد	☐		اگر ثبت‌نشان دیگری نیز در محصول تولید می‌شود، در این بخش به آن اشاره نمایید.
۲	**محصول باید برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید.**		✓	انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است.
	تاریخ و زمان رویداد	☑		
	نوع رویداد	☑		

Commented [SE۶]: این گزینه به تولید ثبت‌نشان برای واکنش محصول به محدودیت نشست اشاره دارد.
- اگر محصول جلوی برقراری نشست‌های جدید را می‌گیرد، باید ثبت‌نشان «برقرار نشدن نشست به دلیل محدودیت نشست» تولید شود.
- اگر محصول نشست‌های قبلی را خاتمه می‌دهد، باید ثبت‌نشان «ورود کاربر (جدید)» و «خاتمه به نشست کاربر (قبلی) به دلیل محدودیت تعداد نشست‌ها» را تولید کند.

	ویژگی‌هایی که در ثبت‌نشان‌ها وجود دارد مشخص شود.	هویت ایجادکننده رویداد	☑		
		نتیجه رویداد	☑		ثبت «موفق» یا «ناموفق» کافی است. (البته بسته به محصول ممکن است موارد دیگری جایگزین شوند)
		آدرس IP ایجادکننده رویداد	☑		
		سایر موارد	☐		اگر اطلاعات دیگری نیز در ثبت‌نشان‌ها وجود دارد، در این بخش به آن اشاره کنید.
۳	**محصول باید ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید.**			✓	انتخاب و پیاده‌سازی این الزام اجباری است.
۴	**ثبت‌نشان‌هایی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند.**			✓	انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است.
	مواردی 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	☑		اجباری است.
		نوع حساب کاربری	☐		
		تاریخ/زمان	☑		اجباری است.
		روش اتصال کاربر	☐		
		نوع رخداد	☑		اجباری است.
		مکان رویداد	☐		
		سایر موارد	☐		
۶	**محصول باید هرگونه حذف و تغییر غیرمجاز در ثبت‌نشان‌ها را تشخیص دهد و در صورت امکان جلوگیری نماید.**			✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
		استفاده از درهم‌سازی (Hash) برای تشخیص تغییرات	☐		

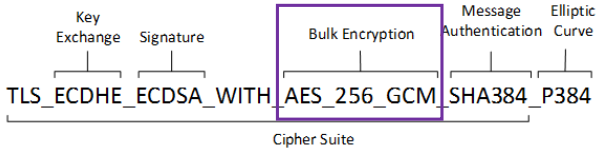
[SE]Commented [V۷]: این الزام توانایی محصول در «مرتب‌سازی» و «انتخاب» (غربال کردن (Filter)) ثبت‌نشان‌ها اشاره دارد.
بدیهی است که این ویژگی باید درون محصول صورت گیرد، نه در پایگاه داده.

	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	☐		
۷	**محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.**			✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری 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.**			✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	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	☐		

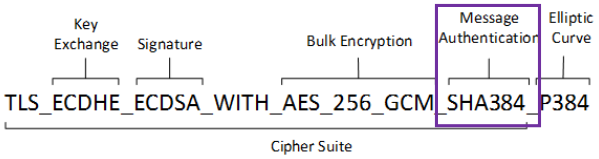
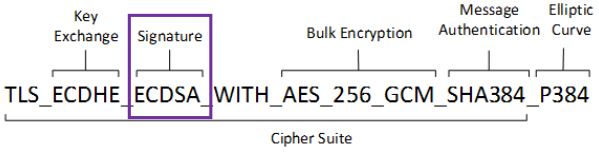
۲-۲- رمزنگاری

[SE ۸Commented]: این جدول، تجمیع تمامی کاربردهای رمزنگاری در محصول است.
برای نمونه:
۱- استفاده از «رمزنگاری» هنگام دریافت فایل از کاربر و ذخیره‌ی آن به صورت رمزشده
۲- استفاده از «درهم‌سازی» برای ذخیره‌ی اطلاعاتی در پایگاه داده (فرضا گذرواژه‌ی کاربرها)
۳- استفاده از «امضای دیجیتال» در بروزرسانی محصول
۴- استفاده از «رمزنگاری»، «درهم‌سازی» و «امضای دیجتال» در پروتکل‌های TLS و SSH

در این رده، توانایی محصول در پیاده‌سازی یا به‌کارگیری واحدهای[۳] رمزنگاری، بررسی می‌گردد. برای حفظ محرمانگی داده، از رمزنگاری استفاده می‌شود و این رمزنگاری‌ها می‌توانند 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 خصوص) صورت می‌گیرد. الگوریتم‌ها می‌توانند با طول کلیدهای مختلف و روش‌های مختلفی (مد عملیاتی) به رمزگذاری و رمزگشایی داده بپردازند که در این رده، توانایی محصول از این جهت مورد بررسی قرار گرفته است. در رده رمزنگاری همچنین الگوریتم‌های درهم‌سازی (Hash) برای برقراری جامعیت داده استفاده می‌گردد.

شماره الزام	رده رمزنگاری				توضیحات
۱	**محصول باید قابلیت رمزنگاری یا واحد رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ISO 18033-3) با توجه به موارد زیر انجام دهد.**			✓	طول کلید(های) مورد استفاده برای هر یک از الگوریتم‌های انتخاب‌شده را در بخش «توضیحات» مشخص نمایید. انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری 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)	☐		
		مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در ISO10116)	☐		

[۳] Modules

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.**			✓ انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است. 
	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)**		☐	
	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)		

[SE Commented ۹]: در الگوریتم TLS، کلید رمزنگاری به کار می‌رود
تولید و تخریب کلید نیز بر عهده‌ی توابع مرتبط است.

[SE Commented ۱۰]: در مجموعه‌های رمز ارائه‌شده در الگوریتم TLS، امضای دیجیتال به کار می‌رود

		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.**			✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	مقدار یا بازه‌ی مورد استفاده در هریک باید مشخص گردد. (وجود یک مورد لازم و کافی است)	یک عدد مثبت ثابت	☐		در صورت انتخاب این گزینه، مقدار این عدد در بخش «توضیحات» مشخص شود.
		یک عدد مثبت قابل تنظیم توسط مدیر	☐		
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.**			✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	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)	☐		در صورت انتخاب این گزینه، مطابق متن آن، سازوکار مورد استفاده در بخش «توضیحات» شرح داده شود.

[SE Commented ۱]: این ویژگی برای تمامی نام‌های کاربری (فارغ از اینکه نام کاربری وارد شده در محصول تعریف‌شده است یا خیر) باید رعایت شود.

[SE Commented ۲]: با توج به اینکه این الزام مکمل بند قبلی است، کماکان واکنش محصول پس از رسیدن تعداد تلاش‌های ناموفق به آستانه‌ی تعریف‌شده باید برای تمامی کاربرها (فارغ از اینکه نام کاربری وارد شده در محصول تعریف‌شده است یا خیر) یکسان باشد.

	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.**		✓	انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است.	
	ویژگی‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.	شناسه کاربر	☑		
		روش احراز هویت مورد استفاده	☑		
		داده احراز هویت	☑		
		وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)	☑		
		نقش کاربر	☑		
		سایر موارد	☐		
۴	**محصول باید قابلیت مدیریت گذرواژه را فراهم آورد.**		✓	انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری 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)	☑	توجه نمایید که طول گذرواژه باید توسط مدیر قابل تغییر باشد و در هیچ شرایطی نباید کمتر از ۸ کاراکتر باشد.	
		سایر موارد	☐		
۵	**محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.**		✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.	
		مشاهده راهنمای نحوه ورود به سیستم	☐		

Commented [SE۱۳]: محصول باید توانایی مدیریت «پیچیدگی گذرواژه» را برای کاربر مجاز فراهم کند. ایجاد امکان انتخاب «اجباری بودن» وجود هر گزینه در گذرواژه راهکار بسیار مناسبی است، اما وجود گزینه‌ای که با انتخاب آن تمامی موارد اجباری شوند نیز مناسب است. در شرایط خاص، اگر امکان مدیریت «پیچیدگی گذرواژه» برای کاربر فراهم نمی‌شود، باید به صورت پیش‌فرض تمامی موارد در تعیین گذرواژه اجباری باشند.

	اقدامات عمومی که کاربر می‌تواند قبل از احراز هویت انجام دهد، انتخاب شود.	بازیابی گذرواژه	☐		
		هیچ اقدامی	☐		
		سایر موارد	☐		
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	☑		اجباری است.
		امضای دیجیتال	☐		
		سامانه‌های احراز هویت مرکزی (مانند Active Directory و ...)	☐		در صورت انتخاب این گزینه، سامانه‌ی مورد نظر در بخش «توضیحات» مشخص شود.
		OTP یا توکن	☐		در صورت انتخاب این گزینه، در بخش «توضیحات»، توضیح داده شود.
		احراز هویت دو فاکتوری	☐		در صورت انتخاب این گزینه، در بخش «توضیحات»، توضیح داده شود.
		سایر موارد	☐		
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 در «سایر موارد» بیان می‌شوند).	شناسه کاربر	☑		اجباری است.
		نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمتهای مختلف برنامه	☑		اجباری است.
		جزئیات واسط کلاینت	☐		
		پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)	☑		اجباری است.
		سایر موارد	☐		

Commented [SE۱٤]: با توجه به متن الزام، پیاده‌سازی بیش از یک راهکار احراز هویت برای دسترسی راه دور الزامی است.

۸	**محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.**		✓	انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است.
	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.)	☑	
		بروزرسانی اطلاعات پیشینه احراز هویت	☑	
		سایر موارد	☐	
۹	**محصول باید بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید.**		✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	قوانینی که در صورت تغییر ویژگی‌های امنیتی کاربر فعال، اعمال می‌شود، مشخص گردد.	غیرمجاز بودن هرگونه تغییر در طول نشست فعال	☑	
		سایر موارد	☐	

[SE Commented [ا٥]: در مواردی که محصول به دلیل رسیدن به محدودیت تعداد نشست‌های موازی، از برقراری نشست جدید جلوگیری می‌کند نیز این گزینه برآورده می‌شود.

[SE Commented [ا٦]: «ویژگی‌های امنیتی کاربر فعال» که در طول نشست کاربر نمی‌توانند تغییر کنند و نیازمند ورود مجدد کاربر هستند، همان گزینه‌های انتخاب‌شده در بند ۷ جدول ۲-۳ (شناسایی و احراز هویت) هستند.

۲-۴- 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.**			✓	انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است.
	موجودیت‌های فعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می شوند، مشخص گردد.	مدیر سیستم	☑		
		کاربر عادی	☑		
		سایر موارد	☐		
	موجودیت‌های غیرفعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می شوند، مشخص گردد.	سوابق، مستندات و فراداده	☑		
		داده متعلق به کاربران	☑		
		داده احراز هویت	☑		
		سایر موارد	☐		
	عملیاتی که خط‌مشی های کنترل دسترسی در رابطه با آنها اعمال	ایجاد موجودیت غیرفعال جدید	☑		
		حذف موجودیت غیرفعال	☑		
		تغییر دسترسی‌ها به موجودیت غیرفعال	☑		
		عملیات بر روی فراداده وابسته به موجودیت غیرفعال	☑		

[SE]Commented [۱۷]: تعریف «موجودیت فعال» و «موجودیت غیرفعال» بر اساس «پروفایل حفاظتی» افتا به شرح زیر است:

موجودیت فعال (Subject): موجودیت فعال، موجودیتی در محصول است که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون سرپرست، کاربر نهایی و غیره؛ به عبارت دیگر موجودیت فعال عامل انجام عملی بر روی محصول است.

موجودیت غیرفعال (Object): موجودیت غیرفعال، موجودیتی در سیستم مورد ارزیابی (محصول) است که شامل اطلاعات است و یا اطلاعات را دریافت می‌نماید و روی آن توسط موجودیت‌های فعال، عملیاتی انجام می‌گیرد. همانند داده‌ها و اطلاعاتی همچون متن‌های رمزشده و کلیدها و غیره؛ به عبارت دیگر موجودیتی است که توسط موجودیت فعال بر روی آن رخدادی اتفاق می‌افتد، مانند لیست کردن رکوردها توسط سرپرست، حذف فایل‌ها توسط حمله‌کننده که در این دو مثال رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.

[SE]Commented [۱۸]: تعریف «موجودیت داده کاربر» بر اساس «پروفایل حفاظتی» افتا به شرح زیر است:

داده کاربر (User Data): به داده‌ای گفته می‌شود که توسط کاربر ایجاد شده یا کاربر مالک آن است. فایل‌هایی که کاربر ایجاد می‌کند، محتویاتی که داخل قسمتی از برنامه یا فایلی وارد می‌کند، عکس، ویدیو، نامه و ... مثال‌هایی از داده کاربر است. همچنین این داده‌ها می‌تواند شامل مستندات تولیدشده با استفاده از برنامه کاربردی مانند: Microsoft Office، نامه‌های ارجاع کار و پاسخ الکترونیکی و اسکن تصویر باشد.

	می‌شوند، مشخص گردد.	سایر موارد	☐		
۲	**محصول باید بر اساس ویژگی‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.**			✓	انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است.
	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.)**			✓	انتخاب و پیاده‌سازی این الزام اجباری است.
۴	**محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.**			✓	انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است.
	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	☑		
		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.**			✓	لطفا نحوه‌ی تضمین امنیت اطلاعات هنگام «تخصیص یا آزادسازی منابع» را در بخش «توضیحات» ذکر نمایید.
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.**			✓	لطفا شرایط محدودکننده برای هر یک از گزینه‌ها را در بخش «توضیحات» مشخص نمایید. (برای نمونه، برای گزینه‌ی «نوع داده»، پسوندهای مجاز قابل قبول مثل pdf، doc، docx در مشخص نمایید.)

	ویژگی‌های امنیتی مرتبط با داده کاربری که در هنگام ورود آن به محصول استفاده می شوند، مشخص شود (در صورتی که کنترل دسترسی برای موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد» بیان گردد).	نوع داده	☐		
		حجم و اندازه	☐		
		فرمت	☐		
		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 گم شدن داده حین انتقال جلوگیری می‌کند.**			✓	لطفا پروتکل مورد استفاده را در بخش «توضیحات» مشخص نمایید.
۸	**محصول باید هنگام انتقال داده به بیرون از محصول، خط‌مشی کنترل دسترسی را اعمال نماید و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.**			✓	لطفا شرایط محدودکننده برای هر یک از گزینه‌ها را در بخش «توضیحات» مشخص نمایید. (برای نمونه، برای گزینه‌ی «نوع داده»، پسوندهای مجاز قابل قبول مثل pdf، doc، docx در مشخص نمایید.)
	ویژگی‌های امنیتی مرتبط با داده کاربری که در هنگام خروج آن از محصول استفاده می شوند، مشخص شوند	نوع داده	☐		
		حجم و اندازه	☐		
		فرمت	☐		
		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.	☑		اجباری است.
		سایر موارد	☐		
۱۰	**محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره‌شده در محصول تشخیص دهد.**			✓	ویژگی‌های داده کاربری می‌تواند انواع فایل‌ها، اندازه فایل و محتوای فایل باشد. محصول به منظور شناسایی خطای صحت داده‌ها، باید ویژگی‌های داده‌های کاربری را پایش (Monitor) کند تا در صورت تغییر و یا حذف، هشدار دهد.
	چگونگی تشخیص تغییر در داده‌های کاربری حساس، مشخص شود.	مقدار درهم‌سازی‌شده داده‌های کاربری ذخیره‌شده، نگهداری می‌شود.	☐		می‌توان برای تشخیص صحت داده‌ها از روش‌هایی همچون HMAC و یا ECC Checksum و دیگر روش‌های درهم‌سازی استفاده نمود.
		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	☐		

[SE Commented ۱۹]: توجه شود که این الزام به «داده‌ی ذخیره‌شده» اشاره دارد و نه «داده‌ی ورودی». (البته لازم به ذکر است که نیاز این الزام، چیزی از اهمیت بررسی داده‌های ورودی و اطمینان از صحت آن‌ها (Improper input validation یا Input Validation) کم نمی‌کند و رعایت این موارد الزامی است.)

[SE Commented ۲۰]: این الزام مکمل بند قبلی است.
در بند قبلی، «روش تشخیص و تا حد امکان جلوگیری از تغییر غیرمجاز» بررسی می‌شود.
در این الزام، «واکنش محصول به تشخیص خطای صحت» بررسی می‌شود.

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.**			✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	فعالیت های 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.**			✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	عملیات بر روی ویژگی های 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.**			✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
		تغییر پیش‌فرض	☐		

[SE Commented [۲۱]: این الزام به وجود «سطح دسترسی» اشاره ندارد، بلکه به «فعالیت‌های مدیریتی قابل انجام» روی توابع محصول (برای کاربرهای مجاز) اشاره دارد.

[SE Commented [۲۲]: این الزام به وجود «سطح دسترسی» اشاره ندارد، بلکه به «عملیات قابل انجام» روی گزینه‌های انتخاب شده در بند ۷ جدول ۲-۳ (شناسایی و احراز هویت) (برای کاربرهای مجاز) اشاره دارد.

[SE Commented [۲۳]: این الزام به وجود «سطح دسترسی» اشاره ندارد، بلکه به «عملیات قابل انجام» روی داده‌های محصول (برای کاربرهای مجاز) اشاره دارد.

	عملیات بر روی داده‌های محصول که در محصول پشتیبانی می‌شوند، مشخص شود.	حذف نمودن	☐		
		پرس‌وجو	☐		
		مقداردهی	☐		
		ایجاد	☐		
		مشاهده	☐		
		سایر موارد	☐		
۴	**محصول باید توانایی انجام کارکردهای زیر را داشته باشد.**			✓	انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است. توجه نمایید که این الزام به توانایی‌های مدیریتی برای موارد زیر اشاره دارد. عملیات یا رفتار ذکر شده، در الزام‌های دیگری (که در زیر نوشته شده است) بررسی می‌شود.
	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	☑		این گزینه مربوط به بند ۱ جدول ۲-۴ (حفاظت از داده‌ی کاربری) است.
		پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشان‌ها	☑		این گزینه مربوط به بند ۳ جدول ۲-۱ (ممیزی امنیت (Log) است.
		پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشان‌ها	☑		این گزینه مربوط به بندهای ۷ و ۸ جدول ۲-۱ (ممیزی امنیت (Log) است.
		مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول	☑		این گزینه مربوط به بند ۲ جدول ۲-۴ (حفاظت از داده کاربری) است.
		انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده که می‌تواند در محصول قابل پیکربندی باشد. (برای مثال، زمان تخصیص و یا زمان آزادسازی منابع)	☑		این گزینه مربوط به بند ۵ جدول ۲-۴ (حفاظت از داده کاربری) است.
		ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول	☑		این گزینه مربوط به بند ۶ جدول ۲-۴ (حفاظت از داده‌ی کاربری) است.
		در نظر گرفتن یک عملیات از پیش تعیین‌شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد.	☑		این گزینه مربوط به بند ۱۱ جدول ۲-۴ (حفاظت از داده‌ی کاربری) است.
		۱. مدیریت حد آستانه برای تلاش‌های ناموفق ۲. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد.	☑		این گزینه مربوط به بندهای ۱ و ۲ جدول ۲-۳ (شناسایی و احراز هویت) است.
		مدیریت معیارها برای تنظیم گذرواژه‌ها	☑		این گزینه مربوط به بند ۴ جدول ۲-۳ (شناسایی و احراز هویت) است.
		۱. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه	☑		این گزینه مربوط به بند ۵ جدول ۲-۳ (شناسایی و احراز هویت) است.

[SE ٢٤Commented]: انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است.

تنها در موارد خاصی که به دلایل منطقی، موردی پیاده‌سازی نشده است، حتما در بخش «توضیحات» و مقابل گزینه‌ی مورد نظر، علت آن درج شود.

		۲. مدیریت یک‌سری عملیاتی که قبل از احراز شدن هویت کاربر انجام می شوند.		
		۱. مدیریت سازوکارهای احراز هویت ۲. مدیریت قوانین مرتبط با احراز هویت	☑	این گزینه مربوط به بند ۶ جدول ۲-۳ (شناسایی و احراز هویت) است.
		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.	☑	این گزینه مربوط به بند ۷ جدول ۲-۸ (دسترسی به محصول) است.
		مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.	☑	این گزینه مربوط به بند ۷ جدول ۲-۳ (شناسایی و احراز هویت) است.
		مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول	☑	این گزینه مربوط به بند ۱ جدول ۲-۴ (حفاظت از داده‌ی کاربری) است.
		مدیریت نقش‌ها در محصول	☑	این گزینه مربوط به بند ۲ جدول ۲-۵ (مدیریت امنیت) است.
		مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر	☑	این گزینه مربوط به بند ۱ جدول ۲-۸ (دسترسی به محصول) است.
		مدیریت شرایط آغاز نشست توسط مدیر مجاز	☑	این گزینه مربوط به بند ۷ جدول ۲-۸ (دسترسی به محصول) است.
		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.	☑	این گزینه مربوط به بندهای ۲ و ۳ جدول ۲-۸ (دسترسی به محصول) است.
۵	**محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد.**		✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	نقش‌هایی که در محصول پشتیبانی می شوند، مشخص گردد.	مدیر سیستم	☐	
		کاربر پیشرفته	☐	
		کاربر عادی	☐	
		سایر موارد	☐	

[SE Commented [ه٥]: داشتن «نقش» در محصول اجباری نیست و دسترسی کاربرها به بخش‌های مختلف می‌تواند به صورت مستقیم به آن‌ها تخصیص یابد. (در چنین شرایطی این الزام و الزام بعدی برآورده می‌شوند)
همچنین محدودیتی در داشتن «نقش» و امکان تعیین دسترسی‌هایی مجزا از نقش کاربر نیز وجود ندارد.

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.**	✓	انتخاب و پیاده‌سازی این الزام اجباری است.

[SE Commented [٦]: هدف اصلی این الزام تبیین صحیح دسترسی‌های کاربر است. یعنی بتوان به درستی تعیین نمود که آیا کاربر اجازه‌ی دسترسی به بخشی را دارد یا خیر.
در شرایط خاصی محصول نیاز دارد تا نقش‌های مختلفی را به کاربر اختصاص دهد، لازم است در بخش «توضیحات» نحوه‌ی اختصاص دسترسی‌ها را شرح دهد.
برای نمونه در شرایطی که نقشی امکان دسترسی به یک بخش را دارد و نقش دیگر امکان دسترسی به آن بخش را ندارد، وضعیت دسترسی کاربری که این دو نقش را دارد به آن بخش چگونه است؟ (به عبارتی، دسترسی‌ها به صورت اشتراک دسترسی‌های نقش‌ها است یا اجتماع آن‌ها)

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.**		✓	انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است.
	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول حفظ می‌شود، مشخص گردد.	خرابی‌های نرم‌افزاری	☑	
		خرابی‌های سخت‌افزاری	☑	
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.**		✓	انتخاب و پیاده‌سازی این الزام اجباری است.
۳	**در صورتی که محصول از محصولات امن IT دیگری 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	☐	
		کلید	☐	
		امضای دیجیتال	☐	
		ثبت‌نشان‌ها (داده‌های ممیزی)	☐	
		سایر موارد	☐	

[SE Commented [۲۷]: در صورت بروز مشکل یا خطا در محصول، نباید سطوح دسترسی از کار بیفتد و امنیت داده‌های کاربری به خطر بیفتد.
همچنین نباید کد محصول (و محل بروز خطا) به کاربر نمایش داده شود.

[SE Commented [۲۸]: در صورتی که بخش‌های مختلف محصول روی ماشین‌های جداگانه قرار دارند، برقراری ارتباط امن، غیرقابل شنود و افشاء الزامی است.
در شرایطی که تمامی بخش‌های محصول روی یک ماشین قرار دارند، نیاز این الزام برآورده می‌شود.

۴	**محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی[۴] معتبر را تولید یا از آن‌ها استفاده نماید.**			✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	روش‌های ایجاد مهرهای زمانی معتبر انتخاب شود. (دیگر رو شهای موجود در محصول، در قسمت «سایر موارد» بیان شود).	گرفتن مهرهای زمانی از سرور NTP	☐		اگر امکان تعیین سرور NTP از داخل محصول وجود دارد، این گزینه را انتخاب نمایید.
		تنظیم مهرهای زمانی از طریق اینترنت	☐		
		تنظیم مهرهای زمانی به صورت پیش‌فرض (معتبر و عدم امکان دستکاری غیرمجاز)	☐		اگر محصول زمان را از سیستم‌عاملی که روی آن نصب شده است دریافت می‌کند، این گزینه را انتخاب نمایید.
		سایر موارد	☐		
۵	**محصول باید امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید.**			✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	روش بروزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).	بروزرسانی دستی	☐		در صورتی که فایل‌های بروزرسانی باید به صورت دستی روی سرور قرار گیرند (معمولا توسط شرکت توسعه‌دهنده) یا نسخه‌ی جدید باید به صورت دستی اجرا و نصب شود، این گزینه را انتخاب نمایید.
		جستجوی خودکار بروزرسانی‌ها	☐		در صورتی که محصول توانایی جستجوی خودکار برای وجود بروزرسانی را دارد و وجود نسخه‌ی جدید را به نحوی به اطلاع مدیر می‌رساند تا مدیر اقدام به بروزرسانی نماید، این گزینه را انتخاب نمایید.
		بروزرسانی‌های خودکار	☐		در صورتی که علاوه بر جستجو برای وجود بروزرسانی، نصب آن نیز بر عهده‌ی محصول است، این گزینه را انتخاب نمایید. (انتخاب این گزینه نیازمند تکمیل الزام بعدی است)
		بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی	☐		در صورتی که محصول فایل‌های بروزرسانی را از کاربر دریافت می‌کند و پیش از نصب یا اعمال آن‌ها، به کمک روش‌های اصالت‌سنجی، از اصلات و یکپارچگی فایل بروزرسانی اطمینان حاصل می‌کند، این گزینه را انتخاب نمایید. (در صورت انتخاب این گزینه، در بخش «توضیحات»، نحوه‌ی اصالت‌سنجی را شرح دهید.)

[۴] Time stamp

					در صورت انتخاب این گزینه، لازم است در بند ۳ جدول ۳-۵ (اعتبارسنجی گواهی‌نامه)، گزینه‌ی «امضای کد برای تأیید یکپارچگی» نیز انتخاب شود.
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.**		☐		در صورت انتخاب گزینه‌ی «بروزرسانی خودکار» در بند قبلی، این الزام اجباری خواهد شد. در غیر این‌صورت نیازی به تکمیل آن نیست.
	سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی) به‌روزرسانی‌ها انتخاب گردد.	امضای دیجیتال	☐		در صورت انتخاب این گزینه، لازم است در بند ۳ جدول ۳-۵ (اعتبارسنجی گواهی‌نامه)، گزینه‌ی «امضای کد برای بروزرسانی‌های نرم‌افزار سیستم» نیز انتخاب شود.
		درهم‌ساز منتشرشده	☐		

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.	✓	انتخاب و پیاده‌سازی این الزام اجباری است.

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.**		✓	انتخاب و پیاده‌سازی این الزام اجباری است.
۲	**محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمانی که غیرفعال هستند (و می بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.**		✓	انتخاب و پیاده‌سازی این الزام اجباری است.
۳	**محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.**		✓	انتخاب و پیاده‌سازی این الزام اجباری است.
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 این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	انتخاب یک مورد لازم و کافی است.	☐ روز		
		☐ زمان		
		☐ سایر موارد		
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 این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	انتخاب یک مورد لازم و کافی است.	☐ روز		
		☐ زمان		
		☐ سایر موارد		

[SE۲۹Commented]: تعداد نشست‌های موازی، فعال یا غیرفعال بودن این ویژگی و نیز واکنش محصول پس از رسیدن به تعداد نشست‌های موازی می‌تواند در اختبار مدیر سیستم قرار گیرد.

[SE۳۰Commented]: زمان مجاز نشست‌های غیرفعال، باید توسط مدیر قابل پیکربندی باشد.

۶	**محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.**		✓	انتخاب و پیاده‌سازی این الزام اجباری است.
۷	**محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.**		✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	پارامترهای موجود برای جلوگیری از نشست، مشخص شوند (وجود یک مورد لازم و کافی است).	☐ مکان		در صورت توانایی ایجاد محدودیت بر اساس IP، این گزینه را انتخاب نمایید.
		☐ شماره پورت		
		☐ روز		
		☐ زمان		
		☐ سایر موارد		

Commented [SE۳۱]: این الزام به «حذف لاگ‌ها» اشاره ندارد. بلکه این الزام مکمل دو الزام قبلی (بندهای ۴ و ۵ جدول ۲-۸ (دسترسی به محصول)) است. در الزام‌های قبلی به نمایش «سوابق دسترسی» کاربر اشاره دارد و در این الزام اشاره شده است که این نمایش سوابق به صورت گذرا نباشد و کاربر آگاهانه آن را رد نماید. به بیان دیگر، از دیده‌شدن «سوابق دسترسی» توسط کاربر اطمینان حاصل شود.
نمایش این اطلاعات به صورت ثابت (در بخش مشخصی) نیز، نیاز این الزام را برآورده می‌کند.

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 ۳-۱- و ۳-۳- و در صورت انتخاب TLS، رعایت الزامات ۳-۲- تا ۳-۴- که در بخش ۳- بیان گردیده است، الزامی است.			✓	انتخاب این الزام و انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
		پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.	HTTPS	☐	در صورت انتخاب این گزینه، پیاده‌سازی جدول ۳-۱ (پروتکل HTTPS) و جدول ۳-۳ (پروتکل TLS Server) اجباری خواهد بود.
			TLS	☐	در صورت انتخاب این گزینه، پیاده‌سازی جدول ۳-۳ (پروتکل TLS Server) و بسته به شرایط محصول، پیاده‌سازی جدول‌های ۳-۲ (پروتکل TLS Client) و ۳-۴ (پروتکل TLS مشترک کلاینت و سرور) اجباری خواهند بود.
			SSH	☐	در صورت انتخاب این گزینه، پیاده‌سازی جدول ۳-۶ (پروتکل SSH) اجباری خواهد بود.
۲	**محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.**			✓	انتخاب و پیاده‌سازی این الزام اجباری است.
۳	**محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.**			✓	انتخاب و پیاده‌سازی این الزام اجباری است.

Commented [SE۳۲]: این گزینه، به استفاده از پروتکل HTTP بر بستر TLS اشاره دارد.

Commented [SE۳۳]: این گزینه به سایر کاربردهای پروتکل TLS اشاره دارد.

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

[SE Commented [۳۴]: در صورت انتخاب گزینه‌ی «HTTPS» در بند ۱ جدول ۲-۹ (کانال‌ها/مسیرهای امن)، انتخاب و پیاده‌سازی تمامی الزام‌های این جدول اجباری خواهند بود.]

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 ۳-۵- انجام می‌شود که در این صورت الزامات بخش ۳-۵- الزامی است.		☐	
	محصول تنها از موارد بیان‌شده می‌تواند استفاده نماید.	اتصال را برقرار نکند.	☐	
		برای برقراری اتصال درخواست مجوز کند.	☐	

[SE Commented [۳۵]: این الزام تضمین می‌کند که پروتکل HTTPS، با استفاده از SSL پیاده‌سازی نشود و تنها از TLS برای پیاده‌سازی آن استفاده شود.]

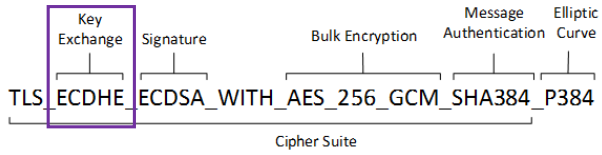
۳-۲- پروتکل TLS Client

[SE Commented [۳۶]: در صورتی که محصول با محصول دیگری به عنوان کلاینت پروتکل TLS در ارتباط است، پیاده‌سازی این جدول اجباری خواهد بود.
ارتباط با سرور میل یا پنل پیامکی نیز باید با استفاده از این پروتکل امن‌سازی شوند.

[SE Commented [۳۷]: مجموعه‌های رمز مورد استفاده در پروتکل TLS در نقش کلاینت را انتخاب نمایید. (در انتخاب مجموعه‌های رمز به موارد نوشته شده در بخش «توضیحات» توجه نمایید.)
منعی برای استفاده از TLS1.3 وجود ندارد و توصیه نیز می‌شود.

شماره الزام	پروتکل TLS Client			توضیحات
۱	**محصول باید (RFC 5246) TLS 1.2 را پیاده‌سازی و دیگر نسخه‌های TLS و SSL را رد کند.** **همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.**		☐	آسیب‌پذیری‌های رایج مرتبط با مجموعه‌های رمز: - LOGJAM (CVE-2015-4000): استفاده از مجموعه‌های رمز شامل DHE با طول کلید کمتر از ۱۰۲۴ - POODLE (CVE-2014-3566): استفاده از SSL2.0 به همراه مجموعه‌های رمز دارای CBC - BEAST (CVE-2011-3389): استفاده از TLS1.0 به همراه مجموعه‌های رمز شامل CBC - CRIME (CVE-2012-4929): پشتیبانی از فشرده‌سازی در TLS1.2 و قبل آن - BREACH (CVE-2013-3587): استفاده از فشرده‌سازی HTTP (معمولا gzip) {بهترین راه حذف gzip است.} - SWEET32 (CVE-2016-2183 و CVE-2016-6329): استفادهاز مجموعه‌های رمز شامل الگوریتم‌های رمزنگاری ضعیف مانند DES و 3DES - LUCKY13 (CVE-2013-0169): استفاده از مجموعه‌های رمز شامل CBC - RC4 (CVE-2013-2566 و CVE-2015-2808): استفاده از مجموعه‌های رمز شامل RC4 با ارائه‌ی TLS1.2 و TLS1.3 و نیز پشتیبانی از مجموعه‌های رمز شامل GCM اغلب این آسیب‌پذیری‌ها برطرف می‌شود.
	مجموعه رمز مورد استفاده و پیاده سازی‌شـــده 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	☐		
		برای برقراری ارتباط درخواست مجوز کند	☐		
		سایر موارد	☐		
۴	**محصول باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید.**			☐	
	در صورتی که محصول از خم‌های بیضوی استفاده می نماید، نوع خم 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.	☐		در صورت انتخاب این گزینه، خم‌های مورد استفاده را در بخش «توضیحات» مشخص نمایید.

Commented [SE۳۸]: در صورت انتخاب مجموعه‌های رمز دارای الگوریتم ECDH یا ECDHE، انتخاب این گزینه اجباری خواهد بود.

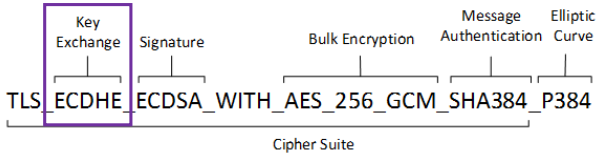
۳-۳- پروتکل TLS Server

[SE Commented [۳۹]: در صورتی که محصول به عنوان سرور TLS عمل می‌کند پیاده‌سازی این جدول الزامی است. (با توجه به اجباری بودن دسترسی امن به محصول، محصول‌هایی تحت‌وب و نرم‌افزارهای ویندوزی برای ارتباط با سرور باید از پروتکل TLS (یا HTTPS) استفاده کنند. بنابراین پیاده‌سازی این جدول اجباری خواهد بود)

[SE Commented [٤٠]: مجموعه‌های رمز مورد استفاده در پروتکل TLS در نقش سرور را انتخاب نمایید. (در انتخاب مجموعه‌های رمز به موارد نوشته شده در بخش «توضیحات» توجه نمایید.) منعی برای استفاده از TLS1.3 وجود ندارد و توصیه نیز می‌شود.

شماره الزام	پروتکل TLS Server			توضیحات
۱	**محصول باید (RFC 5246) TLS 1.2 را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.**		✓	آسیب‌پذیری‌های رایج مرتبط با مجموعه‌های رمز: - LOGJAM (CVE-2015-4000): استفاده از مجموعه‌های رمز شامل DHE با طول کلید کمتر از ۱۰۲۴ - POODLE (CVE-2014-3566): استفاده از SSL2.0 به همراه مجموعه‌های رمز دارای CBC - BEAST (CVE-2011-3389): استفاده از TLS1.0 به همراه مجموعه‌های رمز شامل CBC - CRIME (CVE-2012-4929): پشتیبانی از فشرده‌سازی در TLS1.2 و قبل آن - BREACH (CVE-2013-3587): استفاده از فشرده‌سازی HTTP (معمولا gzip) {بهترین راه حذف gzip است.} - SWEET32 (CVE-2016-2183 و CVE-2016-6329): استفادهاز مجموعه‌های رمز شامل الگوریتم‌های رمزنگاری ضعیف مانند DES و 3DES - LUCKY13 (CVE-2013-0169): استفاده از مجموعه‌های رمز شامل CBC - RC4 (CVE-2013-2566 و CVE-2015-2808): استفاده از مجموعه‌های رمز شامل RC4 با ارائه‌ی TLS1.2 و TLS1.3 و نیز پشتیبانی از مجموعه‌های رمز شامل GCM اغلب این آسیب‌پذیری‌ها برطرف می‌شود.
	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			

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.**		✓	برای هر یک از گزینه‌های زیر، طول کلید یا خم مورد استفاده را در بخش «توضیحات» مشخص نمایید. 
	طولی کلید یا نوع خم مورد استفاده باید مشخص گردد.	☐ استفاده از RSA با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ یا ۴۰۹۶ بیت		(طول کلید)
		☐ پارامترهای ECDH با استفاده از NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگر		(خم مورد استفاده)
		☐ پارامترهای دیفی-هلمن با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ بیت		(طول کلید)

[SE Commented [٤١]: این الزام متناسب با بند ۱ این جدول است.

[SE Commented [٤٢]: در صورت انتخاب مجموعه‌های رمز شامل RSA

[SE Commented [٤٣]: در صورت انتخاب مجموعه‌های رمز شامل ECDH یا ECDHE

[SE Commented [٤٤]: در صورت انتخاب مجموعه‌های رمز شامل DH یا DHE

۳-۴- 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.**	☐	(اگر محصول، کلاینت‌ها را با استفاده از گواهی‌نامه احراز هویت می‌کند)

۳-۵- اعتبارسنجی گواهی‌نامه

شماره الزام	اعتبارسنجی گواهی‌نامه				توضیحات
۱	**محصول باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند.**			✓	انتخاب و پیاده‌سازی این الزام اجباری است.
		تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.	☑		
		مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.	☑		
		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.	☐		(اگر در بند ۵ جدول ۲-۶ (حفاظت از توابع امنیتی محصول)، گزینه‌ی «بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی» انتخاب شده باشد یا در این الزام گزینه‌ی «بروزرسانی خودکار» و در بند ۶ جدول ۲-۶ (حفاظت از توابع امنیتی محصول)، گزینه‌ی «امضای دیجیتال» انتخاب شده باشد.)
		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.	☐		(اگر محصول در پروتکل TLS به عنوان سرور مشارکت دارد.)

		☐	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.		(اگر محصول در پروتکل TLS به عنوان کلاینت مشارکت دارد.)
		☐	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.		(اگر در بخش «روش‌های تأیید وضعیت فسخ گواهی‌نامه»، گزینه‌ی «OCSP» انتخاب شده باشد.)
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.**	✓	انتخاب و پیاده‌سازی این الزام اجباری است.
۳			**محصول باید برای پشتیبانی از احراز هویت برای موارد زیر، از گواهی‌نامه‌های X509v3 تعریف‌شده در RFC 5280 استفاده کند.**	✓	انتخاب و پیاده‌سازی این الزام اجباری است.
	در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.	☐	HTTPS		(اگر ارتباط‌های محصول با استفاده از پروتکل HTTPS انجام می‌شود)
		☐	TLS		(اگر ارتباط‌های محصول با استفاده از پروتکل TLS انجام می‌شود)
		☐	SSH		(اگر ارتباط‌های محصول با استفاده از پروتکل SSH انجام می‌شود)
		☐	امضای کد برای بروزرسانی‌های نرم‌افزار سیستم		(اگر در بند ۵ جدول ۲-۶ (حفاظت از توابع امنیتی محصول)، گزینه‌ی «بروزرسانی خودکار» و در بند ۶ جدول ۲-۶ (حفاظت از توابع امنیتی محصول)، گزینه‌ی «امضای دیجیتال» انتخاب شده باشد.)
		☐	امضای کد برای تأیید یکپارچگی		(اگر در بند ۵ جدول ۲-۶ (حفاظت از توابع امنیتی محصول)، گزینه‌ی «بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی» انتخاب شده باشد.)
		☐	سایر موارد		

Commented [SE۵۰]: کاربردهای گواهی‌نامه‌ی X509v3 را در محصول مشخص نمایید.

۳-۶- پروتکل SSH

[SE] Commented [٤٦]: در صورت استفاده از پروتکل SSH (حتا برای پیکربندی‌های محصول) پیاده‌سازی این جدول اجباری خواهد بود.
(**راهنمایی:** در صورت استفاده از ابزار OpenSSH، توجه شود که حتما هر دو فایل پیکربندی مربوط به کلاینت و سرور (sshd.comf و ssh.conf) اصلاح شوند.)

شماره الزام	پروتکل SSH		توضیحات
۱	**محصول باید پروتکل SSH را مطابق با RFCهای ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۵۶۵۶ و ۶۶۶۸ پیاده‌سازی نماید.**	✓	(**راهنمایی:** در صورت استفاده از ابزار OpenSSH، این ابزار مطابق با RFCهای ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۴۲۵۶، ۵۶۵۶، ۶۶۶۸، ۸۳۰۸ و ۸۳۳۲ پیاده‌سازی شده است.)
۲	**محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4252، از روش‌های احراز هویت زیر پشتیبانی نماید.**	✓	در صورت پشتیبانی از SSH، انتخاب و پیاده‌سازی تمامی گزینه‌های این الزام اجباری است.
	☑ 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.**	✓	لطفا بیشینه‌ی حجم بسته‌ی مجاز در تبادل SSH را در بخش «توضیحات» مشخص نمایید. (**راهنمایی:** در صورت استفاده از ابزار OpenSSH، بیشینه‌ی حجم بسته در این ابزار به صورت پیش‌فرض 256KB است.)
۴	**محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های رمزنگاری زیر استفاده نماید.**	✓	در صورت پشتیبانی از SSH، انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	☐ 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.**		✓	در صورت پشتیبانی از SSH، انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	☐	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.**		✓	در صورت پشتیبانی از SSH، انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	☐	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.**		✓	در صورت پشتیبانی از SSH، انتخاب و پیاده‌سازی دست‌کم یک مورد اجباری است.
	☐	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.**		✓	در صورت پشتیبانی از SSH، انتخاب و پیاده‌سازی این الزام اجباری است. (**راهنمایی:** در ابزار OpenSSH، این ویژگی به صورت پیش‌فرض پشتیبانی می‌شود)
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 ۷,۱) همراه می‌کند، استفاده می‌نماید.**		✓	در صورت پشتیبانی از SSH، انتخاب و پیاده‌سازی این الزام اجباری است. (**راهنمایی:** در ابزار OpenSSH، این ویژگی به صورت پیش‌فرض پشتیبانی می‌شود)