

به نام خدا

# سند هدف امنیتی محصول

ایده ورزان سیستم

بسته مدیریت پروژه ایده ورزان (IPMP)

۱.۸.۵.۰



۱۴۰۰ ۰۷

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

۳	فهرست
۱- مقدمه	Error! Bookmark not defined.
۲- الزامات امنیتی	۶
۲-۱- ممیزی امنیت (لاگ)	۶
۲-۲- رمزنگاری	۱۰
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	۲۳
۲-۷- تخصیص منابع	۲۵
۲-۸- دسترسی به محصول	۲۶
۲-۹- کانال‌ها/مسیرهای مورد اعتماد	۲۸
۳- الزامات امنیتی مبتنی بر انتخاب	۲۹
۳-۱- پروتکل HTTPS	۲۹
۳-۲- پروتکل TLS Client	۳۰
۳-۳- پروتکل TLS Server	۳۴
۳-۴- پروتکل TLS مشترک کلاینت و سرور	۳۶
۳-۵- اعتبارسنجی گواهی‌نامه	۳۷
۳-۶- پروتکل SSH	۳۹

## ۱- معرفی محصول

نرم افزار مدیریت پروژه (IPMP (IVS Project Management Package) در یک جمله یک PMIS است که به مدیران پروژه جهت احاطه بر ابعاد مختلف پروژه‌های خود کمک می‌کند. در طراحی نرم افزار مدیریت پروژه آنلاین ایده ورزان (IPMP) از تجربیات افرادی استفاده شده که سوابق طولانی در پروژه‌های مختلف از جمله پروژه‌های EPC نفت و گاز، خط لوله و عمرانی داشته‌اند. این بسته با قرار گرفتن در مرکز تعاملات اطلاعاتی پروژه و وظیفه هماهنگی اطلاعات در بخش‌های مختلف پروژه را انجام می‌دهد. در طراحی این نرم افزار سعی شده محورهای نه گانه دانش مدیریت پروژه بر مبنای استاندارد PMBOK مد نظر قرار گیرد. نرم افزار کنترل پروژه IPMP هسته‌ای جهت ایجاد مجموعه نرم افزارهای مدیریت پروژه سفارشی‌سازی شده است. بسته‌های مختلفی روی بستر IPMP ایجاد شده که بوسیله آنها قابلیت‌های خاصی به آن افزوده می‌شود.

## ۱-۱- ویژگی‌های فنی محصول

نسخه‌ی نرم‌افزار/میان‌افزار	1,8,5,0
مدل و نسخه سیستم‌عامل	Windows Server 2016
مدل و نسخه وب‌سرور	IIS 10
مدل و نسخه پایگاه داده	SQL Server 2016
زبان برنامه‌نویسی	C#

## ۱-۲- معماری محصول

در معماری کنونی هسته نرم افزار IPMP ارتباط از لایه های متعدد با بکارگیری الگوهای طراحی نظیر Domain Driven Desing ، Unit of Work استفاده شده است. شرح لایه های مختلف به صورت زیر است:

**لایه UI:** به صورت کلی مسئولیت در اختیار قراردادن امکانات سرویس نرم افزار به کاربر نهایی را بر عهده دارد. از نظر فنی هر چند این لایه با تکنولوژی MVC پیاده سازی شده اما تکیه بسیار کمی بر این تکنولوژی داشته و برای پیاده سازی آن از امکانات پایه HTML 5 و جاوااسکریپت استفاده شده. در این لایه روایی سنجی ساختاری و منطقی و تا حدودی یکپارچگی در سمت کاربر انجام میشود. با این حال توسعه سمت سرور با این فرض انجام شده که هیچ روایی سنجی سمت کاربر صورت نمیگیرد.

**لایه App یا WebApi:** ارتباط با جهان خارج منجمله UI خود نرم افزار با استفاده از سرویسهای WebApi و عمدتاً بر مبنای پروتکل Rest صورت میگیرد. در همین لایه عملیات پایه ای ذیل شکل میگیرد:

- روایی سنجی ساختاری
- روایی سنجی منطقی
- ارزیابی دسترسی عمومی: بر اساس پارامترهای کلی درخواست و بدون در نظر گرفتن فرایندهای داخلی منبع مورد درخواست
- لاگ عمومی

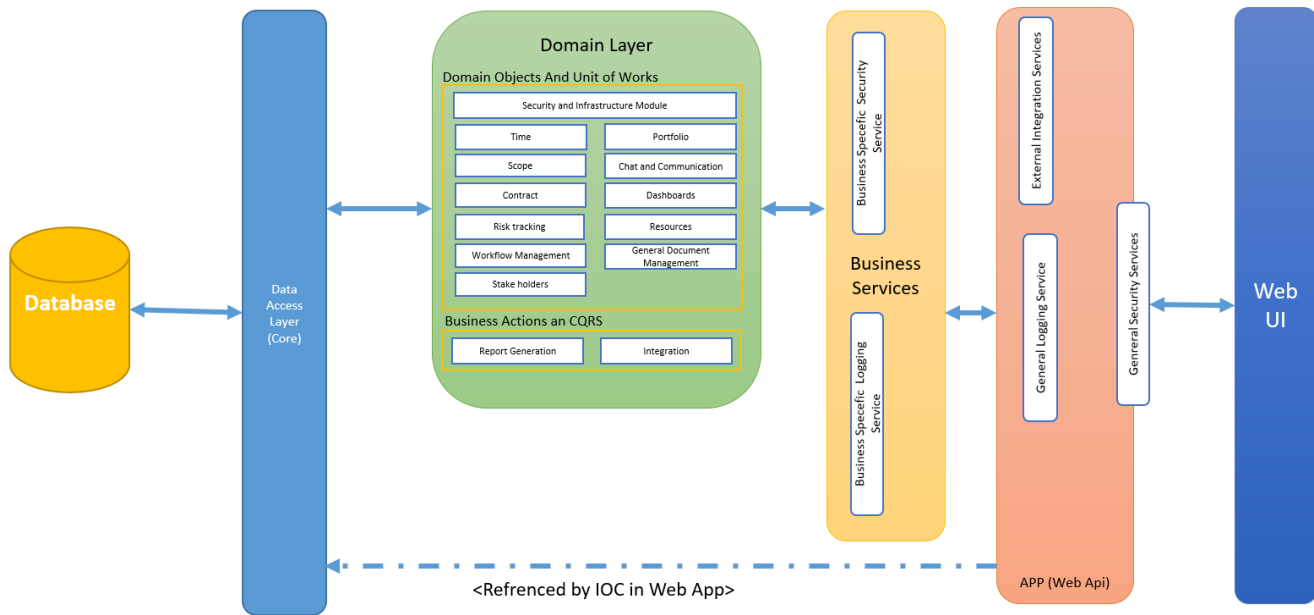
از آنجایی که لایه Data Access به صورت pluggable پیاده سازی شده است و در لایه های بالاتر تنها اینترفیسها مورد استفاده قرار گرفته اند، لایه App وظیفه ایجاد نسخه های قابل اجرای این لایه و در اختیار قراردادن آن به لایه های دیگر بوسیله روش IoC را بر عهده دارد.

**لایه Business Services**: این لایه یکپارچه کننده UoW های لایه دامین برای ارائه کلیه عملیات مورد نیاز در سامانه است. روایی سنجی کامل در همه سطوح و لاگ در سطح روالهای سیستم در این لایه انجام میشود.

**لایه Domain**: در این لایه کلیه کلاسهای دامین و همچنین UoW ها به صورت اینترفیس تعریف شده اند. همچنین گزارشات Ad Hoc و بین دامینی نیز در این لایه در اینترفیسها تعریف میشوند

**لایه دسترسی داده DAL**: این لایه وظیفه پیاده سازی UoW های لایه دامین را برای یک تکنولوژی خاص بر عهده دارد. هم اکنون این لایه با تکنولوژی EF و برای دیتابیس SQL Server پیاده سازی شده است. امکان جابجایی این لایه با کلاسهای متناظر با تکنولوژیها و دیتابیسهای دیگر نیز در آینده وجود دارد.

**لایه DataBase**: هر چند تلاش شده است که این لایه فقط به نگهداری دیتا بپردازد اما به ناچار جهت بهبود Performance این لایه در تهیه گزارشات و خروجیها شامل برخی از منطقهای کسب و کار در Stored Procedure ها نیز شده است.



شمایی از معماری نرم افزار IPMP

## ۲- الزامات امنیتی

الزامات امنیتی این سند بر اساس نسخه ۱.۱ پروفایل 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.

توضیحات	رده ممیزی امنیت (Log)	شماره الزام
	<input checked="" type="checkbox"/> محصول باید برای موارد مشخص شده که در زیر آمده است، ثبت‌نشان <sup>۱</sup> تولید کند (Log ثبت نماید).	۱
	<input checked="" type="checkbox"/> شروع و اتمام توابع	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.
این مورد علاوه بر ثبت در دو محل به صورت اضطراری به وسیله ایمیل به مدیر سیستم اطلاع رسانی میشود	<input checked="" type="checkbox"/> تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها	
این مورد علاوه بر ثبت در دو محل به صورت اضطراری به وسیله ایمیل به مدیر سیستم اطلاع رسانی میشود	<input checked="" type="checkbox"/> خواندن اطلاعات از ثبت‌نشان‌ها	
این مورد علاوه بر ثبت در دو محل به صورت اضطراری به وسیله ایمیل به مدیر سیستم اطلاع رسانی میشود	<input checked="" type="checkbox"/> تمامی تغییرات در پیکربندی ثبت‌نشان‌ها	
این مورد علاوه بر ثبت در دو محل به صورت اضطراری به وسیله ایمیل به مدیر سیستم اطلاع رسانی میشود	<input checked="" type="checkbox"/> عملیات انجام شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه	
	<input checked="" type="checkbox"/> عملیات انجام شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها	
	<input checked="" type="checkbox"/> تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.	

<sup>۱</sup> Log

	<input checked="" type="checkbox"/>	تمام کاربردهای سازوکار احراز هویت	
	<input checked="" type="checkbox"/>	نتایج نهایی عملیات احراز هویت	
	<input checked="" type="checkbox"/>	تلاش موفق و ناموفق هر گذرواژه بررسی شده توسط محصول	
	<input checked="" type="checkbox"/>	شکست و موفقیت انتساب ویژگی‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)	
	<input checked="" type="checkbox"/>	تمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی	
	<input checked="" type="checkbox"/>	تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	
	<input checked="" type="checkbox"/>	تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه ویژگی‌های امنیتی)	
	<input checked="" type="checkbox"/>	همه تلاش‌ها برای خارج کردن اطلاعات از محصول	
	<input checked="" type="checkbox"/>	تمامی تغییرات در رفتارهای توابع کارکردی محصول	
	<input checked="" type="checkbox"/>	استفاده از کارکردهای مدیریتی	
	<input checked="" type="checkbox"/>	تغییرات در گروه کاربران	
	<input checked="" type="checkbox"/>	شکست در کارکردهای امنیتی محصول	
	<input checked="" type="checkbox"/>	تمامی قابلیت‌هایی از محصول که به دلیل شکست (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند.	
	<input checked="" type="checkbox"/>	تلاش موفق یا ناموفق برای برقراری نشست.	
	<input checked="" type="checkbox"/>	ایجاد نشدن نشست به دلیل محدودیت نشست‌های همزمان (حداقل)	
	<input checked="" type="checkbox"/>	خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست	
در سامانه چنین قابلیت وجود ندارد	<input type="checkbox"/>	خاتمه به نشست غیرفعال توسط مدیر سیستم	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید.	۲
	<input checked="" type="checkbox"/>	تاریخ و زمان رویداد	
	<input checked="" type="checkbox"/>	نوع رویداد	

	<input checked="" type="checkbox"/>	هویت ایجادکننده رویداد	ویژگی‌هایی که در ثبت‌نشان‌ها وجود دارد مشخص شود.
	<input checked="" type="checkbox"/>	نتیجه رویداد	
	<input checked="" type="checkbox"/>	آدرس IP ایجادکننده رویداد	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید.	
	<input checked="" type="checkbox"/>	ثبت‌نشان‌هایی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند.	
	<input checked="" type="checkbox"/>	نبود داده نامفهوم در رکوردها	مواردی که در ثبت‌نشان‌ها وجود دارند، مشخص شوند.
	<input checked="" type="checkbox"/>	نبود بخش‌های نامرتب	
	<input checked="" type="checkbox"/>	وجود داده معتبر و مناسب در هر بخش	
	<input checked="" type="checkbox"/>	محصول باید امکان انتخاب و مرتب‌سازی برای ثبت‌نشان‌های تولیدشده را بر اساس بخش‌ها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.	
	<input checked="" type="checkbox"/>	هویت موجودیت فعال	مواردی که بر اساس آنها مرتب‌سازی وجود دارد، مشخص شود.
	<input checked="" type="checkbox"/>	نوع حساب کاربری	
	<input checked="" type="checkbox"/>	تاریخ/زمان	
	<input checked="" type="checkbox"/>	روش اتصال کاربر	
	<input checked="" type="checkbox"/>	نوع رخداد	
	<input checked="" type="checkbox"/>	مکان رویداد	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید هرگونه حذف و تغییر غیرمجاز در ثبت‌نشان‌ها را تشخیص دهد و در صورت امکان جلوگیری نماید.	
	<input type="checkbox"/>	استفاده از درهم‌سازی (Hash) برای تشخیص تغییرات	روش‌های تشخیص (وجود) مشخص شود.
	<input checked="" type="checkbox"/>	پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	



	<input checked="" type="checkbox"/>	فقط خواندنی کردن ثبت‌نشان‌ها در محصول	یک مورد لازم و کافی است
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.	۷
	<input checked="" type="checkbox"/>	استفاده از یک کانال ارتباطی	روش‌های اطلاع‌رسانی
	<input checked="" type="checkbox"/>	ارسال پیام	مشخص شود (وجود)
	<input type="checkbox"/>	از طریق واسط کاربر مجاز	یک مورد لازم و کافی است
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	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.	۸
	<input type="checkbox"/>	نادیده گرفتن ثبت‌نشان‌ها	رویکردهای مورد استفاده در محصول
	<input type="checkbox"/>	ذخیره‌سازی محدود ثبت‌نشان‌ها (آنهايي که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند)	مشخص گردد (وجود)
	<input checked="" type="checkbox"/>	بازنویسی روی قدیمی‌ترین ثبت‌نشان‌های ذخیره‌شده	یک مورد لازم و کافی است
ثبت در دیتابیس مربوط به سامانه انجام میشود و تنظیمی وجود دارد که میتوان در فایل ذخیره کرد و حداکثر حجم را نیز مشخص کرد	<input checked="" type="checkbox"/>	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 <sup>۲</sup> رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف شده ISO 18033-3) با توجه به موارد زیر انجام دهد.	<input checked="" type="checkbox"/>
	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 (تعریف شده در NIST SP 800-38A) <input checked="" type="checkbox"/>
	مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در NIST SP 800-38D) <input checked="" type="checkbox"/>	۲۵۶ بیتی
	مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در ISO10116) <input type="checkbox"/>	۲۵۶ بیتی
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.	<input checked="" type="checkbox"/>
	الگوریتم و اندازه خلاصه پیام مورد استفاده را	الگوریتم SHA-1 با اندازه خلاصه پیام ۱۶۰ بیت <input checked="" type="checkbox"/>
		الگوریتم SHA-256 با اندازه خلاصه پیام ۲۵۶ بیت <input type="checkbox"/>
		تنها دیتای امنیتی داخل سامانه کلمه عبور می‌باشد که توسط پلترفرم hash میشود

<sup>2</sup> Module

	<input type="checkbox"/>	الگوریتم SHA-384 با اندازه خلاصه پیام ۳۸۴ بیت	انتخاب نمایید. (وجود یک مورد لازم و کافی است.)
	<input type="checkbox"/>	الگوریتم SHA-512 با اندازه خلاصه پیام ۵۱۲ بیت	
	<input type="checkbox"/>	در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری)	
	<input type="checkbox"/>	نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یکها، مقدار تصادفی، مقدار جدیدی از کلید)	روش نابودی کلید مشخص گردد. (وجود یک مورد لازم و کافی است)
	<input type="checkbox"/>	نابودی با استفاده از یک واسط مشخص	
	<input type="checkbox"/>	از طریق توابع امنیتی محصول	
	<input type="checkbox"/>	سایر موارد	
	<input type="checkbox"/>	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)	
	<input type="checkbox"/>	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)	الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است)
	<input type="checkbox"/>	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.

توضیحات	رده شناسایی و احراز هویت		شماره الزام									
	<input checked="" type="checkbox"/>	<p>محصول باید بتواند تعداد تلاش‌های ناموفقی را که برای احراز هویت شدن صورت گرفته است (در هر بخش یا قسمتی که نیاز به احراز هویت وجود دارد)، بر اساس موارد زیر مشخص نماید.</p> <table border="1" data-bbox="947 597 1927 846"> <tr> <td data-bbox="947 597 1029 683" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1029 597 1692 683">یک عدد مثبت ثابت</td> <td data-bbox="1692 597 1927 683">مقدار یا یازهی مورد استفاده در هریک باید مشخص گردد. (وجود</td> </tr> <tr> <td data-bbox="947 683 1029 769" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="1029 683 1692 769">یک عدد مثبت قابل تنظیم توسط مدیر</td> <td data-bbox="1692 683 1927 769">یک مورد لازم و کافی</td> </tr> <tr> <td data-bbox="947 769 1029 846" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1029 769 1692 846">یک بازهی قابل قبولی از مقادیر</td> <td data-bbox="1692 769 1927 846">(است)</td> </tr> </table>	<input type="checkbox"/>	یک عدد مثبت ثابت	مقدار یا یازهی مورد استفاده در هریک باید مشخص گردد. (وجود	<input checked="" type="checkbox"/>	یک عدد مثبت قابل تنظیم توسط مدیر	یک مورد لازم و کافی	<input type="checkbox"/>	یک بازهی قابل قبولی از مقادیر	(است)	۱
<input type="checkbox"/>	یک عدد مثبت ثابت	مقدار یا یازهی مورد استفاده در هریک باید مشخص گردد. (وجود										
<input checked="" type="checkbox"/>	یک عدد مثبت قابل تنظیم توسط مدیر	یک مورد لازم و کافی										
<input type="checkbox"/>	یک بازهی قابل قبولی از مقادیر	(است)										
<p>استفاده از کدهای CAPTCHA در سامانه وجود دارد که در زمان لاگین باید تکمیل شود</p>	<input checked="" type="checkbox"/>	<p>محصول باید زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید.</p> <table border="1" data-bbox="947 959 1927 1456"> <tr> <td data-bbox="947 959 1029 1127" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="1029 959 1692 1127">غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)</td> <td data-bbox="1692 959 1927 1127">روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)</td> </tr> <tr> <td data-bbox="947 1127 1029 1294" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="1029 1127 1692 1294">غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)</td> <td data-bbox="1692 1127 1927 1294">لازم به ذکر است روش‌های فوق با توجه به نوع کاربرد می‌تواند از حالت انتخابی به</td> </tr> <tr> <td data-bbox="947 1294 1029 1456" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="1029 1294 1692 1456">استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)</td> <td data-bbox="1692 1294 1927 1456"></td> </tr> </table>	<input checked="" type="checkbox"/>	غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)	روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	<input checked="" type="checkbox"/>	غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)	لازم به ذکر است روش‌های فوق با توجه به نوع کاربرد می‌تواند از حالت انتخابی به	<input checked="" type="checkbox"/>	استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)		۲
<input checked="" type="checkbox"/>	غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)	روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)										
<input checked="" type="checkbox"/>	غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)	لازم به ذکر است روش‌های فوق با توجه به نوع کاربرد می‌تواند از حالت انتخابی به										
<input checked="" type="checkbox"/>	استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)											

		<input type="checkbox"/>	حالت الزامی تغییر یابد. برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست.
	<input checked="" type="checkbox"/>	محصول باید برای هر کاربر، ویژگی‌های امنیتی را که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باشند، نگهداری نماید.	۳
	<input checked="" type="checkbox"/>	شناسه کاربر	ویژگی‌های امنیتی
	<input checked="" type="checkbox"/>	روش احراز هویت مورد استفاده	مورد نیاز که باید برای
	<input checked="" type="checkbox"/>	داده احراز هویت	هر کاربر نگهداری
	<input checked="" type="checkbox"/>	وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)	شوند.
	<input checked="" type="checkbox"/>	نقش کاربر	سایر موارد
	<input type="checkbox"/>	سایر موارد	سایر موارد
	<input checked="" type="checkbox"/>	محصول باید قابلیت مدیریت گذرواژه را فراهم آورد.	۴
	<input checked="" type="checkbox"/>	استفاده از حروف کوچک	موارد نیاز که باید در
	<input checked="" type="checkbox"/>	استفاده از حروف بزرگ	تعریف گذرواژه استفاده
	<input checked="" type="checkbox"/>	استفاده از اعداد	شوند.
	<input checked="" type="checkbox"/>	استفاده از کاراکترهای خاص ("@", "#", "\$", "%", "^", "&", "*", " و ...")	حداقل طول ۸ یا بیشتر (قابل تنظیم)
	<input checked="" type="checkbox"/>	حداقل طول ۸ یا بیشتر (قابل تنظیم)	سایر موارد
	<input type="checkbox"/>	سایر موارد	سایر موارد
	<input checked="" type="checkbox"/>	محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.	۵
	<input checked="" type="checkbox"/>	مشاهده راهنمای نحوه ورود به سیستم	مشاهده راهنمای نحوه ورود به سیستم

	<input type="checkbox"/>	بازیابی گذرواژه	اقدامات عمومی که
	<input checked="" type="checkbox"/>	هیچ اقدامی	کاربر می‌تواند قبل از
	<input type="checkbox"/>	سایر موارد	احراز هویت انجام دهد، انتخاب شود.
	<input checked="" type="checkbox"/>	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).	
	<input checked="" type="checkbox"/>	نام کاربری و گذرواژه	سازوکارهای احراز هویت موجود در محصول مشخص شوند.
داخل خود محصول این قابلیت وجود دارد که امضای دیجیتال تولید شود	<input checked="" type="checkbox"/>	امضای دیجیتال	
	<input type="checkbox"/>	Active Directory	
	<input type="checkbox"/>	OTP یا توکن	
	<input type="checkbox"/>	احراز هویت دو فاکتوری	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید برای هر کاربر فعال، ویژگی‌های امنیتی را نگهداری نماید.	
	<input checked="" type="checkbox"/>	شناسه کاربر	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).
	<input checked="" type="checkbox"/>	نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه	
	<input checked="" type="checkbox"/>	جزئیات واسط کلاینت	
	<input checked="" type="checkbox"/>	پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)	
	<input type="checkbox"/>	سایر موارد	

	<input checked="" type="checkbox"/>	<p>محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.</p>		۸
	<input checked="" type="checkbox"/>	<p>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.</p>	<p>در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند.</p>	
	<input checked="" type="checkbox"/>	<p>بروزرسانی اطلاعات پیشینه احراز هویت</p>		
	<input type="checkbox"/>	<p>سایر موارد</p>		
	<input checked="" type="checkbox"/>	<p>محصول باید بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید.</p>		۹
<p>با انجام تغییرات مثل تغییر پسورد کاربر از نشست خارج میشود</p>	<input checked="" type="checkbox"/>	<p>غیرمجاز بودن هرگونه تغییر در طول نشست فعال</p>	<p>قوانینی که در صورت تغییر ویژگی‌های امنیتی کاربر فعال، اعمال می‌شود، مشخص گردد.</p>	
	<input type="checkbox"/>	<p>سایر موارد</p>		

## 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.

توضیحات	رده حفاظت از داده‌ی کاربری		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید برای موجودیت‌ها و عملیات، خطمشی‌های کنترل دسترسی اعمال نماید.	۱
	<input checked="" type="checkbox"/>	مدیر سیستم موجودیت‌های فعالی که خطمشی‌های	
	<input checked="" type="checkbox"/>	کاربر عادی کنترل دسترسی در مورد آنها اعمال	
راهبر پروژه	<input checked="" type="checkbox"/>	سایر موارد می‌شوند، مشخص گردد.	
	<input checked="" type="checkbox"/>	سوابق، مستندات و فراداده موجودیت‌های غیرفعال که	
	<input checked="" type="checkbox"/>	داده متعلق به کاربران خطمشی‌های کنترل	
	<input checked="" type="checkbox"/>	داده احراز هویت دسترسی در مورد آنها اعمال می‌شوند،	
	<input type="checkbox"/>	سایر موارد مشخص گردد.	
	<input checked="" type="checkbox"/>	ایجاد موجودیت غیرفعال جدید عملیاتی که	
	<input checked="" type="checkbox"/>	حذف موجودیت غیرفعال خطمشی‌های کنترل	
	<input checked="" type="checkbox"/>	تغییر دسترسی‌ها به موجودیت غیرفعال دسترسی در رابطه با	
	<input checked="" type="checkbox"/>	عملیات بر روی فراداده وابسته به موجودیت غیرفعال	



	<input type="checkbox"/>	سایر موارد	آنها اعمال می‌شوند، مشخص گردد.
	<input checked="" type="checkbox"/>	محصول باید بر اساس ویژگی‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.	
	<input checked="" type="checkbox"/>	نقش‌ها و مجوزهای کاربر مجاز	ویژگی‌هایی که بر اساس آن خط‌مشی‌ها
	<input checked="" type="checkbox"/>	اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.	تعریف می‌شوند،
	<input type="checkbox"/>	سایر موارد	انتخاب گردد.
از طریق تخصیص کاربران به نقش‌ها و دادن دسترسی به نقش‌ها انجام می‌پذیرد.	<input checked="" type="checkbox"/>	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.)	
	<input checked="" type="checkbox"/>	محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.	
	<input type="checkbox"/>	عبور تعداد نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف‌شده	قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).
قوانین، همان تخصیص دسترسی‌ها به نقش‌ها و عضو کردن کاربران در آن نقش‌ها می‌باشد	<input checked="" type="checkbox"/>	سایر موارد	
تخصیص و آزادسازی منابع توسط سیستم عامل و پایگاه داده انجام میشود	<input checked="" type="checkbox"/>	محصول باید تضمین نماید تمام اطلاعات قبلی منابع یا در هنگام آزادسازی آنها، غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.	
	<input checked="" type="checkbox"/>	محصول باید هنگام دریافت داده کاربری خط‌مشی کنترل دسترسی را اعمال و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.	

<p>پسوندهای قابل پذیرش عبارتند از pdf، doc، docx، xls، xlsx، txt. تغییر پسوندهای مجاز به صورت تنظیمات در اختیار مدیر سیستم قرار دارد</p>	<input checked="" type="checkbox"/>	<p>نوع داده</p>	<p>ویژگی‌های امنیتی مرتبط با داده کاربری</p>	
<p>حداکثر اندازه فایل قابل بارگذاری 4MB تعیین شده است. این مقدار در بخشهای مختلف بوسیله مدیر سیستم قابل تغییر است.</p>	<input checked="" type="checkbox"/>	<p>حجم و اندازه</p>	<p>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).</p>	
	<input type="checkbox"/>	<p>فرمت</p>		
	<input type="checkbox"/>	<p>تعداد دفعات Import</p>		
	<input type="checkbox"/>	<p>سایر موارد</p>		
<p>استفاده از SSL/TLS</p>	<input checked="" type="checkbox"/>	<p>محصول باید از یک پروتکل امن برای انتقال داده استفاده نماید. این پروتکل ارتباط و همبستگی شفاف را بین داده کاربری دریافت‌شده و ویژگی‌های امنیتی آن فراهم و همچنین از شنود و گم‌شدن داده حین انتقال جلوگیری می‌کند.</p>		
	<input checked="" type="checkbox"/>	<p>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.</p>		
<p>نوع داده در سامانه مشخص هست که اغلب خروجی ها xls یا xlsx هستند و کاربر نمیتواند غیر از این نوع داده ها، نوع خروجی دیگری دریافت نماید</p>	<input checked="" type="checkbox"/>	<p>نوع داده</p>	<p>ویژگی‌های امنیتی مرتبط با داده کاربری</p>	
	<input type="checkbox"/>	<p>حجم و اندازه</p>	<p>که در هنگام خروج آن از محصول استفاده می‌شوند، مشخص</p>	
	<input type="checkbox"/>	<p>فرمت</p>	<p>شوند</p>	
	<input checked="" type="checkbox"/>	<p>محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.</p>		

<p>با استفاده از تعریف دسترسی ها برای کاربران مختلف روی سطوح متفاوت</p>	<input checked="" type="checkbox"/>	<p>مدیر سیستم باید خروج داده‌ها را محدود نماید، به طوریکه کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند.</p>	<p>قوانینی که در هنگام خروج داده از محصول</p>
	<input type="checkbox"/>	<p>سایر موارد</p>	<p>اعمال می‌شوند، مشخص شوند</p>
<p>امکان تغییر غیر مجاز وجود ندارد</p>	<input checked="" type="checkbox"/>	<p>محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره‌شده در محصول تشخیص دهد.</p>	
	<input type="checkbox"/>	<p>مقدار درهم‌سازی شده داده‌های کاربری ذخیره‌شده، نگهداری می‌شود.</p>	<p>چگونگی تشخیص تغییر در داده‌های</p>
<p>با استفاده از تعریف دسترسی ها در سامانه، امکان تغییر غیر مجاز وجود ندارد.</p>	<input checked="" type="checkbox"/>	<p>سایر موارد</p>	<p>کاربری حساس، مشخص شود.</p>
	<input type="checkbox"/>	<p>محصول باید در صورت تشخیص خطای صحت در داده‌ها، اقدامات مقابله‌ای زیر را انجام دهد.</p>	
	<input type="checkbox"/>	<p>ایجاد هشدار/اخطار برای نقش‌های مجاز</p>	<p>اقدام مقابله‌ای در صورت تشخیص خطا،</p>
	<input type="checkbox"/>	<p>تصحیح داده بر اساس مقادیر قبل</p>	<p>مشخص شود (وجود)</p>
<p>با استفاده از تعریف دسترسی ها در سامانه، امکان تغییر غیر مجاز وجود ندارد.</p>	<input checked="" type="checkbox"/>	<p>سایر موارد</p>	<p>یک مورد لازم و کافی است)</p>

## 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.

توضیحات	رده مدیریت امنیت	شماره الزام															
	<p><input checked="" type="checkbox"/> 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.</p> <table border="1" data-bbox="913 646 1927 852"> <tr> <td data-bbox="913 646 949 690"><input type="checkbox"/></td> <td data-bbox="949 646 1696 690">تعیین و تغییر رفتار</td> <td data-bbox="1696 646 1927 690">فعالیت‌های مدیریتی</td> </tr> <tr> <td data-bbox="913 690 949 734"><input checked="" type="checkbox"/></td> <td data-bbox="949 690 1696 734">غیرفعال نمودن</td> <td data-bbox="1696 690 1927 734">که محصول پشتیبانی</td> </tr> <tr> <td data-bbox="913 734 949 777"><input checked="" type="checkbox"/></td> <td data-bbox="949 734 1696 777">فعال نمودن</td> <td data-bbox="1696 734 1927 777">می‌کند، مشخص شوند.</td> </tr> <tr> <td data-bbox="913 777 949 852"><input type="checkbox"/></td> <td data-bbox="949 777 1696 852">سایر موارد</td> <td data-bbox="1696 777 1927 852"></td> </tr> </table>	<input type="checkbox"/>	تعیین و تغییر رفتار	فعالیت‌های مدیریتی	<input checked="" type="checkbox"/>	غیرفعال نمودن	که محصول پشتیبانی	<input checked="" type="checkbox"/>	فعال نمودن	می‌کند، مشخص شوند.	<input type="checkbox"/>	سایر موارد		۱			
<input type="checkbox"/>	تعیین و تغییر رفتار	فعالیت‌های مدیریتی															
<input checked="" type="checkbox"/>	غیرفعال نمودن	که محصول پشتیبانی															
<input checked="" type="checkbox"/>	فعال نمودن	می‌کند، مشخص شوند.															
<input type="checkbox"/>	سایر موارد																
	<p><input checked="" type="checkbox"/> 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.</p> <table border="1" data-bbox="913 1015 1927 1263"> <tr> <td data-bbox="913 1015 949 1058"><input checked="" type="checkbox"/></td> <td data-bbox="949 1015 1696 1058">پرس‌وجو</td> <td data-bbox="1696 1015 1927 1058">عملیات بر روی</td> </tr> <tr> <td data-bbox="913 1058 949 1102"><input checked="" type="checkbox"/></td> <td data-bbox="949 1058 1696 1102">تغییر</td> <td data-bbox="1696 1058 1927 1102">ویژگی‌های امنیتی که</td> </tr> <tr> <td data-bbox="913 1102 949 1146"><input checked="" type="checkbox"/></td> <td data-bbox="949 1102 1696 1146">حذف</td> <td data-bbox="1696 1102 1927 1146">در محصول پشتیبانی</td> </tr> <tr> <td data-bbox="913 1146 949 1190"><input type="checkbox"/></td> <td data-bbox="949 1146 1696 1190">تغییر پیش‌فرض</td> <td data-bbox="1696 1146 1927 1190">می‌شوند، مشخص</td> </tr> <tr> <td data-bbox="913 1190 949 1263"><input type="checkbox"/></td> <td data-bbox="949 1190 1696 1263">سایر موارد</td> <td data-bbox="1696 1190 1927 1263">گردد.</td> </tr> </table>	<input checked="" type="checkbox"/>	پرس‌وجو	عملیات بر روی	<input checked="" type="checkbox"/>	تغییر	ویژگی‌های امنیتی که	<input checked="" type="checkbox"/>	حذف	در محصول پشتیبانی	<input type="checkbox"/>	تغییر پیش‌فرض	می‌شوند، مشخص	<input type="checkbox"/>	سایر موارد	گردد.	۲
<input checked="" type="checkbox"/>	پرس‌وجو	عملیات بر روی															
<input checked="" type="checkbox"/>	تغییر	ویژگی‌های امنیتی که															
<input checked="" type="checkbox"/>	حذف	در محصول پشتیبانی															
<input type="checkbox"/>	تغییر پیش‌فرض	می‌شوند، مشخص															
<input type="checkbox"/>	سایر موارد	گردد.															
	<p><input checked="" type="checkbox"/> محصول باید برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.</p> <table border="1" data-bbox="913 1372 1927 1424"> <tr> <td data-bbox="913 1372 949 1424"><input type="checkbox"/></td> <td data-bbox="949 1372 1696 1424">تغییر پیش‌فرض</td> <td data-bbox="1696 1372 1927 1424"></td> </tr> </table>	<input type="checkbox"/>	تغییر پیش‌فرض		۳												
<input type="checkbox"/>	تغییر پیش‌فرض																

	<input checked="" type="checkbox"/>	حذف نمودن پرس و جو مقدارهی ایجاد مشاهده سایر موارد	عملیات بر روی داده‌های محصول که در محصول پشتیبانی می‌شوند، مشخص شود.
تخصیص و آزادسازی منابع توسط سیستم عامل و پایگاه داده انجام میشود.	<input checked="" type="checkbox"/>	محصول باید توانایی انجام کارکردهای زیر را داشته باشد. پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشده پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشده پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشده 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) ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول در نظر گرفتن یک عملیات از پیش تعیین شده 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. مدیریت معیارها برای تنظیم گذرواژه‌ها ۱. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه ۲. مدیریت یکسری عملیاتی که قبل از احراز شدن هویت کاربر انجام می‌شوند.	۴ در صورتی که هر کدام از موارد مطرح شده، توسط محصول قابل اجرا نیست، در قسمت توضیحات باید دلایل مطرح گردد.

		<input checked="" type="checkbox"/> ۱. مدیریت سازوکارهای احراز هویت <input checked="" type="checkbox"/> ۲. مدیریت قوانین مرتبط با احراز هویت	
		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.	
	مشخصات کاربر مدیر سیستم را میتوان تغییر داد	<input checked="" type="checkbox"/> مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.	
		<input checked="" type="checkbox"/> مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول	
		<input checked="" type="checkbox"/> مدیریت نقش‌ها در محصول	
		<input checked="" type="checkbox"/> مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر	
		<input checked="" type="checkbox"/> مدیریت شرایط آغاز نشست توسط مدیر مجاز	
		<input checked="" type="checkbox"/> 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.	
		<input checked="" type="checkbox"/> محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد.	۵
		<input checked="" type="checkbox"/> نقش‌هایی که در	
	راهبر پروژه	<input checked="" type="checkbox"/> مدیر سیستم <input checked="" type="checkbox"/> کاربر پیشرفته <input checked="" type="checkbox"/> کاربر عادی <input type="checkbox"/> سایر موارد	محصول پشتیبانی می‌شوند، مشخص گردد.
		<input checked="" type="checkbox"/> 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.	۶

## 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.

توضیحات	رده حفاظت از توابع امنیتی محصول		شماره الزام															
	<input checked="" type="checkbox"/>	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.	۱															
بخش‌های سامانه مجزا از هم نیستند و Database و Application روی یک سرور قرار دارند.	<input checked="" type="checkbox"/>	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.	۲															
با محصول دیگری ارتباط ندارد	<input type="checkbox"/>	<p>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.</p> <table border="1" data-bbox="947 1133 1927 1380"> <tr> <td data-bbox="947 1133 1031 1182" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1031 1133 1696 1182">داده‌های احراز هویت</td> <td data-bbox="1696 1133 1927 1182">داده امنیتی قابل</td> </tr> <tr> <td data-bbox="947 1182 1031 1230" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1031 1182 1696 1230">کلید</td> <td data-bbox="1696 1182 1927 1230">اشتراک‌گذاری که در</td> </tr> <tr> <td data-bbox="947 1230 1031 1279" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1031 1230 1696 1279">امضای دیجیتال</td> <td data-bbox="1696 1230 1927 1279">محصول پشتیبانی</td> </tr> <tr> <td data-bbox="947 1279 1031 1328" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1031 1279 1696 1328">ثبت‌نشان‌ها (داده‌های ممیزی)</td> <td data-bbox="1696 1279 1927 1328">می‌شوند، مشخص</td> </tr> <tr> <td data-bbox="947 1328 1031 1380" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1031 1328 1696 1380">سایر موارد</td> <td data-bbox="1696 1328 1927 1380">گردد.</td> </tr> </table>	<input type="checkbox"/>	داده‌های احراز هویت	داده امنیتی قابل	<input type="checkbox"/>	کلید	اشتراک‌گذاری که در	<input type="checkbox"/>	امضای دیجیتال	محصول پشتیبانی	<input type="checkbox"/>	ثبت‌نشان‌ها (داده‌های ممیزی)	می‌شوند، مشخص	<input type="checkbox"/>	سایر موارد	گردد.	۳
<input type="checkbox"/>	داده‌های احراز هویت	داده امنیتی قابل																
<input type="checkbox"/>	کلید	اشتراک‌گذاری که در																
<input type="checkbox"/>	امضای دیجیتال	محصول پشتیبانی																
<input type="checkbox"/>	ثبت‌نشان‌ها (داده‌های ممیزی)	می‌شوند، مشخص																
<input type="checkbox"/>	سایر موارد	گردد.																

	<input checked="" type="checkbox"/>	<p>۴ محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی<sup>۳</sup> معتبر را تولید یا از آن‌ها استفاده نماید.</p>
	<input type="checkbox"/>	<p>روش‌های ایجاد مهرهای زمانی معتبر</p>
	<input type="checkbox"/>	<p>انتخاب شود. (دیگر تنظیم مهرهای زمانی از طریق اینترنت</p>
	<input checked="" type="checkbox"/>	<p>روشهای موجود در محصول، در قسمت تنظیم مهرهای زمانی به صورت پیش‌فرض (معتبر و عدم امکان دستکاری غیرمجاز)</p>
	<input type="checkbox"/>	<p>«سایر موارد» بیان شود). سایر موارد</p>
	<input checked="" type="checkbox"/>	<p>۵ محصول باید امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید.</p>
	<input checked="" type="checkbox"/>	<p>روش بروزرسانی مورد استفاده در محصول،</p>
	<input type="checkbox"/>	<p>مشخص گردد (حداقل جستجوی خودکار بروزرسانی‌ها</p>
	<input type="checkbox"/>	<p>یک مورد لازم و کافی بروزرسانی‌های خودکار</p>
	<input type="checkbox"/>	<p>است). بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی</p>
	<input type="checkbox"/>	<p>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.</p>
	<input type="checkbox"/>	<p>سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی)</p>
	<input type="checkbox"/>	<p>به‌روزرسانی‌ها انتخاب گردد. درهم‌ساز منتشرشده</p>

<sup>3</sup> 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.

توضیحات	رده تخصیص منابع	شماره الزام
به دلیل مستقل بودن بخش ها، این امکان در سامانه بصورت خودکار وجود دارد	<input checked="" type="checkbox"/> محصول باید در زمان رخداد هرگونه اشکال و خرابی (شکست) نرم‌افزاری، از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.	۱

## 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.	<input checked="" type="checkbox"/>
۲	محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمانی که غیرفعال هستند (و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.	<input checked="" type="checkbox"/>
۳	محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.	<input checked="" type="checkbox"/>
۴	در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد.	<input checked="" type="checkbox"/>
		<input checked="" type="checkbox"/> روز
		<input checked="" type="checkbox"/> زمان
		<input type="checkbox"/> سایر موارد
۵	در صورت برقراری نشست به طور موفقیت‌آمیز، 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.	<input checked="" type="checkbox"/>
		<input checked="" type="checkbox"/> روز
		<input checked="" type="checkbox"/> زمان
		<input type="checkbox"/> سایر موارد

	<input checked="" type="checkbox"/>	محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.		۶
	<input checked="" type="checkbox"/>	محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.		۷
بر اساس IP	<input checked="" type="checkbox"/>	مکان	پارامترهای موجود برای	
	<input checked="" type="checkbox"/>	شماره پورت	جلوگیری از نشست،	
	<input type="checkbox"/>	روز	مشخص شوند (وجود)	
	<input type="checkbox"/>	زمان	یک مورد لازم و کافی	
	<input type="checkbox"/>	سایر موارد	است).	

## 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.

توضیحات	رده کانال‌ها/مسیرهای مورد اعتماد	شماره الزام									
	<p>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 افشاء داده تبادلی حفاظت نماید و تغییرات را تشخیص دهد.</p> <p>در صورت انتخاب مورد HTTPS، رعایت الزام ۱-۳- و ۳-۳- و در صورت انتخاب TLS، رعایت الزامات ۲- تا ۴-۳- که در بخش ۳- بیان گردیده است، الزامی است.</p> <table border="1" data-bbox="909 753 1927 984"> <tr> <td data-bbox="909 753 951 833"><input checked="" type="checkbox"/></td> <td data-bbox="951 753 1696 833">HTTPS</td> <td data-bbox="1696 753 1927 833">پروتکل مورد استفاده</td> </tr> <tr> <td data-bbox="909 833 951 912"><input type="checkbox"/></td> <td data-bbox="951 833 1696 912">TLS</td> <td data-bbox="1696 833 1927 912">برای ایجاد کانال امن انتخاب گردد.</td> </tr> <tr> <td data-bbox="909 912 951 984"><input type="checkbox"/></td> <td data-bbox="951 912 1696 984">SSH</td> <td data-bbox="1696 912 1927 984"></td> </tr> </table>	<input checked="" type="checkbox"/>	HTTPS	پروتکل مورد استفاده	<input type="checkbox"/>	TLS	برای ایجاد کانال امن انتخاب گردد.	<input type="checkbox"/>	SSH		۱
<input checked="" type="checkbox"/>	HTTPS	پروتکل مورد استفاده									
<input type="checkbox"/>	TLS	برای ایجاد کانال امن انتخاب گردد.									
<input type="checkbox"/>	SSH										
	<p>محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.</p>	۲									
	<p>محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.</p>	۳									

## 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

توضیحات	پروتکل HTTPS		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند.	۱
	<input checked="" type="checkbox"/>	محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	۲
	<input checked="" type="checkbox"/>	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 ۳-۵-۳ انجام می‌شود که در این صورت الزامات بخش ۳-۵-۳ الزامی است.	۳
	<input checked="" type="checkbox"/>	اتصال را برقرار نکند.	محصول تنها از موارد بیان‌شده می‌تواند استفاده نماید.
	<input type="checkbox"/>	برای برقراری اتصال درخواست مجوز کند.	

## ۲-۳- پروتکل TLS Client

توضیحات	پروتکل TLS Client	شماره الزام											
	<p data-bbox="913 446 1927 592"> <input type="checkbox"/> 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.         </p> <table border="1" data-bbox="913 592 1927 1450"> <tr> <td data-bbox="913 592 1696 683"> <input type="checkbox"/> TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268         </td> <td data-bbox="1696 592 1927 1450" rowspan="10">مجموعه رمز مورد استفاده پیاده‌سازی شده محصول، انتخاب گردد.</td> </tr> <tr> <td data-bbox="913 683 1696 774"> <input type="checkbox"/> TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268         </td> </tr> <tr> <td data-bbox="913 774 1696 865"> <input type="checkbox"/> TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268         </td> </tr> <tr> <td data-bbox="913 865 1696 956"> <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268         </td> </tr> <tr> <td data-bbox="913 956 1696 1047"> <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268         </td> </tr> <tr> <td data-bbox="913 1047 1696 1138"> <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268         </td> </tr> <tr> <td data-bbox="913 1138 1696 1229"> <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492         </td> </tr> <tr> <td data-bbox="913 1229 1696 1320"> <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492         </td> </tr> <tr> <td data-bbox="913 1320 1696 1411"> <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492         </td> </tr> <tr> <td data-bbox="913 1411 1696 1450"> <input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492         </td> </tr> </table>	<input type="checkbox"/> TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	مجموعه رمز مورد استفاده پیاده‌سازی شده محصول، انتخاب گردد.	<input type="checkbox"/> TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/> TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/> TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/> TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/> TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	<input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492	<input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	<input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	۱
<input type="checkbox"/> TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	مجموعه رمز مورد استفاده پیاده‌سازی شده محصول، انتخاب گردد.												
<input type="checkbox"/> TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268													
<input type="checkbox"/> TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268													
<input type="checkbox"/> TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268													
<input type="checkbox"/> TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268													
<input type="checkbox"/> TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268													
<input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492													
<input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492													
<input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492													
<input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492													

<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492		
<input type="checkbox"/>	TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288		
<input type="checkbox"/>	TLS_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5288		
<input type="checkbox"/>	TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA384 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256		

		<table border="1"> <tr> <td data-bbox="909 149 951 203"></td> <td data-bbox="951 149 1694 203">مطابق با RFC 5289</td> </tr> <tr> <td data-bbox="909 203 951 284"><input type="checkbox"/></td> <td data-bbox="951 203 1694 284">                     TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384                      مطابق با RFC 5289                 </td> </tr> <tr> <td data-bbox="909 284 951 365"><input type="checkbox"/></td> <td data-bbox="951 284 1694 365">                     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256                      مطابق با RFC 5289                 </td> </tr> <tr> <td data-bbox="909 365 951 446"><input type="checkbox"/></td> <td data-bbox="951 365 1694 446">                     TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256                      مطابق با RFC 5289                 </td> </tr> <tr> <td data-bbox="909 446 951 527"><input type="checkbox"/></td> <td data-bbox="951 446 1694 527">                     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384                      مطابق با RFC 5289                 </td> </tr> <tr> <td data-bbox="909 527 951 609"><input type="checkbox"/></td> <td data-bbox="951 527 1694 609">                     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256                      مطابق با RFC 5289                 </td> </tr> <tr> <td data-bbox="909 609 951 690"><input type="checkbox"/></td> <td data-bbox="951 609 1694 690">                     TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256                      مطابق با RFC 5289                 </td> </tr> <tr> <td data-bbox="909 690 951 797"><input type="checkbox"/></td> <td data-bbox="951 690 1694 797">                     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384                      مطابق با RFC 5289                 </td> </tr> </table>		مطابق با RFC 5289	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289		
	مطابق با RFC 5289																			
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289																			
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289																			
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289																			
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289																			
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289																			
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289																			
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289																			
	<input type="checkbox"/>	محصول باید مطابقت شناسه ارائه شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تأیید نماید.	۲																	
	<input type="checkbox"/>	<table border="1"> <tr> <td data-bbox="909 911 1694 1024">محصول باید کانال امن را فقط در صورت معتبر بودن گواهی نامه سرور برقرار سازد؛ بنابراین اگر گواهی نامه سرور غیرمعتبر به نظر رسید، محصول باید بر اساس موارد زیر رفتار نماید.</td> <td data-bbox="1694 911 1927 1179" rowspan="3">در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.</td> </tr> <tr> <td data-bbox="909 1024 1694 1078"><input type="checkbox"/></td> <td data-bbox="1694 1024 1927 1078">ارتباط را برقرار نکند</td> </tr> <tr> <td data-bbox="909 1078 1694 1131"><input type="checkbox"/></td> <td data-bbox="1694 1078 1927 1131">برای برقراری ارتباط درخواست مجوز کند</td> </tr> <tr> <td data-bbox="909 1131 1694 1179"><input type="checkbox"/></td> <td data-bbox="1694 1131 1927 1179">سایر موارد</td> </tr> </table>	محصول باید کانال امن را فقط در صورت معتبر بودن گواهی نامه سرور برقرار سازد؛ بنابراین اگر گواهی نامه سرور غیرمعتبر به نظر رسید، محصول باید بر اساس موارد زیر رفتار نماید.	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.	<input type="checkbox"/>	ارتباط را برقرار نکند	<input type="checkbox"/>	برای برقراری ارتباط درخواست مجوز کند	<input type="checkbox"/>	سایر موارد	۳									
محصول باید کانال امن را فقط در صورت معتبر بودن گواهی نامه سرور برقرار سازد؛ بنابراین اگر گواهی نامه سرور غیرمعتبر به نظر رسید، محصول باید بر اساس موارد زیر رفتار نماید.	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.																			
<input type="checkbox"/>		ارتباط را برقرار نکند																		
<input type="checkbox"/>		برای برقراری ارتباط درخواست مجوز کند																		
<input type="checkbox"/>	سایر موارد																			
	<input type="checkbox"/>	<table border="1"> <tr> <td data-bbox="909 1179 1694 1292">محصول باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید.</td> <td data-bbox="1694 1179 1927 1380" rowspan="2"></td> </tr> <tr> <td data-bbox="909 1292 1694 1380"><input type="checkbox"/></td> <td data-bbox="1694 1292 1927 1380">Supported Elliptic Curves Extension را ارائه نکند.</td> </tr> </table>	محصول باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید.		<input type="checkbox"/>	Supported Elliptic Curves Extension را ارائه نکند.	۴													
محصول باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید.																				
<input type="checkbox"/>		Supported Elliptic Curves Extension را ارائه نکند.																		



		<input type="checkbox"/> Supported Elliptic Curves Extension را به همراه NIST Curve های secp256r1 یا secp384r1 یا secp521r1 ارائه نماید.	در صورت که محصول از منحنی استفاده می‌نماید، طول کلید باید مشخص گردد.
--	--	---	---

۳-۳- پروتکل TLS Server

توضیحات	پروتکل TLS Server		شماره الزام																							
	<input checked="" type="checkbox"/>	<p>محصول باید (RFC 5246) TLS 1.2 را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.</p> <table border="1" data-bbox="909 553 1696 1442"> <tr> <td data-bbox="909 553 951 1442" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="951 553 1696 638">                     TLS_RSA_WITH_AES_256_CBC_SHA                      مطابق با RFC 3268                 </td> <td data-bbox="1696 553 1927 1442" rowspan="12">                     مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.                 </td> </tr> <tr> <td data-bbox="909 638 951 1442" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="951 638 1696 722">                     TLS_DHE_RSA_WITH_AES_128_CBC_SHA                      مطابق با RFC 3268                 </td> </tr> <tr> <td data-bbox="909 722 951 1442" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="951 722 1696 807">                     TLS_DHE_RSA_WITH_AES_256_CBC_SHA                      مطابق با RFC 3268                 </td> </tr> <tr> <td data-bbox="909 807 951 1442" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="951 807 1696 891">                     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                      مطابق با RFC 4492                 </td> </tr> <tr> <td data-bbox="909 891 951 1442" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="951 891 1696 976">                     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                      مطابق با RFC 4492                 </td> </tr> <tr> <td data-bbox="909 976 951 1442" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="951 976 1696 1060">                     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                      مطابق با RFC 4492                 </td> </tr> <tr> <td data-bbox="909 1060 951 1442" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="951 1060 1696 1144">                     TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA                      مطابق با RFC 4492                 </td> </tr> <tr> <td data-bbox="909 1144 951 1442" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="951 1144 1696 1229">                     TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA                      مطابق با RFC 4492                 </td> </tr> <tr> <td data-bbox="909 1229 951 1442" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="951 1229 1696 1313">                     TLS_RSA_WITH_AES_128_CBC_SHA256                      مطابق با RFC 5246                 </td> </tr> <tr> <td data-bbox="909 1313 951 1442" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="951 1313 1696 1398">                     TLS_RSA_WITH_AES_256_CBC_SHA256                      مطابق با RFC 5246                 </td> </tr> <tr> <td data-bbox="909 1398 951 1442" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="951 1398 1696 1442">                     TLS_DHE_RSA_WITH_AES_128_CBC_SHA256                 </td> </tr> </table>	<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	<input checked="" type="checkbox"/>	TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246	<input checked="" type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	۱
<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.																								
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268																									
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268																									
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492																									
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492																									
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492																									
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492																									
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492																									
<input checked="" type="checkbox"/>	TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246																									
<input checked="" type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246																									
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256																									

		<p>مطابق با RFC 5246</p> <p><input type="checkbox"/> TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246</p> <p><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289</p> <p><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289</p> <p><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289</p> <p><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289</p> <p><input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289</p> <p><input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289</p>		
	<p><input checked="" type="checkbox"/></p>	<p>محصول باید اتصال‌های کاربرانی که درخواست TLS1.1 و TLS1.0، SSL3.0، SSL2.0، SSL1.0 دارند را رد نماید.</p>		۲
<p>طول کلید ۲۰۴۸ می باشد</p>	<p><input checked="" type="checkbox"/></p>	<p>محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.</p> <p><input checked="" type="checkbox"/> استفاده از RSA با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ یا ۴۰۹۶ بیت</p> <p><input type="checkbox"/> پارامترهای ECDH با استفاده از NIST Curve های secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگر</p> <p><input type="checkbox"/> پارامترهای دیفی-هلمن با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ بیت</p>	<p>در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.</p>	۳

## 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.	<input type="checkbox"/> محصول به عنوان کلاینت یک محصول دیگر نمی باشد و به عنوان سرور کلاینت های خود را احراز هویت نمی کند
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.	<input type="checkbox"/> محصول به عنوان کلاینت یک محصول دیگر نمی باشد و به عنوان سرور کلاینت های خود را احراز هویت نمی کند

۳-۵- اعتبارسنجی گواهی نامه

توضیحات	اعتبارسنجی گواهی نامه	شماره الزام
	<input checked="" type="checkbox"/> محصول باید گواهی نامه‌ها را بر اساس قوانین زیر تأیید کند.	۱
	<input checked="" type="checkbox"/> تأیید گواهی نامه RFC 5280 و تأیید مسیر گواهی نامه که از حداقل طول مسیر دو گواهی نامه پشتیبانی می‌کند.	
	<input checked="" type="checkbox"/> مسیر گواهی نامه باید با یک گواهی نامه CA امن پایان یابد.	
	<input checked="" type="checkbox"/> محصول باید برای تأیید مسیر یک گواهی نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی نامه‌های CA به حالت «TRUE» تنظیم شده است.	
	<input type="checkbox"/> پروتکل وضعیت گواهی نامه آنلاین (OCSP) مشخص شده در RFC 696	روش‌های تأیید وضعیت فسخ گواهی نامه
	<input type="checkbox"/> لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5280 بخش ۶.۳	
	<input type="checkbox"/> لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5759 بخش ۵	
	<input checked="" type="checkbox"/> هیچ روش فسخ دیگری	
	<input type="checkbox"/> گواهی نامه‌های 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.	قوانین تأیید بخش extendedKeyUsage
	<input checked="" type="checkbox"/> گواهی نامه‌های 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.	

	<input type="checkbox"/> گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف « Client Authentication » (با id-kp1 یا OID 1.3.6.1.5.5.7.3.2) را در بخش extendedKeyUsage خود داشته باشند.	
	<input type="checkbox"/> گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ OCSP باید « OCSP Signing » (با id-pk9 یا OID 1.3.6.1.5.5.7.3.9) را در بخش extendedKeyUsage خود داشته باشند.	
۲	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> محصول باید برای پشتیبانی احراز هویت برای موارد زیر از گواهی‌نامه‌های X509v3 تعریف شده در RFC 5280 استفاده کند.	
	<input checked="" type="checkbox"/> HTTPS	در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.
	<input type="checkbox"/> TLS	
	<input type="checkbox"/> SSH	
	<input type="checkbox"/> امضای کد برای بروزرسانی‌های نرم‌افزار سیستم	
	<input type="checkbox"/> امضای کد برای تأیید یکپارچگی	
	<input type="checkbox"/> سایر موارد	

۳-۶- پروتکل SSH

توضیحات	پروتکل SSH		شماره الزام																
	<input type="checkbox"/>	محصول باید پروتکل SSH را مطابق با RFCهای ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۵۶۵۶ و ۶۶۶۸ پیاده‌سازی نماید.	۱																
	<input type="checkbox"/>	<p>محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4252، از روش‌های احراز هویت زیر پشتیبانی نماید.</p> <table border="1" data-bbox="951 667 1696 769"> <tr> <td data-bbox="951 667 1024 716"><input type="checkbox"/></td> <td data-bbox="1024 667 1696 716">احراز هویت مبتنی بر کلید عمومی</td> </tr> <tr> <td data-bbox="951 716 1024 769"><input type="checkbox"/></td> <td data-bbox="1024 716 1696 769">احراز هویت مبتنی بر گذرواژه</td> </tr> </table>	<input type="checkbox"/>	احراز هویت مبتنی بر کلید عمومی	<input type="checkbox"/>	احراز هویت مبتنی بر گذرواژه	۲												
<input type="checkbox"/>	احراز هویت مبتنی بر کلید عمومی																		
<input type="checkbox"/>	احراز هویت مبتنی بر گذرواژه																		
	<input type="checkbox"/>	محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4253، بسته‌های بزرگتر از مقدار مشخصی (در بخش «توضیحات» ذکر شود) را کنار بگذارد.	۳																
	<input type="checkbox"/>	<p>محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های رمزنگاری زیر استفاده نماید.</p> <table border="1" data-bbox="951 997 1696 1364"> <tr><td data-bbox="951 997 1024 1045"><input type="checkbox"/></td><td data-bbox="1024 997 1696 1045">AES128-CBC</td></tr> <tr><td data-bbox="951 1045 1024 1094"><input type="checkbox"/></td><td data-bbox="1024 1045 1696 1094">AES192-CBC</td></tr> <tr><td data-bbox="951 1094 1024 1143"><input type="checkbox"/></td><td data-bbox="1024 1094 1696 1143">AES256-CBC</td></tr> <tr><td data-bbox="951 1143 1024 1192"><input type="checkbox"/></td><td data-bbox="1024 1143 1696 1192">AES128-CTR</td></tr> <tr><td data-bbox="951 1192 1024 1240"><input type="checkbox"/></td><td data-bbox="1024 1192 1696 1240">AES192-CTR</td></tr> <tr><td data-bbox="951 1240 1024 1289"><input type="checkbox"/></td><td data-bbox="1024 1240 1696 1289">AES256-CTR</td></tr> <tr><td data-bbox="951 1289 1024 1338"><input type="checkbox"/></td><td data-bbox="1024 1289 1696 1338">AEAD_AES_128_GCM</td></tr> <tr><td data-bbox="951 1338 1024 1364"><input type="checkbox"/></td><td data-bbox="1024 1338 1696 1364">AEAD_AES_256_GCM</td></tr> </table>	<input type="checkbox"/>	AES128-CBC	<input type="checkbox"/>	AES192-CBC	<input type="checkbox"/>	AES256-CBC	<input type="checkbox"/>	AES128-CTR	<input type="checkbox"/>	AES192-CTR	<input type="checkbox"/>	AES256-CTR	<input type="checkbox"/>	AEAD_AES_128_GCM	<input type="checkbox"/>	AEAD_AES_256_GCM	۴
<input type="checkbox"/>	AES128-CBC																		
<input type="checkbox"/>	AES192-CBC																		
<input type="checkbox"/>	AES256-CBC																		
<input type="checkbox"/>	AES128-CTR																		
<input type="checkbox"/>	AES192-CTR																		
<input type="checkbox"/>	AES256-CTR																		
<input type="checkbox"/>	AEAD_AES_128_GCM																		
<input type="checkbox"/>	AEAD_AES_256_GCM																		

	<input type="checkbox"/>	<p>محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های کلید عمومی زیر استفاده نماید.</p> <table border="1" data-bbox="909 264 1696 868"> <tr><td><input type="checkbox"/></td><td>ssh-ed25519</td></tr> <tr><td><input type="checkbox"/></td><td>ssh-ed448</td></tr> <tr><td><input type="checkbox"/></td><td>rsa-sha2-512</td></tr> <tr><td><input type="checkbox"/></td><td>rsa-sha2-256</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha2-nistp521</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha2-nistp384</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha2-nistp256</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ecdsa-sha2-nistp521</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ecdsa-sha2-nistp384</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ecdsa-sha2-nistp256</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-rsa2048-sha256</td></tr> <tr><td><input type="checkbox"/></td><td>ssh-rsa</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ssh-rsa</td></tr> </table>	<input type="checkbox"/>	ssh-ed25519	<input type="checkbox"/>	ssh-ed448	<input type="checkbox"/>	rsa-sha2-512	<input type="checkbox"/>	rsa-sha2-256	<input type="checkbox"/>	ecdsa-sha2-nistp521	<input type="checkbox"/>	ecdsa-sha2-nistp384	<input type="checkbox"/>	ecdsa-sha2-nistp256	<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp521	<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp384	<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp256	<input type="checkbox"/>	x509v3-rsa2048-sha256	<input type="checkbox"/>	ssh-rsa	<input type="checkbox"/>	x509v3-ssh-rsa	۵
<input type="checkbox"/>	ssh-ed25519																												
<input type="checkbox"/>	ssh-ed448																												
<input type="checkbox"/>	rsa-sha2-512																												
<input type="checkbox"/>	rsa-sha2-256																												
<input type="checkbox"/>	ecdsa-sha2-nistp521																												
<input type="checkbox"/>	ecdsa-sha2-nistp384																												
<input type="checkbox"/>	ecdsa-sha2-nistp256																												
<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp521																												
<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp384																												
<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp256																												
<input type="checkbox"/>	x509v3-rsa2048-sha256																												
<input type="checkbox"/>	ssh-rsa																												
<input type="checkbox"/>	x509v3-ssh-rsa																												
	<input type="checkbox"/>	<p>محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های MAC صحت داده‌های زیر استفاده نماید.</p> <table border="1" data-bbox="909 984 1696 1260"> <tr><td><input type="checkbox"/></td><td>AEAD_AES_256_GCM</td></tr> <tr><td><input type="checkbox"/></td><td>AEAD_AES_128_GCM</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha2-512</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha2-256</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha1-96</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha1</td></tr> </table>	<input type="checkbox"/>	AEAD_AES_256_GCM	<input type="checkbox"/>	AEAD_AES_128_GCM	<input type="checkbox"/>	hmac-sha2-512	<input type="checkbox"/>	hmac-sha2-256	<input type="checkbox"/>	hmac-sha1-96	<input type="checkbox"/>	hmac-sha1	۶														
<input type="checkbox"/>	AEAD_AES_256_GCM																												
<input type="checkbox"/>	AEAD_AES_128_GCM																												
<input type="checkbox"/>	hmac-sha2-512																												
<input type="checkbox"/>	hmac-sha2-256																												
<input type="checkbox"/>	hmac-sha1-96																												
<input type="checkbox"/>	hmac-sha1																												
	<input type="checkbox"/>	<p>محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های تبادل کلید زیر استفاده نماید.</p> <table border="1" data-bbox="909 1375 1696 1464"> <tr><td><input type="checkbox"/></td><td>curve25519-sha256</td></tr> <tr><td><input type="checkbox"/></td><td>curve448-sha512</td></tr> </table>	<input type="checkbox"/>	curve25519-sha256	<input type="checkbox"/>	curve448-sha512	۷																						
<input type="checkbox"/>	curve25519-sha256																												
<input type="checkbox"/>	curve448-sha512																												



	<input type="checkbox"/>	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	
	<input type="checkbox"/>	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 می‌گردد. در صورت پر شدن حد آستانه برای هر کدام از موارد ذکر شده، باید تجدید کلید صورت بگیرد.	۸
	<input type="checkbox"/>	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 (تشریح شده در RFC 4251 بخش ۱.۷) همراه می‌کند، استفاده می‌نماید.	۹