

به نام خدا

سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه

سامانه‌های هوشمند سپهر شریف

«سامانه نظارت، مدیریت تردد و ثبت تخلفات ترافیکی»

نسخه ۲.۰



آبان ۱۴۰۲

نسخه ۱.۷

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
۴	۱- معرفی محصول
۴	۱-۱- ویژگی‌های فنی محصول
۴	۲-۱- معماری محصول
۵	۲- الزامات امنیتی
۵	۱-۲- ممیزی امنیت (Log)
۹	۲-۲- رمزنگاری
۱۱	۳-۲- شناسایی و احراز هویت
۱۵	۴-۲- حفاظت از داده‌ی کاربری
۱۹	۵-۲- مدیریت امنیت
۲۲	۶-۲- حفاظت از توابع امنیتی محصول
۲۴	۷-۲- تخصیص منابع
۲۵	۸-۲- دسترسی به محصول
۲۷	۹-۲- کانال‌ها/مسیرهای مورد اعتماد
۲۸	۳- الزامات امنیتی مبتنی بر انتخاب
۲۸	۱-۳- پروتکل HTTPS
۲۹	۲-۳- پروتکل TLS Client
۳۲	۳-۳- پروتکل TLS Server
۳۵	۴-۳- پروتکل TLS مشترک کلاینت و سرور
۳۶	۵-۳- اعتبارسنجی گواهی‌نامه
۳۸	۳-۶- پروتکل SSH

۱- معرفی محصول

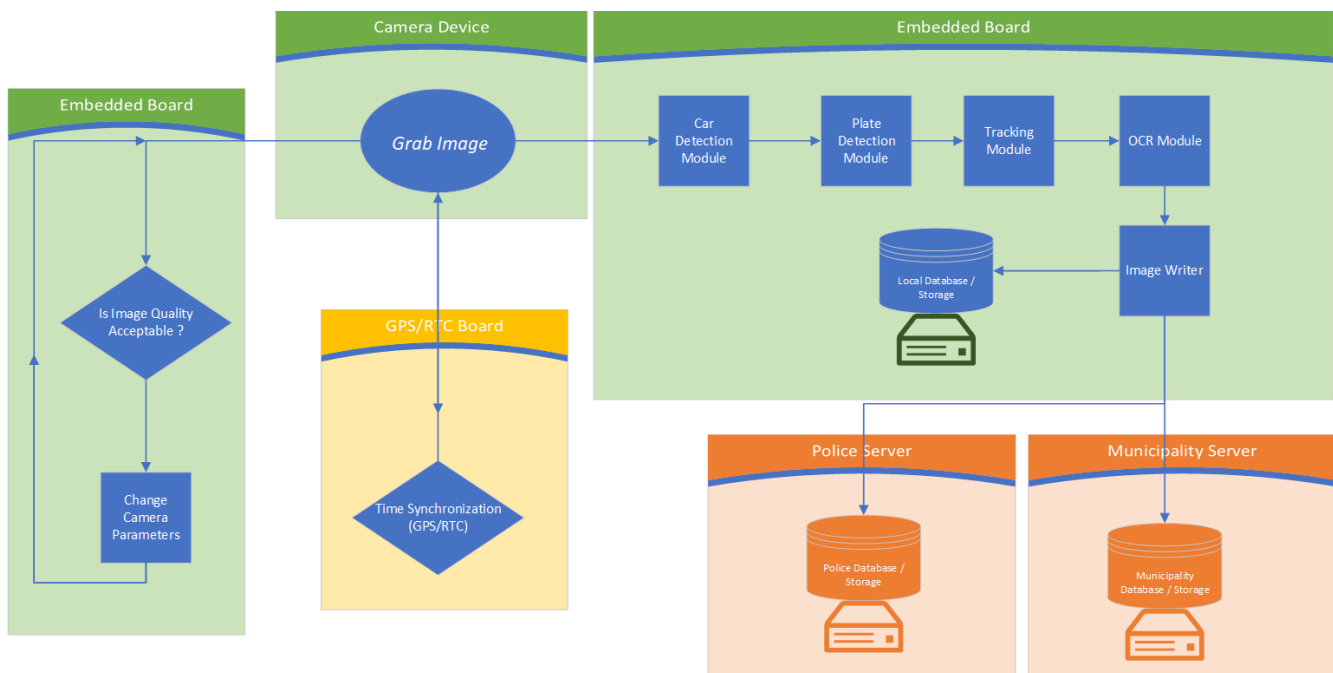
سامانه نظارت، مدیریت تردد و ثبت تخلفات ترافیکی با ارتباط با دوربین‌های نظارتی و یا ترافیکی و همچنین سایر تجهیزات ترافیکی و جانبی از قبیل رادار، رله، واچ داگ و... در کاربردهای نظارت، مدیریت تردد و ثبت تخلفات ترافیکی مورد استفاده قرار می‌گیرد.

۱-۱- ویژگی‌های فنی محصول

نسخه‌ی نرم‌افزار	۲.۰
مدل و نسخه سیستم‌عامل	۱۸,۰۴ Linux Ubuntu و بالاتر
مدل و نسخه وب‌سرور	۲,۴,۴۱ Apache و بالاتر
مدل و نسخه پایگاه داده	MySQL ^۸ و بالاتر
زبان برنامه‌نویسی	C++ , PHP, Html, CSS, JavaScript

۲-۱- معماری محصول

سامانه حاضر شامل هسته نرم‌افزاری است که با زبان C++ و استفاده از کتابخانه‌های استاندارد و متن باز حوزه پردازش تصویر و هوش مصنوعی و... می‌باشد که این هسته نرم‌افزاری با ارتباط گیری با دوربین‌ها از انواع مختلف صنعتی و IP Based در کاربری‌های مختلف ترافیکی و نظارتی اقدام به تشخیص خودرو، خوانش پلاک، مدیریت تردد، پایش و نظارت ترافیکی و همچنین تشخیص انواع پارامترهای ترافیکی جهت تشخیص اتوماتیک وقایع ترافیکی می‌نماید. که این بسته به ماژول‌های متصل شده به سامانه است. هسته نرم‌افزاری مذکور کلیه اطلاعات را در دیتابیس ثبت نموده و همچنین تنظیمات و پارامترهای موردنیاز را از دیتابیس فراخوانی می‌کند. هسته نرم‌افزاری از مدل‌های مختلف یادگیری ماشین استفاده می‌کند که در دسترس هسته قرار دارد. تنظیمات مرتبط و همچنین مشاهده وضعیت سیستم، گزارش گیری و استخراج پارامترها و نظارت‌های سطح بالا در بستر رابط کاربری تحت وب انجام می‌پذیرد. که این رابط کاربری از سمت بکند با زبان PHP توسعه داده شده است. معماری محصول در تصویر زیر توضیح داده شده است:



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.

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 ^۲ تولید کند (Log ثبت نماید).	۱
	<input checked="" type="checkbox"/> شروع و اتمام توابع	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.
	<input checked="" type="checkbox"/> تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها	
	<input checked="" type="checkbox"/> خواندن اطلاعات از ثبت‌نشان‌ها	
	<input checked="" type="checkbox"/> تمامی تغییرات در پیکربندی ثبت‌نشان‌ها	
	<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.	
	<input checked="" type="checkbox"/> تمام کاربردهای سازوکار احراز هویت	
	<input checked="" type="checkbox"/> نتایج نهایی عملیات احراز هویت	

^۱ Profile

^۲ Log

	<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 درخواست‌ها (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	
	<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	ویژگی‌هایی که در ثبت‌نشان‌ها وجود دارد مشخص شود.
	<input checked="" type="checkbox"/>	نوع رویداد	
	<input checked="" type="checkbox"/>	هویت ایجادکننده رویداد	
	<input checked="" type="checkbox"/>	نتیجه رویداد	

	<input checked="" type="checkbox"/>	آدرس IP ایجادکننده رویداد	
	<input type="checkbox"/>	سایر موارد	
۳	<input checked="" type="checkbox"/>	محصول باید ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید.	
۴	<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
	<input checked="" type="checkbox"/>	نبود بخش‌های نامرتب	ثبت‌نشان‌ها وجود
	<input checked="" type="checkbox"/>	وجود داده معتبر و مناسب در هر بخش	دارند، مشخص شوند.
۵	<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 type="checkbox"/>	نوع حساب کاربری	
	<input checked="" type="checkbox"/>	تاریخ/زمان	
	<input type="checkbox"/>	روش اتصال کاربر	
	<input checked="" type="checkbox"/>	نوع رخداد	
	<input checked="" type="checkbox"/>	مکان رویداد	
	<input type="checkbox"/>	سایر موارد	
۶	<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
	<input type="checkbox"/>	پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	مشخص شود. (وجود)
	<input checked="" type="checkbox"/>	فقط خواندنی کردن ثبت‌نشان‌ها در محصول	یک مورد لازم و کافی
	<input type="checkbox"/>	سایر موارد	(است)

	<input checked="" type="checkbox"/>	<p>۷ محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.</p>	
		<input type="checkbox"/>	<p>روش‌های اطلاع‌رسانی استفاده از یک کانال ارتباطی</p>
		<input type="checkbox"/>	<p>مشخص شود (وجود ارسال پیام)</p>
		<input checked="" type="checkbox"/>	<p>یک مورد لازم و کافی از طریق واسط کاربر مجاز</p>
		<input type="checkbox"/>	<p>سایر موارد (است)</p>
	<input checked="" type="checkbox"/>	<p>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.</p>	
		<input type="checkbox"/>	<p>رویکردهای مورد نادیده گرفتن ثبت‌نشان‌ها</p>
		<input type="checkbox"/>	<p>استفاده در محصول ذخیره‌سازی محدود ثبت‌نشان‌ها (آنهايي که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند) (وجود)</p>
		<input checked="" type="checkbox"/>	<p>یک مورد لازم و کافی بازنویسی روی قدیمی‌ترین ثبت‌نشان‌های ذخیره‌شده</p>
		<input type="checkbox"/>	<p>سایر موارد (است)</p>

۲-۲- رمزنگاری

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 خصوصی) 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	<input checked="" type="checkbox"/> محصول باید قابلیت رمزنگاری یا واحد رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ۳-۱۸۰۳۳ ISO) با توجه به موارد زیر انجام دهد.		
		<input type="checkbox"/> مد عملیاتی CBC و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در (NIST SP ۸۰۰-۳۸A)	مد عملیاتی که الگوریتم از آن استفاده می‌کند را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)
		<input checked="" type="checkbox"/> مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در (NIST SP ۸۰۰-۳۸D)	
		<input type="checkbox"/> مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در (ISO ۱۰۱۱۶)	
۲	<input checked="" type="checkbox"/> 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 ۱۰۱۱۸-۳:۲۰۰۴ استفاده نماید.		
		<input type="checkbox"/> الگوریتم SHA-۱ با اندازه خلاصه پیام ۱۶۰ بیت	الگوریتم و اندازه خلاصه پیام مورد استفاده را
		<input checked="" type="checkbox"/> الگوریتم SHA-۲۵۶ با اندازه خلاصه پیام ۲۵۶ بیت	

^۳ Modules

	<input checked="" type="checkbox"/>	الگوریتم SHA-۳۸۴ با اندازه خلاصه پیام ۳۸۴ بیت	انتخاب نمایید. (وجود یک مورد لازم و کافی است.)
	<input type="checkbox"/>	الگوریتم SHA-۵۱۲ با اندازه خلاصه پیام ۵۱۲ بیت	
	<input checked="" 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
	<input type="checkbox"/>	نابودی با استفاده از یک واسط مشخص	یک مورد لازم و کافی
	<input checked="" type="checkbox"/>	از طریق توابع امنیتی محصول	است)
	<input type="checkbox"/>	سایر موارد	
	<input checked="" 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 checked="" type="checkbox"/>	الگوریتم‌های امضای دیجیتال RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت و بزرگتر (بر اساس ۱۸۶-۴ FIPS PUB، استاندارد امضای دیجیتال (DSS) بخش ۵.۵، الگوی امضای RSASSA-PSS نسخه ۱٫۲٫۱ PKCS #۱ و یا RSASSA-ISO/IEC ۹۷۹۶-۲؛ PKCS۱۷_۵، الگوی امضای دیجیتال ۲ و یا الگوی امضای دیجیتال ۳)	الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید.
	<input type="checkbox"/>	الگوریتم‌های امضای دیجیتال ECDSA با کلیدهای رمزنگاری ۲۵۶ بیت یا بزرگتر (بر اساس ۱۴۸۸۸-۳ ISO/IEC بخش ۶.۴، استاندارد امضای دیجیتال (DSS) بخش ۶ و پیوست D، با استفاده از منحنی P-۲۵۶ یا P-۳۸۴ یا P-۵۲۱)	(وجود یک مورد لازم و کافی است)

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						
<p>در صورت ۵ بار ورود ناموفق کاربر مسدود می‌شود</p>	<input checked="" type="checkbox"/>	<p>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.</p> <table border="1" data-bbox="961 597 1948 846"> <tr> <td data-bbox="961 597 1713 721"> <input checked="" type="checkbox"/> </td> <td data-bbox="1713 597 1948 721"> <p>مقدار یا یازهی مورد استفاده در هر یک باید مشخص گردد. (وجود یک مورد لازم و کافی است)</p> </td> </tr> <tr> <td data-bbox="961 721 1713 846"> <input type="checkbox"/> </td> <td data-bbox="1713 721 1948 846"> <p>یک عدد مثبت قابل تنظیم توسط مدیر</p> </td> </tr> </table>	<input checked="" type="checkbox"/>	<p>مقدار یا یازهی مورد استفاده در هر یک باید مشخص گردد. (وجود یک مورد لازم و کافی است)</p>	<input type="checkbox"/>	<p>یک عدد مثبت قابل تنظیم توسط مدیر</p>	۱		
<input checked="" type="checkbox"/>	<p>مقدار یا یازهی مورد استفاده در هر یک باید مشخص گردد. (وجود یک مورد لازم و کافی است)</p>								
<input type="checkbox"/>	<p>یک عدد مثبت قابل تنظیم توسط مدیر</p>								
<p>مسدود شدن حساب کاربر به مدت ۵ دقیقه</p>	<input checked="" type="checkbox"/>	<p>محصول باید هنگامی 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="961 959 1948 1458"> <tr> <td data-bbox="961 959 1713 1122"> <input type="checkbox"/> </td> <td data-bbox="1713 959 1948 1122"> <p>غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)</p> </td> </tr> <tr> <td data-bbox="961 1122 1713 1284"> <input checked="" type="checkbox"/> </td> <td data-bbox="1713 1122 1948 1284"> <p>غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)</p> </td> </tr> <tr> <td data-bbox="961 1284 1713 1458"> <input type="checkbox"/> </td> <td data-bbox="1713 1284 1948 1458"> <p>استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت «توضیحات» بیان شود)</p> </td> </tr> </table>	<input type="checkbox"/>	<p>غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)</p>	<input checked="" type="checkbox"/>	<p>غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)</p>	<input type="checkbox"/>	<p>استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت «توضیحات» بیان شود)</p>	۲
<input type="checkbox"/>	<p>غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)</p>								
<input checked="" type="checkbox"/>	<p>غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)</p>								
<input type="checkbox"/>	<p>استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت «توضیحات» بیان شود)</p>								

	<input type="checkbox"/>	سایر موارد	برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست.													
۳	<input checked="" type="checkbox"/>	محصول باید برای هر کاربر، ویژگی‌های امنیتی را که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت می‌باشند، نگهداری نماید. <table border="1" data-bbox="961 462 1711 766"> <tr> <td data-bbox="961 462 1045 511" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1045 462 1711 511">شناسه کاربر</td> <td data-bbox="1711 462 2030 766" rowspan="6"> ویژگی‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند. </td> </tr> <tr> <td data-bbox="961 511 1045 560" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1045 511 1711 560">روش احراز هویت مورد استفاده</td> </tr> <tr> <td data-bbox="961 560 1045 609" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1045 560 1711 609">داده احراز هویت</td> </tr> <tr> <td data-bbox="961 609 1045 657" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1045 609 1711 657">وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)</td> </tr> <tr> <td data-bbox="961 657 1045 706" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1045 657 1711 706">نقش کاربر</td> </tr> <tr> <td data-bbox="961 706 1045 766" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="1045 706 1711 766">سایر موارد</td> </tr> </table>		<input checked="" type="checkbox"/>	شناسه کاربر	ویژگی‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.	<input checked="" type="checkbox"/>	روش احراز هویت مورد استفاده	<input checked="" type="checkbox"/>	داده احراز هویت	<input checked="" type="checkbox"/>	وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)	<input checked="" type="checkbox"/>	نقش کاربر	<input type="checkbox"/>	سایر موارد
<input checked="" type="checkbox"/>	شناسه کاربر	ویژگی‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.														
<input checked="" type="checkbox"/>	روش احراز هویت مورد استفاده															
<input checked="" type="checkbox"/>	داده احراز هویت															
<input checked="" type="checkbox"/>	وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)															
<input checked="" type="checkbox"/>	نقش کاربر															
<input type="checkbox"/>	سایر موارد															
۴	<input checked="" type="checkbox"/>	محصول باید قابلیت مدیریت گذرواژه را فراهم آورد. <table border="1" data-bbox="961 885 1711 1230"> <tr> <td data-bbox="961 885 1045 933" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1045 885 1711 933">استفاده از حروف کوچک</td> <td data-bbox="1711 885 2030 1230" rowspan="6"> موارد نیاز که باید در تعریف گذرواژه استفاده شوند. </td> </tr> <tr> <td data-bbox="961 933 1045 982" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1045 933 1711 982">استفاده از حروف بزرگ</td> </tr> <tr> <td data-bbox="961 982 1045 1031" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1045 982 1711 1031">استفاده از اعداد</td> </tr> <tr> <td data-bbox="961 1031 1045 1079" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1045 1031 1711 1079">استفاده از کاراکترهای خاص (@, #, \$, %, ^, &, * و ...)</td> </tr> <tr> <td data-bbox="961 1079 1045 1128" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1045 1079 1711 1128">حداقل طول ۸ یا بیشتر (قابل تنظیم)</td> </tr> <tr> <td data-bbox="961 1128 1045 1230" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="1045 1128 1711 1230">سایر موارد</td> </tr> </table>		<input checked="" type="checkbox"/>	استفاده از حروف کوچک	موارد نیاز که باید در تعریف گذرواژه استفاده شوند.	<input checked="" type="checkbox"/>	استفاده از حروف بزرگ	<input checked="" type="checkbox"/>	استفاده از اعداد	<input checked="" type="checkbox"/>	استفاده از کاراکترهای خاص (@, #, \$, %, ^, &, * و ...)	<input checked="" type="checkbox"/>	حداقل طول ۸ یا بیشتر (قابل تنظیم)	<input type="checkbox"/>	سایر موارد
<input checked="" type="checkbox"/>	استفاده از حروف کوچک	موارد نیاز که باید در تعریف گذرواژه استفاده شوند.														
<input checked="" type="checkbox"/>	استفاده از حروف بزرگ															
<input checked="" type="checkbox"/>	استفاده از اعداد															
<input checked="" type="checkbox"/>	استفاده از کاراکترهای خاص (@, #, \$, %, ^, &, * و ...)															
<input checked="" type="checkbox"/>	حداقل طول ۸ یا بیشتر (قابل تنظیم)															
<input type="checkbox"/>	سایر موارد															
۵	<input checked="" type="checkbox"/>	محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید. <table border="1" data-bbox="961 1347 1711 1445"> <tr> <td data-bbox="961 1347 1045 1396" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="1045 1347 1711 1396">مشاهده راهنمای نحوه ورود به سیستم</td> <td data-bbox="1711 1347 2030 1445" rowspan="2"> اقدامات عمومی که کاربر می‌تواند قبل از </td> </tr> <tr> <td data-bbox="961 1396 1045 1445" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="1045 1396 1711 1445">بازیابی گذرواژه</td> </tr> </table>		<input type="checkbox"/>	مشاهده راهنمای نحوه ورود به سیستم	اقدامات عمومی که کاربر می‌تواند قبل از	<input type="checkbox"/>	بازیابی گذرواژه								
<input type="checkbox"/>	مشاهده راهنمای نحوه ورود به سیستم	اقدامات عمومی که کاربر می‌تواند قبل از														
<input type="checkbox"/>	بازیابی گذرواژه															

	<input checked="" type="checkbox"/>	هیچ اقدامی	احراز هویت انجام دهد،
	<input type="checkbox"/>	سایر موارد	انتخاب شود.
۶	<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.
	<input type="checkbox"/>	امضای دیجیتال	
	<input type="checkbox"/>	سامانه‌های احراز هویت مرکزی (مانند Active Directory و ...)	
	<input type="checkbox"/>	OTP یا توکن	
	<input checked="" type="checkbox"/>	احراز هویت دو فاکتوری	
	<input type="checkbox"/>	سایر موارد	
۷	<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	
۸	<input checked="" type="checkbox"/>	محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.	

<p>تعداد ۳ نشست فعال همزمان مجاز می‌باشد.</p>	<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</p>
	<input checked="" type="checkbox"/>	<p>بروزرسانی اطلاعات پیشینه احراز هویت</p>	<p>در «سایر موارد» بیان</p>
	<input type="checkbox"/>	<p>سایر موارد</p>	<p>می‌شوند).</p>
	<input checked="" type="checkbox"/>	<p>محصول باید بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید.</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،</p>
	<input type="checkbox"/>	<p>سایر موارد</p>	<p>اعمال می‌شود، مشخص گردد.</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 می‌شوند، مشخص
	<input type="checkbox"/>	سایر موارد	گردد.
	<input checked="" type="checkbox"/>	سوابق، مستندات و فراداده	موجودیت‌های غیرفعال
	<input checked="" type="checkbox"/>	داده متعلق به کاربران	که خط‌مشی‌های کنترل دسترسی در
	<input checked="" type="checkbox"/>	داده احراز هویت	مورد آنها اعمال می‌شوند، مشخص
	<input type="checkbox"/>	سایر موارد	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 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 تعریف می‌شوند، انتخاب گردد.
	<input type="checkbox"/>	اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید بر اساس قاعده‌ای عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نماید (این قاعده می‌تواند بدین شکل باشد که در فهرست کنترل دسترسی، سابقه (رکوردی) وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده 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 checked="" type="checkbox"/>	عبور تعداد نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف شده	قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).
	<input 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.	
محصول هیچ داده‌ای از کاربر دریافت نمی‌کند	<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.	

	<input type="checkbox"/>	نوع داده	ویژگی‌های امنیتی مرتبط با داده کاربری
	<input type="checkbox"/>	حجم و اندازه	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).
	<input type="checkbox"/>	فرمت	Import
	<input type="checkbox"/>	تعداد دفعات Import	
	<input type="checkbox"/>	سایر موارد	
پروتکل مورد استفاده https میباشد.	<input checked="" type="checkbox"/>	<p>۷ 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>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.</p>	
پسوندهای مجاز: xlsx , html, jpeg	<input checked="" type="checkbox"/>	نوع داده	ویژگی‌های امنیتی مرتبط با داده کاربری
با محدودیت ۱۰۰ مگابایت برای csv و ۸۰۰ کیلوبایت برای jpeg	<input checked="" type="checkbox"/>	حجم و اندازه	که در هنگام خروج آن از محصول استفاده می‌شوند، مشخص شوند
پسوندهای مجاز: xlsx , html, jpeg , .zip	<input checked="" type="checkbox"/>	فرمت	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	<p>۹ محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.</p>	

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

۲-۵- مدیریت امنیت

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

توضیحات	شماره الزام	رده مدیریت امنیت														
	<p>۱</p> <p>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="919 651 1948 852"> <tr> <td data-bbox="919 651 961 695"><input checked="" type="checkbox"/></td> <td data-bbox="961 651 1711 695">تعیین و تغییر رفتار</td> <td data-bbox="1711 651 1948 695">فعالیت‌های مدیریتی</td> </tr> <tr> <td data-bbox="919 695 961 738"><input checked="" type="checkbox"/></td> <td data-bbox="961 695 1711 738">غیرفعال نمودن</td> <td data-bbox="1711 695 1948 738">که محصول پشتیبانی</td> </tr> <tr> <td data-bbox="919 738 961 782"><input checked="" type="checkbox"/></td> <td data-bbox="961 738 1711 782">فعال نمودن</td> <td data-bbox="1711 738 1948 782">می‌کند، مشخص شوند.</td> </tr> <tr> <td data-bbox="919 782 961 852"><input type="checkbox"/></td> <td data-bbox="961 782 1711 852">سایر موارد</td> <td data-bbox="1711 782 1948 852"></td> </tr> </table>	<input checked="" 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				
<input checked="" 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>۲</p> <p>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="919 1015 1948 1265"> <tr> <td data-bbox="919 1015 961 1058"><input type="checkbox"/></td> <td data-bbox="961 1015 1711 1058">پرس‌وجو</td> <td data-bbox="1711 1015 1948 1058">عملیات بر روی</td> </tr> <tr> <td data-bbox="919 1058 961 1102"><input checked="" type="checkbox"/></td> <td data-bbox="961 1058 1711 1102">تغییر</td> <td data-bbox="1711 1058 1948 1102">ویژگی‌های امنیتی که</td> </tr> <tr> <td data-bbox="919 1102 961 1146"><input checked="" type="checkbox"/></td> <td data-bbox="961 1102 1711 1146">حذف</td> <td data-bbox="1711 1102 1948 1146">در محصول پشتیبانی</td> </tr> <tr> <td data-bbox="919 1146 961 1190"><input checked="" type="checkbox"/></td> <td data-bbox="961 1146 1711 1190">تغییر پیش‌فرض</td> <td data-bbox="1711 1146 1948 1190">می‌شوند، مشخص</td> </tr> <tr> <td data-bbox="919 1190 961 1265"><input type="checkbox"/></td> <td data-bbox="961 1190 1711 1265">سایر موارد</td> <td data-bbox="1711 1190 1948 1265">گردد.</td> </tr> </table>	<input type="checkbox"/>	پرس‌وجو	عملیات بر روی	<input checked="" type="checkbox"/>	تغییر	ویژگی‌های امنیتی که	<input checked="" type="checkbox"/>	حذف	در محصول پشتیبانی	<input checked="" type="checkbox"/>	تغییر پیش‌فرض	می‌شوند، مشخص	<input type="checkbox"/>	سایر موارد	گردد.
<input type="checkbox"/>	پرس‌وجو	عملیات بر روی														
<input checked="" type="checkbox"/>	تغییر	ویژگی‌های امنیتی که														
<input checked="" type="checkbox"/>	حذف	در محصول پشتیبانی														
<input checked="" type="checkbox"/>	تغییر پیش‌فرض	می‌شوند، مشخص														
<input type="checkbox"/>	سایر موارد	گردد.														
	<p>۳</p> <p>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="919 1382 1948 1424"> <tr> <td data-bbox="919 1382 961 1424"><input checked="" type="checkbox"/></td> <td data-bbox="961 1382 1711 1424">تغییر پیش‌فرض</td> <td data-bbox="1711 1382 1948 1424"></td> </tr> </table>	<input checked="" type="checkbox"/>	تغییر پیش‌فرض													
<input checked="" type="checkbox"/>	تغییر پیش‌فرض															

	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	حذف نمودن پرس و جو مقداردهی ایجاد مشاهده سایر موارد	عملیات بر روی داده‌های محصول که در محصول پشتیبانی می‌شوند، مشخص شود.
مدیریت این موضوع با سیستم عامل و دیتابیس است.	<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 پیگیری 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 پیگیری 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"/>	<p>۱. مدیریت سازوکارهای احراز هویت</p> <p>۲. مدیریت قوانین مرتبط با احراز هویت</p>												
	<input checked="" type="checkbox"/>	<p>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.</p>												
	<input checked="" type="checkbox"/>	<p>مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.</p>												
	<input checked="" type="checkbox"/>	<p>مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول</p>												
	<input checked="" type="checkbox"/>	<p>مدیریت نقش‌ها در محصول</p>												
	<input checked="" type="checkbox"/>	<p>مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر</p>												
	<input checked="" type="checkbox"/>	<p>مدیریت شرایط آغاز نشست توسط مدیر مجاز</p>												
	<input checked="" type="checkbox"/>	<p>۱. تعیین زمان غیرفعال بودن برای یک کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد.</p> <p>۲. تعیین زمان پیش‌فرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.</p>												
	<input checked="" type="checkbox"/>	<p>۵ محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد.</p> <table border="1" data-bbox="961 1015 2030 1214"> <tr> <td data-bbox="961 1015 1711 1068"><input checked="" type="checkbox"/></td> <td data-bbox="1711 1015 2030 1068">مدیر سیستم</td> <td data-bbox="961 1015 1711 1068">نقش‌هایی که در</td> </tr> <tr> <td data-bbox="961 1068 1711 1122"><input checked="" type="checkbox"/></td> <td data-bbox="1711 1068 2030 1122">کاربر پیشرفته</td> <td data-bbox="961 1068 1711 1122">محصول پشتیبانی</td> </tr> <tr> <td data-bbox="961 1122 1711 1175"><input checked="" type="checkbox"/></td> <td data-bbox="1711 1122 2030 1175">کاربر عادی</td> <td data-bbox="961 1122 1711 1175">می‌شوند، مشخص</td> </tr> <tr> <td data-bbox="961 1175 1711 1214"><input type="checkbox"/></td> <td data-bbox="1711 1175 2030 1214">سایر موارد</td> <td data-bbox="961 1175 1711 1214">گردد.</td> </tr> </table>	<input checked="" type="checkbox"/>	مدیر سیستم	نقش‌هایی که در	<input checked="" type="checkbox"/>	کاربر پیشرفته	محصول پشتیبانی	<input checked="" type="checkbox"/>	کاربر عادی	می‌شوند، مشخص	<input type="checkbox"/>	سایر موارد	گردد.
<input checked="" type="checkbox"/>	مدیر سیستم	نقش‌هایی که در												
<input checked="" type="checkbox"/>	کاربر پیشرفته	محصول پشتیبانی												
<input checked="" type="checkbox"/>	کاربر عادی	می‌شوند، مشخص												
<input type="checkbox"/>	سایر موارد	گردد.												
	<input checked="" type="checkbox"/>	<p>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.</p>												

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
	<input checked="" type="checkbox"/>	خرابی‌های نرم‌افزاری	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول
	<input checked="" type="checkbox"/>	خرابی‌های سخت‌افزاری	حفظ می‌شود، مشخص گردد.
	<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.	
از محصولات دیگر استفاده نمی‌کند.	<input type="checkbox"/>	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.	
	<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.

<p>هر سه قابلیت موجود است. در مواردی که سیاست کارفرما اجازه بدهد زمان از طریق اینترنت تنظیم میشود و در صورت وجود ntp سرور، زمان از این طریق تنظیم میگردد. همچنین با توجه به وجود باتری بکاپ امکان دریافت زمان معتبر از سیستم عامل موجود می‌باشد.</p>	<p>۴ محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی^۴ معتبر را تولید یا از آن‌ها استفاده نماید.</p>												
	<table border="1"> <tr> <td data-bbox="877 349 961 430"><input checked="" type="checkbox"/></td> <td data-bbox="961 349 1711 430">گرفتن مهرهای زمانی از سرور NTP</td> <td data-bbox="1711 349 2028 430">روش‌های ایجاد مهرهای زمانی معتبر</td> </tr> </table>	<input checked="" type="checkbox"/>	گرفتن مهرهای زمانی از سرور NTP	روش‌های ایجاد مهرهای زمانی معتبر									
<input checked="" type="checkbox"/>	گرفتن مهرهای زمانی از سرور NTP	روش‌های ایجاد مهرهای زمانی معتبر											
	<table border="1"> <tr> <td data-bbox="877 430 961 511"><input checked="" type="checkbox"/></td> <td data-bbox="961 430 1711 511">تنظیم مهرهای زمانی از طریق اینترنت</td> <td data-bbox="1711 430 2028 511">انتخاب شود. (دیگر روشهای موجود در محصول، در قسمت «سایر موارد» بیان شود).</td> </tr> </table>	<input checked="" type="checkbox"/>	تنظیم مهرهای زمانی از طریق اینترنت	انتخاب شود. (دیگر روشهای موجود در محصول، در قسمت «سایر موارد» بیان شود).									
<input checked="" type="checkbox"/>	تنظیم مهرهای زمانی از طریق اینترنت	انتخاب شود. (دیگر روشهای موجود در محصول، در قسمت «سایر موارد» بیان شود).											
	<table border="1"> <tr> <td data-bbox="877 511 961 609"><input checked="" type="checkbox"/></td> <td data-bbox="961 511 1711 609">تنظیم مهرهای زمانی به صورت پیش فرض (معتبر و عدم امکان دستکاری غیرمجاز)</td> <td data-bbox="1711 511 2028 609"></td> </tr> </table>	<input checked="" type="checkbox"/>	تنظیم مهرهای زمانی به صورت پیش فرض (معتبر و عدم امکان دستکاری غیرمجاز)										
<input checked="" type="checkbox"/>	تنظیم مهرهای زمانی به صورت پیش فرض (معتبر و عدم امکان دستکاری غیرمجاز)												
	<table border="1"> <tr> <td data-bbox="877 609 961 690"><input type="checkbox"/></td> <td data-bbox="961 609 1711 690">سایر موارد</td> <td data-bbox="1711 609 2028 690"></td> </tr> </table>	<input type="checkbox"/>	سایر موارد										
<input type="checkbox"/>	سایر موارد												
	<p>۵ محصول باید امکان بروزرسانی نرم افزار و میان افزار محصول را برای مدیر سیستم فراهم نماید.</p> <table border="1"> <tr> <td data-bbox="877 690 961 812"><input checked="" type="checkbox"/></td> <td data-bbox="961 690 1711 812">بروزرسانی دستی</td> <td data-bbox="1711 690 2028 812">روش بروزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).</td> </tr> <tr> <td data-bbox="877 812 961 868"><input type="checkbox"/></td> <td data-bbox="961 812 1711 868">جستجوی خودکار بروزرسانی‌ها</td> <td data-bbox="1711 812 2028 868"></td> </tr> <tr> <td data-bbox="877 868 961 925"><input type="checkbox"/></td> <td data-bbox="961 868 1711 925">بروزرسانی‌های خودکار</td> <td data-bbox="1711 868 2028 925"></td> </tr> <tr> <td data-bbox="877 925 961 1055"><input type="checkbox"/></td> <td data-bbox="961 925 1711 1055">بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی</td> <td data-bbox="1711 925 2028 1055"></td> </tr> </table>	<input checked="" type="checkbox"/>	بروزرسانی دستی	روش بروزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).	<input type="checkbox"/>	جستجوی خودکار بروزرسانی‌ها		<input type="checkbox"/>	بروزرسانی‌های خودکار		<input type="checkbox"/>	بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی	
<input checked="" type="checkbox"/>	بروزرسانی دستی	روش بروزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).											
<input type="checkbox"/>	جستجوی خودکار بروزرسانی‌ها												
<input type="checkbox"/>	بروزرسانی‌های خودکار												
<input type="checkbox"/>	بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی												
	<p>۶ در صورت استفاده از بروزرسانی به روش خودکار، محصول باید پیش از نصب بروزرسانی‌های نرم افزاری و میان افزاری، امکان احراز اصالت میان افزار یا نرم افزار را فراهم نماید.</p> <table border="1"> <tr> <td data-bbox="877 1055 961 1287"><input type="checkbox"/></td> <td data-bbox="961 1055 1711 1287">امضای دیجیتال</td> <td data-bbox="1711 1055 2028 1287">سازوکار مورد استفاده برای صحت‌سنجی</td> </tr> </table>	<input type="checkbox"/>	امضای دیجیتال	سازوکار مورد استفاده برای صحت‌سنجی									
<input type="checkbox"/>	امضای دیجیتال	سازوکار مورد استفاده برای صحت‌سنجی											

^۴ Time stamp

	□		(اصالت سنجی) به روزرسانی‌ها انتخاب گردد. 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.

توضیحات	رده تخصیص منابع	شماره الزام
	<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"/>
		انتخاب یک مورد لازم و کافی است.
		روز
		زمان
	سایر موارد	<input type="checkbox"/>
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"/>
		انتخاب یک مورد لازم و کافی است.
		روز
		زمان
	سایر موارد	<input type="checkbox"/>

	<input checked="" type="checkbox"/>	<p>۶ محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.</p>	۶
	<input checked="" type="checkbox"/>	<p>۷ محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.</p>	۷
	<input checked="" type="checkbox"/>	مکان	پارامترهای موجود برای
	<input 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	شماره الزام	رده کانال‌ها/مسیرهای مورد اعتماد								
	<p>۱</p> <p><input checked="" type="checkbox"/> 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.</p> <p>در صورت انتخاب مورد HTTPS، رعایت الزام ۱-۳- و ۳-۳- و در صورت انتخاب TLS، رعایت الزامات ۳-۲- تا ۳-۴- که در بخش ۳- بیان گردیده است، الزامی است.</p> <table border="1" data-bbox="961 755 1948 984"> <tr> <td data-bbox="961 755 1024 831"><input checked="" type="checkbox"/></td> <td data-bbox="1024 755 1711 831">HTTPS</td> <td data-bbox="1711 755 1948 831">پروتکل مورد استفاده</td> </tr> <tr> <td data-bbox="961 831 1024 907"><input type="checkbox"/></td> <td data-bbox="1024 831 1711 907">TLS</td> <td data-bbox="1711 831 1948 907">برای ایجاد کانال امن</td> </tr> <tr> <td data-bbox="961 907 1024 984"><input checked="" type="checkbox"/></td> <td data-bbox="1024 907 1711 984">SSH</td> <td data-bbox="1711 907 1948 984">انتخاب گردد.</td> </tr> </table>	<input checked="" type="checkbox"/>	HTTPS	پروتکل مورد استفاده	<input type="checkbox"/>	TLS	برای ایجاد کانال امن	<input checked="" type="checkbox"/>	SSH	انتخاب گردد.
<input checked="" type="checkbox"/>	HTTPS	پروتکل مورد استفاده								
<input type="checkbox"/>	TLS	برای ایجاد کانال امن								
<input checked="" type="checkbox"/>	SSH	انتخاب گردد.								
	<p>۲</p> <p><input checked="" type="checkbox"/> محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.</p>									
	<p>۳</p> <p><input checked="" type="checkbox"/> محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.</p>									

۳- الزامات امنیتی مبتنی بر انتخاب

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

۳-۱- پروتکل HTTPS

شماره الزام	پروتکل HTTPS	توضیحات
۱	محصول باید پروتکل HTTPS را مطابق با RFC ۲۸۱۸ اجرا کند.	<input checked="" type="checkbox"/>
۲	محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	<input checked="" type="checkbox"/>
۳	در صورتی که گواهی‌نامه ارائه شده از سمت دیگر محصولات IT (در هنگام برقراری ارتباط) نامعتبر باشد، محصول باید بر اساس موارد زیر عمل نماید. اعتبارسنجی گواهی‌نامه بر اساس الزامات بخش ۳-۵-۳-۵ انجام می‌شود که در این صورت الزامات بخش ۳-۵-۳-۵ الزامی است.	<input type="checkbox"/>
	محصول تنها از موارد اتصال را برقرار نکند.	<input type="checkbox"/>
	بیان شده می‌تواند استفاده نماید.	<input type="checkbox"/>
	برای برقراری اتصال درخواست مجوز کند.	<input type="checkbox"/>

۲-۳- پروتکل TLS Client

توضیحات	پروتکل TLS Client		شماره الزام															
	<input type="checkbox"/>	<p>محمول باید (RFC ۵۲۴۶) TLS ۱.۲ 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="955 553 1728 1453"> <tr> <td data-bbox="955 553 1018 1453"> <input type="checkbox"/> </td> <td data-bbox="1018 553 1728 691"> <p>TLS_AES_۲۵۶_GCM_SHA۳۸۴ ۰x۱۳۰۲</p> <p>مطابق با RFC ۸۴۴۶</p> </td> <td data-bbox="1728 553 1948 1453" rowspan="8"> <p>مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.</p> </td> </tr> <tr> <td data-bbox="955 691 1018 829"> <input type="checkbox"/> </td> <td data-bbox="1018 691 1728 829"> <p>TLS_AES_۱۲۸_GCM_SHA۲۵۶ ۰x۱۳۰۱</p> <p>مطابق با RFC ۸۴۴۶</p> </td> </tr> <tr> <td data-bbox="955 829 1018 967"> <input type="checkbox"/> </td> <td data-bbox="1018 829 1728 967"> <p>TLS_DHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ ۰x۰۰۹F</p> <p>مطابق با RFC ۵۲۸۸</p> </td> </tr> <tr> <td data-bbox="955 967 1018 1105"> <input type="checkbox"/> </td> <td data-bbox="1018 967 1728 1105"> <p>TLS_DHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ ۰x۰۰۹E</p> <p>مطابق با RFC ۵۲۸۸</p> </td> </tr> <tr> <td data-bbox="955 1105 1018 1243"> <input type="checkbox"/> </td> <td data-bbox="1018 1105 1728 1243"> <p>TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ ۰xC۰۲F</p> <p>مطابق با RFC ۵۲۸۹</p> </td> </tr> <tr> <td data-bbox="955 1243 1018 1382"> <input type="checkbox"/> </td> <td data-bbox="1018 1243 1728 1382"> <p>TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ ۰xC۰۳۰</p> <p>مطابق با RFC ۵۲۸۹</p> </td> </tr> <tr> <td data-bbox="955 1382 1018 1453"> <input type="checkbox"/> </td> <td data-bbox="1018 1382 1728 1453"> <p>TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴</p> </td> </tr> </table>	<input type="checkbox"/>	<p>TLS_AES_۲۵۶_GCM_SHA۳۸۴ ۰x۱۳۰۲</p> <p>مطابق با RFC ۸۴۴۶</p>	<p>مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.</p>	<input type="checkbox"/>	<p>TLS_AES_۱۲۸_GCM_SHA۲۵۶ ۰x۱۳۰۱</p> <p>مطابق با RFC ۸۴۴۶</p>	<input type="checkbox"/>	<p>TLS_DHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ ۰x۰۰۹F</p> <p>مطابق با RFC ۵۲۸۸</p>	<input type="checkbox"/>	<p>TLS_DHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ ۰x۰۰۹E</p> <p>مطابق با RFC ۵۲۸۸</p>	<input type="checkbox"/>	<p>TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ ۰xC۰۲F</p> <p>مطابق با RFC ۵۲۸۹</p>	<input type="checkbox"/>	<p>TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ ۰xC۰۳۰</p> <p>مطابق با RFC ۵۲۸۹</p>	<input type="checkbox"/>	<p>TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴</p>	<p>۱</p>
<input type="checkbox"/>	<p>TLS_AES_۲۵۶_GCM_SHA۳۸۴ ۰x۱۳۰۲</p> <p>مطابق با RFC ۸۴۴۶</p>	<p>مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.</p>																
<input type="checkbox"/>	<p>TLS_AES_۱۲۸_GCM_SHA۲۵۶ ۰x۱۳۰۱</p> <p>مطابق با RFC ۸۴۴۶</p>																	
<input type="checkbox"/>	<p>TLS_DHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ ۰x۰۰۹F</p> <p>مطابق با RFC ۵۲۸۸</p>																	
<input type="checkbox"/>	<p>TLS_DHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ ۰x۰۰۹E</p> <p>مطابق با RFC ۵۲۸۸</p>																	
<input type="checkbox"/>	<p>TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ ۰xC۰۲F</p> <p>مطابق با RFC ۵۲۸۹</p>																	
<input type="checkbox"/>	<p>TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ ۰xC۰۳۰</p> <p>مطابق با RFC ۵۲۸۹</p>																	
<input type="checkbox"/>	<p>TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴</p>																	

	<input type="checkbox"/> ۰xC۰۲C مطابق با RFC ۵۲۸۹	
	<input type="checkbox"/> ۰xC۰۲B TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹	
	<input type="checkbox"/> ۰x۰۰۹D TLS_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۸	
	<input type="checkbox"/> ۰x۰۰۹C TLS_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۸	
	<input type="checkbox"/> ۰xC۰۲E TLS_ECDH_ECDSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۸	
	<input type="checkbox"/> ۰xC۰۲D TLS_ECDH_ECDSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹	
	<input type="checkbox"/> ۰xC۰۳۲ TLS_ECDH_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۹	
	<input type="checkbox"/> ۰xC۰۳۱ TLS_ECDH_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹	
	<input type="checkbox"/> ۰x۰۰A۱ TLS_DH_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۸	
	<input type="checkbox"/> TLS_DH_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶	

		۰x۰۰A۰	مطابق با RFC ۵۲۸۸		
	<input type="checkbox"/>	محصل باید مطابقت شناسه ارائه شده با شناسه مرجع را با توجه به بخش ۶ از RFC ۶۱۲۵، تأیید نماید.			۲
	<input type="checkbox"/>	محصل 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.			۳
	<input type="checkbox"/>	ارتباط را برقرار نکند	در صورت پشتیبانی		
	<input type="checkbox"/>	برای برقراری ارتباط درخواست مجوز کند	از اقدامات دیگر، در		
	<input type="checkbox"/>	سایر موارد	«سایر موارد» بیان گردد.		
	<input type="checkbox"/>	محصل باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید.			۴
	<input type="checkbox"/>	Supported Elliptic Curves Extension را ارائه نکند.	در صورتی که محصول از خم‌های		
	<input type="checkbox"/>	Supported Elliptic Curves Extension را به همراه NIST Curve های $secp^{۲۵۶r۱}$ یا $secp^{۳۸۴r۱}$ یا $secp^{۵۲۱r۱}$ ارائه نماید.	بیضوی استفاده می‌نماید، نوع خم باید مشخص گردد.		

۳-۳- پروتکل TLS Server

توضیحات	پروتکل TLS Server		شماره الزام
<p>TLS_CHACHA۲۰_POLY۱۳۰۵_SHA۲۵۶</p>	<input checked="" type="checkbox"/>	<p>محصول باید (RFC ۵۲۴۶) TLS ۱٫۲ را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.</p>	<p>۱</p> <p>مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.</p>
		<p>TLS_AES_۲۵۶_GCM_SHA۳۸۴ ۰x۱۳۰۲</p> <p>مطابق با RFC ۸۴۴۶</p>	
		<p>TLS_AES_۱۲۸_GCM_SHA۲۵۶ ۰x۱۳۰۱</p> <p>مطابق با RFC ۸۴۴۶</p>	
		<p>TLS_DHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ ۰x۰۰۹F</p> <p>مطابق با RFC ۵۲۸۸</p>	
		<p>TLS_DHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ ۰x۰۰۹E</p> <p>مطابق با RFC ۵۲۸۸</p>	
		<p>TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ ۰xC۰۲F</p> <p>مطابق با RFC ۵۲۸۹</p>	
		<p>TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ ۰xC۰۳۰</p> <p>مطابق با RFC ۵۲۸۹</p>	

	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۹	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹	
	<input type="checkbox"/>	TLS_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۸	
	<input type="checkbox"/>	TLS_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۸	
	<input type="checkbox"/>	TLS_ECDH_ECDSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۸	
	<input type="checkbox"/>	TLS_ECDH_ECDSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹	
	<input type="checkbox"/>	TLS_ECDH_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۹	
	<input type="checkbox"/>	TLS_ECDH_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶ مطابق با RFC ۵۲۸۹	
	<input type="checkbox"/>	TLS_DH_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴ مطابق با RFC ۵۲۸۹	

		مطابق با RFC ۵۲۸۸	
		TLS_DH_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶	
	<input type="checkbox"/>	x00A0	
		مطابق با RFC ۵۲۸۸	
	<input checked="" type="checkbox"/>	محمول باید اتصال‌های کاربرانی که درخواست SSL۱,۰, SSL۲,۰, SSL۳,۰ و TLS۱,۰ دارند را رد نماید.	۲
	<input checked="" type="checkbox"/>	محمول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.	۳
	<input type="checkbox"/>	استفاده از RSA با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ یا ۴۰۹۶ بیت	طول کلید یا نوع خم مورد استفاده باید مشخص گردد.
	<input checked="" type="checkbox"/>	پارامترهای ECDH(E) با استفاده از NIST Curve های secp۲۵۶r۱ یا secp۳۸۴r۱ و هیچ مورد دیگر	
	<input type="checkbox"/>	پارامترهای دیفی-هلمن با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ بیت	
از خم‌های secp۲۱r۱ و secp۳۸۴r۱ استفاده شده است.			

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.

توضیحات	پروتکل TLS مشترک کلاینت و سرور	شماره الزام
	<input type="checkbox"/> محصول باید احراز هویت دوطرفه کلاینت‌ها/سرورهای TLS را با استفاده از گواهی‌نامه‌های X۵۰۹۷۳ پشتیبانی نماید.	۱
	<input type="checkbox"/> 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.	۲

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 ۵۲۸۰ RFC 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 ۶۹۶	روش‌های تأیید وضعیت فسخ گواهی نامه
	<input type="checkbox"/> لیست فسخ گواهی نامه (CRL) مشخص شده در RFC ۵۲۸۰ بخش ۶.۳	
	<input type="checkbox"/> لیست فسخ گواهی نامه (CRL) مشخص شده در RFC ۵۷۵۹ 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-kp۳) با OID ۱.۳.۶.۱.۵.۵.۷.۳.۱ 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-kp۱) با OID ۱.۳.۶.۱.۵.۵.۷.۳.۱ را در بخش extendedKeyUsage خود داشته باشند.	

		<p>گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف « Client Authentication » (id-kp۱ با ۱,۳,۶,۱,۵,۵,۷,۳,۲ OID) را در بخش extendedKeyUsage خود داشته باشند.</p>														
		<p>گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ OCSP باید « OCSP Signing » (id-pk۹ با ۱,۳,۶,۱,۵,۵,۷,۳,۹ OID) را در بخش extendedKeyUsage خود داشته باشند.</p>														
	<input checked="" type="checkbox"/>	<p>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.</p>	۲													
	<input checked="" type="checkbox"/>	<p>محصول باید برای پشتیبانی از احراز هویت برای موارد زیر، از گواهی‌نامه‌های X۵۰۹۷۳ تعریف شده در RFC ۵۲۸۰ استفاده کند.</p> <table border="1" data-bbox="919 722 1711 1021"> <tr> <td data-bbox="919 722 961 771"> <input checked="" type="checkbox"/> </td> <td data-bbox="961 722 1711 771">HTTPS</td> <td data-bbox="1711 722 1948 1021" rowspan="6"> <p>در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.</p> </td> </tr> <tr> <td data-bbox="919 771 961 820"> <input type="checkbox"/> </td> <td data-bbox="961 771 1711 820">TLS</td> </tr> <tr> <td data-bbox="919 820 961 868"> <input checked="" type="checkbox"/> </td> <td data-bbox="961 820 1711 868">SSH</td> </tr> <tr> <td data-bbox="919 868 961 917"> <input type="checkbox"/> </td> <td data-bbox="961 868 1711 917">امضای کد برای بروزرسانی‌های نرم‌افزار سیستم</td> </tr> <tr> <td data-bbox="919 917 961 966"> <input type="checkbox"/> </td> <td data-bbox="961 917 1711 966">امضای کد برای تأیید یکپارچگی</td> </tr> <tr> <td data-bbox="919 966 961 1021"> <input type="checkbox"/> </td> <td data-bbox="961 966 1711 1021">سایر موارد</td> </tr> </table>	<input checked="" type="checkbox"/>	HTTPS	<p>در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.</p>	<input type="checkbox"/>	TLS	<input checked="" 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
<input checked="" type="checkbox"/>	HTTPS	<p>در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.</p>														
<input type="checkbox"/>	TLS															
<input checked="" 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															

۶-۳- پروتکل SSH

توضیحات	پروتکل SSH		شماره الزام																
	<input checked="" type="checkbox"/>	محصول باید پروتکل SSH را مطابق با RFC های ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۵۶۵۶ و ۶۶۶۸ پیاده‌سازی نماید.	۱																
	<input checked="" type="checkbox"/>	<p>محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC ۴۲۵۲، از روش‌های احراز هویت زیر پشتیبانی نماید.</p> <table border="1" data-bbox="919 667 1711 769"> <tr> <td data-bbox="919 667 961 716"><input checked="" type="checkbox"/></td> <td data-bbox="961 667 1711 716">احراز هویت مبتنی بر کلید عمومی</td> </tr> <tr> <td data-bbox="919 716 961 769"><input checked="" type="checkbox"/></td> <td data-bbox="961 716 1711 769">احراز هویت مبتنی بر گذرواژه</td> </tr> </table>	<input checked="" type="checkbox"/>	احراز هویت مبتنی بر کلید عمومی	<input checked="" type="checkbox"/>	احراز هویت مبتنی بر گذرواژه	۲												
<input checked="" type="checkbox"/>	احراز هویت مبتنی بر کلید عمومی																		
<input checked="" type="checkbox"/>	احراز هویت مبتنی بر گذرواژه																		
۲۵۶kb	<input checked="" type="checkbox"/>	محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC ۴۲۵۳، بسته‌های بزرگتر از مقدار مشخصی (در بخش «توضیحات» ذکر شود) را کنار بگذارد.	۳																
	<input checked="" type="checkbox"/>	<p>محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های رمزنگاری زیر استفاده نماید.</p> <table border="1" data-bbox="919 997 1711 1365"> <tr> <td data-bbox="919 997 961 1045"><input type="checkbox"/></td> <td data-bbox="961 997 1711 1045">AES۱۲۸-CBC</td> </tr> <tr> <td data-bbox="919 1045 961 1094"><input type="checkbox"/></td> <td data-bbox="961 1045 1711 1094">AES۱۹۲-CBC</td> </tr> <tr> <td data-bbox="919 1094 961 1143"><input type="checkbox"/></td> <td data-bbox="961 1094 1711 1143">AES۲۵۶-CBC</td> </tr> <tr> <td data-bbox="919 1143 961 1192"><input checked="" type="checkbox"/></td> <td data-bbox="961 1143 1711 1192">AES۱۲۸-CTR</td> </tr> <tr> <td data-bbox="919 1192 961 1240"><input checked="" type="checkbox"/></td> <td data-bbox="961 1192 1711 1240">AES۱۹۲-CTR</td> </tr> <tr> <td data-bbox="919 1240 961 1289"><input checked="" type="checkbox"/></td> <td data-bbox="961 1240 1711 1289">AES۲۵۶-CTR</td> </tr> <tr> <td data-bbox="919 1289 961 1338"><input type="checkbox"/></td> <td data-bbox="961 1289 1711 1338">AEAD_AES_۱۲۸_GCM</td> </tr> <tr> <td data-bbox="919 1338 961 1365"><input type="checkbox"/></td> <td data-bbox="961 1338 1711 1365">AEAD_AES_۲۵۶_GCM</td> </tr> </table>	<input type="checkbox"/>	AES۱۲۸-CBC	<input type="checkbox"/>	AES۱۹۲-CBC	<input type="checkbox"/>	AES۲۵۶-CBC	<input checked="" type="checkbox"/>	AES۱۲۸-CTR	<input checked="" type="checkbox"/>	AES۱۹۲-CTR	<input checked="" type="checkbox"/>	AES۲۵۶-CTR	<input type="checkbox"/>	AEAD_AES_۱۲۸_GCM	<input type="checkbox"/>	AEAD_AES_۲۵۶_GCM	۴
<input type="checkbox"/>	AES۱۲۸-CBC																		
<input type="checkbox"/>	AES۱۹۲-CBC																		
<input type="checkbox"/>	AES۲۵۶-CBC																		
<input checked="" type="checkbox"/>	AES۱۲۸-CTR																		
<input checked="" type="checkbox"/>	AES۱۹۲-CTR																		
<input checked="" type="checkbox"/>	AES۲۵۶-CTR																		
<input type="checkbox"/>	AEAD_AES_۱۲۸_GCM																		
<input type="checkbox"/>	AEAD_AES_۲۵۶_GCM																		

	<p><input checked="" type="checkbox"/> محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های کلید عمومی زیر استفاده نماید.</p> <table border="1" data-bbox="919 266 1713 867"> <tr><td><input checked="" type="checkbox"/></td><td>ssh-ed۲۵۵۱۹</td></tr> <tr><td><input type="checkbox"/></td><td>ssh-ed۴۴۸</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>rsa-sha۲-۵۱۲</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>rsa-sha۲-۲۵۶</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha۲-nistp۵۲۱</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha۲-nistp۳۸۴</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>ecdsa-sha۲-nistp۲۵۶</td></tr> <tr><td><input type="checkbox"/></td><td>x۵۰۹۷۳-ecdsa-sha۲-nistp۵۲۱</td></tr> <tr><td><input type="checkbox"/></td><td>x۵۰۹۷۳-ecdsa-sha۲-nistp۳۸۴</td></tr> <tr><td><input type="checkbox"/></td><td>x۵۰۹۷۳-ecdsa-sha۲-nistp۲۵۶</td></tr> <tr><td><input type="checkbox"/></td><td>x۵۰۹۷۳-rsa۲۰۴۸-sha۲۵۶</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>ssh-rsa</td></tr> <tr><td><input type="checkbox"/></td><td>x۵۰۹۷۳-ssh-rsa</td></tr> </table>	<input checked="" type="checkbox"/>	ssh-ed۲۵۵۱۹	<input type="checkbox"/>	ssh-ed۴۴۸	<input checked="" type="checkbox"/>	rsa-sha۲-۵۱۲	<input checked="" type="checkbox"/>	rsa-sha۲-۲۵۶	<input type="checkbox"/>	ecdsa-sha۲-nistp۵۲۱	<input type="checkbox"/>	ecdsa-sha۲-nistp۳۸۴	<input checked="" type="checkbox"/>	ecdsa-sha۲-nistp۲۵۶	<input type="checkbox"/>	x۵۰۹۷۳-ecdsa-sha۲-nistp۵۲۱	<input type="checkbox"/>	x۵۰۹۷۳-ecdsa-sha۲-nistp۳۸۴	<input type="checkbox"/>	x۵۰۹۷۳-ecdsa-sha۲-nistp۲۵۶	<input type="checkbox"/>	x۵۰۹۷۳-rsa۲۰۴۸-sha۲۵۶	<input checked="" type="checkbox"/>	ssh-rsa	<input type="checkbox"/>	x۵۰۹۷۳-ssh-rsa	۵
<input checked="" type="checkbox"/>	ssh-ed۲۵۵۱۹																											
<input type="checkbox"/>	ssh-ed۴۴۸																											
<input checked="" type="checkbox"/>	rsa-sha۲-۵۱۲																											
<input checked="" type="checkbox"/>	rsa-sha۲-۲۵۶																											
<input type="checkbox"/>	ecdsa-sha۲-nistp۵۲۱																											
<input type="checkbox"/>	ecdsa-sha۲-nistp۳۸۴																											
<input checked="" type="checkbox"/>	ecdsa-sha۲-nistp۲۵۶																											
<input type="checkbox"/>	x۵۰۹۷۳-ecdsa-sha۲-nistp۵۲۱																											
<input type="checkbox"/>	x۵۰۹۷۳-ecdsa-sha۲-nistp۳۸۴																											
<input type="checkbox"/>	x۵۰۹۷۳-ecdsa-sha۲-nistp۲۵۶																											
<input type="checkbox"/>	x۵۰۹۷۳-rsa۲۰۴۸-sha۲۵۶																											
<input checked="" type="checkbox"/>	ssh-rsa																											
<input type="checkbox"/>	x۵۰۹۷۳-ssh-rsa																											
	<p><input checked="" type="checkbox"/> محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های MAC صحت داده‌های زیر استفاده نماید.</p> <table border="1" data-bbox="919 980 1713 1260"> <tr><td><input type="checkbox"/></td><td>AEAD_AES_۲۵۶_GCM</td></tr> <tr><td><input type="checkbox"/></td><td>AEAD_AES_۱۲۸_GCM</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>hmac-sha۲-۵۱۲</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>hmac-sha۲-۲۵۶</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha۱-۹۶</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha۱</td></tr> </table>	<input type="checkbox"/>	AEAD_AES_۲۵۶_GCM	<input type="checkbox"/>	AEAD_AES_۱۲۸_GCM	<input checked="" type="checkbox"/>	hmac-sha۲-۵۱۲	<input checked="" type="checkbox"/>	hmac-sha۲-۲۵۶	<input type="checkbox"/>	hmac-sha۱-۹۶	<input type="checkbox"/>	hmac-sha۱	۶														
<input type="checkbox"/>	AEAD_AES_۲۵۶_GCM																											
<input type="checkbox"/>	AEAD_AES_۱۲۸_GCM																											
<input checked="" type="checkbox"/>	hmac-sha۲-۵۱۲																											
<input checked="" type="checkbox"/>	hmac-sha۲-۲۵۶																											
<input type="checkbox"/>	hmac-sha۱-۹۶																											
<input type="checkbox"/>	hmac-sha۱																											
	<p><input checked="" type="checkbox"/> محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های تبادل کلید زیر استفاده نماید.</p> <table border="1" data-bbox="919 1373 1713 1463"> <tr><td><input type="checkbox"/></td><td>curve۲۵۵۱۹-sha۲۵۶</td></tr> <tr><td><input type="checkbox"/></td><td>curve۴۴۸-sha۵۱۲</td></tr> </table>	<input type="checkbox"/>	curve۲۵۵۱۹-sha۲۵۶	<input type="checkbox"/>	curve۴۴۸-sha۵۱۲	۷																						
<input type="checkbox"/>	curve۲۵۵۱۹-sha۲۵۶																											
<input type="checkbox"/>	curve۴۴۸-sha۵۱۲																											

	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	diffie-hellman-group-exchange-sha۲۵۶ diffie-hellman-group۱۸-sha۵۱۲ diffie-hellman-group۱۷-sha۵۱۲ diffie-hellman-group۱۶-sha۵۱۲ diffie-hellman-group۱۵-sha۵۱۲ ecdh-sha۲-nistp۵۲۱ ecdh-sha۲-nistp۳۸۴ ecdh-sha۲-nistp۲۵۶ rsa۲۰۴۸-sha۲۵۶ diffie-hellman-group-exchange-sha۱ diffie-hellman-group۱۴-sha۲۵۶	
	<input checked="" type="checkbox"/>	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.	
	<input checked="" type="checkbox"/>	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 (تشریح شده در RFC ۴۲۵۱ بخش ۱.۷) همراه می‌کند، استفاده می‌نماید.	