

به نام خدا

# سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه

سیستم‌های مدیریتی تارگان

سامانه تارگان

۵.۶



۱۴۰۰/۱۱

نسخه ۱.۹

### 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                   | ۵                            |
| ۲-۱- ممیزی امنیت (لاگ)              | ۵                            |
| ۲-۲- رمزنگاری                       | ۹                            |
| ۲-۳- شناسایی و احراز هویت           | ۱۱                           |
| ۲-۴- حفاظت از داده‌ی کاربری         | ۱۵                           |
| ۲-۵- مدیریت امنیت                   | ۱۹                           |
| ۲-۶- حفاظت از توابع امنیتی محصول    | ۲۲                           |
| ۲-۷- تخصیص منابع                    | ۲۴                           |
| ۲-۸- دسترسی به محصول                | ۲۵                           |
| ۲-۹- کانال‌ها/مسیرهای مورد اعتماد   | ۲۷                           |
| ۳- الزامات امنیتی مبتنی بر انتخاب   | ۲۸                           |
| ۳-۱- پروتکل HTTPS                   | ۲۸                           |
| ۳-۲- پروتکل TLS Client              | ۲۹                           |
| ۳-۳- پروتکل TLS Server              | ۳۳                           |
| ۳-۴- پروتکل TLS مشترک کلاینت و سرور | ۳۵                           |
| ۳-۵- اعتبارسنجی گواهی‌نامه          | ۳۶                           |
| ۳-۶- پروتکل SSH                     | ۳۸                           |

## ۱- معرفی محصول

محصول شامل سامانه مدیریت محتوی است و کاربران مدیریتی می توانند به بخش مدیریتی وارد شده و منوها و بنرها و همچنین محتوای هر صفحه را ایجاد و ویرایش کنند.

محصول کاملاً قابلیت شخصی سازی دارد و برای مصارف مختلف از ماژولهایی که مورد درخواست کارفرماست بهره می گیرد برای مثال، یکی از ماژولهای درخواستی دانشگاههای کشور، ثبت نام و فلوی دانشجویی دانشجویان خارجی است که برای این منظور ماژول ثبت نام دانشجویان خارجی طراحی شده است. کاربران خارجی که قصد ثبت نام و ادامه تحصیل در دانشگاه را دارند می توانند به کنترل پانل کاربری خود لاگین کنند و اقدام به ثبت نام و پیگیری ثبت نام خود نمایند.

## 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   |  |   |                                     |                    |                                     |  |                                     |                               |                                     |                                       |                                     |   |                                     |   |                                     |  |                                     |                                   |                                     |                               |                                     |  |
|-------------------------------------|---|---|--|---|-------------------------------------|--------------------|-------------------------------------|--|-------------------------------------|-------------------------------|-------------------------------------|---------------------------------------|-------------------------------------|---|-------------------------------------|---|-------------------------------------|--|-------------------------------------|-----------------------------------|-------------------------------------|-------------------------------|-------------------------------------|--|
|                                     | <table border="1"> <tr> <td data-bbox="877 708 915 821"><input checked="" type="checkbox"/></td> <td data-bbox="915 708 1948 821">محصول باید برای موارد مشخص شده که در زیر آمده است، ثبت‌نشان<sup>۱</sup> تولید کند (Log) ثبت نماید).</td> <td data-bbox="1948 708 2020 1321" rowspan="13">                     ۱<br/><br/>                     رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.                 </td> </tr> <tr> <td data-bbox="877 821 915 870"><input checked="" type="checkbox"/></td> <td data-bbox="915 821 1948 870">شروع و اتمام توابع</td> </tr> <tr> <td data-bbox="877 870 915 919"><input checked="" type="checkbox"/></td> <td data-bbox="915 870 1948 919">تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها</td> </tr> <tr> <td data-bbox="877 919 915 967"><input checked="" type="checkbox"/></td> <td data-bbox="915 919 1948 967">خواندن اطلاعات از ثبت‌نشان‌ها</td> </tr> <tr> <td data-bbox="877 967 915 1016"><input checked="" type="checkbox"/></td> <td data-bbox="915 967 1948 1016">تمامی تغییرات در پیکربندی ثبت‌نشان‌ها</td> </tr> <tr> <td data-bbox="877 1016 915 1065"><input checked="" type="checkbox"/></td> <td data-bbox="915 1016 1948 1065">عملیات انجام شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه</td> </tr> <tr> <td data-bbox="877 1065 915 1114"><input checked="" type="checkbox"/></td> <td data-bbox="915 1065 1948 1114">عملیات انجام شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها</td> </tr> <tr> <td data-bbox="877 1114 915 1162"><input checked="" type="checkbox"/></td> <td data-bbox="915 1114 1948 1162">تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.</td> </tr> <tr> <td data-bbox="877 1162 915 1211"><input checked="" type="checkbox"/></td> <td data-bbox="915 1162 1948 1211">تمام کاربردهای سازوکار احراز هویت</td> </tr> <tr> <td data-bbox="877 1211 915 1260"><input checked="" type="checkbox"/></td> <td data-bbox="915 1211 1948 1260">نتایج نهایی عملیات احراز هویت</td> </tr> <tr> <td data-bbox="877 1260 915 1321"><input checked="" type="checkbox"/></td> <td data-bbox="915 1260 1948 1321">تلاش موفق و ناموفق هر گذرواژه بررسی شده توسط محصول</td> </tr> </table> | <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<br><br>رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید. | <input checked="" type="checkbox"/> | شروع و اتمام توابع | <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 | <input checked="" type="checkbox"/> | تلاش موفق و ناموفق هر گذرواژه بررسی شده توسط محصول |
| <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<br><br>رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید. |  |   |                                     |                    |                                     |  |                                     |                               |                                     |                                       |                                     |   |                                     |   |                                     |  |                                     |                                   |                                     |                               |                                     |  |
| <input checked="" type="checkbox"/> | شروع و اتمام توابع  |   |  |   |                                     |                    |                                     |  |                                     |                               |                                     |                                       |                                     |   |                                     |   |                                     |  |                                     |                                   |                                     |                               |                                     |  |
| <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   |   |  |   |                                     |                    |                                     |  |                                     |                               |                                     |                                       |                                     |   |                                     |   |                                     |  |                                     |                                   |                                     |                               |                                     |  |
| <input checked="" type="checkbox"/> | تلاش موفق و ناموفق هر گذرواژه بررسی شده توسط محصول  |   |  |   |                                     |                    |                                     |  |                                     |                               |                                     |                                       |                                     |   |                                     |   |                                     |  |                                     |                                   |                                     |                               |                                     |  |

<sup>۱</sup> Log

|  |                                     |  |  |
|--|-------------------------------------|--|--|
|  | <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  |  |
|  | <input type="checkbox"/>            | خاتمه به نشست غیرفعال توسط مدیر سیستم  |  |
|  | <input type="checkbox"/>            | سایر موارد   |  |
|  | <input checked="" type="checkbox"/> | <b>محصول باید برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید.</b>                     | 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"/> | نیوداده نامفهوم در رکوردها  | مواردی که در  |
|   | <input checked="" type="checkbox"/> | نیودبخش‌های 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 checked="" type="checkbox"/> | نوع حساب کاربری   |   |
|   | <input checked="" type="checkbox"/> | تاریخ‌ازمان   |   |
|   | <input checked="" 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 checked="" type="checkbox"/> | پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)   | مشخص شود. (وجود)                                      |
|   | <input type="checkbox"/>            | فقط خواندنی کردن ثبت‌نشان‌ها در محصول   | یک مورد لازم و کافی                                   |
|   | <input type="checkbox"/>            | سایر موارد  | (است)   |

|  |                                     |  |  |
|--|-------------------------------------|--|--|
|  | <input checked="" type="checkbox"/> | <p>محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.</p>  | ۷  |
|  | <input type="checkbox"/>            | <p>استفاده از یک کانال ارتباطی</p>   | <p>روش‌های اطلاع‌رسانی</p>                   |
|  | <input type="checkbox"/>            | <p>ارسال پیام</p>  | <p>مشخص شود (وجود)</p>                       |
|  | <input checked="" type="checkbox"/> | <p>از طریق واسط کاربر مجاز</p>   | <p>یک مورد لازم و کافی</p>                   |
|  | <input type="checkbox"/>            | <p>سایر موارد</p>  | <p>(است)</p>                                 |
|  | <input checked="" type="checkbox"/> | <p>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> | ۸  |
|  | <input type="checkbox"/>            | <p>نادیده گرفتن ثبت‌نشان‌ها</p>  | <p>رویکردهای مورد</p>                        |
|  | <input type="checkbox"/>            | <p>ذخیره‌سازی محدود ثبت‌نشان‌ها (آنهايي که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند)</p>   | <p>استفاده در محصول<br/>مشخص گردد (وجود)</p> |
|  | <input checked="" type="checkbox"/> | <p>بازنویسی روی قدیمی‌ترین ثبت‌نشان‌های ذخیره‌شده</p>  | <p>یک مورد لازم و کافی</p>                   |
|  | <input type="checkbox"/>            | <p>سایر موارد</p>  | <p>(است)</p>                                 |



## 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           | <input checked="" type="checkbox"/> 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 ۱۸۰۳۳-۳) با توجه به موارد زیر انجام دهد. | <input type="checkbox"/> مد عملیاتی CBC و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در (NIST SP ۸۰۰-۳۸A) 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 (تعریف شده در (NIST SP ۸۰۰-۳۸D)  |
|             |  | <input type="checkbox"/> مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در (ISO ۱۰۱۱۶)   |
|             |  | <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. |
| ۲           | <input type="checkbox"/> الگوریتم SHA-۱ با اندازه خلاصه پیام ۱۶۰ بیت<br><input checked="" type="checkbox"/> الگوریتم SHA-۲۵۶ با اندازه خلاصه پیام ۲۵۶ بیت  | <input type="checkbox"/> الگوریتم و اندازه خلاصه پیام مورد استفاده را   |

<sup>۲</sup> Module

|  |                                     |  |  |
|--|-------------------------------------|--|--|
|  | <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 type="checkbox"/>            | از طریق توابع امنیتی محصول   | (است)  |
|  | <input checked="" 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-۱۷_۵؛ PKCS ۹۷۹۶-۲، ISO/IEC، الگوی امضای دیجیتال ۲ و یا الگوی امضای دیجیتال ۳) | الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید. |
|  | <input checked="" 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                         |  |   |                          |   |   |                                     |  |  |   |
|-------------------------------------|---|---|-------------------------------------|--|---|--------------------------|---|---|-------------------------------------|--|--|---|
|                                     | <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="957 602 1709 846"> <tr> <td data-bbox="957 602 1024 683" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="1024 602 1709 683">یک عدد مثبت ثابت</td> <td data-bbox="1709 602 1948 683">مقدار یا یازهی مورد استفاده در هر یک باید</td> </tr> <tr> <td data-bbox="957 683 1024 764" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1024 683 1709 764">یک عدد مثبت قابل تنظیم توسط مدیر</td> <td data-bbox="1709 683 1948 764">مشخص گردد. (وجود</td> </tr> <tr> <td data-bbox="957 764 1024 846" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1024 764 1709 846">یک بازهی قابل قبولی از مقادیر</td> <td data-bbox="1709 764 1948 846">یک مورد لازم و کافی است)</td> </tr> </table>  | <input checked="" type="checkbox"/> | یک عدد مثبت ثابت   | مقدار یا یازهی مورد استفاده در هر یک باید               | <input type="checkbox"/> | یک عدد مثبت قابل تنظیم توسط مدیر  | مشخص گردد. (وجود  | <input type="checkbox"/>            | یک بازهی قابل قبولی از مقادیر  | یک مورد لازم و کافی است)   | ۱ |
| <input checked="" type="checkbox"/> | یک عدد مثبت ثابت  | مقدار یا یازهی مورد استفاده در هر یک باید   |                                     |  |   |                          |   |   |                                     |  |  |   |
| <input type="checkbox"/>            | یک عدد مثبت قابل تنظیم توسط مدیر  | مشخص گردد. (وجود  |                                     |  |   |                          |   |   |                                     |  |  |   |
| <input type="checkbox"/>            | یک بازهی قابل قبولی از مقادیر   | یک مورد لازم و کافی است)  |                                     |  |   |                          |   |   |                                     |  |  |   |
|                                     | <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="957 963 1709 1458"> <tr> <td data-bbox="957 963 1024 1125" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1024 963 1709 1125">غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)</td> <td data-bbox="1709 963 1948 1125">روش استفاده شده برای پیچیدمتر کردن احراز هویت را انتخاب</td> </tr> <tr> <td data-bbox="957 1125 1024 1287" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1024 1125 1709 1287">غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)</td> <td data-bbox="1709 1125 1948 1287">نمایید. (وجود یک مورد لازم و کافی است). لازم به ذکر است روش‌های فوق با توجه</td> </tr> <tr> <td data-bbox="957 1287 1024 1458" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="1024 1287 1709 1458">استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)</td> <td data-bbox="1709 1287 1948 1458">به نوع کاربرد می‌تواند از حالت انتخابی به حلت الزامی تغییر یابد.</td> </tr> </table> | <input type="checkbox"/>            | غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد) | روش استفاده شده برای پیچیدمتر کردن احراز هویت را انتخاب | <input type="checkbox"/> | غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد) | نمایید. (وجود یک مورد لازم و کافی است). لازم به ذکر است روش‌های فوق با توجه | <input checked="" type="checkbox"/> | استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود) | به نوع کاربرد می‌تواند از حالت انتخابی به حلت الزامی تغییر یابد. | ۲ |
| <input type="checkbox"/>            | غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)                                | روش استفاده شده برای پیچیدمتر کردن احراز هویت را انتخاب   |                                     |  |   |                          |   |   |                                     |  |  |   |
| <input type="checkbox"/>            | غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد) | نمایید. (وجود یک مورد لازم و کافی است). لازم به ذکر است روش‌های فوق با توجه   |                                     |  |   |                          |   |   |                                     |  |  |   |
| <input checked="" type="checkbox"/> | استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)                | به نوع کاربرد می‌تواند از حالت انتخابی به حلت الزامی تغییر یابد.  |                                     |  |   |                          |   |   |                                     |  |  |   |



|   |                                     |   |  |
|---|-------------------------------------|---|--|
|   | <input type="checkbox"/>            | هیچ اقدامی  | احراز هویت انجام دهد،  |
|   | <input checked="" 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"/>            | Active Directory  |  |
|   | <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.   |  |

|  |                                     |  |   |
|--|-------------------------------------|--|---|
|  | <input checked="" type="checkbox"/> | 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). | در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین |
|  | <input checked="" type="checkbox"/> | بروزرسانی اطلاعات پیشینه احراز هویت  | در «سایر موارد» بیان  |
|  | <input type="checkbox"/>            | سایر موارد   | می‌شوند).   |
|  | <input checked="" type="checkbox"/> | محصول باید بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید.  |   |
|  | <input checked="" type="checkbox"/> | غیرمجاز بودن هرگونه تغییر در طول نشست فعال   | قوانینی که در صورت تغییر ویژگی‌های  |
|  | <input type="checkbox"/>            | سایر موارد   | امنیتی کاربر فعال، اعمال می‌شود، مشخص گردد.                                   |

## 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 |
|---------|---|--|-------------|
|         | محصول باید برای موجودیت‌ها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید. |  | ۱           |
|         | <input checked="" type="checkbox"/>                                       | مدیر سیستم<br>موجودیت‌های فعالی که خط‌مشی‌های            |             |
|         | <input checked="" type="checkbox"/>                                       | کاربر عادی<br>کنترل دسترسی در مورد آنها اعمال            |             |
|         | <input checked="" type="checkbox"/>                                       | سایر موارد<br>می‌شوند، مشخص گردد.                        |             |
|         | <input checked="" type="checkbox"/>                                       | سوابق، مستندات و فراداده<br>موجودیت‌های غیرفعال          |             |
|         | <input checked="" type="checkbox"/>                                       | داده متعلق به کاربران<br>که خط‌مشی‌های                   |             |
|         | <input checked="" type="checkbox"/>                                       | داده احراز هویت<br>کنترل دسترسی در مورد آنها اعمال       |             |
|         | <input type="checkbox"/>  | سایر موارد<br>می‌شوند، مشخص گردد.                        |             |
|         | <input checked="" type="checkbox"/>                                       | ایجاد موجودیت غیرفعال جدید<br>عملیاتی که                 |             |
|         | <input checked="" type="checkbox"/>                                       | حذف موجودیت غیرفعال<br>خط‌مشی‌های کنترل                  |             |
|         | <input checked="" type="checkbox"/>                                       | تغییر دسترسی‌ها به موجودیت غیرفعال<br>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.  |  |
| ۲ | <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  |  |
| ۳ | <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 لیست 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). |   |  |
|   |                                     |   |   |  |
| ۴ | <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 checked="" type="checkbox"/>   | سایر موارد  |  |
| ۵ | <input checked="" type="checkbox"/> | محصول باید تضمین نماید تمام اطلاعات قبلی منابع یا در هنگام تخصیص و یا در هنگام آزادسازی آنها، غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.  |   |  |
| ۶ | <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 checked="" type="checkbox"/> | نوع داده  | ویژگی‌های امنیتی مرتبط با داده کاربری   |
|  | <input checked="" type="checkbox"/> | حجم و اندازه  | که در هنگام ورود آن به محصول استفاده می‌شوند، مشخص شود  |
|  | <input checked="" type="checkbox"/> | فرمت  | (در صورتی که کنترل دسترسی برای موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد» بیان گردد). |
|  | <input type="checkbox"/>            | تعداد دفعات Import  |   |
|  | <input type="checkbox"/>            | سایر موارد  |   |
|  | <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 اعمال نماید و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.</p>   |   |
|  | <input checked="" type="checkbox"/> | نوع داده  | ویژگی‌های امنیتی مرتبط با داده کاربری   |
|  | <input checked="" type="checkbox"/> | حجم و اندازه  | که در هنگام خروج آن از محصول استفاده می‌شوند، مشخص شوند                                       |
|  | <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 |
|  | <input type="checkbox"/>            | سایر موارد   | اعمال می‌شوند، مشخص شوند               |
|  | <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         |
|  | <input type="checkbox"/>            | سایر موارد   | کاربری حساس، مشخص شود.                 |
|  | <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،     |
|  | <input type="checkbox"/>            | تصحیح داده بر اساس مقادیر قبل  | مشخص شود (وجود                         |
|  | <input type="checkbox"/>            | سایر موارد   | یک مورد لازم و کافی است)               |

## 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   |                                     |                     |                    |                                     |               |                     |                                     |            |                    |                                     |               |               |                          |            |       |
|-------------------------------------|---------------------|--|-------------------------------------|---------------------|--------------------|-------------------------------------|---------------|---------------------|-------------------------------------|------------|--------------------|-------------------------------------|---------------|---------------|--------------------------|------------|-------|
|                                     | ۱                   | <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"> <tr> <td data-bbox="961 651 1024 699"><input checked="" type="checkbox"/></td> <td data-bbox="1024 651 1711 699">تعیین و تغییر رفتار</td> <td data-bbox="1711 651 2022 699">فعالیت‌های مدیریتی</td> </tr> <tr> <td data-bbox="961 699 1024 748"><input checked="" type="checkbox"/></td> <td data-bbox="1024 699 1711 748">غیرفعال نمودن</td> <td data-bbox="1711 699 2022 748">که محصول پشتیبانی</td> </tr> <tr> <td data-bbox="961 748 1024 797"><input checked="" type="checkbox"/></td> <td data-bbox="1024 748 1711 797">فعال نمودن</td> <td data-bbox="1711 748 2022 797">می‌کند، مشخص شوند.</td> </tr> <tr> <td data-bbox="961 797 1024 846"><input type="checkbox"/></td> <td data-bbox="1024 797 1711 846">سایر موارد</td> <td data-bbox="1711 797 2022 846"></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          |  |                                     |                     |                    |                                     |               |                     |                                     |            |                    |                                     |               |               |                          |            |       |
|                                     | ۲                   | <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"> <tr> <td data-bbox="961 1015 1024 1063"><input checked="" type="checkbox"/></td> <td data-bbox="1024 1015 1711 1063">پرس‌وجو</td> <td data-bbox="1711 1015 2022 1063">عملیات بر روی</td> </tr> <tr> <td data-bbox="961 1063 1024 1112"><input checked="" type="checkbox"/></td> <td data-bbox="1024 1063 1711 1112">تغییر</td> <td data-bbox="1711 1063 2022 1112">ویژگی‌های امنیتی که</td> </tr> <tr> <td data-bbox="961 1112 1024 1161"><input checked="" type="checkbox"/></td> <td data-bbox="1024 1112 1711 1161">حذف</td> <td data-bbox="1711 1112 2022 1161">در محصول پشتیبانی</td> </tr> <tr> <td data-bbox="961 1161 1024 1209"><input checked="" type="checkbox"/></td> <td data-bbox="1024 1161 1711 1209">تغییر پیش‌فرض</td> <td data-bbox="1711 1161 2022 1209">می‌شوند، مشخص</td> </tr> <tr> <td data-bbox="961 1209 1024 1258"><input type="checkbox"/></td> <td data-bbox="1024 1209 1711 1258">سایر موارد</td> <td data-bbox="1711 1209 2022 1258">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 checked="" type="checkbox"/> | تغییر پیش‌فرض | می‌شوند، مشخص | <input type="checkbox"/> | سایر موارد | گردد. |
| <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 checked="" type="checkbox"/> | تغییر پیش‌فرض       | می‌شوند، مشخص  |                                     |                     |                    |                                     |               |                     |                                     |            |                    |                                     |               |               |                          |            |       |
| <input type="checkbox"/>            | سایر موارد          | گردد.  |                                     |                     |                    |                                     |               |                     |                                     |            |                    |                                     |               |               |                          |            |       |
|                                     | ۳                   | <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"> <tr> <td data-bbox="961 1382 1024 1424"><input checked="" type="checkbox"/></td> <td data-bbox="1024 1382 1711 1424">تغییر پیش‌فرض</td> <td data-bbox="1711 1382 2022 1424"></td> </tr> </table>   | <input checked="" type="checkbox"/> | تغییر پیش‌فرض       |                    |                                     |               |                     |                                     |            |                    |                                     |               |               |                          |            |       |
| <input checked="" type="checkbox"/> | تغییر پیش‌فرض       |  |                                     |                     |                    |                                     |               |                     |                                     |            |                    |                                     |               |               |                          |            |       |

|   |  |   |   |
|---|--|---|---|
| <input checked="" type="checkbox"/><br><input checked="" type="checkbox"/><br><input checked="" type="checkbox"/><br><input checked="" type="checkbox"/><br><input checked="" type="checkbox"/><br><input type="checkbox"/>   | حذف نمودن<br>پرس و جو<br>مقداره‌ی<br>ایجاد<br>مشاهده<br>سایر موارد   | عملیات بر روی داده‌های محصول که در محصول پشتیبانی می‌شوند، مشخص شود.                                    |   |
| <input checked="" type="checkbox"/>   | محصول باید توانایی انجام کارکردهای زیر را داشته باشد.  |   | ۴ |
| <input checked="" type="checkbox"/><br><input checked="" type="checkbox"/><br><input checked="" type="checkbox"/><br><input checked="" type="checkbox"/><br><input type="checkbox"/><br><input checked="" type="checkbox"/><br><input checked="" type="checkbox"/><br><input checked="" type="checkbox"/><br><input checked="" type="checkbox"/><br><input checked="" type="checkbox"/> | پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشده‌ها<br>پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشده‌ها<br>پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشده‌ها<br>مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول<br>انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده که می‌تواند در محصول قابل پیکربندی باشد. (برای مثال، زمان تخصیص و یا زمان آزادسازی منابع)<br>ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول<br>در نظر گرفتن یک عملیات از پیش تعیین‌شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد.<br>۱. مدیریت حد آستانه برای تلاش‌های ناموفق<br>۲. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد.<br>مدیریت معیارها برای تنظیم گذرواژه‌ها<br>۱. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه<br>۲. مدیریت یک‌سری عملیاتی که قبل از احراز شدن هویت کاربر انجام می‌شوند. | در صورتی که هر کدام از موارد مطرح‌شده، 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>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 1039 1068"><input checked="" type="checkbox"/></td> <td data-bbox="1039 1015 1711 1068">مدیر سیستم</td> <td data-bbox="1711 1015 2030 1068">نقش‌هایی که در</td> </tr> <tr> <td data-bbox="961 1068 1039 1122"><input checked="" type="checkbox"/></td> <td data-bbox="1039 1068 1711 1122">کاربر پیشرفته</td> <td data-bbox="1711 1068 2030 1122">محصول پشتیبانی</td> </tr> <tr> <td data-bbox="961 1122 1039 1175"><input checked="" type="checkbox"/></td> <td data-bbox="1039 1122 1711 1175">کاربر عادی</td> <td data-bbox="1711 1122 2030 1175">می‌شوند، مشخص</td> </tr> <tr> <td data-bbox="961 1175 1039 1214"><input type="checkbox"/></td> <td data-bbox="1039 1175 1711 1214">سایر موارد</td> <td data-bbox="1711 1175 2030 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. | ۵ |
| <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>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>   | 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   |
|         | <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.  |   |
|         | <input type="checkbox"/>            | 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.   |   |
|         | <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> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 5%; text-align: center;"><input type="checkbox"/></td> <td style="width: 75%;">گرفتن مهرهای زمانی از سرور NTP</td> <td style="width: 20%;">روش‌های ایجاد مهرهای زمانی معتبر</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>تنظیم مهرهای زمانی از طریق اینترنت</td> <td>انتخاب شود. (دیگر روشهای موجود در محصول، در قسمت «سایر موارد» بیان شود).</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>تنظیم مهرهای زمانی به صورت پیش فرض (معتبر و عدم امکان دستکاری غیرمجاز)</td> <td></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>سایر موارد</td> <td></td> </tr> </table> | <input type="checkbox"/>            | گرفتن مهرهای زمانی از سرور NTP | روش‌های ایجاد مهرهای زمانی معتبر  | <input 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 به صورت پیش فرض (معتبر و عدم امکان دستکاری غیرمجاز) |  | <input type="checkbox"/> | سایر موارد  |  |
| <input type="checkbox"/>            | گرفتن مهرهای زمانی از سرور NTP   | روش‌های ایجاد مهرهای زمانی معتبر   |                                     |                                |   |                          |                                    |  |                                     |  |  |                          |   |  |
| <input 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 به صورت پیش فرض (معتبر و عدم امکان دستکاری غیرمجاز) |  |                                     |                                |   |                          |                                    |  |                                     |  |  |                          |   |  |
| <input type="checkbox"/>            | سایر موارد   |  |                                     |                                |   |                          |                                    |  |                                     |  |  |                          |   |  |
|                                     | <input checked="" type="checkbox"/>                                    | <p>۵ محصول باید امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 5%; text-align: center;"><input checked="" type="checkbox"/></td> <td style="width: 75%;">بروزرسانی دستی</td> <td style="width: 20%;">روش بروزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>جستجوی خودکار بروزرسانی‌ها</td> <td></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>بروزرسانی‌های خودکار</td> <td></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی</td> <td></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        |  |                                     |                                |   |                          |                                    |  |                                     |  |  |                          |   |  |
|                                     | <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> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 5%; text-align: center;"><input type="checkbox"/></td> <td style="width: 75%;">امضای دیجیتال</td> <td style="width: 20%;">سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی)</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>درهم‌ساز منتشرشده</td> <td>به‌روزرسانی‌ها انتخاب گردد.</td> </tr> </table>  | <input type="checkbox"/>            | امضای دیجیتال                  | سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی)                                 | <input type="checkbox"/> | درهم‌ساز منتشرشده                  | به‌روزرسانی‌ها انتخاب گردد.  |                                     |  |  |                          |   |  |
| <input type="checkbox"/>            | امضای دیجیتال  | سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی)  |                                     |                                |   |                          |                                    |  |                                     |  |  |                          |   |  |
| <input type="checkbox"/>            | درهم‌ساز منتشرشده  | به‌روزرسانی‌ها انتخاب گردد.  |                                     |                                |   |                          |                                    |  |                                     |  |  |                          |   |  |

<sup>۳</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 |
|---------|---|-------------|
|         | <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.

| توضیحات                             | رده دسترسی به محصول                 |   | شماره الزام                         |     |                                 |                                     |      |                          |            |   |
|-------------------------------------|-------------------------------------|---|-------------------------------------|-----|---------------------------------|-------------------------------------|------|--------------------------|------------|---|
|                                     | <input checked="" type="checkbox"/> | محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.   | ۱                                   |     |                                 |                                     |      |                          |            |   |
|                                     | <input checked="" type="checkbox"/> | محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمانی که غیرفعال هستند (و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.  | ۲                                   |     |                                 |                                     |      |                          |            |   |
|                                     | <input checked="" type="checkbox"/> | محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.  | ۳                                   |     |                                 |                                     |      |                          |            |   |
|                                     | <input checked="" type="checkbox"/> | <p>در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد.</p> <table border="1" data-bbox="919 938 1948 1092"> <tr> <td data-bbox="919 938 961 987" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="961 938 1709 987">روز</td> <td data-bbox="1709 938 1948 1092" rowspan="3">انتخاب یک مورد لازم و کافی است.</td> </tr> <tr> <td data-bbox="919 987 961 1036" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="961 987 1709 1036">زمان</td> </tr> <tr> <td data-bbox="919 1036 961 1092" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="961 1036 1709 1092">سایر موارد</td> </tr> </table>   | <input checked="" type="checkbox"/> | روز | انتخاب یک مورد لازم و کافی است. | <input checked="" type="checkbox"/> | زمان | <input type="checkbox"/> | سایر موارد | ۴ |
| <input checked="" type="checkbox"/> | روز                                 | انتخاب یک مورد لازم و کافی است.   |                                     |     |                                 |                                     |      |                          |            |   |
| <input checked="" type="checkbox"/> | زمان                                |   |                                     |     |                                 |                                     |      |                          |            |   |
| <input type="checkbox"/>            | سایر موارد                          |   |                                     |     |                                 |                                     |      |                          |            |   |
|                                     | <input checked="" type="checkbox"/> | <p>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.</p> <table border="1" data-bbox="919 1255 1948 1401"> <tr> <td data-bbox="919 1255 961 1304" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="961 1255 1709 1304">روز</td> <td data-bbox="1709 1255 1948 1401" rowspan="3">انتخاب یک مورد لازم و کافی است.</td> </tr> <tr> <td data-bbox="919 1304 961 1352" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="961 1304 1709 1352">زمان</td> </tr> <tr> <td data-bbox="919 1352 961 1401" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="961 1352 1709 1401">سایر موارد</td> </tr> </table> | <input checked="" type="checkbox"/> | روز | انتخاب یک مورد لازم و کافی است. | <input checked="" type="checkbox"/> | زمان | <input type="checkbox"/> | سایر موارد | ۵ |
| <input checked="" type="checkbox"/> | روز                                 | انتخاب یک مورد لازم و کافی است.   |                                     |     |                                 |                                     |      |                          |            |   |
| <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 |
|  | <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 | رده کانال‌ها/مسیرهای مورد اعتماد    |  | شماره الزام   |
|---------|-------------------------------------|--|---|
|         | <input checked="" type="checkbox"/> | <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 ۳-۲- تا ۳-۴- که در بخش ۳- بیان گردیده است، الزامی است.</p> | ۱   |
|         | <input checked="" type="checkbox"/> | HTTPS  | پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد. |
|         | <input checked="" type="checkbox"/> | TLS  |   |
|         | <input type="checkbox"/>            | SSH  |   |
|         | <input checked="" type="checkbox"/> | محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.  | ۲   |
|         | <input checked="" type="checkbox"/> | محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.   | 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

| 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.<br>اعتبارسنجی گواهی‌نامه بر اساس الزامات بخش ۳-۵-۳ انجام می‌شود که در این صورت الزامات بخش ۳-۵-۳ الزامی است. | <input checked="" type="checkbox"/> |
|             | محصول تنها از موارد اتصال را برقرار نکند.  | <input checked="" type="checkbox"/> |
|             | بیان شده می‌تواند استفاده نماید.<br>برای برقراری اتصال درخواست مجوز کند.   | <input type="checkbox"/>            |

۲-۳- پروتکل TLS Client

| توضیحات                  | پروتکل TLS Client  |  | شماره الزام              |   |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |   |
|--------------------------|--|--|--------------------------|---|---|--------------------------|---|--------------------------|---|--------------------------|---|--------------------------|---|--------------------------|---|--------------------------|---|--------------------------|---|--------------------------|---|--------------------------|---|---|
|                          | <input checked="" type="checkbox"/> <p>محصل باید (RFC ۵۲۴۶) TLS ۱٫۲ و/یا (RFC ۴۳۴۶) TLS ۱٫۱ را پیاده‌سازی و دیگر نسخه‌های TLS و SSL را رد کند. همچنین محصل باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.</p> | <table border="1"> <tr> <td data-bbox="919 597 961 678"><input type="checkbox"/></td> <td data-bbox="961 597 1711 678">                     TLS_RSA_WITH_AES_۱۲۸_CBC_SHA<br/>                     مطابق با RFC ۳۲۶۸                 </td> <td data-bbox="1711 597 1948 1450" rowspan="10">                     مجموعه رمز مورد استفاده و پیاده‌سازی شده محصل، انتخاب گردد.                 </td> </tr> <tr> <td data-bbox="919 678 961 760"><input type="checkbox"/></td> <td data-bbox="961 678 1711 760">                     TLS_RSA_WITH_AES_۱۹۲_CBC_SHA<br/>                     مطابق با RFC ۳۲۶۸                 </td> </tr> <tr> <td data-bbox="919 760 961 841"><input type="checkbox"/></td> <td data-bbox="961 760 1711 841">                     TLS_RSA_WITH_AES_۲۵۶_CBC_SHA<br/>                     مطابق با RFC ۳۲۶۸                 </td> </tr> <tr> <td data-bbox="919 841 961 922"><input type="checkbox"/></td> <td data-bbox="961 841 1711 922">                     TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br/>                     مطابق با RFC ۳۲۶۸                 </td> </tr> <tr> <td data-bbox="919 922 961 1003"><input type="checkbox"/></td> <td data-bbox="961 922 1711 1003">                     TLS_DHE_RSA_WITH_AES_۱۹۲_CBC_SHA<br/>                     مطابق با RFC ۳۲۶۸                 </td> </tr> <tr> <td data-bbox="919 1003 961 1084"><input type="checkbox"/></td> <td data-bbox="961 1003 1711 1084">                     TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br/>                     مطابق با RFC ۳۲۶۸                 </td> </tr> <tr> <td data-bbox="919 1084 961 1166"><input type="checkbox"/></td> <td data-bbox="961 1084 1711 1166">                     TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br/>                     مطابق با RFC ۴۴۹۲                 </td> </tr> <tr> <td data-bbox="919 1166 961 1247"><input type="checkbox"/></td> <td data-bbox="961 1166 1711 1247">                     TLS_ECDHE_RSA_WITH_AES_۱۹۲_CBC_SHA<br/>                     مطابق با RFC ۴۴۹۲                 </td> </tr> <tr> <td data-bbox="919 1247 961 1328"><input type="checkbox"/></td> <td data-bbox="961 1247 1711 1328">                     TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br/>                     مطابق با RFC ۴۴۹۲                 </td> </tr> <tr> <td data-bbox="919 1328 961 1450"><input type="checkbox"/></td> <td data-bbox="961 1328 1711 1450">                     TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA<br/>                     مطابق با RFC ۴۴۹۲                 </td> </tr> </table> | <input type="checkbox"/> | TLS_RSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۳۲۶۸ | مجموعه رمز مورد استفاده و پیاده‌سازی شده محصل، انتخاب گردد. | <input type="checkbox"/> | TLS_RSA_WITH_AES_۱۹۲_CBC_SHA<br>مطابق با RFC ۳۲۶۸ | <input type="checkbox"/> | TLS_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۳۲۶۸ | <input type="checkbox"/> | TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۳۲۶۸ | <input type="checkbox"/> | TLS_DHE_RSA_WITH_AES_۱۹۲_CBC_SHA<br>مطابق با RFC ۳۲۶۸ | <input type="checkbox"/> | TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۳۲۶۸ | <input type="checkbox"/> | TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۴۴۹۲ | <input type="checkbox"/> | TLS_ECDHE_RSA_WITH_AES_۱۹۲_CBC_SHA<br>مطابق با RFC ۴۴۹۲ | <input type="checkbox"/> | TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۴۴۹۲ | <input type="checkbox"/> | TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۴۴۹۲ | ۱ |
| <input type="checkbox"/> | TLS_RSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۳۲۶۸  | مجموعه رمز مورد استفاده و پیاده‌سازی شده محصل، انتخاب گردد.  |                          |   |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |   |
| <input type="checkbox"/> | TLS_RSA_WITH_AES_۱۹۲_CBC_SHA<br>مطابق با RFC ۳۲۶۸  |  |                          |   |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |   |
| <input type="checkbox"/> | TLS_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۳۲۶۸  |  |                          |   |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |   |
| <input type="checkbox"/> | TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۳۲۶۸  |  |                          |   |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |   |
| <input type="checkbox"/> | TLS_DHE_RSA_WITH_AES_۱۹۲_CBC_SHA<br>مطابق با RFC ۳۲۶۸  |  |                          |   |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |   |
| <input type="checkbox"/> | TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۳۲۶۸  |  |                          |   |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |   |
| <input type="checkbox"/> | TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۴۴۹۲  |  |                          |   |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |   |
| <input type="checkbox"/> | TLS_ECDHE_RSA_WITH_AES_۱۹۲_CBC_SHA<br>مطابق با RFC ۴۴۹۲  |  |                          |   |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |   |
| <input type="checkbox"/> | TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۴۴۹۲  |  |                          |   |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |   |
| <input type="checkbox"/> | TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۴۴۹۲  |  |                          |   |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |                          |   |   |

|                                     |  |  |  |
|-------------------------------------|--|--|--|
| <input type="checkbox"/>            | TLS_ECDHE_ECDSA_WITH_AES_۱۹۲_CBC_SHA<br>مطابق با RFC ۴۴۹۲    |  |  |
| <input type="checkbox"/>            | TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۴۴۹۲    |  |  |
| <input type="checkbox"/>            | TLS_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۴۶         |  |  |
| <input type="checkbox"/>            | TLS_RSA_WITH_AES_۱۹۲_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۴۶         |  |  |
| <input type="checkbox"/>            | TLS_RSA_WITH_AES_۲۵۶_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۴۶         |  |  |
| <input type="checkbox"/>            | TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۴۶     |  |  |
| <input type="checkbox"/>            | TLS_DHE_RSA_WITH_AES_۱۹۲_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۴۶     |  |  |
| <input type="checkbox"/>            | TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۴۶     |  |  |
| <input type="checkbox"/>            | TLS_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶<br>مطابق با RFC ۵۲۸۸         |  |  |
| <input type="checkbox"/>            | TLS_RSA_WITH_AES_۱۹۲_GCM_SHA۲۵۶<br>مطابق با RFC ۵۲۸۸         |  |  |
| <input type="checkbox"/>            | TLS_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴<br>مطابق با RFC ۵۲۸۸         |  |  |
| <input type="checkbox"/>            | TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۸۹ |  |  |
| <input type="checkbox"/>            | TLS_ECDHE_ECDSA_WITH_AES_۱۹۲_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۸۹ |  |  |
| <input type="checkbox"/>            | TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA۳۸۴<br>مطابق با RFC ۵۲۸۹ |  |  |
| <input checked="" type="checkbox"/> | TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶<br>مطابق با RFC ۵۲۸۹ |  |  |
| <input type="checkbox"/>            | TLS_ECDHE_ECDSA_WITH_AES_۱۹۲_GCM_SHA۲۵۶                      |  |  |

|  |                                     |  |   |
|--|-------------------------------------|--|---|
|  |                                     | <input type="checkbox"/> مطابق با RFC ۵۲۸۹<br><input checked="" type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴<br>مطابق با RFC ۵۲۸۹<br><input checked="" type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶<br>مطابق با RFC ۵۲۸۹<br><input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۱۹۲_GCM_SHA۲۵۶<br>مطابق با RFC ۵۲۸۹<br><input checked="" type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴<br>مطابق با RFC ۵۲۸۹<br><input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۸۹<br><input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۱۹۲_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۸۹<br><input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA۳۸۴<br>مطابق با RFC ۵۲۸۹ |   |
|  | <input checked="" type="checkbox"/> | محصول باید مطابقت شناسه ارائه شده با شناسه مرجع را با توجه به بخش ۶ از RFC ۶۱۲۵ تأیید نماید.   | ۲   |
|  | <input checked="" type="checkbox"/> | 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.   | ۳   |
|  | <input checked="" type="checkbox"/> | ارتباط را برقرار نکند  | در صورت پشتیبانی از اقدامات دیگر، در «سایر» برای برقراری ارتباط درخواست مجوز کند<br>سایر موارد بیان گردد. |
|  | <input type="checkbox"/>            | سایر موارد   |   |
|  | <input type="checkbox"/>            | سایر موارد   |   |
|  | <input checked="" type="checkbox"/> | محصول 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.   |   |

|  |                                     |   |   |
|--|-------------------------------------|---|---|
|  | <input checked="" type="checkbox"/> | <p>Supported Elliptic Curves Extension را به همراه NIST Curve های</p> <p>secp<sup>۲۵۶</sup>r<sup>۱</sup> یا secp<sup>۳۸۴</sup>r<sup>۱</sup> یا secp<sup>۵۲۱</sup>r<sup>۱</sup> ارائه نماید.</p> | <p>در صورت که محصول از منحنی استفاده می‌نماید، طول کلید باید مشخص گردد.</p> |
|--|-------------------------------------|---|---|



۳-۳- پروتکل TLS Server

| توضیحات   | پروتکل TLS Server  |   | شماره الزام                                       |  |  |  |  |  |  |  |  |   |   |  |   |
|---|--|---|---|--|--|--|--|--|--|--|--|---|---|--|---|
|   | <input checked="" type="checkbox"/>                          | <p>محمول باید (RFC ۵۲۴۶) TLS ۱.۲ را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.</p> <table border="1" data-bbox="961 553 1711 1440"> <tr> <td data-bbox="961 553 1711 639">                     TLS_RSA_WITH_AES_۲۵۶_CBC_SHA<br/>                     مطابق با RFC ۳۲۶۸                 </td> <td data-bbox="1711 553 1948 1440" rowspan="12">                     مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.                 </td> </tr> <tr> <td data-bbox="961 639 1711 725"> <input type="checkbox"/>                     TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br/>                     مطابق با RFC ۳۲۶۸                 </td> </tr> <tr> <td data-bbox="961 725 1711 812"> <input type="checkbox"/>                     TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br/>                     مطابق با RFC ۳۲۶۸                 </td> </tr> <tr> <td data-bbox="961 812 1711 898"> <input type="checkbox"/>                     TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br/>                     مطابق با RFC ۴۴۹۲                 </td> </tr> <tr> <td data-bbox="961 898 1711 984"> <input type="checkbox"/>                     TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br/>                     مطابق با RFC ۴۴۹۲                 </td> </tr> <tr> <td data-bbox="961 984 1711 1070"> <input type="checkbox"/>                     TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br/>                     مطابق با RFC ۴۴۹۲                 </td> </tr> <tr> <td data-bbox="961 1070 1711 1156"> <input type="checkbox"/>                     TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA<br/>                     مطابق با RFC ۴۴۹۲                 </td> </tr> <tr> <td data-bbox="961 1156 1711 1242"> <input type="checkbox"/>                     TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_CBC_SHA<br/>                     مطابق با RFC ۴۴۹۲                 </td> </tr> <tr> <td data-bbox="961 1242 1711 1328"> <input type="checkbox"/>                     TLS_RSA_WITH_AES_۱۲۸_CBC_SHA<sup>۲۵۶</sup><br/>                     مطابق با RFC ۵۲۴۶                 </td> </tr> <tr> <td data-bbox="961 1328 1711 1414"> <input type="checkbox"/>                     TLS_RSA_WITH_AES_۲۵۶_CBC_SHA<sup>۲۵۶</sup><br/>                     مطابق با RFC ۵۲۴۶                 </td> </tr> <tr> <td data-bbox="961 1414 1711 1440"> <input type="checkbox"/>                     TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA<sup>۲۵۶</sup> </td> </tr> </table> | TLS_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۳۲۶۸ | مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد. | <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۳۲۶۸ | <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۳۲۶۸ | <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۴۴۹۲ | <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۴۴۹۲ | <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۴۴۹۲ | <input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۴۴۹۲ | <input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۴۴۹۲ | <input type="checkbox"/> TLS_RSA_WITH_AES_۱۲۸_CBC_SHA <sup>۲۵۶</sup><br>مطابق با RFC ۵۲۴۶ | <input type="checkbox"/> TLS_RSA_WITH_AES_۲۵۶_CBC_SHA <sup>۲۵۶</sup><br>مطابق با RFC ۵۲۴۶ | <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA <sup>۲۵۶</sup> | ۱ |
| TLS_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۳۲۶۸   | مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد. |   |   |  |  |  |  |  |  |  |  |   |   |  |   |
| <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۳۲۶۸            |  |   |   |  |  |  |  |  |  |  |  |   |   |  |   |
| <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۳۲۶۸            |  |   |   |  |  |  |  |  |  |  |  |   |   |  |   |
| <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۴۴۹۲          |  |   |   |  |  |  |  |  |  |  |  |   |   |  |   |
| <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۴۴۹۲          |  |   |   |  |  |  |  |  |  |  |  |   |   |  |   |
| <input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۴۴۹۲          |  |   |   |  |  |  |  |  |  |  |  |   |   |  |   |
| <input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA<br>مطابق با RFC ۴۴۹۲        |  |   |   |  |  |  |  |  |  |  |  |   |   |  |   |
| <input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_CBC_SHA<br>مطابق با RFC ۴۴۹۲        |  |   |   |  |  |  |  |  |  |  |  |   |   |  |   |
| <input type="checkbox"/> TLS_RSA_WITH_AES_۱۲۸_CBC_SHA <sup>۲۵۶</sup><br>مطابق با RFC ۵۲۴۶ |  |   |   |  |  |  |  |  |  |  |  |   |   |  |   |
| <input type="checkbox"/> TLS_RSA_WITH_AES_۲۵۶_CBC_SHA <sup>۲۵۶</sup><br>مطابق با RFC ۵۲۴۶ |  |   |   |  |  |  |  |  |  |  |  |   |   |  |   |
| <input type="checkbox"/> TLS_DHE_RSA_WITH_AES_۱۲۸_CBC_SHA <sup>۲۵۶</sup>                  |  |   |   |  |  |  |  |  |  |  |  |   |   |  |   |

|  |   |  |
|--|---|--|
|  | <input type="checkbox"/> مطابق با RFC ۵۲۴۶<br><input type="checkbox"/> TLS_DHE_RSA_WITH_AES_۲۵۶_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۴۶<br><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_CBC_SHA۲۵۶<br>مطابق با RFC ۵۲۸۹<br><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_CBC_SHA۳۸۴<br>مطابق با RFC ۵۲۸۹<br><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶<br>مطابق با RFC ۵۲۸۹<br><input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴<br>مطابق با RFC ۵۲۸۹<br><input checked="" type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۱۲۸_GCM_SHA۲۵۶<br>مطابق با RFC ۵۲۸۹<br><input checked="" type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_۲۵۶_GCM_SHA۳۸۴<br>مطابق با RFC ۵۲۸۹ |  |
|  | <input checked="" type="checkbox"/> محصول باید اتصال‌های کاربرانی که درخواست SSL۱٫۰، SSL۲٫۰، SSL۳٫۰ و TLS۱٫۰ دارند را رد نماید.   | ۲  |
|  | <input checked="" type="checkbox"/> محصول 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<br><input checked="" type="checkbox"/> پارامترهای ECDH با استفاده از NIST Curve های secp۲۵۶r۱ یا secp۳۸۴r۱ و هیچ مورد دیگر<br><input type="checkbox"/> پارامترهای دیفی-هلمن با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ بیت   | در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد. |

## 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 checked="" 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 گواهی‌نامه

| توضیحات | اعتبارسنجی گواهی‌نامه   | شماره الزام                       |
|---------|---|-----------------------------------|
|         | <input checked="" type="checkbox"/> محصول باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند.   | ۱                                 |
|         | <input checked="" type="checkbox"/> تأیید گواهی‌نامه ۵۲۸۰ RFC و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.   |                                   |
|         | <input checked="" type="checkbox"/> مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.  |                                   |
|         | <input checked="" type="checkbox"/> محصول باید برای تأیید مسیر یک گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم شده است.             |                                   |
|         | <input type="checkbox"/> پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC ۶۹۶  |                                   |
|         | <input type="checkbox"/> لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC ۵۲۸۰ بخش ۶.۳   | روش‌های تأیید وضعیت               |
|         | <input type="checkbox"/> لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC ۵۷۵۹ بخش ۵   | فسخ گواهی‌نامه                    |
|         | <input checked="" type="checkbox"/> هیچ روش فسخ دیگری   |                                   |
|         | <input type="checkbox"/> گواهی‌نامه‌های 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"/> گواهی‌نامه‌های 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-kp<sup>۱</sup> 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-pk<sup>۹</sup> 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 احراز هویت برای موارد زیر از گواهی‌نامه‌های X<sup>۵۰۹۷۳</sup> تعریف شده در RFC ۵۲۸۰ استفاده کند.</p> <table border="1" data-bbox="961 722 1711 1021"> <tr> <td data-bbox="961 722 997 771"> <input checked="" type="checkbox"/> </td> <td data-bbox="997 722 1711 771">HTTPS</td> <td data-bbox="1711 722 1948 1021" rowspan="7"> <p>در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.</p> </td> </tr> <tr> <td data-bbox="961 771 997 820"> <input checked="" type="checkbox"/> </td> <td data-bbox="997 771 1711 820">TLS</td> </tr> <tr> <td data-bbox="961 820 997 868"> <input type="checkbox"/> </td> <td data-bbox="997 820 1711 868">SSH</td> </tr> <tr> <td data-bbox="961 868 997 917"> <input type="checkbox"/> </td> <td data-bbox="997 868 1711 917">امضای کد برای بروزرسانی‌های نرم‌افزار سیستم</td> </tr> <tr> <td data-bbox="961 917 997 966"> <input type="checkbox"/> </td> <td data-bbox="997 917 1711 966">امضای کد برای تأیید یکپارچگی</td> </tr> <tr> <td data-bbox="961 966 997 1015"> <input type="checkbox"/> </td> <td data-bbox="997 966 1711 1015">سایر موارد</td> </tr> <tr> <td data-bbox="961 1015 997 1021"></td> <td data-bbox="997 1015 1711 1021"></td> </tr> </table> | <input checked="" type="checkbox"/> | HTTPS | <p>در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.</p> | <input checked="" 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 |
| <input checked="" type="checkbox"/> | HTTPS                                       | <p>در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.</p>  |                                     |       |   |                                     |     |                          |     |                          |   |                          |                              |                          |            |  |  |   |
| <input checked="" 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 RFC های ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۵۶۵۶ و ۶۶۶۸ پیاده‌سازی نماید.   | ۱                        |                                |                          |                             |                          |            |                          |            |                          |            |                          |            |                          |                  |                          |                  |   |
|                          | <input 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="957 667 1711 769"> <tr> <td data-bbox="957 667 1024 716"><input type="checkbox"/></td> <td data-bbox="1024 667 1711 716">احراز هویت مبتنی بر کلید عمومی</td> </tr> <tr> <td data-bbox="957 716 1024 769"><input type="checkbox"/></td> <td data-bbox="1024 716 1711 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 ۴۲۵۳، 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="957 997 1711 1365"> <tr> <td data-bbox="957 997 1024 1045"><input type="checkbox"/></td> <td data-bbox="1024 997 1711 1045">AES۱۲۸-CBC</td> </tr> <tr> <td data-bbox="957 1045 1024 1094"><input type="checkbox"/></td> <td data-bbox="1024 1045 1711 1094">AES۱۹۲-CBC</td> </tr> <tr> <td data-bbox="957 1094 1024 1143"><input type="checkbox"/></td> <td data-bbox="1024 1094 1711 1143">AES۲۵۶-CBC</td> </tr> <tr> <td data-bbox="957 1143 1024 1192"><input type="checkbox"/></td> <td data-bbox="1024 1143 1711 1192">AES۱۲۸-CTR</td> </tr> <tr> <td data-bbox="957 1192 1024 1240"><input type="checkbox"/></td> <td data-bbox="1024 1192 1711 1240">AES۱۹۲-CTR</td> </tr> <tr> <td data-bbox="957 1240 1024 1289"><input type="checkbox"/></td> <td data-bbox="1024 1240 1711 1289">AES۲۵۶-CTR</td> </tr> <tr> <td data-bbox="957 1289 1024 1338"><input type="checkbox"/></td> <td data-bbox="1024 1289 1711 1338">AEAD_AES_۱۲۸_GCM</td> </tr> <tr> <td data-bbox="957 1338 1024 1365"><input type="checkbox"/></td> <td data-bbox="1024 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 type="checkbox"/> | AES۱۲۸-CTR | <input type="checkbox"/> | AES۱۹۲-CTR | <input 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 type="checkbox"/> | AES۱۲۸-CTR                     |   |                          |                                |                          |                             |                          |            |                          |            |                          |            |                          |            |                          |                  |                          |                  |   |
| <input type="checkbox"/> | AES۱۹۲-CTR                     |   |                          |                                |                          |                             |                          |            |                          |            |                          |            |                          |            |                          |                  |                          |                  |   |
| <input type="checkbox"/> | AES۲۵۶-CTR                     |   |                          |                                |                          |                             |                          |            |                          |            |                          |            |                          |            |                          |                  |                          |                  |   |
| <input type="checkbox"/> | AEAD_AES_۱۲۸_GCM               |   |                          |                                |                          |                             |                          |            |                          |            |                          |            |                          |            |                          |                  |                          |                  |   |
| <input type="checkbox"/> | AEAD_AES_۲۵۶_GCM               |   |                          |                                |                          |                             |                          |            |                          |            |                          |            |                          |            |                          |                  |                          |                  |   |

|                          |   |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
|--------------------------|---|--------------------------|-------------------|--------------------------|------------------|--------------------------|---------------|--------------------------|---------------|--------------------------|--------------------|--------------------------|---------------------|--------------------------|---------------------|--------------------------|---------------------------|--------------------------|----------------------------|--------------------------|----------------------------|--------------------------|-----------------------|--------------------------|---------|--------------------------|----------------|---|
|                          | <p><input 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 type="checkbox"/></td><td>ssh-ed۲۵۵۱۹</td></tr> <tr><td><input type="checkbox"/></td><td>ssh-ed۴۴۸</td></tr> <tr><td><input type="checkbox"/></td><td>rsa-sha۲-۵۱۲</td></tr> <tr><td><input type="checkbox"/></td><td>rsa-sha۲-۲۵۶</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha۲-nistp۲۱</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha۲-nistp۳۸۴</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha۲-nistp۲۵۶</td></tr> <tr><td><input type="checkbox"/></td><td>x۵۰۹۷۳-ecdsa-sha۲-nistp۲۱</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 type="checkbox"/></td><td>ssh-rsa</td></tr> <tr><td><input type="checkbox"/></td><td>x۵۰۹۷۳-ssh-rsa</td></tr> </table> | <input type="checkbox"/> | ssh-ed۲۵۵۱۹       | <input type="checkbox"/> | ssh-ed۴۴۸        | <input type="checkbox"/> | rsa-sha۲-۵۱۲  | <input type="checkbox"/> | rsa-sha۲-۲۵۶  | <input type="checkbox"/> | ecdsa-sha۲-nistp۲۱ | <input type="checkbox"/> | ecdsa-sha۲-nistp۳۸۴ | <input type="checkbox"/> | ecdsa-sha۲-nistp۲۵۶ | <input type="checkbox"/> | x۵۰۹۷۳-ecdsa-sha۲-nistp۲۱ | <input type="checkbox"/> | x۵۰۹۷۳-ecdsa-sha۲-nistp۳۸۴ | <input type="checkbox"/> | x۵۰۹۷۳-ecdsa-sha۲-nistp۲۵۶ | <input type="checkbox"/> | x۵۰۹۷۳-rsa۲۰۴۸-sha۲۵۶ | <input type="checkbox"/> | ssh-rsa | <input type="checkbox"/> | x۵۰۹۷۳-ssh-rsa | ۵ |
| <input type="checkbox"/> | ssh-ed۲۵۵۱۹   |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | ssh-ed۴۴۸   |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | rsa-sha۲-۵۱۲  |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | rsa-sha۲-۲۵۶  |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | ecdsa-sha۲-nistp۲۱  |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | ecdsa-sha۲-nistp۳۸۴   |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | ecdsa-sha۲-nistp۲۵۶   |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | x۵۰۹۷۳-ecdsa-sha۲-nistp۲۱   |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | x۵۰۹۷۳-ecdsa-sha۲-nistp۳۸۴  |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | x۵۰۹۷۳-ecdsa-sha۲-nistp۲۵۶  |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | x۵۰۹۷۳-rsa۲۰۴۸-sha۲۵۶   |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | ssh-rsa   |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | x۵۰۹۷۳-ssh-rsa  |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
|                          | <p><input type="checkbox"/> محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های MAC صحت داده‌های زیر استفاده نماید.</p> <table border="1" data-bbox="919 982 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 type="checkbox"/></td><td>hmac-sha۲-۵۱۲</td></tr> <tr><td><input 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 type="checkbox"/> | hmac-sha۲-۵۱۲ | <input 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 type="checkbox"/> | hmac-sha۲-۵۱۲   |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | hmac-sha۲-۲۵۶   |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | hmac-sha۱-۹۶  |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
| <input type="checkbox"/> | hmac-sha۱   |                          |                   |                          |                  |                          |               |                          |               |                          |                    |                          |                     |                          |                     |                          |                           |                          |                            |                          |                            |                          |                       |                          |         |                          |                |   |
|                          | <p><input type="checkbox"/> محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های تبادل کلید زیر استفاده نماید.</p> <table border="1" data-bbox="919 1375 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"/> | diffie-hellman-group-exchange-sha۲۵۶<br>diffie-hellman-group۱۸-sha۵۱۲<br>diffie-hellman-group۱۷-sha۵۱۲<br>diffie-hellman-group۱۶-sha۵۱۲<br>diffie-hellman-group۱۵-sha۵۱۲<br>ecdh-sha۲-nistp۵۲۱<br>ecdh-sha۲-nistp۳۸۴<br>ecdh-sha۲-nistp۲۵۶<br>rsa۲۰۴۸-sha۲۵۶<br>diffie-hellman-group-exchange-sha۱<br>diffie-hellman-group۱۴-sha۲۵۶ |  |   |
|  | <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 ۴۲۵۱ بخش ۱.۷) همراه می‌کند، استفاده می‌نماید.   |  | ۹ |