

## سند هدف امنیتی

### اتوماسیون طراحان مقدم نسخه وب

موضوع	تهیه کننده	شماره ویرایش	تاریخ تهیه
سند هدف امنیتی برنامه های کاربردی تحت شبکه	واحد فنی شرکت طراحان بهینه	1.4	1400/01/25
کلیه حقوق مالکیت این مستند، مربوط به شرکت صنایع فناوری طراحان بهینه می باشد. هرگونه نشر، کپی برداری، انتقال به غیر و افشاسازی، بدون مجوز کتبی شرکت طراحان بهینه، منع قانونی دارد.			

## فهرست مطالب

صفحه	عنوان
2	فهرست
3	معرفی
4	ادعای انطباق
4	انطباق با استاندارد ارزیابی امنیتی معیار مشترک
4	شرح محصول
5	مسائل امنیتی
7	تهدیدات
8	خط مشی امنیت
9	فرضیات
9	اهداف امنیتی
9	اهداف امنیتی برای محصول
11	اهداف عملیاتی برای محیط عملیاتی
12	الزامات امنیتی
12	ممیزی امنیت (لاگ)
16	رمزنگاری
18	شناسایی و احراز هویت
22	حفاظت از داده های کاربری
26	مدیریت امنیت
29	حفاظت از توابع امنیتی محصول
31	تخصیص منابع
32	دسترسی به محصول
34	الزامات امنیتی مبتنی بر انتخاب
36	پروتکل HTTPS
36	پروتکل TLS Client
39	پروتکل TLS Server
42	پروتکل TLS مشترک کلاینت و سرور
43	اعتبارسنجی گواهی نامه

## 1- معرفی

### 1-1- مشخصات سند و محصول

عنوان سند هدف امنیتی	سند هدف امنیتی
نسخه	1.4
تاریخ	1400/01/25
نویسندگان	واحد فنی شرکت صنایع فن آوری طراحان بهینه

نام شرکت	صنایع فن آوری طراحان بهینه
نام محصول	اتوماسیون طراحان مقدم تحت وب
نوع محصول	محصولات کاربردی سازمانی
نسخه‌ی محصول	96.0.6

### حداقل نیازمندی نرم‌افزاری / سخت‌افزاری / میان‌افزاری محصول

سخت‌افزار / نرم‌افزار / میان‌افزار	حداقل الزامات
پیش نیاز نرم افزارهای خاص (مورد نیاز سامانه و نصب توسط پیمانکار)	sql server 2019 Management Studio 17 , Management Studio 18
نوع OS (Linux-windows)	windows
فضای ذخیره سازی مورد نیاز شامل نوع و حجم Data (برآورد رشد دیتا و ...)	C : 100 GB OS D : 200+ GB MDF LDF F : 200+ GB Backup
میزان Ram مورد نیاز	32-64 GB
تعداد CPU Core مورد نیاز	16-32

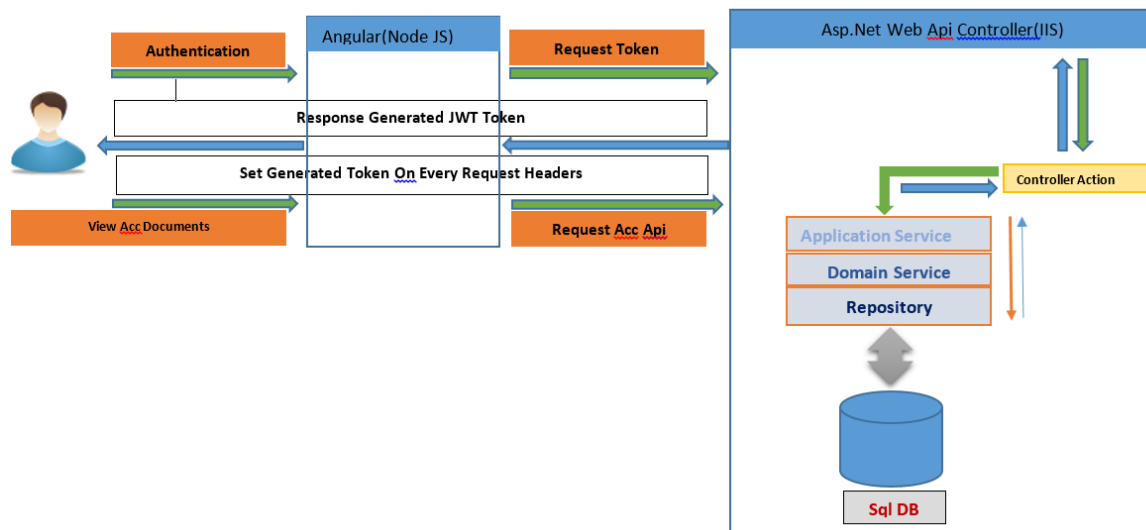
## 2- ادعای انطباق

### 1-2- انطباق با استاندارد ارزیابی امنیتی معیار مشترک

ISO 15408 V3.1 R4	انطباق با استاندارد ارزیابی امنیتی معیار مشترک
پرو فایل حفاظتی برنامه های کاربردی تحت شبکه	نام پرو فایل حفاظتی
EAL1	سطح تضمین امنیتی

### 2-2- شرح محصول

#### 1-2-2-1 حوزه فیزیکی



شکل 1: حوزه فیزیکی محصول با تفکیک حوزه محصول و محیط عملیاتی آن

### 2-2-2- حوزه منطقی

کارکردها	توصیف
احراز هویت	ارتباط نرم افزار با سرور Directory Active و شناسایی هویت فرد ، احراز هویت با استفاده از ارسال پیامک
رویداد نگاری	تمامی فعالیت های انجام شده توسط کاربران ثبت شده و قابل مشاهده می باشد
کنترل دسترسی ها	هدف از این ارزیابی کنترل سطوح دسترسی هم در سطح عملیات و هم در سطح دیتا می باشد. بطوریکه تنها موجودیت های مجاز خاص دارای دسترسی به داده و کارکردها هستند. برای کاربران مجاز کنترل سطوح دسترسی معمولا با استفاده از داده احراز هویت انجام می گیرد.

### 3- مسائل امنیتی

#### 3-1- تهدیدات

تهدیدات	توضیحات
دسترسی غیرمجاز	<p>مهاجم میتواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا نماید. این دسترسی میتواند با استفاده از هویت سرقتی، آدرس IP جعلی و غیره صورت گیرد.</p> <p>مهاجم میتواند با سود بردن از نقضهای امنیتی همچون تغییر ندادن کلمه عبور و نام کاربری، استفاده از کلمه عبور ساده، غیرفعال نکردن حساب کاربری تست بر روی سیستم واقعی به محصول دسترسی پیدا نماید. همچنین مهاجم میتواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد.</p> <p>این داده ها میتوانند داده های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم میتواند با دسترسی به داده ها و خود محصول سبب آسیب شود.</p>

توضیحات	تهدیدات
<p>رکوردهای، مستندات و داده های حفاظت شده توسط محصول میتواند بدون مجوز تغییر یابند. مهاجم میتواند با گمراه نمودن مدیر سیستم، وارد کننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می تواند از طرق غیر قانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده های حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ میدهد که صحت رکوردها و مستندات تضمین شده نمیشود. مهاجم ممکن است در صدد تغییر داده ممیزی یا کد منبع برآید. و بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا نماید.</p>	<p>تغییر غیرمجاز</p>
<p>یک اقدام یا یک تراکنش صورت گرفته بر روی محصول میتواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول میباشد تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم میتواند از رکوردهای ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم میتواند با اضافه نمودن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه نماید.</p>	<p>انکار</p>
<p>داده های محرمانه که توسط محصول محافظت میشوند میتواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی میتواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی میتواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور وارد کننده داده میتواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.</p>	<p>افشای اطلاعات</p>

توضیحات	تهدیدات
<p>مهاجم میتواند سبب گردد محصول در یک بازه زمانی غیر قابل دسترسی یا بلا استفاده گردد. این امر معمولاً با ارسال درخواستهای بسیار در یک بازه زمانی کوتاه صورت میگیرد طوری که محصول قادر به پاسخ نخواهد بود.</p> <p>نوع ساده ای از حمله شامل ارسال درخواستهای بسیار از یک رنج IP مشخص میباشد که به نام حمله DOS شناخته میشود. نوع دیگر پیشرفته تر حمله DDoS میباشد که از BOTNET استفاده مینماید و محدودیتی بر روی آدرس IP ورودی ندارد.</p>	<p>انکار سرویس</p>
<p>مهاجم میتواند یک رکورد، سند یا داده مضر را در داخل محصول وارد نماید. با استفاده از این تهدید، مهاجم میتواند به داده کاربر خاص دسترسی پیدا نماید، حساب کاربری یک کاربر را به دست گیرد یا به بخشی از کارکردها یا تمام کارکردهای محصول دسترسی یابد.</p>	<p>داده های ورودی مخرب</p>
<p>مهاجم میتواند با سود بردن از دسترسی غیرمجاز، ورود داده های مخرب و تغییر داده ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاتر نماید.</p>	<p>سطح دسترسی بالاتر</p>
<p>در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر میشود تا انتقال دادههای حساس بین محصول و مقصد موردنظر را مورد نظارت قرار دهد. این حمله شامل نظارت بر دادههای ردوبدل شده بین محصول و یک یا چند کاربر از راه دور و یا محلی است. به عنوان مثال میتوان به موردی اشاره کرد که در آن یک کاربر تلاش میکند تا جهت احراز هویت و ورود به برنامه، اطلاعات محرمانه خود را وارد میکند.</p>	<p>شنود شبکه</p>

### 3-2- خط مشی امنیتی

توضیحات	خط مشی ها
<p>تمام رخدادهای بر روی محیط کاری محصول باید ثبت گردد، رکوردها محافظت شده هستند و معمولاً به منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار میگیرند.</p>	<p>ممیزی کامل</p>

خط مشی ها	توضیحات
ارتباطات امن مبتنی بر TLS	تمام کانالهای ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.
پیکربندی مناسب	پیکربندی پیشفرض محصول و مولفه های تعاملی تحت کنترل محصول باید تغییر یابند. طوریکه مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویسهایی که مورد استفاده نیستند، باید غیرفعال گردند. پارامترهای پیکربندی همچون دایرکتوری root پیشفرض، خطاهای پیشفرض و صفحات 404، مقادیر احراز هویت پیشفرض، نام کاربری پیشفرض، پورتهای پیشفرض، صفحات پیشفرض که اطلاعات داخلی همچون شماره نسخه را آشکار مینمایند. این خط مشی سازمانی بسیار مهم است به خصوص زمانیکه محصول یا هر مولفه تعاملی به طور گسترده مورد استفاده قرار میگیرد. بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی میتوان از حملهی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.
امضای دیجیتال	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تأیید موجود باشد.

### 3-3- فرضیات

فرضیات	توضیحات
کاربران آموزش دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده اند و قوانین را دنبال مینمایند.
توسعه دهندگان آموزش دیده	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال مینمایند.
توسعه دهندگان مجرب	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب پذیری های شناخته شده را اتخاذ مینمایند.



توضیحات	فرضیات
فرض شده است که تمام پیش بینی های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری محصول به طور مناسب محدود شده و رکوردهای دسترسی برای یک بازه زمانی منطقی حفظ شده است. فرض شده است که سازوکاری وجود دارد تا رکوردها و مستندات که غیر قانونی از محصول به دست آمده را تشخیص دهد. همچنین فرض شده است که در قبال حملات DOS اقدامات مناسبی صورت میگیرد.	محیط امن
فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره سازی و دیگر مولفه های سخت افزاری دارای پشتیبان مناسبی هستند، و بنابر وجود نسخه پشتیبان هیچ داده ای از دست نمیروند همچنین به علت شکست در سیستم، قطع سرویسی رخ نمیدهد	پشتیبان گیری مناسب
فرض شده است که تمام ارتباطات و کانالهای ارتباطی مورد استفاده توابع امنیتی محصول جهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به طور مناسبی در قبال حملاتی چون DOS و شنود شبکه و غیره حفاظت میشوند.	ارتباطات
فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت میگیرد.	تحویل امن
فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ میشود.	انکار سرویس توزیع شده

#### 4- اهداف امنیتی

##### 4-1- اهداف امنیتی برای محصول

توضیحات	هدف امنیتی
محصول باید هر رخدادی که در زمینه امنیتی دارای ارزش است را در حوزه مالکیتش رکورد نماید. محصول باید از این رکوردها در قبال تغییرات و حذف محافظت نماید. محصول باید به	ممیزی

توضیحات	هدف امنیتی
کاربران مجاز امکان بررسی آسان و سریع رکوردها را بدهد و مدیر سیستم را به موقع از رخداد امنیتی بحرانی آگاه نماید.	
محصول باید هر کاربری را تعریف نموده و آنها را به طور امن احراز هویت نماید و مطابق با نقش و مجوزهایشان مجاز نماید. محصول باید برای احراز هویت کاربر، قوانینی تعریف نماید طوری که کاربران را ملزم به استفاده از کلمه های عبور قدرتمند نماید. محصول باید اجازه طبقه بندی رکوردها و مستندات را دهد و با توجه به طبقه بندی آنها قوانینی را تعریف نماید. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم مینماید. محصول باید برای کاربران به صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها فراهم نماید. مهاجم در تلاش است تا از تهدیدی چون رسیدن به سطح دسترسی بالاتر نهایت سود را ببرد. برای جلوگیری از این تهدید، محصول باید با استفاده از سازوکارهای قویتری مدیر سیستم را احراز هویت نماید. از جمله سازوکارها میتوان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احراز هویت براساس توکن، احراز هویت چند فاکتوری و ترکیبی از این روشها اشاره نمود.	احراز هویت
محصول باید گردش داده های غیرمجاز را کنترل و مدیریت نماید. داده های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواستها از یک رنج IP تعریف شده میتواند بیانگر حمله DOS باشد. محصول باید برای مدیر سیستم واسطی را فراهم نماید که به وی اجازه حفظ ترافیک شبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده نماید.	کنترل جریان داده
محصول باید نسبت به صحت داده ممیزی و داده ی رکورد با تشخیص هرگونه تغییر بر روی این داده ها اطمینان حاصل نماید و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد	صحت داده
محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارآمد سیستم فراهم نماید. محصول باید سازوکارهای کنترل دسترسی مناسبی جهت حفاظت از واسطهای مدیریتی در نظر گیرد. محصول باید برای مدیر سیستم امکان تغییر مجوزها و نقشهای کاربران را فراهم آورد و مدیر بتواند برای یک کاربر خاص و/یا گروهی از کاربران نقشها و مجوزهایی تنظیم نماید.	مدیریت

توضیحات	هدف امنیتی
محصول باید صورت امن و کارآمد سازوکار مدیریت خطا فراهم نماید. خطاهای رخ داده در طول عملیات محصول باید به کاربر به صورت امن و معنادار نشان داده شود. برای مثال، محصول باید اطلاعات کلی مربوط به احراز هویت ناموفق را برگرداند، همچنین برای کاربر عادی نباید اطلاعات جزئی چون شماره خط خطا برگردانده شود. از سوی دیگر مدیر سیستم باید سریعاً از شکست بحرانی که رخ داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صورت رخ دادن خطا باید وضعیت امنی را حفظ نماید.	مدیریت خطا
محصول باید اطمینان دهد که هر داده ی باقیمانده از محصول زمانیکه دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس میگردد.	مدیریت داده های باقیمانده
تمام کانالهای ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.	ارتباطات امن مبتنی بر TLS

#### 2-4- اهداف امنیتی برای محیط عملیاتی

توضیحات	هدف امنیتی
محیط عملیاتی محصول باید نسبت به امنیت محیطی و فیزیکی محصول اطمینان دهد. دسترسی غیرمجاز باید محدود گردیده و تمام مولفه ها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مولفه های حساس را داشته باشند. محیط عملیاتی محصول باید اطمینان دهد محصول به طور مناسب در قبال هر حمله DOS یا DDOS محافظت شده است. از جمله سازوکارهای حفاظتی میتوان به غیرفعال نمودن سرویسها، پورتهای و دیگر موارد استفاده شده اشاره نمود.	محیط امن
محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه های ارتباطی امن فراهم گردد.	ارتباطات
محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده مینمایند.	کاربران آموزش دیده
محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده مینمایند.	توسعه دهندگان آموزش دیده

توضیحات	هدف امنیتی
محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهندهی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابله‌ای لازم برای تمام آسیب‌پذیریهای امنیتی شناخته شده را در نظر می‌گیرد.	توسعه دهندگان مجرب
محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مولفه‌های غیر از محصول نیز مورد ممیزی قرار می‌گیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول می‌باشد. رکوردهای ممیزی محصول در صورت ترکیب با باقی رکوردهای ممیزی بسیار معنادار خواهند بود	ممیزی کامل
تحویل و نصب محصول باید بدون به خطر افتادن هرگونه محدودیت امنیتی انجام شود. علاوه بر این، کارکردها و/یا پارامترهای استفاده شده به منظور تست باید پاک یا غیر قابل دسترس گردند.	تحویل امن
نسخه پشتیبان باید ایجاد گردیده و برای یک بازه زمانی منطقی تمام داده‌های باقیمانده در محیط عملیاتی محصول را حفظ نماید. برای این منظور ممکن است از روالهای از پیش تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره‌سازی و دیگر مولفه‌های سخت‌افزاری نیز نسخه پشتیبان تهیه گردد.	پشتیبان-گیری مناسب

## 5- الزامات امنیتی

الزامات امنیتی این سند بر اساس نسخه 1.1 پروفایل حفاظتی «برنامه‌های کاربردی تحت شبکه» تهیه شده است. ساختار این سند بدین صورت است که برای هر کلاس در پروفایل حفاظتی مربوطه، یک دسته الزام بیان شده است.

### 5-1- ممیزی امنیت (لاگ)

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

توضیحات	کلاس ممیزی (لاگ)		شماره الزام																																					
	<input checked="" type="checkbox"/>	<p>محصول باید برای موارد مشخص شده که در ذیل آمده است، رکورد ممیزی تولید کند (لاگ ثبت 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>شروع و اتمام توابع</td> <td rowspan="18" style="vertical-align: middle; text-align: center;">                     رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.                 </td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>تلاشهای ناموفق برای خواندن اطلاعات از رکوردهای لاگ</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>خواندن اطلاعات از رکوردهای لاگ</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>تمامی تغییرات در پیکربندی لاگ</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>عملیات انجام شده به دلیل سرریز حافظه لاگ از حد آستانه</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>عملیات انجام شده به دلیل شکست در ذخیره‌سازی لاگها</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>تمام کاربردهای سازوکار احراز هویت</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>نتایج نهایی عملیات احراز هویت</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>تلاش موفق و ناموفق هر کلمه عبور تست شده توسط محصول</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>تمامی درخواستهای (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه مشخصه‌های امنیتی)</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>همه تلاش‌ها برای خارج کردن اطلاعات از محصول</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>تمامی تغییرات در رفتارهای توابع کارکردی محصول</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>استفاده از کارکردهای مدیریتی</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>تغییرات در گروه کاربران</td> </tr> </table>	<input checked="" type="checkbox"/>	شروع و اتمام توابع	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.	<input checked="" type="checkbox"/>	تلاشهای ناموفق برای خواندن اطلاعات از رکوردهای لاگ	<input checked="" type="checkbox"/>	خواندن اطلاعات از رکوردهای لاگ	<input checked="" type="checkbox"/>	تمامی تغییرات در پیکربندی لاگ	<input checked="" type="checkbox"/>	عملیات انجام شده به دلیل سرریز حافظه لاگ از حد آستانه	<input checked="" type="checkbox"/>	عملیات انجام شده به دلیل شکست در ذخیره‌سازی لاگها	<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 کلمه عبور تست شده توسط محصول	<input checked="" type="checkbox"/>	شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)	<input checked="" type="checkbox"/>	تمامی تغییرات بر روی مقادیر مشخصه‌های 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 مشخصه‌های 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	1
<input checked="" type="checkbox"/>	شروع و اتمام توابع	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.																																						
<input checked="" type="checkbox"/>	تلاشهای ناموفق برای خواندن اطلاعات از رکوردهای لاگ																																							
<input checked="" type="checkbox"/>	خواندن اطلاعات از رکوردهای لاگ																																							
<input checked="" type="checkbox"/>	تمامی تغییرات در پیکربندی لاگ																																							
<input checked="" type="checkbox"/>	عملیات انجام شده به دلیل سرریز حافظه لاگ از حد آستانه																																							
<input checked="" type="checkbox"/>	عملیات انجام شده به دلیل شکست در ذخیره‌سازی لاگها																																							
<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 کلمه عبور تست شده توسط محصول																																							
<input checked="" type="checkbox"/>	شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)																																							
<input checked="" type="checkbox"/>	تمامی تغییرات بر روی مقادیر مشخصه‌های 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 مشخصه‌های 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، نمی‌توانند عملیات موردنظر را انجام دهند.	
		<input checked="" type="checkbox"/>	تلاش موفق یا ناموفق برای برقراری نشست.	
		<input checked="" type="checkbox"/>	عدم ایجاد نشست به دلیل محدودیت نشست‌های هم‌زمان (حداقل)	
		<input checked="" type="checkbox"/>	خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست	
		<input checked="" type="checkbox"/>	خاتمه به نشست غیرفعال توسط مدیر سیستم	
		<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید برای هر رکورد ممیزی تولید شده، مشخصاتی که در ذیل آمده است را ثبت نماید.		2
		<input checked="" type="checkbox"/>	تاریخ و زمان رویداد	مشخصاتی که در رکوردهای ممیزی 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	
	<input checked="" type="checkbox"/>	محصول باید رکوردهای ممیزی را در برابر دسترسی غیرمجاز محافظت نماید.		3
	<input checked="" type="checkbox"/>	رکوردهای ممیزی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند.		4
		<input checked="" type="checkbox"/>	عدم وجود داده نامفهوم در رکوردها	مواردی که در رکوردهای ممیزی وجود دارند، مشخص شوند.
		<input checked="" type="checkbox"/>	عدم وجود فیلدهای نامرتب	
		<input checked="" type="checkbox"/>	وجود داده معتبر و مناسب در هر فیلد	
	<input checked="" type="checkbox"/>	محصول باید امکان انتخاب و مرتب‌سازی برای رکوردهای ممیزی تولید شده را بر اساس فیلدها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.		5

		<input checked="" type="checkbox"/>	هویت موجودیت فعال	مواردی که بر اساس آنها مرتب‌سازی وجود دارد، مشخص شود.	
		<input checked="" type="checkbox"/>	نوع حساب کاربری		
		<input checked="" type="checkbox"/>	تاریخ/زمان		
		<input type="checkbox"/>	روش اتصال کاربر		
		<input checked="" type="checkbox"/>	نوع رخداد		
		<input checked="" type="checkbox"/>	مکان رویداد		
		<input checked="" type="checkbox"/>	سایر موارد		
	<input checked="" type="checkbox"/>	محصول باید هرگونه حذف و تغییر غیرمجاز در رکوردهای ممیزی را تشخیص دهد و در صورت امکان جلوگیری نماید.			6
		<input checked="" type="checkbox"/>	استفاده از هش برای تشخیص تغییرات	روش‌های تشخیص مشخص شود. (وجود یک مورد لازم و کافی است)	
		<input type="checkbox"/>	پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)		
		<input type="checkbox"/>	فقط خواندنی کردن ممیزی‌ها در محصول		
		<input checked="" type="checkbox"/>	سایر موارد		
	<input checked="" type="checkbox"/>	محصول باید وقتی که حجم داده‌های ممیزی، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.			7
		<input type="checkbox"/>	استفاده از یک کانال ارتباطی	روش‌های اطلاع رسانی مشخص شود (وجود یک مورد لازم و کافی است)	
		<input checked="" type="checkbox"/>	ارسال پیام		
		<input type="checkbox"/>	از طریق واسط کاربر مجاز		
		<input type="checkbox"/>	سایر موارد		
	<input checked="" type="checkbox"/>	محصول باید توانایی ممیزی (ثبت لاگ) هنگام از کار افتادن محصول و/یا پر شدن حافظه ممیزی را داشته باشد و برای این کار از رویکردهای بیان شده استفاده نماید.			8
		<input type="checkbox"/>	نادیده گرفتن رویدادهای ممیزی	رویکردهای مورد استفاده در محصول مشخص گردد (وجود یک مورد لازم و کافی است)	
		<input checked="" type="checkbox"/>	ذخیره‌سازی محدود رویدادهای ممیزی، (آنهايي که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند)		
		<input checked="" type="checkbox"/>	بازنویسی روی قدیمی‌ترین رکوردهای ممیزی ذخیره شده		
		<input type="checkbox"/>	سایر موارد		

## 5-2- رمزنگاری

در این کلاس، 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 پردازند که در این کلاس، توانایی محصول از این حیث مورد بررسی قرار گرفته است. در کلاس رمزنگاری همچنین از الگوریتمهای درهم‌سازی (هش) برای برقراری جامعیت داده استفاده می‌گردد.

توضیحات	کلاس رمزنگاری	شماره الزام
<input checked="" type="checkbox"/>	محصول باید قابلیت رمزنگاری یا ماژول رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف شده ISO 18033-3) با توجه به موارد زیر انجام دهد.	1
	<input checked="" type="checkbox"/> مد عملیاتی CBC و طول کلید 128 یا 192 یا 256 بیتی (تعریف شده در NIST SP 800-38A)	مد عملیاتی که الگوریتم از آن استفاده می‌کند را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)
	<input checked="" type="checkbox"/> مد عملیاتی GCM و طول کلید 128 یا 192 یا 256 بیتی (تعریف شده در NIST SP 800-38D)	
	<input type="checkbox"/> مد عملیاتی CTR و طول کلید 128 یا 192 یا 256 بیتی (تعریف شده در ISO10116)	
<input checked="" type="checkbox"/>	محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (هش) را داشته باشد؛ بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده نماید.	2
	<input type="checkbox"/> الگوریتم SHA-1 با اندازه خلاصه پیام 160 یا 256 یا 384 یا 512	الگوریتم و اندازه خلاصه پیام مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)
	<input checked="" type="checkbox"/> الگوریتم SHA-256 با اندازه خلاصه پیام 160 یا 256 یا 384 یا 512	



		<input checked="" type="checkbox"/> الگوریتم SHA-384 با اندازه خلاصه پیام 160 یا 256 یا 384 یا 512	مورد لازم و کافی است.
		<input type="checkbox"/> الگوریتم SHA-512 با اندازه خلاصه پیام 160 یا 256 یا 384 یا 512	
	<input checked="" type="checkbox"/>	<b>در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری)</b>	3
	<input type="checkbox"/>	نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یکها، مقدار تصادفی، مقدار جدیدی از کلید)	روش نابودی کلید
	<input type="checkbox"/>	نابودی با استفاده از یک واسط مشخص	مشخص گردد. (وجود)
	<input checked="" type="checkbox"/>	از طریق توابع امنیتی محصول	یک مورد لازم و کافی است
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	<b>در صورتی که امضاء دیجیتال در محصول پشتیبانی می‌شود، نیاز است که سرویس‌های امضاء رمزنگاری (تولید و تأیید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری)</b>	4
	<input checked="" type="checkbox"/>	الگوریتم‌های امضاء دیجیتال RSA با کلیدهای رمزنگاری 2048 بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضاء دیجیتال (DSS) بخش 5.5، الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 <input checked="" type="checkbox"/> و/یا RSASSA-PKCS1v_5_2؛ ISO/IEC 9796-2، الگوی امضای دیجیتال 2 و یا الگوی امضای دیجیتال (3)	الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است)
	<input type="checkbox"/>	الگوریتم‌های امضاء دیجیتال ECDSA با کلیدهای رمزنگاری 256 بیت یا بزرگتر (بر اساس ISO/IEC 14888-3 بخش 6.4، استاندارد امضای دیجیتال (DSS) بخش 6 و پیوست D، با استفاده از منحنی P-256 یا P-384 یا P-521)	

### 5-3- شناسایی و احراز هویت

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

توضیحات	کلاس شناسایی و احراز هویت		شماره الزام	
	<input checked="" type="checkbox"/>	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.	1	
		<input type="checkbox"/>		مقدار یا یازهی مورد استفاده در هریک باید
		<input checked="" type="checkbox"/>		مشخص گردد. (وجود یک عدد مثبت قابل تنظیم توسط مدیر
		<input type="checkbox"/>		یک مورد لازم و کافی است) یک بازهی قابل قبولی از مقادیر
	<input checked="" type="checkbox"/>	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.	2	
		<input checked="" type="checkbox"/>		غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)
		<input checked="" type="checkbox"/>		غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)

		<input type="checkbox"/> استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)	به نوع کاربرد می‌تواند از حالت انتخابی به حالت الزامی تغییر یابد. برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست.
		<input type="checkbox"/> سایر موارد	
	<input checked="" type="checkbox"/>	<b>3</b> محصول باید برای هر کاربر، مشخصه‌های امنیتی که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باشند را نگهداری نماید.	
	<input checked="" type="checkbox"/>	شناسه کاربر	مشخصه‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.
	<input type="checkbox"/>	روش احراز هویت مورد استفاده	
	<input checked="" type="checkbox"/>	داده احراز هویت	
	<input checked="" type="checkbox"/>	وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)	
	<input checked="" type="checkbox"/>	نقش کاربر	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	<b>4</b> محصول باید قابلیت مدیریت کلمه عبور را فراهم آورد.	
	<input checked="" type="checkbox"/>	استفاده از حروف کوچک	موارد نیاز که باید در تعریف کلمه عبور استفاده شوند.
	<input checked="" type="checkbox"/>	استفاده از حروف بزرگ	
	<input checked="" type="checkbox"/>	استفاده از اعداد	
	<input checked="" type="checkbox"/>	استفاده از کاراکترهای خاص ("@", "#", "\$", "%", "^", "!", "&", "*", "(", ")", " ", " " و ...)	
	<input checked="" type="checkbox"/>	حداقل طول 8 یا بیشتر (قابل تنظیم)	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	<b>5</b> محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.	

		<input type="checkbox"/> مشاهده راهنمای نحوه ورود به سیستم <input checked="" type="checkbox"/> بازیابی کلمه عبور <input type="checkbox"/> هیچ اقدامی <input type="checkbox"/> سایر موارد	اقدامات عمومی که کاربر می تواند قبل از احراز هویت انجام دهد، انتخاب شود.	
	<input checked="" type="checkbox"/>	محصول باید از سازوکار احراز هویت پشتیبانی نماید (برای احراز هویت کاربران راه دور، باید بیش از یک سازوکار احراز هویت در محصول به کار رفته باشد).	سازوکارهای احراز هویت موجود در محصول مشخص شوند.	6
		<input checked="" type="checkbox"/> نام کاربری و کلمه عبور <input type="checkbox"/> امضاء دیجیتال <input type="checkbox"/> Active Directory <input checked="" type="checkbox"/> OTP یا توکن <input type="checkbox"/> احراز هویت دو فاکتوری <input type="checkbox"/> سایر موارد		
	<input checked="" type="checkbox"/>	محصول باید برای هر کاربر فعال، مشخصه های امنیتی نگهداری نماید.	مشخصه هایی امنیتی که محصول برای هر کاربر نگهداری می کند، مشخص گردد (در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می نماید، این قوانین در «سایر موارد» بیان می شوند).	7
		<input checked="" type="checkbox"/> شناسه کاربر <input checked="" type="checkbox"/> نقشها و یا مجموعه دسترسی های کاربر به قسمت های مختلف برنامه <input type="checkbox"/> جزئیات واسط کلاینت <input checked="" type="checkbox"/> پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق) <input type="checkbox"/> سایر موارد		
	<input checked="" type="checkbox"/>	محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.		8

		<p>از بین رفتن اعتبار نشستهای قبلی هنگام برقراری یک نشست جدید</p> <p><input checked="" type="checkbox"/> (به جزء مواردی که فعال بودن همزمان چندین نشست مورد نیاز کارکردی برنامه باشد. در این موارد، هنگام فعال شدن نشستهای جدید، باید به صفحه کاربر اصلی (نشست اول) اطلاع داده شود).</p>	<p>در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می نماید، این قوانین در «سایر موارد» بیان می شوند.</p>	
		<p><input checked="" type="checkbox"/> به روزرسانی اطلاعات پیشینه احراز هویت</p>		
		<p><input type="checkbox"/> سایر موارد</p>		
	<p><input checked="" type="checkbox"/></p>	<p>محصول باید بر روی تغییرات مشخصه های امنیتی کاربر فعال قوانینی را اعمال نماید.</p>		<p>9</p>
		<p><input checked="" type="checkbox"/> غیرمجاز بودن هرگونه تغییر در طول نشست فعال</p>	<p>قوانینی که در صورت تغییر مشخصه های امنیتی کاربر فعال، اعمال می شود، مشخص گردد.</p>	
		<p><input type="checkbox"/> سایر موارد</p>		

## 4-5- 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 کلاس، توانایی محصول در حفاظت از این داده‌ها مورد بررسی قرار می‌گیرد.

توضیحات	کلاس حفاظت از داده‌ی کاربری		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید برای موجودیتها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید.	1
	<input checked="" type="checkbox"/>	مدیر سیستم	موجودیت‌های فعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می‌شوند، مشخص گردد.
	<input checked="" type="checkbox"/>	کاربر عادی	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	رکوردها، مستندات و فراداده <sup>۱</sup>	موجودیت‌های غیرفعال که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می‌شوند، مشخص گردد.
	<input checked="" type="checkbox"/>	داده متعلق به کاربران	
	<input checked="" type="checkbox"/>	داده احراز هویت	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	ایجاد موجودیت غیرفعال جدید	عملیاتی که خط‌مشی‌های کنترل
	<input checked="" type="checkbox"/>	حذف موجودیت غیرفعال	

<sup>۱</sup> Metadata

		<input checked="" type="checkbox"/>	تغییر دسترسیها به موجودیت غیرفعال	دسترسی در رابطه با آنها اعمال می‌شوند، مشخص گردد.	
		<input checked="" type="checkbox"/>	عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال		
		<input type="checkbox"/>	سایر موارد		
	<input checked="" type="checkbox"/>	<p>محصول باید بر اساس مشخصه‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.</p>			2
		<input checked="" type="checkbox"/>	نقش‌ها و مجوزهای کاربر مجاز	مشخصه‌هایی که بر اساس آن خط‌مشی‌ها تعریف می‌شوند، انتخاب گردد.	
		<input checked="" type="checkbox"/>	اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.		
		<input type="checkbox"/>	سایر موارد		
	<input checked="" type="checkbox"/>	<p>محصول باید بر اساس قاعده‌های 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، 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).</p>			3
	<input checked="" type="checkbox"/>	<p>محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.</p>			4
		<input checked="" type="checkbox"/>	تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه <sup>۲</sup> از پیش تعریف شده	قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).	
		<input type="checkbox"/>	سایر موارد		
	<input checked="" type="checkbox"/>	<p>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.</p>			5

<sup>۲</sup> Threshold

	<input checked="" type="checkbox"/>	<p>6 محصول باید هنگام دریافت داده کاربری خطمشی کنترل دسترسی را اعمال نماید و برای این کار از مشخصه‌های امنیتی مرتبط با داده کاربری استفاده کند.</p> <table border="1" data-bbox="443 450 1394 1122"> <tr> <td data-bbox="443 450 501 584" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="501 450 1163 584"> <p>نوع داده</p> </td> <td data-bbox="1163 450 1394 584"> <p>مشخصه‌های امنیتی</p> </td> </tr> <tr> <td data-bbox="443 584 501 719" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="501 584 1163 719"> <p>حجم و اندازه</p> </td> <td data-bbox="1163 584 1394 719"> <p>مرتبط با داده کاربری که در هنگام ورود آن به محصول استفاده می‌شوند، مشخص</p> </td> </tr> <tr> <td data-bbox="443 719 501 853" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="501 719 1163 853"> <p>فرمت</p> </td> <td data-bbox="1163 719 1394 853"> <p>شود (در صورتی که کنترل دسترسی برای</p> </td> </tr> <tr> <td data-bbox="443 853 501 987" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="501 853 1163 987"> <p>تعداد دفعات Import</p> </td> <td data-bbox="1163 853 1394 987"> <p>موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد»</p> </td> </tr> <tr> <td data-bbox="443 987 501 1122" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="501 987 1163 1122"> <p>سایر موارد</p> </td> <td data-bbox="1163 987 1394 1122"> <p>بیان گردد).</p> </td> </tr> </table>	<input checked="" type="checkbox"/>	<p>نوع داده</p>	<p>مشخصه‌های امنیتی</p>	<input checked="" type="checkbox"/>	<p>حجم و اندازه</p>	<p>مرتبط با داده کاربری که در هنگام ورود آن به محصول استفاده می‌شوند، مشخص</p>	<input checked="" type="checkbox"/>	<p>فرمت</p>	<p>شود (در صورتی که کنترل دسترسی برای</p>	<input type="checkbox"/>	<p>تعداد دفعات Import</p>	<p>موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد»</p>	<input type="checkbox"/>	<p>سایر موارد</p>	<p>بیان گردد).</p>	
<input checked="" type="checkbox"/>	<p>نوع داده</p>	<p>مشخصه‌های امنیتی</p>																
<input checked="" type="checkbox"/>	<p>حجم و اندازه</p>	<p>مرتبط با داده کاربری که در هنگام ورود آن به محصول استفاده می‌شوند، مشخص</p>																
<input checked="" type="checkbox"/>	<p>فرمت</p>	<p>شود (در صورتی که کنترل دسترسی برای</p>																
<input type="checkbox"/>	<p>تعداد دفعات Import</p>	<p>موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد»</p>																
<input type="checkbox"/>	<p>سایر موارد</p>	<p>بیان گردد).</p>																
	<input checked="" type="checkbox"/>	<p>7 محصول باید از یک پروتکل امن برای انتقال داده استفاده نماید. این پروتکل ارتباط و همبستگی شفاف را بین داده کاربری دریافت شده و مشخصه‌های امنیتی آن فراهم می‌کند و همچنین از شنود و گمشدن داده حین انتقال جلوگیری می‌کند.</p>																
	<input checked="" type="checkbox"/>	<p>8 محصول باید هنگام انتقال داده به بیرون از محصول، خطمشی کنترل دسترسی اعمال نماید و برای این کار از مشخصه‌های امنیتی مرتبط با داده کاربری استفاده کند.</p> <table border="1" data-bbox="443 1435 1394 1720"> <tr> <td data-bbox="443 1435 501 1503" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="501 1435 1163 1503"> <p>نوع داده</p> </td> <td data-bbox="1163 1435 1394 1503"> <p>مشخصه‌های امنیتی</p> </td> </tr> <tr> <td data-bbox="443 1503 501 1570" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="501 1503 1163 1570"> <p>حجم و اندازه</p> </td> <td data-bbox="1163 1503 1394 1570"> <p>مرتبط با داده کاربری که در هنگام خروج آن از محصول استفاده</p> </td> </tr> <tr> <td data-bbox="443 1570 501 1637" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="501 1570 1163 1637"> <p>فرمت</p> </td> <td data-bbox="1163 1570 1394 1637"> <p>می‌شوند، مشخص</p> </td> </tr> <tr> <td data-bbox="443 1637 501 1720" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="501 1637 1163 1720"> <p>سایر موارد</p> </td> <td data-bbox="1163 1637 1394 1720"> <p>شوند</p> </td> </tr> </table>	<input type="checkbox"/>	<p>نوع داده</p>	<p>مشخصه‌های امنیتی</p>	<input type="checkbox"/>	<p>حجم و اندازه</p>	<p>مرتبط با داده کاربری که در هنگام خروج آن از محصول استفاده</p>	<input checked="" type="checkbox"/>	<p>فرمت</p>	<p>می‌شوند، مشخص</p>	<input checked="" type="checkbox"/>	<p>سایر موارد</p>	<p>شوند</p>				
<input type="checkbox"/>	<p>نوع داده</p>	<p>مشخصه‌های امنیتی</p>																
<input type="checkbox"/>	<p>حجم و اندازه</p>	<p>مرتبط با داده کاربری که در هنگام خروج آن از محصول استفاده</p>																
<input checked="" type="checkbox"/>	<p>فرمت</p>	<p>می‌شوند، مشخص</p>																
<input checked="" type="checkbox"/>	<p>سایر موارد</p>	<p>شوند</p>																
	<input checked="" type="checkbox"/>	<p>9 محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.</p>																



		<input checked="" type="checkbox"/> مدیر سیستم باید خروج رکوردها را محدود نماید، به طوریکه کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند.	قوانینی که در هنگام خروج داده از محصول اعمال می‌شوند، مشخص شوند
		<input type="checkbox"/> سایر موارد	
	<input checked="" type="checkbox"/>	<b>محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره شده در محصول تشخیص دهد.</b>	
		<input checked="" type="checkbox"/> درهم شده <sup>۳</sup> داده‌های کاربری ذخیره شده، نگهداری می‌شود	چگونگی تشخیص تغییر در داده‌های کاربری حساس، مشخص شود.
		<input type="checkbox"/> سایر موارد	
	<input checked="" type="checkbox"/>	<b>محصول باید در صورت تشخیص خطای صحت در داده‌ها، اقدامات مقابله‌ای زیر را انجام دهد.</b>	
		<input type="checkbox"/> ایجاد هشدار/اخطار برای نقش‌های مجاز	اقدام مقابله‌ای در صورت تشخیص خطا، مشخص شود (وجود یک مورد لازم و کافی است)
		<input type="checkbox"/> تصحیح داده بر اساس مقادیر قبل	
		<input checked="" type="checkbox"/> سایر موارد	

<sup>۳</sup> Hash

### 5-5- مدیریت امنیت

در این کلاس 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	کلاس مدیریت امنیت		شماره الزام											
	<input checked="" type="checkbox"/>	<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><input checked="" type="checkbox"/></td> <td>تعیین و تغییر رفتار</td> <td rowspan="4">فعالیت‌های مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند.</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>غیرفعال نمودن</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>فعال نمودن</td> </tr> <tr> <td><input type="checkbox"/></td> <td>سایر موارد</td> </tr> </table>	<input checked="" type="checkbox"/>	تعیین و تغییر رفتار	فعالیت‌های مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند.	<input checked="" type="checkbox"/>	غیرفعال نمودن	<input checked="" type="checkbox"/>	فعال نمودن	<input type="checkbox"/>	سایر موارد	1		
<input checked="" type="checkbox"/>	تعیین و تغییر رفتار	فعالیت‌های مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند.												
<input checked="" type="checkbox"/>	غیرفعال نمودن													
<input checked="" type="checkbox"/>	فعال نمودن													
<input type="checkbox"/>	سایر موارد													
	<input checked="" type="checkbox"/>	<p>محصول باید با اعمال خط‌مشی کنترل دسترسی؛ امکان تغییر پیش‌فرض و سایر عملیات زیر را بر روی مشخصه‌های امنیتی الزام 7 از کلاس شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.</p> <table border="1"> <tr> <td><input checked="" type="checkbox"/></td> <td>پرس‌وجو</td> <td rowspan="5">عملیات بر روی مشخصه‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد.</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>تغییر</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>حذف</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>تغییر پیش‌فرض</td> </tr> <tr> <td><input type="checkbox"/></td> <td>سایر موارد</td> </tr> </table>	<input checked="" type="checkbox"/>	پرس‌وجو	عملیات بر روی مشخصه‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد.	<input checked="" type="checkbox"/>	تغییر	<input checked="" type="checkbox"/>	حذف	<input checked="" type="checkbox"/>	تغییر پیش‌فرض	<input type="checkbox"/>	سایر موارد	2
<input checked="" type="checkbox"/>	پرس‌وجو	عملیات بر روی مشخصه‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد.												
<input checked="" type="checkbox"/>	تغییر													
<input checked="" type="checkbox"/>	حذف													
<input checked="" type="checkbox"/>	تغییر پیش‌فرض													
<input type="checkbox"/>	سایر موارد													
	<input checked="" type="checkbox"/>	<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><input checked="" type="checkbox"/></td> <td>تغییر پیش‌فرض</td> <td rowspan="2">عملیات بر روی داده‌های محصول که</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>حذف نمودن</td> </tr> </table>	<input checked="" type="checkbox"/>	تغییر پیش‌فرض	عملیات بر روی داده‌های محصول که	<input checked="" type="checkbox"/>	حذف نمودن	3						
<input checked="" type="checkbox"/>	تغییر پیش‌فرض	عملیات بر روی داده‌های محصول که												
<input checked="" type="checkbox"/>	حذف نمودن													

		<input checked="" type="checkbox"/>	پرس و جو	در محصول پشتیبانی	
		<input checked="" type="checkbox"/>	مقداردهی	می نشوند، مشخص	
		<input checked="" type="checkbox"/>	ایجاد	شود.	
		<input checked="" type="checkbox"/>	مشاهده		
		<input type="checkbox"/>	سایر موارد		
	<input checked="" type="checkbox"/>	محصول باید توانایی انجام کارکردهای زیر را داشته باشد.			4
		<input checked="" type="checkbox"/>	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی		
		<input checked="" type="checkbox"/>	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی		
		<input checked="" type="checkbox"/>	پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره سازی ممیزی		
		<input checked="" type="checkbox"/>	مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول		
		<input type="checkbox"/>	انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده که می تولند در محصول قابل پیگیری باشد. (برای مثال، زمان تخصیص و یا زمان آزادسازی منابع)	در صورتی که هر کدام از موارد مطرح شده، توسط محصول قابل اجرا نیست، در قسمت توضیحات باید دلایل مطرح گردد.	
		<input type="checkbox"/>	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول		
		<input checked="" type="checkbox"/>	در نظر گرفتن یک عملیات از پیش تعیین شده پس از تشخیص یک خطای صحت داده که می تواند قابل پیگیری نیز باشد.		
		<input checked="" type="checkbox"/>	1. مدیریت حد آستانه برای تلاشهای ناموفق 2. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد.		
		<input checked="" type="checkbox"/>	مدیریت معیارها برای تنظیم کلمات عبور		
		<input checked="" type="checkbox"/>	1. مدیریت دادههای احراز هویت توسط مدیر یا کاربر مربوطه 2. مدیریت یکسری عملیاتی که قبل از احراز شدن هویت کاربر انجام میشوند.		
		<input checked="" type="checkbox"/>	1. مدیریت سازوکارهای احراز هویت		

		<p>2. مدیریت قوانین مرتبط با احراز هویت</p> <p>مدیریت تغییرات و فرایندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می تواند قبل از شناسایی کاربر انجام دهد.</p> <p>مدیر مجاز می تواند مشخصه های امنیتی موجودیت های فعال پیش فرض را تعریف کند و تغییر دهد.</p> <p>مدیریت مقادیر پیش فرض برای کنترل دسترسی محصول</p> <p>مدیریت نقشها در محصول</p> <p>مدیریت حداکثر تعداد مجاز نشستهای همزمان کاربران توسط مدیر</p> <p>مدیریت شرایط آغاز نشست توسط مدیر مجاز</p> <p>1. تعیین زمان غیرفعال بودن برای یک کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد.</p> <p>2. تعیین زمان پیش فرض 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"> <tr> <td><input checked="" type="checkbox"/></td> <td>مدیر سیستم</td> <td rowspan="4">نقش هایی که در محصول پشتیبانی می شوند، مشخص گردد.</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>کاربر پیشرفته</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>کاربر عادی</td> </tr> <tr> <td><input type="checkbox"/></td> <td>سایر موارد</td> </tr> </table>	<input checked="" type="checkbox"/>	مدیر سیستم	نقش هایی که در محصول پشتیبانی می شوند، مشخص گردد.	<input checked="" type="checkbox"/>	کاربر پیشرفته	<input checked="" type="checkbox"/>	کاربر عادی	<input type="checkbox"/>	سایر موارد	5
<input checked="" type="checkbox"/>	مدیر سیستم	نقش هایی که در محصول پشتیبانی می شوند، مشخص گردد.										
<input checked="" type="checkbox"/>	کاربر پیشرفته											
<input checked="" type="checkbox"/>	کاربر عادی											
<input type="checkbox"/>	سایر موارد											
	<input checked="" type="checkbox"/>	<p>محصول باید قادر باشد کاربران را به نقش های تعریف شده یا قابل تعریف مرتبط نماید، همچنین لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد، اما ممکن است نقش ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.</p>	6									

### 5-6- حفاظت از توابع امنیتی محصول

در این کلاس، 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	کلاس حفاظت از توابع امنیتی محصول		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید هنگام رخ دادن هرگونه شکست مانند از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول، در وضعیت امنی قرار گرفته و صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید.	1
	<input checked="" type="checkbox"/>	شکست‌های نرم‌افزاری	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول حفظ می‌شود، مشخص گردد.
	<input checked="" type="checkbox"/>	شکست‌های سخت‌افزاری	
	<input checked="" type="checkbox"/>	محصول باید از طریق فراهم نمودن بستر و زیرساخت امن، توانایی محافظت از افساء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد.	2
	<input checked="" type="checkbox"/>	در صورتی که محصول از محصولات امن IT استفاده می‌کند، باید تفسیر سازگار و یکسانی را از داده امنیتی در زمان اشتراک گذاری آن بین خود و دیگر محصولات امن IT، فراهم آورد.	3
	<input type="checkbox"/>	داده‌های احراز هویت	داده امنیتی قابل اشتراک گذاری که در محصول پشتیبانی می‌شوند، مشخص گردد.
	<input type="checkbox"/>	کلید	
	<input type="checkbox"/>	امضای دیجیتال	
	<input type="checkbox"/>	داده‌های ممیزی	

	<input checked="" type="checkbox"/>	سایر موارد	
4	<input checked="" type="checkbox"/>	محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهره‌های زمانی معتبر، تولید یا استفاده نماید.	
		<input type="checkbox"/>	گرفتن مهرهای زمانی از سرور NTP
		<input type="checkbox"/>	تنظیم مهرهای زمانی از طریق اینترنت
		<input checked="" type="checkbox"/>	تنظیم مهرهای زمانی به صورت پیشفرض (معتبر و عدم امکان دستکاری غیرمجاز)
		<input type="checkbox"/>	سایر موارد
		روش‌های ایجاد مهرهای زمانی معتبر انتخاب شود. (دیگر روشهای موجود در محصول، در قسمت «سایر موارد» بیان شود).	
5	<input checked="" type="checkbox"/>	محصول باید امکان به‌روزرسانی نرم افزار و میان افزار محصول را برای مدیر سیستم فراهم نماید.	
		<input checked="" type="checkbox"/>	به‌روز رسانی دستی
		<input type="checkbox"/>	جستجوی خودکار به روزرسانی ها
		<input type="checkbox"/>	به روزرسانی‌های خودکار
		<input type="checkbox"/>	به‌روزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل به‌روزرسانی
		روش به‌روزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).	
6	<input type="checkbox"/>	در صورت استفاده از به‌روزرسانی به روش خودکار، محصول باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، امکان احراز اصالت میان‌افزار یا نرم‌افزار را فراهم نماید.	
		<input type="checkbox"/>	امضاء دیجیتال
		<input type="checkbox"/>	درهم‌ساز منتشرشده
		سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی) به‌روزرسانی‌ها انتخاب گردد.	

### 5-7- تخصیص منابع

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

توضیحات	کلاس تخصیص منابع		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید در زمان رخداد هرگونه شکست نرم‌افزاری؛ از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.	1

### 5-8- دسترسی به محصول

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

توضیحات	کلاس دسترسی به محصول		شماره الزام	
	<input checked="" type="checkbox"/>	محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.	1	
	<input checked="" type="checkbox"/>	محصول باید کلیه نشست‌های تعاملی راه دور <sup>۴</sup> را پس از مدت زمانی که غیرفعال هستند (و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.	2	
	<input checked="" type="checkbox"/>	محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.	3	
	<input checked="" type="checkbox"/>	در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد.	4	
	<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"/>	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.	5	
	<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.	6	

<sup>۴</sup> Remote



<input checked="" type="checkbox"/>	محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.		7	
	<input checked="" type="checkbox"/>	مکان		پارامترهای موجود برای جلوگیری از نشست، مشخص شوند (وجود یک مورد لازم و کافی است).
	<input type="checkbox"/>	شماره پورت		
	<input type="checkbox"/>	روز		
	<input checked="" type="checkbox"/>	زمان		
	<input type="checkbox"/>	سایر موارد		

## 5-9- کانال‌ها/مسیرهای مورد اعتماد

در این کلاس 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	کلاس کانال‌ها/مسیرهای مورد اعتماد		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید قادر باشد مسیر ارتباطی امنی بین خود، کاربران و دیگر محصولات IT فراهم نماید که به طور منطقی از دیگر کانال‌ها متمایز باشد. سپس از طریق این کانال احراز هویت را انجام داده و از تغییر و افشاء داده تبادلی حفاظت نموده و تغییرات را تشخیص دهد. در صورت انتخاب مورد HTTPS، رعایت الزام 1-6- و در صورت انتخاب TLS، رعایت الزامات 2-6- تا 4-6- که در بخش 6- بیان گردیده است، الزامی است.	1
		<input checked="" type="checkbox"/>	پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.
		<input type="checkbox"/>	TLS
	<input checked="" type="checkbox"/>	محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.	2
	<input checked="" type="checkbox"/>	محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.	3

## 6- 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 کلاس کانال امن، پروتکل HTTPS انتخاب شود، آنگاه رعایت الزامات HTTPS که در این بخش بیان شده است، اجباری می‌گردد.

### 1-6- پروتکل HTTPS

توضیحات	کلاس کانال‌ها/مسیرهای مورد اعتماد		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند.	1
	<input checked="" type="checkbox"/>	محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	2
	<input checked="" type="checkbox"/>	در صورتی که گواهی‌نامه ارائه شده از سمت دیگر محصولات IT (در هنگام برقراری ارتباط) نامعتبر باشد، محصول باید بر اساس موارد زیر عمل نماید. اعتبارسنجی گواهی‌نامه بر اساس الزامات بخش 5-6- انجام می‌شود که در این صورت الزامات بخش 5-6- الزامی است.	3
	<input checked="" type="checkbox"/>	اتصال را برقرار نکند.	محصول تنها از موارد بیان شده می‌تواند استفاده نماید.
	<input type="checkbox"/>	برای برقراری اتصال درخواست مجوز کند.	

### 2-6- پروتکل TLS Client

توضیحات	پروتکل TLS Client		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید TLS 1.2 (RFC 5246) و/یا TLS 1.1 (RFC 4346) را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه رمزهای زیر پیاده‌سازی نماید.	1
	<input type="checkbox"/>	TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	مجموعه رمز مورد استفاده و پیاده‌سازی شده
	<input type="checkbox"/>	TLS_RSA_WITH_AES_192_CBC_SHA	

			مطابق با RFC 3268	محصول، انتخاب گردد.
	<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA	مطابق با RFC 3268	
	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	مطابق با RFC 3268	
	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_192_CBC_SHA	مطابق با RFC 3268	
	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	مطابق با RFC 3268	
	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	مطابق با RFC 4492	
	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA	مطابق با RFC 4492	
	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	مطابق با RFC 4492	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	مطابق با RFC 4492	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA	مطابق با RFC 4492	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	مطابق با RFC 4492	
	<input type="checkbox"/>	TLS_RSA_WITH_AES_128_CBC_SHA256	مطابق با RFC 5246	
	<input type="checkbox"/>	TLS_RSA_WITH_AES_192_CBC_SHA256	مطابق با RFC 5246	
	<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA256	مطابق با RFC 5246	
	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	مطابق با RFC 5246	
	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_192_CBC_SHA256	مطابق با RFC 5246	
	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	مطابق با RFC 5246	

	<input type="checkbox"/>	TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288	
	<input type="checkbox"/>	TLS_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5288	
	<input type="checkbox"/>	TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA384 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289	
	<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289	
	<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289	
	<input checked="" type="checkbox"/>	محصول باید مطابقت شناسه ارائه شده با شناسه مرجع را با توجه به بخش 6 از RFC 6125، تأیید نماید.	2

	<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.		3	
		<input checked="" type="checkbox"/>	ارتباط را برقرار نکند		در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.
		<input type="checkbox"/>	برای برقراری ارتباط درخواست مجوز کند		
		<input type="checkbox"/>	سایر موارد		
	<input checked="" type="checkbox"/>	محصول باید در پیام <b>ClientHello</b> برای استفاده از منحنی‌ها، بر اساس موارد زیر عمل نماید.		4	
		<input type="checkbox"/>	Supported Elliptic Curves Extension را ارائه نکند		در صورت که محصول از منحنی استفاده می‌نماید، طول کلید باید مشخص گردد.
		<input checked="" type="checkbox"/>	Supported Elliptic Curves Extension را به همراه NIST Curve های secp256r1 یا secp384r1 یا secp521r1 ارائه نماید		
		<input type="checkbox"/>	هیچ منحنی دیگری		

### 3-6- پروتکل TLS Server

توضیحات	پروتکل TLS Server		شماره الزام		
	<input checked="" type="checkbox"/>	محصول باید <b>TLS 1.2 (RFC 5246)</b> را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه رمزهای زیر پیاده‌سازی نماید.		5	
		<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268		مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.
		<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268		
		<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268		

	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	
	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	
		TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	
	<input type="checkbox"/>	TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246	
	<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246	
	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246	
	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289	
	<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289	
	<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289	
	<input checked="" type="checkbox"/>	محصول باید اتصالاتی کاربرانی که درخواست <b>SSL1.0, SSL2.0, SSL3.0, TLS1.0</b> و <b>TLS1.1</b> دارند را رد نماید.	6

<input checked="" type="checkbox"/>	محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.		7
	<input type="checkbox"/>	استفاده از RSA با اندازه کلید 2048 یا 3072 یا 4096 بیت	
	<input checked="" type="checkbox"/>	پارامترهای ECDH با استفاده از NIST Curve های secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگری	
	<input type="checkbox"/>	پارامترهای دیفی-هلمن با اندازه کلید 2048 یا 3072 بیت	
		در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.	



#### 4-6- پروتکل TLS مشترک کلاینت و سرور

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

توضیحات	پروتکل TLS مشترک کلاینت و سرور		شماره الزام
	<input type="checkbox"/>	محصول باید احراز هویت دوطرفه کلاینت‌ها/سرورهای TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.	1
	<input type="checkbox"/>	محصول در صورت مطابقت نداشتن نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه از شناساننده <sup>۵</sup> کلاینت مورد انتظار بوده است، نباید کانال امن را برقرار سازد.	2

<sup>۵</sup> Identifier

5-6- اعتبارسنجی گواهی نامه

توضیحات	شناسایی و احراز هویت	شماره الزام																							
	<p data-bbox="339 667 368 701"><input checked="" type="checkbox"/></p> <p data-bbox="762 658 1393 696">محصول باید گواهی نامه‌ها را بر اساس قوانین زیر تأیید کند.</p> <table border="1" data-bbox="379 734 1401 1803"> <tr> <td data-bbox="379 734 427 824"><input checked="" type="checkbox"/></td> <td data-bbox="427 734 1161 824">تأیید گواهی نامه RFC 5280 و تأیید مسیر گواهی نامه که از حداقل طول مسیر دو گواهی نامه پشتیبانی می‌کند.</td> <td data-bbox="1161 734 1401 1377" rowspan="5">روش‌های تأیید وضعیت فسخ گواهی نامه</td> </tr> <tr> <td data-bbox="379 824 427 891"><input checked="" type="checkbox"/></td> <td data-bbox="427 824 1161 891">مسیر گواهی نامه باید با یک گواهی نامه CA امن پایان یابد.</td> </tr> <tr> <td data-bbox="379 891 427 1032"><input checked="" type="checkbox"/></td> <td data-bbox="427 891 1161 1032">محصول باید برای تأیید مسیر یک گواهی نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی نامه‌های CA به حالت «TRUE» تنظیم شده است.</td> </tr> <tr> <td data-bbox="379 1032 427 1122"><input type="checkbox"/></td> <td data-bbox="427 1032 1161 1122">پروتکل وضعیت گواهی نامه آنلاین (OCSP) مشخص شده در RFC 696</td> </tr> <tr> <td data-bbox="379 1122 427 1211"><input type="checkbox"/></td> <td data-bbox="427 1122 1161 1211">لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5280 بخش 6.3</td> </tr> <tr> <td data-bbox="379 1211 427 1301"><input type="checkbox"/></td> <td data-bbox="427 1211 1161 1301">لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5759 بخش 5</td> <td data-bbox="1161 1211 1401 1377" rowspan="2">قوانین تأیید فیلد extendedKeyUsage</td> </tr> <tr> <td data-bbox="379 1301 427 1377"><input type="checkbox"/></td> <td data-bbox="427 1301 1161 1377">هیچ روش فسخ دیگری</td> </tr> <tr> <td data-bbox="379 1377 427 1570"><input type="checkbox"/></td> <td data-bbox="427 1377 1161 1570">گواهی نامه‌های مورد استفاده برای تأیید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی باید هدف «Code Signing» (id-kp3 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.</td> <td data-bbox="1161 1377 1401 1803" rowspan="3"></td> </tr> <tr> <td data-bbox="379 1570 427 1711"><input checked="" type="checkbox"/></td> <td data-bbox="427 1570 1161 1711">گواهی نامه‌های سرور ارائه شده برای TLS باید هدف «Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.</td> </tr> <tr> <td data-bbox="379 1711 427 1803"><input type="checkbox"/></td> <td data-bbox="427 1711 1161 1803">گواهی نامه‌های کلاینت ارائه شده برای TLS باید هدف «Client Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.</td> </tr> </table>	<input checked="" type="checkbox"/>	تأیید گواهی نامه RFC 5280 و تأیید مسیر گواهی نامه که از حداقل طول مسیر دو گواهی نامه پشتیبانی می‌کند.	روش‌های تأیید وضعیت فسخ گواهی نامه	<input checked="" type="checkbox"/>	مسیر گواهی نامه باید با یک گواهی نامه CA امن پایان یابد.	<input checked="" type="checkbox"/>	محصول باید برای تأیید مسیر یک گواهی نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی نامه‌های CA به حالت «TRUE» تنظیم شده است.	<input type="checkbox"/>	پروتکل وضعیت گواهی نامه آنلاین (OCSP) مشخص شده در RFC 696	<input type="checkbox"/>	لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5280 بخش 6.3	<input type="checkbox"/>	لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5759 بخش 5	قوانین تأیید فیلد extendedKeyUsage	<input type="checkbox"/>	هیچ روش فسخ دیگری	<input type="checkbox"/>	گواهی نامه‌های مورد استفاده برای تأیید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی باید هدف «Code Signing» (id-kp3 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.		<input checked="" type="checkbox"/>	گواهی نامه‌های سرور ارائه شده برای TLS باید هدف «Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.	<input type="checkbox"/>	گواهی نامه‌های کلاینت ارائه شده برای TLS باید هدف «Client Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.	1
<input checked="" type="checkbox"/>	تأیید گواهی نامه RFC 5280 و تأیید مسیر گواهی نامه که از حداقل طول مسیر دو گواهی نامه پشتیبانی می‌کند.	روش‌های تأیید وضعیت فسخ گواهی نامه																							
<input checked="" type="checkbox"/>	مسیر گواهی نامه باید با یک گواهی نامه CA امن پایان یابد.																								
<input checked="" type="checkbox"/>	محصول باید برای تأیید مسیر یک گواهی نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی نامه‌های CA به حالت «TRUE» تنظیم شده است.																								
<input type="checkbox"/>	پروتکل وضعیت گواهی نامه آنلاین (OCSP) مشخص شده در RFC 696																								
<input type="checkbox"/>	لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5280 بخش 6.3																								
<input type="checkbox"/>	لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5759 بخش 5	قوانین تأیید فیلد extendedKeyUsage																							
<input type="checkbox"/>	هیچ روش فسخ دیگری																								
<input type="checkbox"/>	گواهی نامه‌های مورد استفاده برای تأیید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی باید هدف «Code Signing» (id-kp3 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.																								
<input checked="" type="checkbox"/>	گواهی نامه‌های سرور ارائه شده برای TLS باید هدف «Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.																								
<input type="checkbox"/>	گواهی نامه‌های کلاینت ارائه شده برای TLS باید هدف «Client Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.																								

		را در فیلد extendedKeyUsage خود داشته باشند.	
	<input type="checkbox"/>	گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ OCSP باید «OCSP Signing» (id-pk9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.	
	<input checked="" type="checkbox"/>	محصول باید تنها در صورتی که افزونه مربوط به basicConstraints از پیش تنظیم شده باشد و همچنین، پرچم CA به حالت «TRUE» تنظیم شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA بپذیرد.	2
	<input checked="" type="checkbox"/>	محصول باید جهت پشتیبانی احراز هویت برای موارد زیر از گواهی‌نامه‌های X509v3 تعریف شده در RFC 5280 استفاده کند.	3
	<input checked="" type="checkbox"/>	HTTPS	در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.
	<input type="checkbox"/>	TLS	
	<input type="checkbox"/>	امضای کد برای به‌روزرسانی‌های نرم‌افزار سیستم	
	<input type="checkbox"/>	امضای کد برای تأیید یکپارچگی	
	<input type="checkbox"/>	سایر موارد	