فرم خود اظهاری آزمایشگاه ارزیابی قابلیت‌های رمزنگاری محصول	
نام تولیدکننده/ فروشنده:	تاریخ:
عنوان محصول:	نسخه:
نماینده تولیدکننده/فروشنده:	
شماره تلفن:	ایمیل:
خلاصه‌ای از توصیف محصول:	

به منظور بیان قابلیت‌های رمزنگاری در محصول به صورت صریح و درک بهتر تولیدکننده از نیازمندی‌های آزمایشگاه در خصوص شاخص‌های کلاس پشتیبانی از رمزنگاری این سند در قالب پرسشنامه تدوین شده است. علاوه بر تکمیل سند پیش رو تولیدکننده می‌بایست متناسب با قابلیت‌های محصول، در خصوص ارزیابی پاره‌ای از الزامات مانند صحت عملکرد الگوریتم در تولید کلید، عملیات رمزنگاری و رمزگشایی به آزمایشگاه API ارائه نماید.(به دلیل موجود نبودن سورس کد در آزمایشگاه و انجام ارزیابی امنیتی در حالت جعبه سیاه) لازم به ذکر است مسئولیت ناشی از تغییرات در سورس کد برنامه در بخش رمزنگاری و مغایرت API با محصول به عهده تولیدکننده خواهد بود.

ردیف	پرسش	پاسخ
۱	آیا ارتباط میان پایگاه داده و محصول مبتنی بر SSL است؟ (در صورت برقرار بودن این ویژگی، چگونگی آن شرح داده شود)	
۲	در صورت استفاده از پروتکل TLS و برقراری ارتباط امن سمت سرور این قابلیت توسط چه بخشی پاسخ داده می‌شود؟	
۳	آیا در محصول رکوردهای ممیزی به صورت رمزشده نگهداری می‌شوند؟در صورت مثبت بودن پاسخ بیان فرمایید نحوه و نوع رمزنگاری رکوردهای ممیزی به چه صورت خواهد بود.	
۴	از چه قابلیت‌ها و رویدادهای رمزنگاری در محصول رکورد ممیزی(log) تهیه می‌شود؟	
۵	آیا رویدادهای ثبت‌شده، امضا می‌شوند؟ در صورت مثبت بودن جواب مکانیسم تولید و تصدیق امضا را شرح دهید.	
۶	آیا از مکانیزم خاصی جهت اطمینان از حفظ تمامیت و یا حفظ	

ردیف	پرسش	پاسخ
	محرمانگی نسخه پشتیبان استفاده شده است؟	
۷	آیا امکان پشتیبانی از ماژول‌های سخت‌افزاری رمزنگاری مختلف در سامانه وجود دارد؟	
۸	آیا فایل‌های پشتیبان پایگاه داده و پیکربندی به‌صورت رمز شده نگهداری می‌شوند؟ در صورت مثبت بودن پاسخ کلید مورد استفاده برای رمزگذاری کجا نگهداری می‌شود؟	
۹	توابع کتابخانه‌ای مورد استفاده در محصول جهت پیاده‌سازی قابلیت رمزنگاری چیست؟(نام و نسخه آن ذکر شود) در صورتی که از توابعی استفاده شود که به صورت آماده موجود نیست و توسط تولید کننده محصول نوشته شده است باید کلیه اطلاعات لازم در این مورد ارائه گردد.	
۱۰	قابلیت رمزنگاری در محصول در کدام قسمت و به چه طریقی وجود دارد؟(لازم است در هر قسمت محصول که از قابلیت رمزنگاری مانند Encryption، Decryption، HMAC، Hash، تولید کلید و ...استفاده می‌شود. نوع قابلیت، روش کار و همچنین ورودی و خروجی این موارد ذکرشود)	
۱۱	توابع و کتابخانه مورد استفاده و همچنین مکانیزم بکارگیری جهت از بین بردن کلید تولید شده در محصول ذکر شود؟ از بین بردن کلید : بعد از تولید کلید در محصول توسط بکارگیری توابع و کتابخانه‌های رمزنگاری در صورتی که کلید مورد استفاده قرار نگیرد و یا نیاز به کلید جدید وجود داشته باشد، می‌بایست کلید قبلی در محل ذخیره‌سازی(فایل یا حافظه) پاک شود(متناسب با نوع حافظه و محل ذخیره‌سازی روش‌های از بین بردن کلید متفاوت خواهد بود)، در واقع باید به صورت دقیق به این نکته پی برده شود که کلید رمزنگاری اولیه در کدام مسیر و در کدام نقاط ذخیره شده است و سپس مشخص شود کلید به چه طریقی از بین خواهد رفت. جهت انجام این عملیات الگوریتم‌ها و مکانیزم‌های مختلفی وجود دارد، تولید کننده باید روشی که جهت از بین بردن کلید در محصول اتخاذ کرده است(در صورت استفاده از کتابخانه‌ی آماده مکانیزم مورد استفاده در آن کتابخانه) را تشریح کند و در سند ST محصول در شاخص	

ردیف	پرسش	پاسخ
	(FCS_CKM.4.1) ادعای خود را بیان کند.	
۱۲	توابع و کتابخانه مورد استفاده و همچنین مکانیزم بکارگیری جهت تولید بیت تصادفی در محصول ذکر شود؟ سازنده می بایست مکانیزم تولید عدد تصافی خود را بر اساس موارد زیر مشخص کند : □بر اساس نوع الگوریتم مورد استفاده در محصول □مطابق استاندارد NIST SP 800-90 و یا FIPS 140-2 □مکانیزم‌های سخت‌افزاری و یا نرم‌افزاری و یا هر دو مورد جهت تولید بیت تصادفی دو روش وجود خواهد داشت : اولین مورد تولید بیت تصادفی به صورت غیر قطعی که در آن بیت خروجی حاصل از یک فرآیند فیزیکی بوده (مثلا حرکت موس و ...) و کاملا غیر قابل پیش‌بینی است این کلاس را RBG گویند. در مولفه RBG یک دستگاه یا الگوریتم است که خروجی، دنباله‌ای از بیت‌های باینری که به صورت مستقل است را شامل می‌شود. دومین مورد برای تولید بیت‌های تصادفی استفاده از یک الگوریتم برای تولید بیت تصادفی است که در آن از یک دنباله اولیه (به عنوان نمونه Seed) و یا هر دنباله اولیه برای تولید بیت استفاده می‌کنند که این روش بیشتر شبیه شبه تصادفی است، این کلاس را DRBG گویند.	
۱۳	توابع و کتابخانه مورد استفاده جهت حداقل بیت آنتروپی و اندازه طول بیت آنتروپی ذکر شود. (منظور از طول بیت آنتروپی، مقدار طولی است که با استفاده از آن سیستم قادر به تولید بیت تصادفی است) تولید کننده می‌بایست مقدار حداقل بیت آنتروپی مورد نیاز که به منظور عملیات RBG استفاده می شود را مشخص کند. در صورتی که سیستم قادر به تامین و تولید آنتروپی لازم به منظور تولید بیت تصادفی نباشد، از چه روشی و ابزاری برای بالا بردن و تولید آنتروپی استفاده خواهد شد.	