| **فرم خود اظهاری آزمایشگاه ارزیابی سامانه‌های صدور و مدیریت گواهی الکترونیکی** |
| --- |
| نام تولیدکننده/ فروشنده: | تاریخ: |
| عنوان محصول: | نسخه: |
| نماینده تولیدکننده/فروشنده: |
| شماره تلفن: | ایمیل: |
| نماینده فنی تولیدکننده: |
| شماره تلفن: | ایمیل: |
| خلاصه‌ای از توصیف محصول: |

| **ردیف** | **پرسش** | **پاسخ** |
| --- | --- | --- |
| 1 | نوع مخزن پشتیبانی شده چیست؟ آیا این مخزن با SSL و یا TLS سازگاری دارد؟ |  |
| 2 | آیا سرویس OCSP در این محصول ارائه شده است؟ |  |
| 3 | آیا امکان معرفی سرویس‌دهنده‌های OCSP دیگر وجود دارد؟ (در صورت برقرار بودن این ارتباط چگونگی آن شرح داده شود) |  |
| 4 | آیا سرویس TSA در این محصول پیاده‌سازی شده است؟ |  |
| 5 | آیا امکان ارتباط با سایر سرویس‌دهنده‌های TSA وجود دارد؟ (در صورت برقرار بودن این ارتباط چگونگی آن شرح داده شود)  |  |
| 6 | آیا از استاندارد PKCS#11 پشتیبانی می‌شود؟ در صورت پشتیبانی در کدام بخش محصول این استاندارد بکار گرفته شده است؟ |  |
| 7 | آیا برای ارتباط با توکن‌ها یا HSM از CSP (CAPI) نیز استفاده شده است؟ در صورت پشتیبانی در کدام بخش محصول از این واسط استفاده شده است؟ |  |
| 8 | آیا از استاندارد PKCS#10 پشتیبانی می‌شود؟ |  |
| 9 | از استاندارد PKCS#10 در کدام بخش از محصول بهره گرفته شده است؟ |  |
| 10 | آیا از استاندارد CMP (RFC4210) پشتیبانی می‌شود؟ |  |
| 11 | از استاندارد CMP در کدام بخش از محصول بهره گرفته شده است؟ |  |
| 12 | آیا از استاندارد CMC (RFC5272-4) پشتیبانی می‌شود؟ |  |
| 13 | از استاندارد CMC در کدام بخش از محصول بهره گرفته شده است؟ |  |
| 14 | آیا از استاندارد PKCS#8 پشتیبانی می‌شود؟ |  |
| 15 | از استاندارد PKCS#8 در کدام بخش از محصول بهره گرفته شده است؟ |  |
| 16 | آیا از استاندارد PKCS#12 پشتیبانی می‌شود؟ |  |
| 17 | از استاندارد PKCS#12 در کدام بخش از محصول بهره گرفته شده است؟ |  |
| 18 | آیا ارتباط میان پایگاه داده و CA مبتنی بر SSL است؟ (در صورت برقرار بودن این ویژگی، چگونگی آن شرح داده شود) |  |
| 19 | آیا ارتباط میان RA و CA مبتنی بر SSL است؟ (در صورت برقرار بودن این ویژگی، چگونگی آن شرح داده شود) |  |
| 20 | آیا نرم‌افزار RA به‌صورت ماژول جدا معرفی شده است؟ |  |
| 21 | نرم‌افزار از چه وقایعی رویدادنگاری می‌کند؟ |  |
| 22 | آیا ماژول نصاب برای CA ارائه شده است؟ |  |
| 23 | آیا امکان استفاده از HSM در CA وجود دارد؟ |  |
| 24 | چه نقش‌هایی را می‌توان در کنسول CA برای کاربران تعریف کرد؟ |  |
| 25 | ارتباط میان کنسول CA و RA به چه صورت است؟  |  |
| 26 | مکانیسم احراز هویت کاربران در کنسول CA و RA به تفکیک چگونه است؟ |  |
| 27 | در صورت ثبت رویدادها، آیا امکان گزارش‌گیری مجزا از رویدادها وجود دارد؟ |  |
| 28 | آیا رویدادهای ثبت‌شده امضا می‌شوند؟ در صورت مثبت بودن جواب مکانیسم تولید و تصدیق امضا را شرح دهید. |  |
| 29 | در صورت استفاده از SSL، برای برقرار ارتباط SSL از چه کلیدها و گواهی‌هایی استفاده می‌شود؟ |  |
| 30 | آیا امکان به‌روزرسانی گواهی‌های SSL وجود دارد؟ (در صورت برقرار بودن این ویژگی، چگونگی آن شرح داده شود) |  |
| 31 | آیا می‌توان از طریق RA کاربران جدید تعریف کرد؟ |  |
| 32 | آیا امکان پشتیبان گیری از پایگاه داده در کنسول CA ارائه شده است؟ |  |
| 33 | آیا امکان پشتیبان گیری مستقیماً از پایگاه داده فراهم شده است؟ |  |
| 34 | آیا از مکانیسم خاصی جهت اطمینان از حفظ تمامیت و یا حفظ محرمانگی نسخه پشتیبان استفاده شده است؟ |  |
| 35 | الگوریتم‌های رمزنگاری مورداستفاده را نام ببرید. |  |
| 36 | آیا امکان پشتیبانی از ماژول‌های سخت‌افزاری رمزنگاری مختلف در سامانه وجود دارد؟ |  |
| 37 | نرم‌افزار CA بر روی چه سیستم‌عامل‌هایی قابل‌نصب است؟ |  |
| 38 | آیا امکان نصب نرم‌افزار CA در سیستم‌عامل‌های متن‌باز وجود دارد؟ |  |
| 39 | آیا امکان استفاده از سرویس‌های پایگاه داده متن‌باز به همراه CA وجود دارد؟ |  |
| 40 | روش استفاده از سرویس‌های پایگاه داده مختلف به هنگام نصب شرح داده شود. |  |
| 41 | روش پشتیبان گیری از پیکربندی جاری سیستم شرح داده شود. |  |
| 42 | چه پارامترهایی از سیستم در پشتیبان گیری از پیکربندی سیستم موردتوجه قرار می‌گیرند؟ |  |
| 43 | آیا فایل‌های پشتیبان پایگاه داده و پیکربندی به‌صورت رمز شده نگهداری می‌شود؟ در صورت مثبت بودن پاسخ کلید مورداستفاده برای رمزگذاری کجا نگهداری می‌شود؟ |  |
| 44 | آیا فایل‌های پشتیبان پایگاه داده و پیکربندی امضا می‌شوند؟ در صورت مثبت بودن پاسخ از چه کلیدی برای امضا کردن فایل‌ها استفاده می‌شود؟ |  |
| 45 | آیا امکان login بدون استفاده از توکن وجود دارد؟ |  |
| 46 | نوع احراز هویت مورداستفاده برای کاربران چیست؟ |  |
| 47 | آیا امکان تعریف پروفایل‌های جدید گواهی وجود دارد؟ |  |
| 48 | مؤلفه RA چگونه از تعریف پروفایل‌های جدید آگاه می‌شود؟ |  |
| 49 | آیا می‌توان زمان‌بندی و محل انتشار CRL ها را تغییر داد؟ |  |
| 50 | آیا امکان تعریف پروفایل‌های جدید برای صدور گواهی وجود دارد؟ |  |
| 51 | آیا نرم‌افزار CA تمامی فیلدهای موجود در پروفایل‌های مرکز دولتی صدور گواهی الکترونیکی ریشه را پشتیبانی می‌کند؟ |  |
| 52 | آیا می‌توان بدون استفاده از HSM گواهی‌های جدید را توسط نرم‌افزار CA تولید کرد؟ |  |
| 53 | آیا انجام عملیات تولید کلید برای کاربران توسط RA یا CA پشتیبانی می‌شود؟ در صورت مثبت بودن پاسخ این عملیات به چه صورت انجام می‌پذیرد؟ |  |
| 54 | عملیات تولید کلید برای درخواست‌کنندگان گواهی توسط چه موجودیتی و چگونه صورت می‌گیرد؟ |  |
| 55 | آیا شرکت ارائه‌دهنده محصول به متن اصلی برنامه برای توسعه و پشتیبانی محصول ارائه‌شده دسترسی دارد؟  |  |
| 56 | در صورت تأیید محصول در آزمایشگاه، مایل به انتشار نام محصول از طریق پورتال مرکز ریشه هستید؟ |  |