| **فرم خود اظهاری آزمایشگاه ارزیابی برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی** |
| --- |
| نام تولیدکننده/ فروشنده: | تاریخ: |
| عنوان محصول: | نسخه: |
| نماینده تولیدکننده/فروشنده: |
| شماره تلفن: | ایمیل: |
| نماینده فنی تولیدکننده: |
| شماره تلفن: | ایمیل: |
| خلاصه‌ای از توصیف محصول: |

| **حوزه‌های کاربرد برنامه تحت آزمون (توجه داشته باشید که ممکن است برنامه کاربردی شما شامل مؤلفه‌های مختلف مرتبط با چند حوزه باشد)** |
| --- |
| 🞏 | **پست الکترونیکی امن** | برنامه‌هایی که امکان استفاده از سرویس Secure Email را فراهم می‌کنند. |
| 🞏 | **میان‌افزار** | برنامه‌هایی که به‌عنوان یک لایه میانی بین برنامه‌های دیگر و شبکه عمل می‌کنند و امکان استفاده از سرویس‌هایی چون احراز هویت، کنترل دسترسی، دایرکتوری را فراهم می‌کنند. |
| 🞏 | **ابزارهای احراز هویت** | ابزارهای احراز هویت می‌توانند به‌صورت برنامه‌های مجزا یا به‌صورت بخشی از برنامه‌های دیگر، مورد ارزیابی قرار گیرند. ویژگی اصلی این برنامه‌ها، فراهم آوردن امکان احراز هویت دوعاملی مبتنی بر فرایند پرسش و پاسخ منطبق بر الزامات استاندارد FIPS 196 می‌باشد. |
| 🞏 | **امضای دیجیتال** | ابزارهای امضای دیجیتال می‌توانند به‌صورت مستقل و یا در قالب سایر برنامه‌های کاربردی برای ارزیابی به آزمایشگاه ارائه شوند. ابزارهای مزبور برای پیاده‌سازی توابع تولید و بازبینی امضای دیجیتال مورداستفاده قرار می‌گیرند و سرویس عدم انکار و یکپارچگی را برای کاربران فراهم می‌کنند. |
| 🞏 | **ابزارهای امضا و رمزگذاری اسناد** | ابزارهای امضا و رمزگذاری اسناد، علاوه بر فراهم آوردن امکان تولید و بازبینی امضای دیجیتال، با استفاده از فراخوانی توابع رمزنگاری مختلف، سرویس محرمانگی را نیز در اختیار کاربران قرار می‌دهند. |
| 🞏 | **برنامه‌های توزیع‌شده مبتنی بر ارسال پیام** | برنامه‌های توزیع‌شده مبتنی بر ارسال پیام، برنامه‌هایی هستند که دارای مؤلفه‌های مختلفی هستند که هرکدام از آن می‌توانند بر روی یک منبع پردازشی مجزا به اجرا درآیند، در این نوع برنامه‌های کاربردی ارتباط میان مؤلفه‌های مختلف از طریق الگوی انتقال پیام انجام می‌شوند. این دسته از برنامه‌ها معمولاً سرویس‌های محرمانگی، یکپارچگی، عدم انکار و احراز اصالت پیام[[1]](#footnote-2) را از طریق استانداردهای امنیتی ارائه‌شده برای پروتکل‌های انتقال پیام به کاربران فراهم می‌کنند. باید توجه داشت که این دسته از برنامه‌ها به دلیل ارتباطات ناهمگام خود، معمولاً نیازی به استفاده از امن سازی کانال با استفاده از پروتکل SSL ندارند. |
| 🞏 | **سیستم‌عامل‌ها** | سیستم‌عامل‌ها به‌عنوان زیرساخت اصلی مدیریت امنیت کاربران و برنامه‌های کاربردی مورداستفاده قرار می‌گیرند. این دسته از نرم‌افزارها باید امکان دسترسی کاربران به سرویس‌های متفاوتی را فراهم کرده باشند. برخی از سیستم‌عامل‌ها به‌صورت درونی برخی از توابع رمزنگاری و سرویس‌های زیرساخت کلید عمومی را پیاده‌سازی می‌کنند که صحت این پیاده‌سازی‌ها باید در آزمایشگاه زیرساخت کلید عمومی مورد ارزیابی قرار گیرد. |
| 🞏 | **ابزارهای برقرار ارتباط امن مبتنی بر SSL** | ابزارهایی هستند که یا در سمت سرور و یا در کلاینت کتابخانه مربوط به پروتکل SSL را مورداستفاده قرار می‌دهند. |

| **ردیف** | **پرسش** | **پاسخ** |
| --- | --- | --- |
| 1 | نرم‌افزار به‌صورت مستقل[[2]](#footnote-3) و یا به‌صورت سرور و کلاینت عمل می‌نماید. |  |
| 2 | آیا در نرم‌افزار نقش‌های مختلف با دسترسی‌های مختلف تعریف شده است. |  |
| 3 | آیا داده‌های مرتبط با سامانه نرم‌افزاری نیاز به محرمانگی دارند؟ |  |
| 4 | آیا نرم‌افزار پایگاه داده دارد؟ |  |
| 5 | برنامه کاربردی چه سخت‌افزار و سیستم‌عامل‌هایی را پشتیبانی می‌کند؟ |  |
| 6 | برنامه کاربردی به چه برنامه‌های دیگری وابسته است؟ (مثل Netscape، IE، Opera) |  |
| 7 | آیا برنامه کاربردی قابلیت درخواست و اخذ گواهی را دارد؟ |  |
| 8 | آیا برنامه کاربردی قابلیت وارد نمودن و صادر نمودن گواهی در قالب pkcs#12 را دارد؟ چگونه؟  |  |
| 9 | آیا برنامه کاربردی قابلیت تولید جفت کلید و یا گواهینامه را دارد؟ |  |
| 10 | آیا برنامه کاربردی قابلیت استفاده از کارت‌های هوشمند و توکن‌های رایج را دارد؟ |  |
| 11 | آیا برنامه کاربردی عملیات اعتبارسنجی و پردازش مسیر بر اساس X.509 را انجام می‌دهد. |  |
| 12 | آیا برنامه کاربردی قابلیت بازیابی گواهی‌های مرتبط با سایر موجودیت‌های دیگر را دارد (مانند بازیابی کلید عمومی از سرویس‌دهنده دایرکتوری) |  |
| 13 | لطفاً نحوه مدیریت و ذخیره نقاط مورداطمینان (مراکز CA) را توضیح دهید. مجوز تنظیم نقاط مورداطمینان (مراکز CA) در اختیار چه کسی است؟ (کاربر و یا مدیر شبکه) |  |
| 14 | آیا برنامه کاربردی از پروتکل‌های ارتباطی LDAP، HTTP و یا HTTPS استفاده می‌کند |  |
| 15 | آیا برنامه کاربردی وضعیت ابطال گواهی را بررسی می‌کند؟ (به‌طور مثال آیا از سرویس‌دهنده دایرکتوری استفاده می‌کند، به‌صورت دستی باید CRL ها را بارگذاری کرد، به‌صورت آنلاین وضعیت گواهی را بررسی می‌کند) |  |
| 16 | برنامه کاربردی در چه حوزه‌هایی PKI را پشتیبانی می‌کند؟ (احراز هویت، امضا اسناد، رمزنگاری، امضای تراکنش‌ها، سرویس‌دهنده دایرکتوری و ...)  |  |
| 17 |  با توجه به بندهای قبل، درخواست آزمون و ارزیابی در چه حوزه‌ای را دارید؟ (برای مثال در حوزه‌های احراز هویت) |  |
| 18 | آیا نرم‌افزار امکان استفاده از OCSP را فراهم کرده است؟ |  |
| 19 | آیا نرم‌افزار امضای دیجیتال را پیاده‌سازی کرده است؟ |  |
| 20 | درصورتی‌که امضای دیجیتال در نرم‌افزار پیاده‌سازی شده است. قالب تولید امضا را به‌صورت کامل شرح دهید. |  |
| 21 | آیا نرم‌افزار از فرایند احراز هویت مبتنی بر FIPS-196 را پشتیبانی می‌کند؟ |  |
| 22 | آیا نرم‌افزار امکان استفاده از سرویس‌های S/MIME را دارد؟ |  |
| 23 | آیا نرم‌افزار امکان استفاده از SSL را فراهم می‌کند؟ |  |
| 24 | آیا نرم‌افزار برای ارتباط با پایگاه داده و سرویس‌دهنده دایرکتوری از ارتباط امن استفاده می‌کند؟ |  |
| 25 | آیا نرم‌افزار فرایند log گیری را در داخل پایگاه داده به‌صورت log Chaining انجام می‌دهد؟ |  |
| 26 | در صورت تولید و ذخیره زوج کلید، کلیدهای تولیدشده کجا نگهداری می‌شوند؟ |  |
| 27 | چه الگوریتم‌های رمزنگاری در نرم‌افزار مورداستفاده قرار می‌گیرند؟ |  |
| 28 | آیا امکان پیکربندی مراکز OCSP در داخل نرم‌افزار وجود دارد؟ |  |
| 29 | در صورت تأیید محصول در آزمایشگاه، مایل به انتشار نام محصول از طریق پورتال مرکز ریشه هستید؟ |  |

1. Message Authentication Code (MAC) [↑](#footnote-ref-2)
2. Stand alone [↑](#footnote-ref-3)