| **فرم خوداظهاری ارزیابی PKE SDK** | |
| --- | --- |
| 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 | محصول از چه ماژول‌های سخت‌افزاری پشتیبانی می‌کند؟ |  |
| 2 | از محصول در چه سیستم‌عامل‌هایی می‌توان استفاده نمود؟ |  |
| 3 | از محصول در چه پلتفرم‌ها و چهارچوب‌هایی می‌توان استفاده نمود؟ |  |
| 4 | از محصول در چه محیط‌های برنامه‌نویسی می‌توان استفاده نمود؟ |  |
| 6 | محصول به چه برنامه‌های دیگری وابسته است؟ (مثل Netscape، IE، Opera) |  |
| 7 | آیا محصول عملیات اعتبارسنجی و پردازش مسیر انجام می‌دهد؟ در صورت مثبت بودن پاسخ چه الزاماتی در آن جهت اعتبارسنجی در نظر گرفته شده است. |  |
| 8 | آیا محصول قابلیت واکشی را دارد؟ (مانند بازیابی کلید عمومی و CRL از سرویس‌دهنده دایرکتوری) |  |
| 9 | آیا محصول از پروتکل‌های ارتباطی LDAP، HTTP و یا HTTPS استفاده می‌کند؟ در صورت مثبت بودن پاسخ جایگاه استفاده از پروتکل‌های مزبور را توصیف کنید. |  |
| 10 | آیا محصول امکان استفاده از OCSP را فراهم کرده است؟ |  |
| 11 | آیا ساختار پیام‌های رمزنگاری مورداستفاده در محصول (به‌عنوان‌مثال ساختار امضای تولیدشده) از استاندارد PKCS#7 (CMS) تبعیت می‌نماید؟ آیا کدگذاری BER در محصول پشتیبانی می‌شود؟ |  |
| 12 | آیا در محصول ابزار احراز هویت کلید عمومی مبتنی بر چالش و پاسخ ارائه شده است؟ |  |
| 13 | آیا محصول امکان استفاده از SSL را فراهم می‌کند؟ |  |
| 14 | آیا محصول امکان استفاده از S-MIME را فراهم می‌کند؟ |  |
| 15 | در صورت تولید و ذخیره زوج کلید، کلیدهای تولیدشده در چه قالبی و بر اساس چه استانداردی نگهداری می‌شوند؟ |  |
| 16 | چه الگوریتم‌های رمزنگاری در محصول مورداستفاده قرار می‌گیرند؟ |  |
| 17 | در صورت تأیید محصول در آزمایشگاه، مایل به انتشار نام محصول از طریق پورتال مرکز ریشه هستید؟ |  |