



جمهوری اسلامی ایران
مرکز دولتی صدور گواهی الکترونیکی ریشه

نتایج ارزیابی نرم افزارهای PKI

طبقه بندی: عادی

شماره بازنگری: 9.0

تاریخ بازنگری: 97/08/27

فهرست مطالب	
صفحه	عنوان
2.....	1 مقدمه
4.....	2 روال آزمون
5.....	3 گزارش ارزیابی سامانه های صدور و مدیریت گواهی الکترونیکی
8.....	4 گزارش ارزیابی ابزارهای توسعه نرم افزارهای PKE (PKE SDK)
13	5 گزارش ارزیابی نرم افزارهای PKE

1 مقدمه

کاربرد روزافزون زیر ساخت کلید عمومی (PKI¹) و گواهی الکترونیکی در بسترهای اطلاعاتی کشور، اهمیت به‌کارگیری و استفاده صحیح مؤلفه‌های این زیر ساخت در نرم‌افزارها و نیز لزوم پیاده‌سازی صحیح و اصولی نرم‌افزارهای صدور و مدیریت گواهی الکترونیکی بر اساس استانداردهای زیرساخت کلید عمومی را بیش‌ازپیش نشان می‌دهد. بر اساس بند ت ماده 5 آیین‌نامه اجرایی ماده 32 قانون تجارت الکترونیکی در رابطه با بررسی و احراز شرایط لازم و صلاحیت متقاضیان ایجاد مراکز میانی و صدور مجوز برای آن‌ها و نیز مطابق با سیاست‌های گواهی الکترونیکی م‌صوب شورای سیاست‌گذاری گواهی الکترونیکی کشور، مرکز دولتی صدور گواهی الکترونیکی ریشه، [استانداردهای ملی زیرساخت کلید عمومی](#) را تدوین و ارائه نموده است. این مرکز آزمایشگاه ارزیابی محصولات مرتبط با این زیرساخت را به‌منظور بررسی تطابق با استانداردهای مذکور راه‌اندازی کرده است.

آزمایشگاه‌های نرم‌افزارهای PKI با هدف آزمون و ارزیابی محصولات نرم‌افزاری مبتنی بر زیرساخت کلید عمومی یا PKI، شامل نرم‌افزارهای صدور و مدیریت گواهی الکترونیکی و نرم‌افزارهای مجهز به زیرساخت کلید عمومی (PKE) تحت نظارت مرکز دولتی صدور گواهی الکترونیکی ریشه تأسیس و راه‌اندازی شده است و ارزیابی‌های خود را بر اساس استانداردها و سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور انجام می‌دهد.

در این گزارش لیست محصولات نرم‌افزاری مورد آزمون در حوزه PKI به تفکیک نوع محصول نرم‌افزاری در دو بخش سامانه‌های صدور و مدیریت گواهی الکترونیکی و ابزارهای توسعه نرم‌افزارهای PKE (-PKI Enabled) آورده شده است.

با توجه به دسته‌بندی نرم‌افزارهای PKI به دو دسته: سامانه‌های صدور و مدیریت گواهی الکترونیکی و برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی (PKI) و ابزارهای توسعه آن، در حال حاضر ارزیابی این نرم‌افزارها در آزمایشگاه‌های ارزیابی سامانه‌های صدور و مدیریت گواهی الکترونیکی و ارزیابی برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی کشور (PKE)، تحت نظارت مرکز دولتی صدور گواهی الکترونیکی ریشه، انجام می‌گیرد.

¹ Public Key Infrastructure

آزمایشگاه‌های مرکز دولتی ریشه، ارزیابی‌های خود را بر اساس استانداردهای ملی و سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور انجام داده و نتایج را بر اساس مشخصات مربوطه و همچنین سطح اطمینان کسب‌شده ارائه می‌دهد.

سطوح اطمینان

سطوح اطمینان موردقبول برای هر یک از محصولات مطابق با الزامات مندرج در سند «سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور» و سند «جامع پروفایل‌های زیرساخت کلید عمومی کشور» تعیین شده است. سطوح اطمینان چهارگانه مصوب در سند سیاست‌های گواهی الکترونیکی کشور شامل سطح اطمینان اول (برنز)، سطح اطمینان دوم (نقره)، سطح اطمینان سوم (طلا) و سطح اطمینان چهارم (پلاتین) می‌باشد. تعریف هر یک از سطوح اطمینان گواهی در جدول 2 از سند «سیاست‌های گواهی الکترونیکی» در آدرس <http://www.rca.gov.ir> آمده است. سطح اطمینان اعلام‌شده در جدول نتایج، نشان می‌دهد که محصول SDK، قابلیت کار با گواهی‌های متنظر با کدام‌یک از سطوح اطمینان را دارد. برای کار با گواهی‌های سطوح اطمینان بالاتر (مثلاً سطوح سوم و چهارم)، برخورداری از برخی امکانات خاص (مثلاً مدیریت کلیدهای رمزنگاشتی با طول بیش از 1024 بیت) ضروری است.

نکات قابل توجه

- 1- ارزیابی محصول منحصراً در حوزه زیرساخت کلید عمومی (PKI) انجام شده و مؤید رعایت سایر استانداردهای تولید نرم‌افزار (از جمله استانداردهای امنیت و کارایی) نیست.
- 2- گزارش و نتایج ارزیابی محصول از سوی مرکز دولتی صدور گواهی الکترونیکی ریشه به مالک محصول تحویل داده می‌شود. لذا متقاضیان در صورت نیاز می‌توانند گزارش مهور به مهر مرکز توسعه تجارت الکترونیکی را از مالک محصول مطالبه نمایند.
- 3- استفاده از زیرساخت کلید عمومی کشور نیازمند بهره‌گیری از مجموعه‌ای از تجهیزات سخت‌افزاری و نرم‌افزاری استاندارد است. برای ارزیابی هر یک از اجزاء سخت‌افزاری و نرم‌افزاری، محیط آزمون جداگانه‌ای طراحی شده است که صرفاً محدوده عملکرد آن جزء را (با فرض درستی عملکرد سایر اجزای زیرساخت کلید عمومی) مورد ارزیابی قرار می‌دهد.

لذا از آنجاکه به کارگیری هر تجهیز غیراستاندارد می‌تواند اثر مخربی بر روی عملکرد نهایی مورد انتظار از زیرساخت کلید عمومی داشته باشد، به نحوی که خدشه جدی بر کل عملیات انجام شده در استفاده از گواهی الکترونیکی وارد نماید، نسبت به هرگونه استفاده از تجهیزات غیراستاندارد، هشدار داده می‌شود.

مؤلفه‌های سخت‌افزاری و نرم‌افزاری مورداستفاده در حوزه زیرساخت کلید عمومی عبارتند از: نرم‌افزارهای صدور و مدیریت گواهی (CA)، سرورهای استعلام برخط وضعیت گواهی (OCSP)، سرورهای مهر زمانی (TSA)، سخت‌افزارها یا نرم‌افزارهای ماژول رمزنگاری و سامانه‌های کاربردی دارای قابلیت استفاده از گواهی/امضای الکترونیکی.

2 روال آزمون

فرآیند آزمون از مرحله درخواست ارزیابی محصول تا ارائه گزارش آن مطابق با [سند راهنمای درخواست آزمون نرم افزارهای زیرساخت کلید عمومی](#) منتشرشده در وبسایت مرکز دولتی ریشه صورت می پذیرد. مشخصات کلی ارائه شده در جدول نتایج، به شرح زیر می باشد:

- ❖ **کد محصول:** شماره پرونده ای است که پس از ارسال تقاضای ارزیابی از جانب متقاضی، مرکز دولتی ریشه به محصول مورد ارزیابی تخصیص می دهد.
- ❖ **مالک محصول / متقاضی ارزیابی:** شرکت یا سازمان تولیدکننده / واردکننده و یا شرکت یا سازمانی که قصد استفاده از محصول را دارد، می باشد.
- ❖ **نام تجاری محصول:** نام تجاری محصول که از جانب متقاضی ارزیابی، عنوان می گردد.
- ❖ **محیط آزمون (فقط در جدول نتایج نرم افزارهای PKE و PKE SDK):** مشخص کننده سیستم عامل یا پلتفرمی است که بنا به اظهار متقاضی، محصول در آن عملیاتی شده و مورد آزمون قرار گرفته است.
- ❖ **تکنولوژی مورد آزمون (فقط در جدول نتایج نرم افزارهای PKE و PKE SDK):** مشخص کننده تکنولوژی و شیوه ای است که بنا به اظهار متقاضی، محصول با آن پیاده سازی شده است.
- ❖ **محدوده گواهی اعطاء شده:** سرویس ها یا قابلیت های یک محصول که در آزمایشگاه مورد ارزیابی قرار گرفته است.

توجه: عملکرد نرم افزار در هر یک از محیط های عملیاتی مورد ادعای متقاضی به طور جداگانه ارزیابی می گردد.

3 گزارش ارزیابی سامانه‌های صدور و مدیریت گواهی الکترونیکی

سامانه صدور و مدیریت گواهی الکترونیکی همان‌طور که از نام آن پیداست جهت درخواست، صدور و مدیریت گواهی‌های الکترونیکی X509 بکار می‌رود که به‌طور معمول در مراکز صدور گواهی الکترونیکی مورد استفاده قرار می‌گیرد و دارای مؤلفه‌های مختلف شامل موارد ذیل می‌باشد:

1. CA: جهت صدور و مدیریت گواهی الکترونیکی و انتشار آن؛
 2. RA: جهت مدیریت درخواست گواهی الکترونیکی؛
 3. OCSP: جهت اعلام برخط وضعیت ابطال یا عدم ابطال گواهی‌های الکترونیکی؛ این مؤلفه می‌تواند به‌عنوان یک نرم‌افزار مستقل از سامانه صدور و مدیریت گواهی الکترونیکی نیز عمل کرده و به آزمایشگاه ارائه گردد.
 4. TSA: به‌منظور تولید مهر زمانی؛ این مؤلفه می‌تواند به‌عنوان یک نرم‌افزار مستقل از سامانه صدور و مدیریت گواهی الکترونیکی نیز عمل کرده و به آزمایشگاه ارائه گردد.
- ارزیابی سامانه‌های صدور و مدیریت گواهی الکترونیکی بر اساس سند [سیاست‌های گواهی الکترونیکی](#) [زیرساخت کلید عمومی کشور](#)، [سند جامع پروفایل‌های زیرساخت کلید عمومی کشور](#) و [استانداردهای مرتبط](#) (که از طریق وب‌سایت مرکز دولتی ریشه منتشر شده است)، صورت می‌پذیرد. در جدول صفحه بعد لیست محصولات مورد آزمون در این حوزه با ذکر سطح اطمینان مورد قبول ارائه شده است.

جدول 1- گزارش ارزیابی سامانه های صدور و مدیریت گواهی الکترونیکی

نتیجه آزمون				نام مؤلفه	محیط عملیاتی	مرتبه آزمون	نام تجاری محصول	مالک محصول / متقاضی ارزیابی	کد محصول	ردیف
سرویس TSA	سرویس OCSP	مدیریت ثبت نام (RA)	مدیریت گواهی الکترونیکی (CA)							
-	نقره (2)	طلا (3)	طلا (3)	سطح اطمینان	Linux/Windows	اول	ParsSign	شرکت امن افزار گستر شریف	CA-10001-01	1
-	R9006 B4	R9006 B8	R9006 B21	نسخه محصول						
-	طلا (3)	-	نقره (2)	سطح اطمینان	Windows	سوم	PKA	شرکت پندار کوشک ایمن	CA-10005-03	2
-	4.0.3	-	4.0.3	نسخه محصول						
طلا (3)	پلاتین (4)	طلا (3)	طلا (3)	سطح اطمینان	Linux/Windows	دوم	ParsTrust	شرکت امن افزار گستر شریف	CA-10010-02	3
R9221 B2	R9212 B9	R9212 B5	R9212 B14	نسخه محصول						
-	طلا (3)	طلا (3)	طلا (3)	سطح اطمینان	Linux/Windows	دوم	MegaCA	شرکت فاونفت صباکیش	CA-10012-02	4
-	1.3.1	1.3.1	1.3.1	نسخه محصول						
-	-	نقره (2)	نقره (2)	سطح اطمینان	Windows	سوم	ExpressCA	شرکت ره آورد سامانه های امن	CA-10006-02	5
-	-	Express RA 1.0	Express CA 1.0	نسخه محصول						
	طلا (3)	برنز (1)	نقره (2)	سطح اطمینان	Windows	دوم	Avanoc-CA	شرکت سبا پردازش	CA-10003-02	6
	5.2	5.2	5.2	نسخه محصول						
	نقره (2)	نقره (2)	طلا (3)	سطح اطمینان	Windows	دوم		شرکت سرمایه گذاران فناوری	CA-10018-02	7

	6.0.4	6.0.4	6.0.4	نسخه محصول			Smart Trust CA	تکوست		
طلا (3)	طلا (3)	برنز (1)	طلا (3)	سطح اطمینان			RCA	شرکت فناوران اعتماد راهبر	CA-10014-02	8
2.1.0	2.1.0	2.1.0	2.1.0	نسخه محصول		دوم				

4 گزارش ارزیابی ابزارهای توسعه نرم افزارهای PKE (PKE SDK)

سامانه های نرم افزاری نظیر سیستم های اتوما سیون (اداری، مالی، بانکی و ...) جهت به کارگیری قابلیت های مختلف زیر ساخت کلید عمومی از طریق گواهی های الکترونیکی X509، نیازمند ابزارهای توسعه نرم افزاری¹ هستند. به فرآیند تجهیز نرم افزارهای مختلف به قابلیت کار با زیرساخت کلید عمومی اصطلاحاً PK-Enabling و به یک نرم افزار مجهز شده به این قابلیت ها، نرم افزار PKE² گفته می شود. همچنین ابزارهای توسعه نرم افزارهای PKE که معمولاً به صورت توابع کتابخانه ای در اختیار توسعه دهندگان قرار می گیرد را اصطلاحاً PKE SDK می نامیم. برای انتخاب یک PKE SDK مناسب باید به فاکتورهایی همچون محیط توسعه نرم افزار، تکنولوژی مورد استفاده برای توسعه نرم افزار و سطح اطمینان گواهی های مورد استفاده توجه کرد.

PKE SDK، با برخورداری از توابع و ماژول های برنامه نویسی آماده، فرایند توسعه محصول را برای برنامه نویسانی که با مباحث تخصصی زیر ساخت کلید عمومی آشنایی ندارند، ساده می کند؛ زیرا برنامه نویس فارغ از دغدغه های پیاده سازی همه جزئیات استانداردهای زیر ساخت کلید عمومی، صرفاً با فراخوانی توابع آماده به توسعه و تجهیز نرم افزار خود می پردازد.

برنامه های کاربردی PKE که با کمک یک PKE SDK به قابلیت کار با گواهی های الکترونیکی مجهز می شوند، در نهایت بایستی برای اطمینان از صحت عملکرد، در آزمایشگاه های ارزیابی نرم افزارهای مجهز به زیر ساخت کلید عمومی کنترل شوند؛ زیرا ممکن است توسعه دهندگان نرم افزار علیرغم استفاده از یک ابزار توسعه ای استاندارد، در به کارگیری توابع و ماژول های آماده دچار خطا شوند و نرم افزار نهایی عملکرد درستی نداشته باشد؛ هرچند استفاده از ابزارهای توسعه ای استاندارد تأثیر قابل ملاحظه ای در تسریع فرایند توسعه نرم افزار و کاهش پیچیدگی ها و خطاهای برنامه نویسی خواهد داشت.

لازم به ذکر است که ارزیابی نرم افزارهای PKE و ابزارهای توسعه این نرم افزارها بر اساس استاندارد «الزامات برنامه های کاربردی مجهز به زیرساخت کلید عمومی ایران» صورت می پذیرد.

در ارزیابی ابزارهای SDK ارائه شده به آزمایشگاه دو دسته شاخص مورد توجه اند:

1- الزامات پایه ای که جزء الزامات حیاتی هر PKE SDK به شمار می روند.

¹ Software Development Kit (SDK)

² Public Key Enabled Application

2- قابلیت های جانبی محصول که بنا به خوداظهاری متقاضی آزمون، مطابق استانداردهای ملی پیاده سازی و عملیاتی شده است. پیاده سازی این قابلیت های در صورت ادعای متقاضی مبنی بر پیاده سازی، بایستی صحت عملکرد آنها مورد آزمون قرار گیرد.

لازم به ذکر است در مواردی بنا به اظهار مالک محصول، قابلیت در محصول وجود دارد، اما درستی عملکرد آن طی آزمون اثبات نشده، لذا قابلیت مذکور در جدول نتایج آن محصول مورد تأیید قرار نگرفته است. شرح مختصر الزامات پایه ای و قابلیت های جانبی در جدول زیر آمده است:

الزامات پایه ای PKE SDK	
توضیح	قابلیت
امکان برقراری ارتباط و به کارگیری پودمان رمزنگاشتی مطابق با استاندارد «الزامات پودمان های رمزنگاشتی در زیرساخت کلید عمومی»	کار با پودمان رمزنگاشتی
امکان کنترل و رسیدگی و عکس العمل مناسب در مقابل کلیه خطاها	مدیریت خطا
امکان پشتیبانی از کلیدهای رمزنگاشتی با طول مجاز و پارامترها، مطابق با سیاست های گواهی الکترونیکی کشور	مدیریت کلید
توانایی استخراج و پردازش انواع فیلدها و الحاقیه های گواهی و لیست های ابطال	مدیریت گواهی و لیست ابطال
پیاده سازی حداقل یک الگوریتم رمزنگاری مورد تأیید در زیرساخت کلید عمومی کشور در هر یک از حوزه های الگوریتم های نامتقارن، توابع درهم ساز و مولدهای اعداد تصادفی	رمزنگاری نامتقارن
مطابقت ساختارهای رمزنگاری مطابق با استاندارد «الزامات ساختار نحوی پیام های رمزنگاری در زیرساخت کلید عمومی کشور»	تعامل پذیری
اجرای فرآیند تشکیل و اعتبارسنجی زنجیره گواهی مطابق با استاندارد ملی «تشکیل و اعتبارسنجی مسیر گواهی دیجیتالی»	تشکیل و اعتبارسنجی مسیر گواهی

قابلیت های جانبی PKE SDK	
توضیح	قابلیت
پیاده سازی سازوکار احراز هویت مبتنی بر رمزنگاری کلید عمومی منطبق با استاندارد ملی «الزامات پروتکل احراز هویت در زیرساخت کلید عمومی ایران»	احراز هویت
پیاده سازی حداقل یک الگوریتم رمزنگاری متقارن مورد تأیید در زیرساخت کلید عمومی کشور	رمزنگاری متقارن
امکان ارتباط با سرویس دهنده های دایرکتوری و درخواست واکشی گواهی و لیست ابطال	ارتباط با سرویس دهنده دایرکتوری
امکان ارتباط با سرویس دهنده های پاسخگوی OCSP و درخواست اعتبارسنجی گواهی	اعتبارسنجی برخط گواهی

قابلیت‌های جانبی PKE SDK	
توضیح	قابلیت
امکان ارتباط با سرویس دهنده‌های TSA و درخواست مهر زمانی معتبر	الصاق مهر زمانی
امکان تولید درخواست گواهی الکترونیکی مطابق با استاندارد «پروتکل درخواست گواهی الکترونیکی در زیرساخت کلید عمومی ایران»	درخواست گواهی

در جدول صفحه بعد گزارش آزمون ابزارهای PKE SDK، ارائه شده است.

ردیف	کد محصول	مالک محصول / متقاضی ارزیابی	نام تجاری محصول	محیط عملیاتی آزمون	تکنولوژی مورد آزمون	شماره نسخه	بشپینی از سطح اطمینان							محدوده گواهی اعطاء شده						
							بزنز (1)	نقره (2)	طلا (3)	پلاتین (4)	کار با یودمان رمزنگاشتی	مدیریت خطا	مدیریت کلید	مدیریت گواهی و لیست ابطال	رمزنگاری نامتقارن	تعامل پذیری	تشکیل و اعتبارسنجی مسیر گواهی	احراز هویت	رمزنگاری متقارن	ارتباط با سرویس دهنده دایرکتوری
1	SDK-10001-02	شرکت ره آورد سامانه های امن	Power PKI SDK	Windows	ActiveX	1.0.0.0	✓	✓	-	-	✓	✓	✓	✓	✓	✓	-	-	-	-
2	SDK-10002-03	شرکت امن افزار گستر شریف	ParsKit PKE	Windows / Linux	ActiveX / JavaApplet / PHP extension	1.4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

ردیف	کد محصول	مالک محصول / متقاضی ارزیابی	نام تجاری محصول	محیط عملیاتی آزمون	تکنولوژی مورد آزمون	شماره نسخه	پشتیبانی از سطح اطمینان												
							الزامات پایه‌ای						سایر قابلیت‌ها						
3	SDK-10003-02	شرکت پندار کوشک ایمن	دستپایه	Windows	.NET	2.0.0.3	کار با پودمان رمزنگارشی	مدیریت خطا	مدیریت کلید	مدیریت گواهی و لیست ابطال	رمزنگاری نامتقارن	تعامل پذیری	تشکیل و اعتبارسنجی مسیر	احراز هویت	رمزنگاری متقارن	ارتباط با سرویس دهنده	اعتبارسنجی بر خط گواهی	الصاق مهر زمانی	درخواست گواهی
							✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	✓

جدول 2 - گزارش ارزیابی ابزارهای توسعه نرم‌افزارهای (PKE SDK) PKE

5 گزارش ارزیابی نرم‌افزارهای PKE

سامانه‌های نرم‌افزاری نظیر سیستم‌های اتوماسیون (اداری، مالی، بانکی و ...) جهت به‌کارگیری گواهی‌های الکترونیکی و برخورداری از قابلیت‌هایی همچون امضای دیجیتال یا احراز هویت کاربران، باید مجموعه‌ای از الزامات را رعایت نمایند. الزامات برنامه‌های کاربردی دارای قابلیت کار با گواهی الکترونیکی، در استاندارد با همین عنوان و از طریق پورتال مرکز صدور گواهی الکترونیکی ریشه (به آدرس www.rca.gov.ir) قابل‌دستیابی است. به فرآیند تجهیز نرم‌افزارهای مختلف به قابلیت کار با گواهی‌های الکترونیکی اصطلاحاً PK-Enabling و به یک نرم‌افزار تجهیز شده به این قابلیت‌ها، نرم‌افزار PKE¹ گفته می‌شود. امضای دیجیتال و احراز هویت دو عامله پرکاربردترین موارد استفاده از گواهی‌های الکترونیکی هستند. نکته حائز اهمیت در این میان اینکه؛ عدم رعایت دقیق الزامات تجهیز سامانه‌های نرم‌افزاری به قابلیت کار با گواهی الکترونیکی، مخاطراتی از قبیل به‌کارگیری گواهی‌های الکترونیکی منقضی یا باطل‌شده، به‌کارگیری الگوریتم‌های رمزنگاری جعلی، عدم امکان تعامل نرم‌افزار با سایر مؤلفه‌های زیرساخت کلید عمومی کشور، عدم اطمینان از صحت و اعتبار امضای الکترونیکی انجام‌شده، عدم اطمینان از امضای اطلاعات موردنظر و مواردی از این دست را به دنبال دارد.

در جدول 3 لیست نرم‌افزارهای کاربردی که موفق به اخذ تأییدیه آزمایشگاه مرکز دولتی صدور گواهی الکترونیکی ریشه شده‌اند قابل‌مشاهده است.

¹ Public Key Enabled Application

جدول 3 - گزارش ارزیابی سامانه‌های کاربردی دارای قابلیت کار با گواهی الکترونیکی

ردیف	کد محصول	مالک محصول / متقاضی ارزیابی	نام تجاری محصول	محیط عملیاتی آزمون	شماره نسخه	پشتیبانی از سطح اطمینان				قابلیت کار با گواهی الکترونیکی	
						برنز (1)	نقره (2)	طلا (3)	پلاتین (4)	امضای دیجیتال	اجراز هویت دو عامله
1	PKE-10011-02	شرکت همکاران سیستم	اتوماسیون اداری تحت شبکه	Windows / Linux	8	✓	✓	-	-	✓	✓