جمهوری اسلامی ایران
مرکز دولتی صدور گواهی الکترونیکی ریشه

نتایج ارزیابی نرم‌افزارهای PKI

طبقه‌بندی: عادی

شماره بازنگری: ۹,۰

تاریخ بازنگری: ۹۷/۰۳/۰۵

فهرست مطالب

۱ مقدمه

کاربرد روزافزون زیر ساخت کلید عمومی (PKI[1]) و گواهی الکترونیکی در بسترهای اطلاعاتی کشور، اهمیت به‌کارگیری و استفاده صحیح مؤلفه‌های این زیر ساخت در نرم‌افزارها و نیز لزوم پیاده سازی صحیح و اصولی نرم‌افزارهای صدور و مدیریت گواهی الکترونیکی بر اساس استانداردهای زیرساخت کلید عمومی را بیش‌ازپیش نشان می‌دهد. بر اساس بند ت ماده ۵ آیین‌نامه اجرایی ماده ۳۲ 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 زیر ساخت 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» تعیین‌شده 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 ۲ 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 متناظر 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 ۱۰۲۴ بیت) ضروری است.

نکات قابل‌توجه

۱- ارزیابی محصول منحصراً در حوزه زیرساخت کلید عمومی (PKI) انجام شده و مؤید رعایت سایر استانداردهای تولید نرم‌افزار (ازجمله استانداردهای امنیت و کارایی) نیست.

۲- 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 ممهور به مهر مرکز توسعه تجارت الکترونیکی را از مالک محصول مطالبه نمایند.

۳- 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 ازآنجاکه به‌کارگیری هر تجهیز غیراستاندارد می‌تواند اثر مخربی بر روی عملکرد نهایی مورد انتظار از زیرساخت کلید عمومی داشته باشد، به‌نحوی‌که 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 عبارت‌اند 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.

۲ روال آزمون

فرآیند آزمون از مرحله درخواست ارزیابی محصول تا ارائه گزارش آن مطابق با سند راهنمای درخواست آزمون نرم‌افزارهای زیرساخت کلید عمومی منتشرشده در وب‌سایت مرکز دولتی ریشه صورت می‌پذیرد.

مشخصات کلی ارائه‌شده در جدول نتایج، به شرح زیر می‌باشد:

- **کد محصول**: شماره پرونده‌ای است که پس از ارسال تقاضای ارزیابی از جانب متقاضی، مرکز دولتی ریشه به محصول مورد ارزیابی تخصیص می‌دهد.
- **مالک محصول/متقاضی ارزیابی**: شرکت یا سازمان تولیدکننده / واردکننده و یا شرکت یا سازمانی که قصد استفاده از محصول را دارد، می‌باشد.
- **نام تجاری محصول**: نام تجاری محصول که از جانب متقاضی ارزیابی، عنوان می‌گردد.
- **محیط آزمون** (فقط در جدول نتایج نرم‌افزارهای **PKE** و **PKE SDK**): مشخص‌کننده سیستم‌عامل یا پلتفرمی است که بنا به اظهار متقاضی، محصول در آن عملیاتی شده و مورد آزمون قرارگرفته است.
- **تکنولوژی مورد آزمون** (فقط در جدول نتایج نرم‌افزارهای **PKE** و **PKE SDK**): مشخص‌کننده تکنولوژی و شیوه‌ای است که بنا به اظهار متقاضی، محصول با آن پیاده‌سازی شده است.
- **محدوده گواهی اعطاء شده**: سرویس‌ها یا قابلیت‌های یک محصول که در آزمایشگاه مورد ارزیابی قرارگرفته است.

توجه: عملکرد نرم‌افزار در هر یک از محیط‌های عملیاتی مورداداعای متقاضی به‌طور جداگانه ارزیابی می‌گردد.

۳ 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 به‌طورمعمول در مراکز صدور گواهی الکترونیکی مورداستفاده قرار می‌گیرد و دارای مؤلفه‌های مختلف شامل موارد ذیل می‌باشد:

۱. CA: جهت صدور و مدیریت گواهی الکترونیکی و انتشار آن؛
۲. RA: جهت مدیریت درخواست گواهی الکترونیکی؛
۳. 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.
۴. 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 موردقبول ارائه‌شده است.

جدول ۱ -گزارش ارزیابی سامانه‌های صدور و مدیریت گواهی الکترونیکی

ردیف	کد محصول	مالک محصول/ متقاضی ارزیابی	نام تجاری محصول	مرتبه آزمون	محیط عملیاتی	نتیجه آزمون				
							نام مؤلفه			
							مدیریت گواهی الکترونیکی (CA)	مدیریت ثبت‌نام (RA)	سرویس OCSP	سرویس TSA
۱	CA-10001-01	شرکت امن‌افزارگستر شریف	ParsSign	اول	Linux/ Windows	سطح اطمینان	طلا (۳)	طلا (۳)	نقره (۲)	–
						نسخه محصول	R9006 B21	R9006 B8	R9006 B4	–
۲	CA-10005-03	شرکت پندارکوشک ایمن	PKA	سوم	Windows	سطح اطمینان	نقره (۲)	–	طلا (۳)	–
						نسخه محصول	4.0.3	–	4.0.3	–
۳	CA-10010-02	شرکت امن‌افزارگستر شریف	ParsTrust	دوم	Linux/ Windows	سطح اطمینان	طلا (۳)	طلا (۳)	پلاتین (۴)	طلا (۳)
						نسخه محصول	R9212 B14	R9212 B5	R9212 B9	R9221 B2
۴	CA-10012-02	شرکت فاوانفت صباکیش	Mega CA	دوم	Linux/ Windows	سطح اطمینان	طلا (۳)	طلا (۳)	طلا (۳)	-
						نسخه محصول	1.3.1	1.3.1	1.3.1	–
۵	CA-10006-02	شرکت ره‌آورد سامانه‌های امن	Express CA	سوم	Windows	سطح اطمینان	نقره (۲)	نقره (۲)	–	–
						نسخه محصول	Express CA 1.0	Express RA 1.0	–	–
۶	CA-10003-02	شرکت سبا پردازش	Avanoc-CA	دوم	Windows	سطح اطمینان	نقره (۲)	برنز (۱)	طلا (۳)	
						نسخه محصول	5.2	5.2	5.2	

۴ گزارش ارزیابی ابزارهای توسعه نرم‌افزارهای PKE (PKE SDK)

سامانه‌های نرم‌افزاری نظیر سیستم‌های اتوماسیون (اداری، مالی، بانکی و ...) جهت به‌کارگیری قابلیت‌های مختلف زیرساخت کلید عمومی از طریق گواهی‌های الکترونیکی X509، نیازمند ابزارهای توسعه نرم‌افزاری[1] هستند. به فرآیند تجهیز نرم‌افزارهای مختلف به قابلیت کار با زیرساخت کلید عمومی اصطلاحاً PK-Enabling و به یک نرم‌افزار مجهز شده به این قابلیت‌ها، نرم‌افزار PKE[2] گفته می‌شود. همچنین ابزارهای توسعه نرم‌افزارهای PKE که معمولاً به‌صورت توابع کتابخانه‌ای در اختیار توسعه‌دهندگان قرار می‌گیرد را اصطلاحاً PKE SDK می‌نامیم. برای انتخاب یک PKE SDK مناسب باید به فاکتورهایی همچون محیط توسعه نرم‌افزار، تکنولوژی مورداستفاده برای توسعه نرم‌افزار و سطح اطمینان گواهی‌های مورداستفاده توجه کرد.

PKE SDK، با برخورداری از توابع و ماژول‌های برنامه‌نویسی آماده، فرایند توسعه محصول را برای برنامه‌نویسانی که با مباحث تخصصی زیرساخت کلید عمومی آشنایی ندارند، ساده می‌کند؛ زیرا برنامه‌نویس فارغ از دغدغه‌های پیاده سازی همه جزئیات استانداردهای زیر ساخت کلید عمومی، صرفاً با فراخوانی توابع آماده به توسعه و تجهیز نرم‌افزار خود می‌پردازد.

برنامه‌های کاربردی PKE که با کمک یک PKE SDK به قابلیت کار با گواهی‌های الکترونیکی مجهز می‌شوند، درنهایت بایستی برای اطمینان از صحت عملکرد، در آزمایشگاه‌های ارزیابی نرم‌افزارهای مجهز به زیرساخت کلید عمومی کنترل شوند؛ زیرا ممکن است توسعه‌دهندگان نرم‌افزار علیرغم استفاده از یک ابزار توسعه‌ای استاندارد، در به‌کارگیری توابع و ماژول‌های آماده دچار خطا شوند و نرم‌افزار نهایی عملکرد درستی نداشته باشد؛ هرچند استفاده از ابزارهای توسعه‌ای استاندارد تأثیر قابل‌ملاحظه‌ای در تسریع فرایند توسعه نرم‌افزار و کاهش پیچیدگی‌ها و خطاهای برنامه‌نویسی خواهد داشت.

لازم به ذکر است که ارزیابی نرم‌افزارهای PKE و ابزارهای توسعه این نرم‌افزارها بر اساس استاندارد «الزامات برنامه‌های کاربردی مجهز به زیرساخت کلید عمومی ایران» صورت می‌پذیرد.

در ارزیابی ابزارهای SDK ارائه‌شده به آزمایشگاه دو دسته شاخص مورد توجه‌اند:

۱- الزامات پایه‌ای که جزء الزامات حیاتی هر PKE SDK به شمار می‌روند.

---

[1] Software Development Kit (SDK)

[2] Public Key Enabled Application

۲- قابلیت‌های جانبی محصـــول که بنا به خوداظهاری متقاضـــی آزمون، مطابق اســـتانداردهای ملی پیاده سازی و عملیاتی شده ا ست. پیاده سازی این قابلیت‌های در صورت ادعای متقا ضی مبنی بر پیاده‌سازی، بایستی صحت عملکرد آن‌ها مورد آزمون قرار گیرد.

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

الزامات پایه‌ای PKE SDK	
قابلیت	**توضیح**
کار با پودمان رمزنگاشتی	امکان برقراری ارتباط و به‌کارگیری پودمان رمزنگاشـــتی مطابق با اســـتاندارد «الزامات پودمان‌های رمزنگاشتی در زیرساخت کلید عمومی»
مدیریت خطا	امکان کنترل و رسیدگی و عکس‌العمل مناسب در مقابل کلیه خطاها
مدیریت کلید	امکان پشـــتیبانی از کلیدهای رمزنگاشـــتی با طول مجاز و پارامترها، مطابق با ســـیاســـت‌های گواهی الکترونیکی کشور
مدیریت گواهی و لیست ابطال	توانایی استخراج و پردازش انواع فیلدها و الحاقیه‌های گواهی و لیست‌های ابطال
رمزنگاری نامتقارن	پیاده‌ســازی حداقل یک الگوریتم رمزنگاری مورد تائید در زیرســاخت کلید عمومی کشــور در هریک از حوزه‌های الگوریتم‌های نامتقارن، توابع درهم‌ساز و مولدهای اعداد تصادفی
تعامل‌پذیری	مطابقت ســـاختارهای رمزنگاری مطابق با اســـتاندارد «الزامات ســـاختار نحوی پیام‌های رمزنگاری در زیرساخت کلید عمومی کشور»
تشکیل و اعتبارسنجی مسیر گواهی	اجرای فرآیند تشکیل و اعتبار سنجی زنجیره گواهی مطابق با استاندارد ملی «تشکیل و اعتبار سنجی مسیر گواهی دیجیتالی»

قابلیت‌های جانبی PKE SDK	
قابلیت	**توضیح**
احراز هویت	پیاده‌سازی سازوکار احراز هویت مبتنی بر رمزنگاری کلید عمومی منطبق با استاندارد ملی «الزامات پروتکل احراز هویت در زیرساخت کلید عمومی ایران»
رمزنگاری متقارن	پیاده‌سازی حداقل یک الگوریتم رمزنگاری متقارن مورد تائید در زیرساخت کلید عمومی کشور
ارتباط با سرویس‌دهنده دایرکتوری	امکان ارتباط با سرویس‌دهنده‌های دایرکتوری و درخواست واکشی گواهی و لیست ابطال
اعتبارسنجی برخط گواهی	امکان ارتباط با سرویس‌دهنده‌های پاسخگوی OCSP و درخواست اعتبارسنجی گواهی

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

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	پشتیبانی از سطح اطمینان				محدوده گواهی اعطاء شده								
							برنز (۱)	نقره (۲)	طلا (۳)	پلاتین (۴)	الزامات پایه‌ای						سایر قابلیت‌ها		
											کار با پودمان رمزنگاشتی	مدیریت خطا	مدیریت کلید	مدیریت گواهی و لیست ابطال	رمزنگاری نامتقارن	تعامل‌پذیری	تشکیل و اعتبارسنجی مسیر گواهی	احراز هویت	رمزنگاری متقارن	ارتباط با سرویس‌دهنده دایرکتوری	اعتبارسنجی برخط گواهی	الصاق مهر زمانی	درخواست گواهی
۱	SDK-10001-02	شرکت ره‌آورد سامانه‌های امن	Power PKI SDK	Windows	ActiveX	1.0.0.0	✓	✓	–	–	✓	✓	✓	✓	✓	✓	✓	–	–	–	–	–	–
۲	SDK-10002-03	شرکت امن‌افزار 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				محدوده گواهی اعطاء شده									
							برنز (۱)	نقره (۲)	طلا (۳)	پلاتین (۴)	الزامات پایه‌ای						سایر قابلیت‌ها			
											کار با پودمان رمزنگاشتی	مدیریت خطا	مدیریت کلید	مدیریت گواهی و لیست ابطال	رمزنگاری نامتقارن	تعامل‌پذیری	تشکیل و اعتبارسنجی مسیر	احراز هویت	رمزنگاری متقارن	ارتباط با سرویس‌دهنده	اعتبارسنجی برخط گواهی	الصاق مهر زمانی	درخواست گواهی
۳	SDK-10003-02	شرکت پندار کوشک ایمن	دستینه	Windows	.NET	2.0.0.3	✓	✓	–	–	✓	✓	✓	✓	✓	✓	✓	✓	–	✓	✓	✓

جدول ۲ – گزارش ارزیابی ابزارهای توسعه نرم‌افزارهای PKE (PKE SDK)

۵ 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 استانداردی 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 PKE[1] 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 الکترونیکیِ 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 ازاین‌دست را به دنبال دارد.

در جدول ۳ لیست نرم‌افزارهای کاربردی که موفق به اخذ تأییدیه آزمایشگاه مرکز دولتی صدور گواهی الکترونیکی ریشه شده‌اند قابل‌مشاهده است.

[1] Public Key Enabled Application

جدول ۳ - 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 (۱)	نقره (۲)	طلا (۳)	پلاتین (۴)	امضای دیجیتال	احراز هویت دو عامله
۱	PKE-10011-02	شرکت همکاران‌سیستم	اتوماسیون اداری تحت	Windows / Linux	8	✓	✓	-	-	✓	✓