بسم الله الرحمن الرحیم

راهنمای بسته نرم‌افزاری

توکن امنیتی سخت افزاری

گونه ۱،۰

شرکت مهندسی ارتباطی

پیام پرداز

پیشران اطلاعات و ارتباطات امن

آبان ماه ۱۳۹۰

شرکت مهندسی ارتباطی
پیام پرداز
پیشران اطلاعات و ارتباطات امن

فـــــهرســـت

۱ – مروری بر ماژول کیا

۱-۱ مقدمه

کیا (*KeyA*)، به عنوان یک ماژول امنیت سخت‌افزاری، ابزاری جهت تأمین امنیت در کاربردهای متنوع رایانه‌ای است. این محصول با ابعادی کوچک و قابل حمل، به درگاه *USB* رایانه متصل می‌شود و می‌تواند انواع سرویس‌های امنیتی محرمانگی، صحت و احراز اصالت را ارائه نماید. برنامه‌نویسان با به کارگیری ابزارهای ارائه شده در محیطهای مختلف، می‌توانند سرویس‌های متنوعی همچون ذخیره‌سازی امن اطلاعات حساس، احراز اصالت هویت کاربران، قفل‌گذاری محصولات نرم‌افزاری، رمزنگاری داده‌ها، امن‌سازی برنامه‌های کاربردی تحت وب و ... را در شبکه‌های رایانه‌ای محلی (*LAN*) و گسترده (*WAN*) پیاده‌سازی نمایند.

در گونه ۲ ماژول **کیا**، قابلیت‌های سخت‌افزاری و نرم‌افزاری ماژول نسبت به گونه ۱ افزایش یافته و امکان استفاده از ماژول به صورت یک توکن امن[1] فراهم شده است. گونه ۳ ماژول **کیا** با طراحی کاملاً جدید و با استفاده از یک پردازنده به‌مراتب قوی‌تر از گونه ۲ در شرکت پیام‌پرداز تولید شده است. گونه جدید نه تنها به عنوان یک توکن تمام‌عیار با قابلیت‌های بسیار وسیع‌تر از گونه ۲، بلکه به عنوان یک کارت هوشمند نیز قابل استفاده است. در قلمرو توکن، **کیای** گونه ۳ الگوریتم‌های رمز متقارن متعددی را در مقایسه با کیا ۲ ارائه می‌کند. الگوریتم‌های رمزنگاری *AES* در سه طول بلوک ۱۲۸، ۱۹۲ و ۲۵۶ بیتی، *DES*، *3DES* و *PAYA2* (الگوریتم رمز اختصاصی شرکت) الگوریتم‌های پشتیبانی شده در **کیای** گونه ۳ هستند. در زمینه الگوریتم‌های چکیده‌گیری[2] نیز الگوریتم‌های *SHA1*، *MD5*، *CRC32* و *HMAC* در ماژول تعبیه شده‌اند. تحول بزرگ دیگر در زمینه الگوریتم‌های رمز ماژول **کیا** در این گونه جدید پشتیبانی ماژول از

[1] *Secure Token*
[2] *Hash & Checksum algorithms*

الگوریتم‌های رمز نامتقارن در سطح سخت‌افزار است. **کیای** گونه ۳ قابلیت انجام عملیات رمز و امضای دیجیتال با الگوریتم *RSA* در اندازه‌های ۵۱۲، ۱۰۲۴، ۲۰۴۸ و ۴۰۹۶ بیت را دارد. علاوه بر این، شرکت قابلیت ارائه این ماژول با الگوریتم‌های اختصاصی مورد درخواست مشتریان در هر سه حوزه الگوریتم‌های رمز متقارن، نامتقارن و چکیده‌گیری را دارد. قابلیت جدید دیگر در **کیای** گونه ۳ سیستم مدیریت حافظه مبتنی بر سیستم فایل آن است. در مدل کارت هوشمند **کیای** گونه ۳ کاربر امکان استفاده از یک سیستم‌فایل کامل کارت هوشمند مبتنی بر استانداردهای جهانی کارت هوشمند را دارد. همچنین سیستم کنترل دسترسی تعبیه شده ضامن حفاظت از داده‌های خصوصی کاربران خواهد بود. علاوه بر قابلیت‌های افزوده شده در هسته ماژول **کیا** در گونه ۳، سعی شده تا با یک بررسی کامل بر روی **کیای** گونه ۲ و مقایسه آن با توکن‌های مطرح در جهان و همچنین ملاحظه و درنظرگرفتن نیازمندی‌های کاربران داخلی روال‌های امنیتی معیوب، اشکال‌دار یا ناصحیح موجود در گونه ۲ به طور کامل اصلاح شوند.

۱-۲ محتویات بسته نرم‌افزاری

سی‌دی ابزارهای برنامه‌نویسی **کیا** با عنوان *KeyA software Developers Kit* یا اصطلاحاً *KDK* حاوی ابزارهایی است که به صورت یک بسته نرم‌افزاری در اختیار شما قرار داده شده است. سی‌دی *KDK* شامل ابزارهای کار با ماژول در محیط‌های مبتنی بر *PKI* (شاخه *PKI*)، ابزارهای مدیریت ماژول (شاخه *Tools*)، کتابخانه توابع(شاخه *Library*) و مثال‌های برنامه‌نویسی(شاخه *Sample*) و دموی نرم‌افزاری محصول(شاخه *Demo*) می‌باشد.

کیا دارای کتابخانه‌ای نرم‌افزاری برای استفاده در برنامه‌هایی است که به یکی از زبان‌های *C*، *C++* و *C#* تهیه شده‌اند.

سی‌دی *KDK* همچنین شامل نرم‌افزاری به نام *KeyA3Initializer* است که می‌توان آن را از شاخه *Tools\Token Initializer* نصب کرد. نرم‌افزار *KeyA3Initializer* برای پروگرام کردن ماژول‌های **کیا** تهیه شده است. راهنمای استفاده از این نرم‌افزار نیز در شاخه مزبور موجود می‌باشد.

در شاخه *Demo*، یک نرم‌افزار با عنوان *KeyA3Demo* قرار دارد که کلیه قابلیت‌های کتابخانه اختصاصی ماژول در آن قابل مشاهده است.

سی‌دی *KDK* شامل نرم‌افزاری به نام *KeyA3 – Certificate Manager* است که می‌توان آن را از شاخه *PKI\Certificate Manager* نصب کرد. با استفاده از این نرم‌افزار و راهنمای استفاده از آن که در شاخه مزبور موجود است می‌توان در ابزارهای مبتنی بر *PKI* با کیا۳ ارتباط برقرار نموده و از آن استفاده نمود.