بسم الله الرحمن الرحیم

راهنمای استفاده از

توکن امنیتی کیا ۳

در نرم‌افزارهای مبتنی بر *PKI*

گونه ۱.۰

شرکت مهندسی پیام‌پرداز

آبان ماه ۱۳۹۱

فـــــهرســـت

۱ مقدمه

پست الکترونیک یا *Email* یکی از همگانی‌ترین سرویس‌های اینترنت محسوب می‌شود. افراد با بهره‌گیری از این سرویس قادرند در ظرف مدت بسیار کوتاهی، نامه‌های الکترونیک خود را با هزینه کم به دورترین نقاط جهان ارسال نمایند. نامه‌های الکترونیک در طی مسیر خود از مبدأ تا مقصد و نیز در زمانی که بر روی سرویس‌دهنده ذخیره می‌شوند، به راحتی قابل مشاهده، تغییر، حذف و یا حتی جعل می‌باشند. همچنین در اکثر سرویس‌دهنده‌های *Email* برای کنترل دسترسی کاربر جهت ورود به صندوق نامه و خواندن پیام‌های رسیده یا ارسال پیام، از نام و کلمه عبور استفاده می‌شود. بنابراین در صورتی که شخص دیگری از نام و کلمه عبور کاربر اطلاع داشته باشد، می‌تواند وارد صندوق نامه کاربر شده و پیام‌های دریافتی را مشاهده کند و یا از طرف او پیامی را برای دیگران ارسال کند.

برای مقابله با چنین تهدیداتی در سرویس *Email* از ساختار رمزنگاری کلید عمومی[1] (*PKI*) استفاده می‌شود. این ساختار به وسیله اکثر نرم‌افزارهای سرویس‌گیرنده پست الکترونیک[2] همچون *Netscape*، *Mozilla Thunderbird* و *Microsoft Outlook* پشتیبانی می‌شود. روش انجام کار بدین ترتیب است که فرستنده، ابتدا نامه الکترونیک ارسالی را با استفاده از کلید عمومی گیرنده رمز نموده و سپس با استفاده از کلید خصوصی خود امضای دیجیتال می‌کند. در طرف مقابل گیرنده با استفاده از کلید عمومی

[1] *Public Key Infrastructure*
[2] *Email Client*

فرستنده، صحت امضای دیجیتال را بررسی نموده و پس از تأیید هویت فرستنده، متن نامه را با استفاده از کلید خصوصی خود رمزگشایی می‌نماید. بدین ترتیب محرمانگی و صحت پیام‌های *Email* تأمین خواهد شد.

در این معماری، کلید عمومی هر شخص بایستی به تأیید یک مرجع معتمد به نام مرکز صدور گواهی (*CA*)[1] رسیده و به صورت یک گواهی دیجیتال در اختیار همگان قرار گیرد. همچنین کلید خصوصی فرد بایستی به صورت کاملاً امن و حفاظت شده نگهداری گردد. معمولاً افراد کلیدهای خصوصی را بر روی هارد سیستم خود ذخیره می‌نمایند که از لحاظ امنیتی خطرات زیادی همچون سرقت وسوء استفاده را به دنبال دارد. یک روش مناسب‌تر برای ذخیره‌سازی امن کلیدهای خصوصی، استفاده از توکن‌های امن[2] است. نرم‌افزارهایی مانند *Netscape* و *Mozilla Thunderbird* با حمایت از استانداردی به نام *PKCS#11*[3] امکان کار با توکن‌های امن را فراهم می‌آورند. در نرم‌افزار *Outlook*، استاندارد میکروسافت به نام *CSP*[4] امکان استفاده از توکن‌های امن را فراهم می‌آورد.

استانداردهای *PKCS#11* و *CSP* به منظور پیاده‌سازی امکانات *PKI* در مرورگرها (نظیر *Mozilla Firefox* و *IE*) جهت استفاده از *SSL*[5] دو طرفه نیز به کار می‌رود.

ماژول امنیتی کیا گونه ۳، یک نمونه از توکن‌های امن است که با استفاده از پروتکل‌های امنیتی قوی، قابلیت‌های مناسبی را در عملیات رمزنگاری و ذخیره امن داده‌های حساس ایجاد می‌کند. ماژول کیا با پشتیبانی از استاندارد *PKCS#11* می‌تواند به راحتی در نرم‌افزارهای متداول ارسال و دریافت *Email* و یا مرورگرها به کار گرفته شود و از کلید خصوصی فرد به خوبی محافظت نماید. ماژول کیا همچنین امکان ذخیره‌سازی چند کلید خصوصی به طور همزمان را دارا می‌باشد، بنابراین در صورتی که کاربر دارای صندوق نامه‌های متفاوتی باشد کلید خصوصی تمامی آنها را می‌تواند در یک ماژول کیا ذخیره کرده و همراه خود داشته باشد.

---

[1] *Certificate Authority*
[2] *Secure Token*
[3] *Public Key Cryptographic System*
[4] *Cryptographic Service Provider*
[5] *Secure Socket Layer*

بسته نرم‌افزاری *Certificate Manager* ماژول کیا۳ جهت ارایه امکانات *PKI* این ماژول عرضه شده است. این بسته شامل برنامه *KeyA3 Certificate Manager* و کتابخانه مربوط به استاندارد *PKCS#11* می‌باشد. برنامه *KeyA3 Certificate Manager* به منظور مدیریت گواهی‌ها و کلیدهای خصوصی و عمومی ذخیره شده بر روی ماژول کیا به کار می‌رود. با استفاده از این نرم‌افزارمی‌توان گواهی‌ها را با استفاده از فایل‌های *p12* و *pfx* مطابق با استاندارد *PKCS#12*[1] و یا فایل‌های *cer*. در حافظه کیا نوشت.

در این راهنما ابتدا با امکانات نرم‌افزار *KeyA3 Certificate Manager* آشنا می‌شویم. پس از آن به نحوه به کارگیری ماژول کیا برای امن‌سازی سرویس *Email* در برنامه *Mozilla Thunderbird* می‌پردازیم. سپس نحوه اتصال به یک سایت *SSL* با استفاده از *Mozilla Firefox* را توضیح خواهیم داد.

۲ تعاریف و اصطلاحات برنامه

در این بخش به معرفی کلمات و اصطلاحات استفاده شده در این راهنما می‌پردازیم.

- **مرکز گواهی:** ساختار *PKI* استفاده از تعدادی طرف سوم مورد اعتماد را برای امن کردن مبادلات بین فرستنده و گیرنده پیشنهاد می‌کند. این مراکز مورد اطمینان، به نام مراکز گواهی هویت شناخته می‌شوند و وظیفه اصلی آنها صدور و نگهداری گواهی‌های الکترونیکی برای کاربران است. وظایف دیگر مرکز گواهی، مدیریت وضعیت گواهی‌ها و انتشار لیست گواهی‌های باطل شده است.
- **گواهی:** گواهی یک سند الکترونیکی امضا شده است که توسط مرکز گواهی برای یک شخص، کامپیوتر یا نرم‌افزار صادر می‌شود و از اطلاعات درون آن می‌توان برای شناسایی دارنده گواهی و نیز کلید عمومی وی جهت برقراری ارتباط امن استفاده کرد.گواهی، قابل جعل نمی‌باشد، یعنی دارنده گواهی، کلید

[1] *Personal Information Exchange Syntax*

خصوصی متناظر با آن را در اختیار دارد. علت این امر امضا مرکز گواهی است که تولید آن بدون دسترسی به کلید خصوصی مرکز، غیر ممکن است. گواهی یک سند عمومی است که می‌توان آن را به همه نشان داد.

- **کلید خصوصی:** متناظر با کلید عمومی موجود در هر گواهی، داده یکتایی به نام کلید خصوصی وجود دارد. کلید خصوصی کاملاً محرمانه است و نباید در اختیار دیگران قرار گیرد. پیام‌هایی که با کلید عمومی موجود در یک گواهی رمز شده‌اند، تنها با کلید خصوصی مربوط به همان گواهی قابل رمزگشایی هستند و بالعکس.

User PIN[1]: شناسه شخصی مربوط به فعال کردن یک ماژول کیاست که حداکثر ۳۲ کاراکتر می‌باشد. به طور پیش‌فرض *PINUser* ماژول‌های کیا کلمه *usr1* می‌باشد. البته به لحاظ مسایل امنیتی اکیداً توصیه می‌شود مقدار پیش‌فرض در ابتدای کار توسط کاربر تغییر یابد.

- ***SO PIN***: هر ماژول کیا غیر از شناسه شخصی عادی یا *User PIN*، دارای یک ***SO****PIN* (به طول حداکثر ۳۲ کاراکتر) نیز هست. توصیه می‌شود ***SO****PIN* تنها در اختیار مدیر باشد. به طور پیش‌فرض ***SO****PIN* ماژول کیا، کلمه *keya3* می‌باشد. به لحاظ مسایل امنیتی اکیداً توصیه می‌شود این مقدار پیش‌فرض نیز در ابتدای کار تغییر داده شود.

۳ عملیات نرم‌افزار *KeyA3 Certificate Manager*

با اجرای نرم‌افزار *KeyA3 Certificate Manager*، پنجره اصلی برنامه مطابق شکل ۱ بر روی صفحه نمایش ظاهر می‌شود.

۳-۱ کار با ماژول کیا

در این قسمت دستورات و عملیات مرتبط با ماژول کیا در برنامه *KeyA3 Certificate Manager* ارایه می‌شود.

[1] *Personal Identity Number*

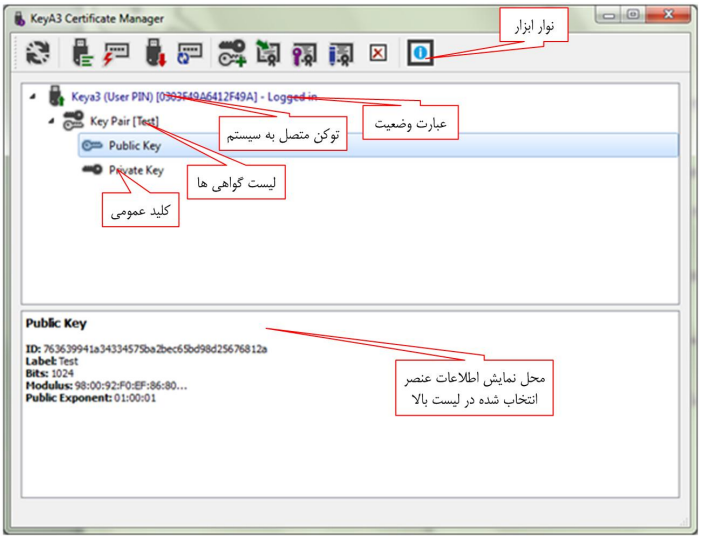
۳-۱-۱ ورود به ماژول کیا

برای کار با ماژول کیا در برنامه *KeyA3 Certificate Manager*، بایستی ابتدا بـه آن *Login* نمود. بدین منظور مراحل زیر را دنبال کنید:

۱- ماژول کیا را به پورت *USB* متصل نمایید. در صورتی که توکن توسط برنامه به درستی شناسایی شده باشد، کلمه *logged out* در عبارت وضعیت ظاهر می‌شود. چنانچـه عبارت وضعیت برابر *uninitialized* باشد می‌بایست مطابق بخش ۳-۲-۱ و بخش۳-۲-۲ به فرمت کردن ماژول و *User PIN* اقدام نمایید.

۲- دکمه *Login* را فشار دهید.

۳- در پنجره ظاهر شده *PIN* ماژول را وارد کنید. در صـورت موفقیـت‌آمیـز بـودن ورود، عبارت وضعیت به *logged in* تغییر می‌کند.



شکل ۱: پنجره اصلی برنامه KeyA3 Certificate Manager

هشدار: کاربران بایستی دقت داشته باشند که ده بار اشتباه وارد کردن متوالی *User PIN* باعث از بین رفتن *PINUser* می‌شود.

تذکر: این گونه از برنامه *KeyA3 Certificate Manager* تنهـا از یـک مـاژول کیـا

پشتیبانی می‌کند. بنابراین برای عملکرد صحیح، در هنگام استفاده فقط یک ماژول کیا را به پورت *USB* متصل نمایید.

۳-۱-۲ خروج از ماژول کیا۳

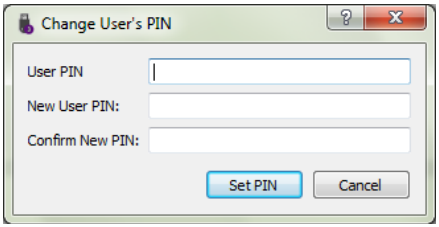
توصیه می‌شود در پایان کار با ماژول آن را از وضعیت احراز اصالت شده خارج نمایید. برای این کار باید چنانچه قبلاً جهت کار با ماژول به آن *Login* نموده‌اید، دکمه *Logout* را فشاردهید. در صورتی که خروج با موفقیت انجام شود، عبارت وضعیت به *logged out* تغییر می‌کند.

۳-۱-۳ تغییر *PINUser* ماژول کیا توسط کاربر

برای تغییر *User PIN* ماژول کیا مراحل زیر را دنبال کنید:

۱- دکمه *Change the user's PIN* را فشار دهید.

۲- در پنجره ظاهر شده (شکل ۲)، *PIN User* فعلی، *PINUser* جدید و تأیید *PINUser* جدید را وارد کنید.



شکل ۲: پنجره تغییر User PIN

هشدار: توصیه اکید می‌شود مقادیر پیش‌فرض *PINUser* و *SO PIN* ماژول کیا تعویض گردیده و رشته‌های تصادفی به جای آنها انتخاب شود (به بخش‌های بعد مراجعه کنید). در غیر این صورت یک فرد غیر مجاز می‌تواند با دسترسی به کیای کاربر، *User PIN* یا *SO PIN* را حدس زده و به کلید خصوصی کاربر دسترسی پیدا کند. به عنوان مثال *Email*های رمز شده کاربر را خوانده و یا به جای او *Email*ها را امضا نماید.

۳-۱-۴ تغییر *PINSO* ماژول کیا

برای تغییر *SO PIN* ماژول کیا مراحل زیر را دنبال کنید:

۱- دکمه *Change SO's PIN* را فشار دهید.

۲- در پنجره ظاهر شده، *PIN SO* فعلی، *PINSO* جدید و تأیید *PINSO* جدید را وارد کنید.

۳-۲ کار با اشیای ماژول

در این قسمت عملیات مرتبط با ذخیره یا حذف گواهی‌های دیجیتال و کلیدهای خصوصی بر روی ماژول کیا بیان می‌گردد.

۳-۲-۱ فرمت کردن ماژول

برای فرمت کردن و حذف تمامی گواهی‌ها و کلیدها از روی ماژول کیا مراحل زیر را طی کنید:

۱- دکمه *Initialize Token* را فشار دهید.

۲- *PINSO* ماژول را وارد کنید.

توجه: اگر برای اولین بار قصد استفاده از یک ماژول را دارید ***حتماً*** باید آنرا با استفاده از این امکان برنامه، فرمت کنید.

۳-۲-۲ فرمت کردن *User PIN*

۱- دکمه *Initialize User PIN* را فشار دهید.

۲- *SO PIN* و *User PIN* دلخواه و تکرار *User PIN* را در قسمت‌های مربوطه وارد نمایید، و سپس دکمه *OK* را فشار دهید.

توجه۱: اگر برای اولین بار قصد استفاده از یک ماژول را دارید ***حتماً*** *User PIN* آن را با استفاده از این امکان، فرمت کنید.

هشدار: کاربران بایستی دقت داشته باشند که ده بار اشتباه وارد کردن متوالی *PINSO* باعث از بین رفتن *PINSO* می‌شود.

۳-۲-۳ ذخیره گواهی و کلید خصوصی در ماژول کیا

برنامه *KeyA3 Certificate Manager* برای وارد کردن یک جفت کلید خصوصی و گواهی دیجیتال در ماژول کیا از فایل‌هایی با پسوند *p12* یا *pfx* استفاده می‌کند. در این فایل‌ها، کلید خصوصی و گواهی شخص به همراه گواهی مرکز *CA* با روش مشخص شده در استاندارد *PKCS#12* نوشته می‌شوند.

برای ذخیره گواهی و کلید خصوصی از یک فایل *p12* یا *pfx* در حافظه ماژول، مراحل زیر را دنبال کنید:

۱- دکمه *Import a PKCS#12 file* را فشار دهید.

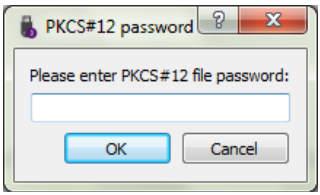
۲- در پنجره *Open*، فایل *p12* یا *pfx* مورد نظر را انتخاب نمایید.

۳- در پنجره درخواست کلمه عبور (شکل ۳)، کلمه عبور فایل *p12* یا *pfx* را وارد کنید.

۴- در صورت نیاز *PINUser* ماژول را وارد کنید (پنجره *Login* در صورتی ظاهر می‌شود که کاربر قبلاً به ماژول کیا وارد نشده باشد).

۵- با ذخیره گواهی دیجیتال و کلید خصوصی در ماژول کیا، گواهی و کلید خصوصی مربوطه در لیست گواهی‌های موجود در پنجره بالا ظاهر می‌شوند. پس از این مرحله کاربر می‌تواند با اطمینان خاطر فایل *p12* یا *pfx* موجود بر روی هارد را برای جلوگیری از تهدیدات احتمالی حذف نماید.

هشدار: کلید خصوصی ذخیره شده در ماژول کیا به دلیل ملاحظات امنیتی قابل بازیابی نیست. لذا توصیه می‌شود قبل از حذف فایل *p12* یا *pfx* از روی هارد، یک کپی از این فایل تهیه کرده و در یک محل مطمئن نگهداری کنید.



شکل ۳: پنجره درخواست کلمه عبور فایل P12

۳-۲-۴ ذخیره گواهی عمومی در ماژول کیا

برنامه *KeyA3 Certificate Manager* برای وارد کردن گواهی‌های دیجیتال عمومی در ماژول کیا از فایل‌هایی با پسوند *cer* استفاده می‌کند. در این فایل‌ها، کلید عمومی و گواهی شخص در قالب استاندارد *X509* نوشته می‌شوند.

برای ذخیره گواهی عمومی از یک فایل *cer* در حافظه ماژول، مراحل زیر را دنبال کنید:

۱- دکمه *Import a certificate to the token* را فشار دهید.

۲- در پنجره *Open*، فایل *cer* مورد نظر را انتخاب نمایید.

۳- در صورت نیاز *PINUser* ماژول را وارد کنید (پنجره *Login* در صورتی ظاهر می‌شود که کاربر قبلاً به ماژول کیا وارد نشده باشد).

۴- با ذخیره گواهی دیجیتال و کلید عمومی در ماژول کیا، گواهی و کلید عمومی مربوطه در لیست گواهی‌های موجود در پنجره بالا ظاهر می‌شوند.

۳-۲-۵ حذف گواهی یا کلید ذخیره شده

برای حذف کردن گواهی و یا کلید خصوصی یا عمومی از روی کیا مراحل زیر را دنبال کنید:

۱- گواهی و یا کلید مورد نظر را در لیست گواهی‌های موجود در توکن انتخاب کنید.

۲- دکمه *selected object Delete* را فشار دهید.

۳-۲-۶ ذخیره گواهی روی هارد

برای ذخیره یک گواهی دیجیتال به صورت فایلی با پسوند *cer* (مطابق با استاندارد *X509*) بر روی هارد یا یک رسانه دیگر مراحل زیر را دنبال کنید:

۱- در لیست گواهی‌ها، گواهی مورد نظر را انتخاب کنید.

۲- دکمه *Export selected certificate from token* را فشار دهید.

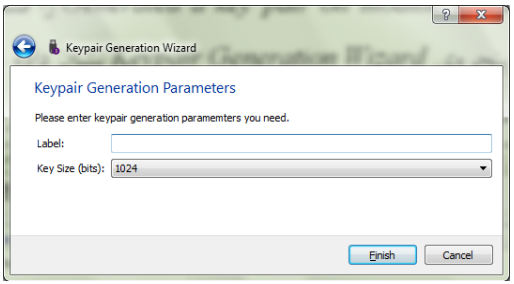
۳-۲-۷ ایجاد جفت کلید روی توکن

برای تولید جفت کلید روی ماژول مراحل زیر را دنبال کنید:

۱- دکمه *Generated a key pair on module* را فشار دهید تا پنجره *Keypair Generation Wizard* نشان داده شود.

۲- در این پنجره دکمه *Next* را فشار دهید و در پنجره *Keypair Parameters* (شکل ۴) یک *Label* دلخواه نوشته و سپس طول مورد نظر خود را در قسمت مربوطه انتخاب کنید.

۳- در صورت ایجاد شدن جفت کلید پیام موفقیت عملیات نشان داده خواهد شد.



شکل ٤: پنجره ایجاد جفت کلید

۳-۲-۸ درباره نرم افزار

اطلاعات کلی در مورد نسخه نرم افزار و تولید کننده و ... را می‌توان با فشار دادن دکمه *About* مشاهده کرد.

۳-۲-۹ بازخوانی اطلاعات نمایش داده شده در نرم‌افزار

هنگام کار با نرم‌افزار در صورتی که ماژولی را از سیستم جدا کرده و یا ماژولی را به سیستم وصل کنیم برای نمایش اطلاعات صحیح در منوی اصلی برنامه باید دکمه *Refresh the list of module* را فشار دهیم.

۳-۲-۱۰ خروج از نرم افزار

برای خروج از نرم‌افزار، دکمه*Close* را فشار دهید.

۴ نحوه استفاده از کیا برای مبادله امن *E-mail*

نرم‌افزارهایی مانند *Mozilla Thunderbird* و *Netscape* از طریق استاندارد *PKCS#11* امکان استفاده از ماژول‌ها یا توکن‌های حاوی کلید خصوصی را فراهم آورده‌اند. ماژول کیا با پشتیبانی از استاندارد *PKCS#11* از طریق کتابخانه‌ای با عنوان (*K3PKCS*) در این نرم‌افزارها قابل استفاده است.

در این بخش نحوه استفاده از کیا برای مبادله امن *E-mail* در نرم‌افزار *Thunderbird* توضیح داده می‌شود.

۴-۱ نرم‌افزار *Mozilla Thunderbird*

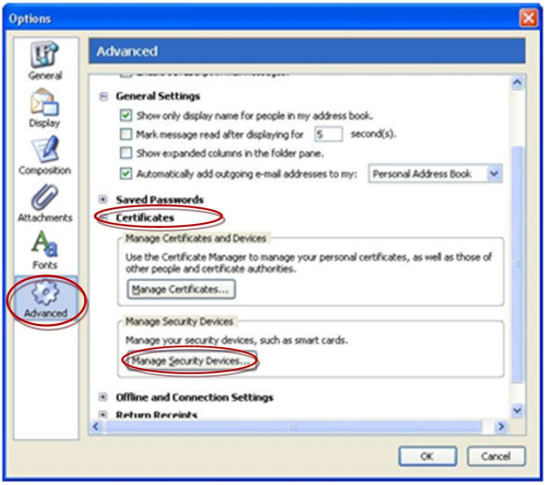
در این قسمت با نحوه نصب کتابخانه *PKCS#11* برای کیا و نحوه استفاده از کیا برای مبادله امن *E-mail* در نرم‌افزار *Mozilla Thunderbird* آشنا می‌شویم.

۴-۱-۱ معرفی *K3PKCS*

۱- در نرم‌افزار *Mozilla Thunderbird*، منوی *Tools | Options* را انتخاب کنید.

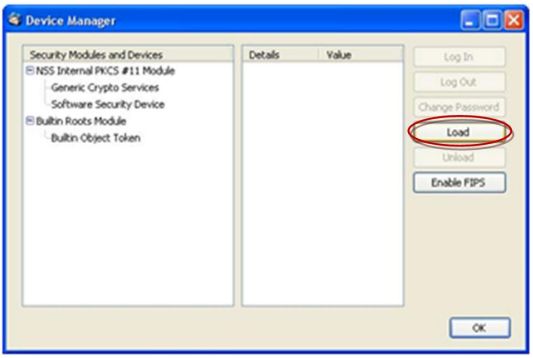
۲- از قسمت چپ پنجره *Options* (شکل ۵)، گزینه *Advanced* را انتخاب کنید.

۳- در سمت راست پنجره ظاهر شده (شکل ۵)، گزینه *Certificates* را انتخاب کرده و دکمه *Manage Security Devices* را فشار دهید. شکل ۵



شکل ۵: پنجره Options

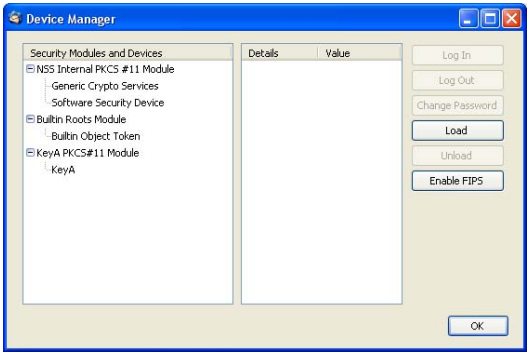
۴- در پنجره *Device Manager* (شکل ٦)، دکمه *Load* را انتخاب کنید.



شکل ٦: پنجره Device Manager

۵- در پنجره ظاهر شده نام ماژول کیا و آدرس کتابخانه آنرا وارد کنید.کتابخانه *PKCS#11*کیا، فایلی با نام*K3PKCS.dll* است که درمسیر *%system32%* (مثلاً *C:\windows\system32*) قرار دارد.

۶- در صورتی که عملیات نصب ماژول با موفقیت انجام شود در پنجره *Device Manager* نام ماژول کیا اضافه می‌شود (شکل ۷).



شکل ۷: پنجره Device Manager پس از نصب ماژول کیا

۴-۱-۲ تنظیمات

برای استفاده از نرم‌افزار *Mozilla Thunderbird* ابتدا بایستی یک اشتراک تعریف نمود. بدین منظور منوی *File | New | Account...* را انتخاب کرده و مراحل مورد نظر را طی نمایید. در طول ایجاد این اشتراک باید نام سرور *POP* و *SMTP* را وارد کنید.

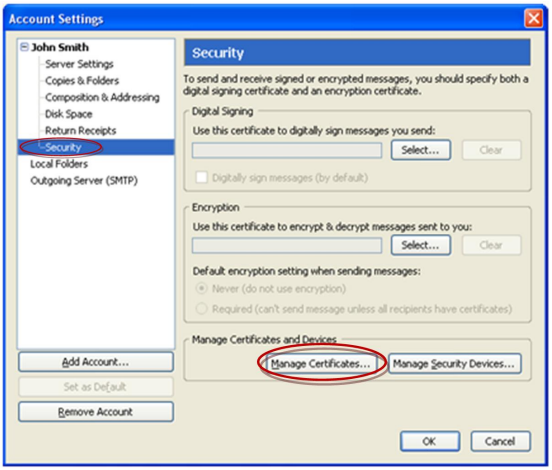
پس از ایجاد اشتراک مورد نظر، باید گواهی مرکز *CA*، گواهی خود و نیز گواهی طرف مقابل را به *Mozilla Thunderbird* معرفی کنید.

۴-۱-۲-۱ تعیین گواهی مرکز *CA*

برای معرفی گواهی مرکز *CA* به *Mozilla Thunderbird* می‌توان از فایل‌هایی با پسوند *cer* (استاندارد *X509*) استفاده کرد. برای این کار مراحل زیر را دنبال کنید:

۱- منوی *Tools | Account Settings* را انتخاب کنید و از قسمت چپ پنجره *Account Settings* (شکل ۸)، زیر نام اشتراک مورد نظر، گزینه *Security* را انتخاب کنید.

۲- در سمت راست پنجره *Account Settings* (شکل ۸)، دکمه *Manage Certificates...* را فشار دهید.



شکل ۸: پنجره Account Settings

۳- در پنجره باز شده قسمت *Authorities* را انتخاب کنید.

۴- با کلیک کردن روی دکمه *Import* فایل گواهی *CA* مورد نظر (با پسوند *cer*) را به نرم‌افزار معرفی کنید.

۵- در قسمت *Authorities* گواهی *CA* را انتخاب کرده و سپس دکمه *Edit* را انتخاب نمایید.

۶- در پنجره باز شده، گزینه *This certificate can identify mail users* را علامت بزنید.

۴-۱-۲-۲ تعیین گواهی خود

برای معرفی گواهی شامل کلید خصوصی ذخیره شده خود در ماژول کیا، به برنامه *Mozilla Thunderbird* جهت استفاده در عملیات امضا و رمزگشایی پیام‌ها، مراحل زیر را دنبال کنید:

۱- منوی *Tools | Account Settings* را انتخاب کنید و از قسمت چپ پنجره *Account Settings* (شکل ۸)، زیر نام اشتراک مورد نظر، گزینه *Security* را انتخاب کنید.

۲- برای انتخاب کلید خصوصی مورد استفاده برای امضا کردن در قسمت *Digital*

Signing دکمه *Select* را فشار دهید (شکل ۸).

۳- در صورت نیاز *PIN* ماژول کیا را وارد کنید.

۴- در صورتی که چند جفت گواهی و کلید خصوصی روی کیا یافت شود پنجره‌ای باز می‌شود که از طریق آن می‌توانید کلید مورد نظر خود را انتخاب کنید.

برای انتخاب کلید خصوصی مورد استفاده برای رمزگشایی پیام‌ها، در قسمت *Encryption* از پنجره *Account Settings* گام‌های ۳ و ۴ را اجرا کنید.

۴-۱-۲-۳ تعیین گواهی طرف مقابل

برای معرفی گواهی طرف مقابل به برنامه *Mozilla Thunderbird* جهت استفاده در عملیات رمزگذاری پیامها و اطمینان از صحت امضا، می‌توان از فایل‌هایی با پسوند *cer* (استاندارد *X509*) استفاده کرد. بدین منظور مراحل زیر را دنبال کنید:

۱- منوی *Tools* | *Account Settings* را انتخاب کنید و از قسمت چپ پنجره *Account Settings* (شکل ۸)، زیر نام اشتراک مورد نظر، گزینه *Security* را انتخاب کنید.

۲- در سمت راست پنجره *Account Settings*، دکمه *Manage Certificates...* را فشار دهید.

۳- در پنجره باز شده قسمت *Other People's* را انتخاب کنید.

۴- با کلیک کردن روی دکمه *Import*، فایل گواهی مورد نظر (با پسوند *cer*) را به نرم‌افزار معرفی کنید.

۴-۱-۳ رمزگذاری پیام

ابتدا برای ارسال یک نامه، منوی *File* | *New* | *Message* را انتخاب کنید. در پنجره *Compose* آدرس گیرنده را وارد کنید.

حال در صورتی که علاقه‌مند به رمزگذاری پیام مورد نظر هستید در پنجره *Compose*، منوی *Security* | *Options* را انتخاب کرده و سپس گزینه *Encrypt this Message* را فعال نمایید. در این صورت در گوشه پایین سمت راست پنجره *Compose* آیکون  ظاهر می‌شود.

۴-۱-۴ امضای پیام

در صورتی که علاقه‌مند به امضای پیام ارسالی هستید در پنجره *Compose*، منوی *Security* | *Options* و سپس گزینه *Digitally Sign This Message* را انتخاب کنید. در این صورت در گوشه پایین سمت راست پنجره *Compose* آیکون  ظاهر می‌شود.

۴-۱-۵ دریافت امن *E-mail*

در صورتی که کلید خصوصی خود و گواهی طرف مقابل را معرفی کرده باشید، پس از کلیک کردن روی نام نامه رسیده، در پنجره اصلی *Mozilla Thunderbird* متن نامه، رمزگشایی شده و امضای آن بررسی می‌گردد. در صورتی که این کار به درستی انجام شود در قسمت بالای پنجره اصلی که متن نامه در آن نشان داده می‌شود آیکون‌های کلید و قلم قابل رؤیت است.

۵ نحوه اتصال به سایت‌های استفاده کننده از *SSL* دوطرفه

سایت‌های وب حساسی که نیاز به ارتباط امن دارند، از تکنولوژی *SSL* استفاده می‌کنند. معمولاً ارتباط *SSL* به گونه‌ای است که فقط سرور با استفاده از گواهی خود، هویت‌ش را به کاربر اثبات می‌کند. این امر باعث می‌شود که کاربر از اصالت سایت اطمینان حاصل کرده و داده‌های حساسی مانند شماره کارت اعتباری، کلمه عبور و ... را به صورت امن در اختیار سایت قرار دهد. در بعضی موارد خود سایت نیز نیاز به تأیید اصالت کاربر دارد. در چنین مواردی از کاربر گواهی دیجیتال دریافت می‌شود. می‌توان گواهی را با استفاده از توکن‌های امن مانند کیا ذخیره کرد و با استفاده از مرورگرها این گواهی را برای سایت ارسال نمود.

۵-۱ تنظیمات *Mozilla Firefox* برای استفاده از *SSL*

مشابه بخش ۴-۱-۱، *K3PKCS* را به *Mozilla Firefox* معرفی می‌کنیم. هنگام وصل شدن به سایت، اگر گواهی سایت معتبر و مورد قبول ما باشد آنگاه با وارد کردن *PIN* در پنجره مربوطه و انتخاب گواهی به سایت مورد نظر دسترسی پیدا می‌کنیم. برای

درج گواهی سایت از فرایندی شبیه ۴-۱-۲-۱ استفاده می‌شود با این تفاوت که به جای درج گواهی در قسمت *Authorities*، آنرا در قسمت *Servers* اضافه می‌کنیم. واضح است که گواهی مرکز *CA* هم در مورد گواهی سایت و هم در مورد گواهی کاربر باید در قسمت *Authorities* وارد شده باشد.

۶ امضای دیجیتال فایل‌های *PDF* در نرم‌افزار *Adobe Acrobat*

برای تایید هویت ایجاد کننده فایل‌های*PDF*، می‌توان از مکانیزم امضای دیجیتال استفاده کرد. در این روش فرستنده با استفاده از کلید خصوصی خود، فایل مورد نظر را امضای دیجیتال می‌کند. در طرف مقابل، گیرنده با استفاده از گواهی مرکز *CA* و کلید عمومی فرستنده (که در فایل *PDF* ضمیمه شده است)، صحت امضای دیجیتال را بررسی نموده و صحت فایل تأمین خواهد شد.

در این نوشتار با نحوه استفاده از گواهی موجود در ماژول کیای گونه ۳ برای امضا کردن فایل‌ها در نرم‌افزار *Adobe Acrobat 9 Pro Extended* آشنا می‌شویم.

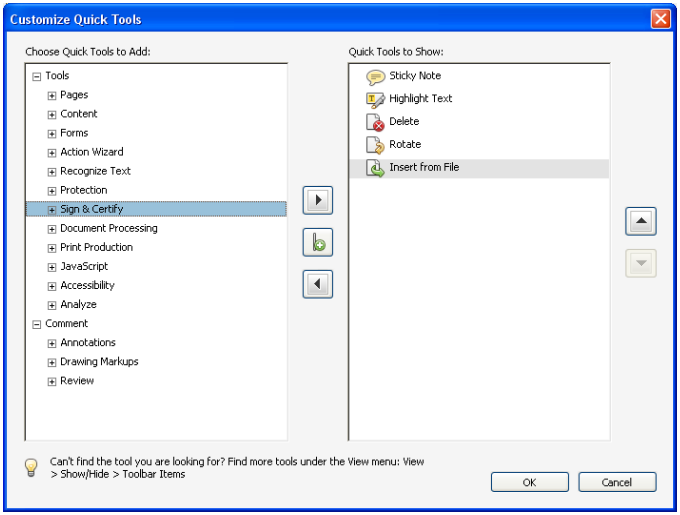
مراحل اصلی کار عبارتند از:

- صدور گواهی برای فرستنده توسط یک مرکز *CA*
- نصب بسته *PKI* کیا در سمت فرستنده
- معرفی کتابخانه *PKCS#11* کیا در برنامه *Adobe Acrobat* در سمت فرستنده
- امضای فایل *PDF* توسط فرستنده
- نصب گواهی مرکز *CA* به عنوان گواهی مورد اعتماد در سیستم‌عامل گیرنده
- وارسی امضا توسط گیرنده

در ادامه برخی از این مراحل تشریح می‌شود.

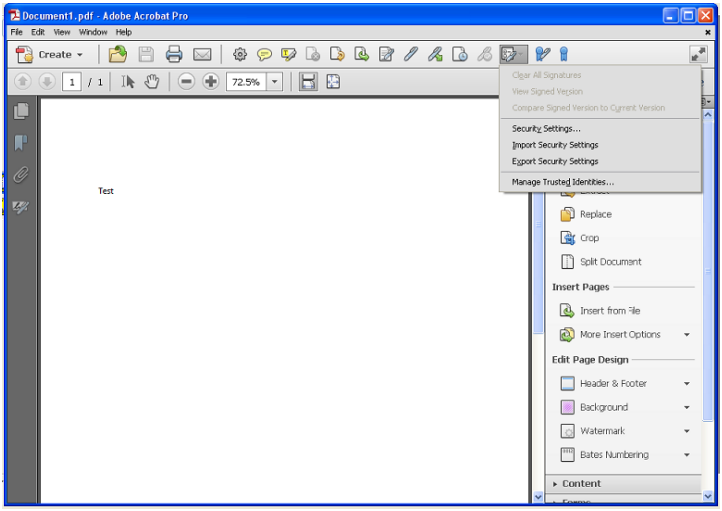
۶-۱ معرفی کتابخانه *K3PKCS*

۱- در نرم‌افزار*Adobe Acrobat ProAdobe Acrobat 10* ، آیکون ⚙ را انتخاب کنید تا شکل ۹ را مشاهده کنید. در این شکل بر روی گزینه *Sign & Certify* کلیک کرده و آیکون ▶ را فشار دهید تا گزینه مربوط با کار با گواهی به برنامه اضافه شوند.

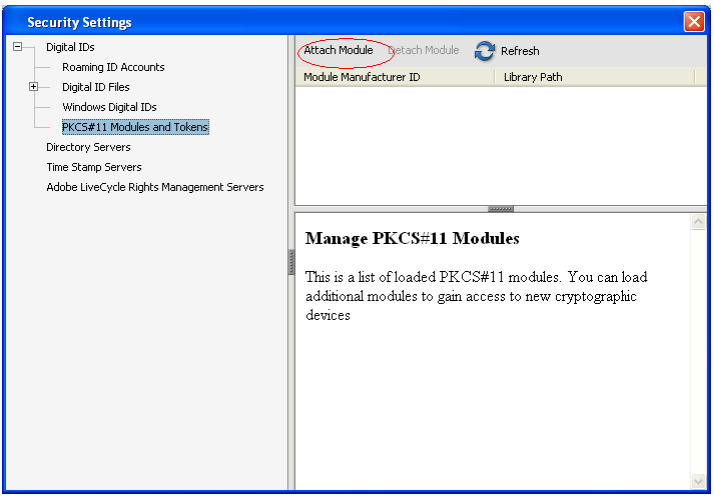


شکل ۹: معرفی کتابخانه K3PKCS

۲- از قسمت منو بار گزینه *Security Setting* را انتخاب کنید (شکل ۱۰) تا پنجره شکل ۱۱ نشان داده شود.



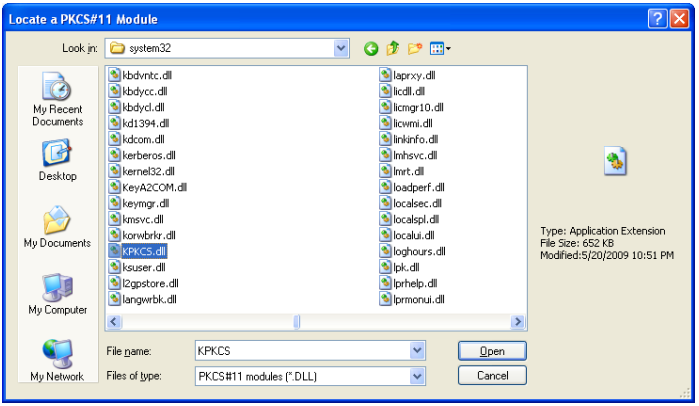
شکل ۱۰: انتخاب گزینه Security Setting



شکل ۱۱: اضافه کردن KeyA3 PKCS

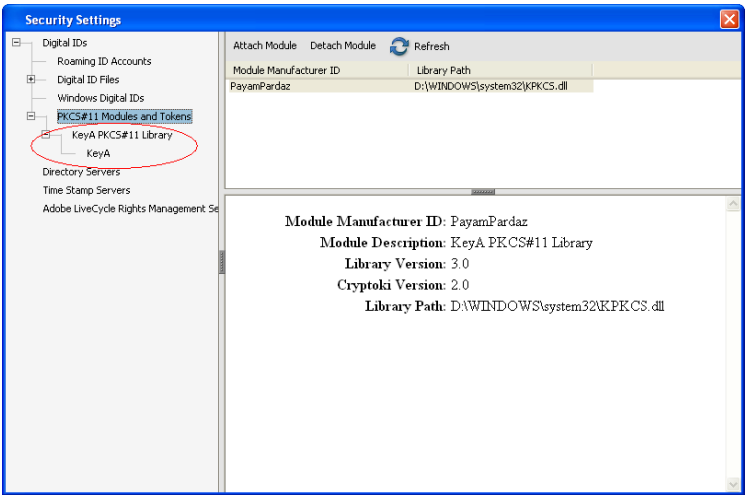
۲- از قسمت چپ پنجره شکل ۱۱ گزینه *PKCS#11 Modules and Token* را انتخاب کنید.

۳- در قسمت بالای سمت راست پنجره شکل ۱۱، گزینه *Attach Module* را انتخاب کنید تا پنجره معرفی *K3PKCS* ظاهرشود (شکل ۱۲). در این پنجره، آدرس کتابخانه کیا را وارد کنید. کتابخانه *PKCS#11* کیا، فایلی با نام *K3PKCS.dll* است که در مسیر نصب نرم‌افزار *KeyA3 certificate Manager* قرار دارد.



شکل ۱۲: انتخاب KPKCS

اگر معرفی کتابخانه به درستی انجام شده باشد در قسمت سمت چپ پنجره شکل ۱۱، اسم کتابخانه کیا اضافه می‌شود. (مطابق شکل ۱۳)



شکل ۱۳: نمایش KeyA3

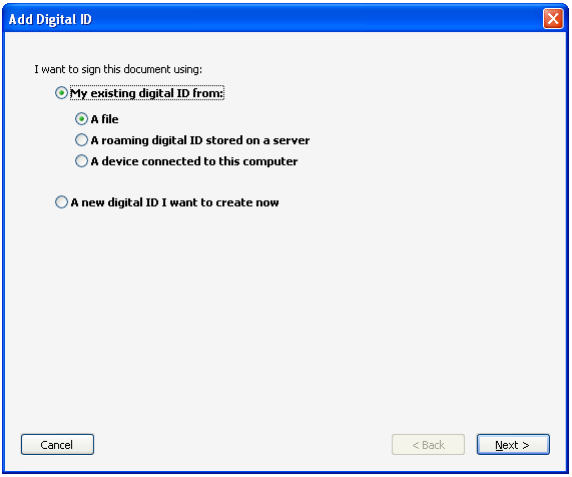
تذکر: برای اینکه در این پنجره بتوان ماژول متصل شده به سیستم را مشاهده کرد، باید ماژول قبل از اجرای برنامه *Adobe Acrobat* به سیستم وصل شده باشد.

۶-۲ امضا کردن یک فایل *PDF*

برای امضای یک فایل *PDF* ابتدا باید یک بار گواهی دیجیتال خود را (که مثلا بر روی ماژول کیاست) به برنامه *Adobe Acrobat* معرفی نماییم. پس از این مرحله برای هر بار امضا می‌توان از گواهی‌های معرفی شده استفاده نمود.

۶-۲-۱ معرفی گواهی به برنامه

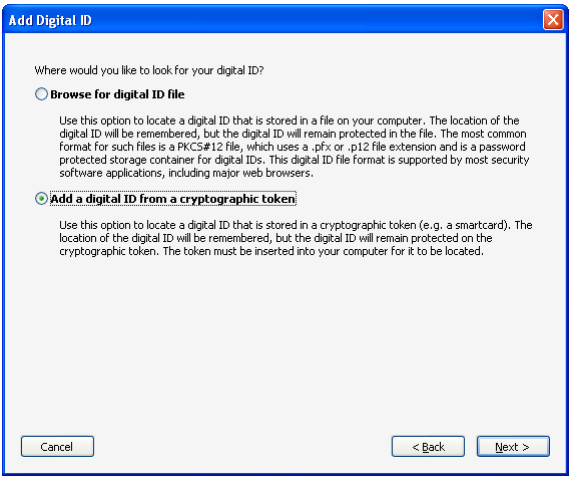
۱- منوی *Sign & Certify |PlaceSignature | Advanced* را انتخاب می‌کنیم و سپس قسمتی از صفحه‌ی *PDF* را که می‌خواهیم نقش امضا در آن قسمت قرار گیرد با استفاده از *Drag and Drop* انتخاب می‌نماییم. پنجره شکل ۱٤ ظاهر می‌شود.



شکل ۱٤: انتخاب گواهی مورد نظر

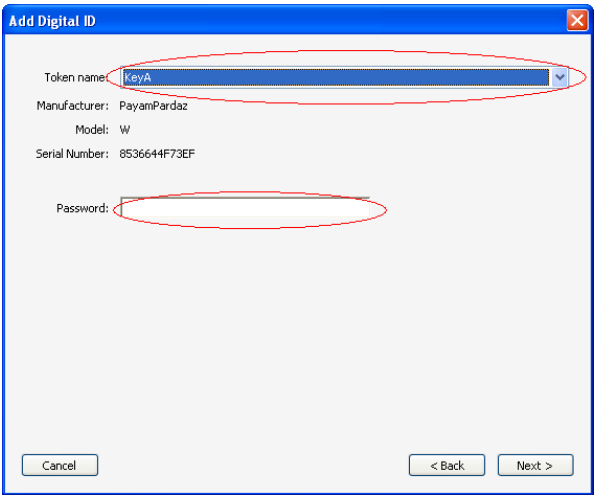
۲- در پنجره شکل ۱٤ گزینه *My existing digital ID from* و همچنین در زیرگروه آن گزینه *A File* را انتخاب می‌کنیم و با زدن دکمه*Next* به پنجره بعد می‌رویم تا شکل ۱۵ را ببینیم.

۳- در پنجره شکل ۱۵ برای استفاده از گواهی موجود در ماژول کیا، گزینه *Add a digital ID from a cryptograph token* را انتخاب می‌کنیم.

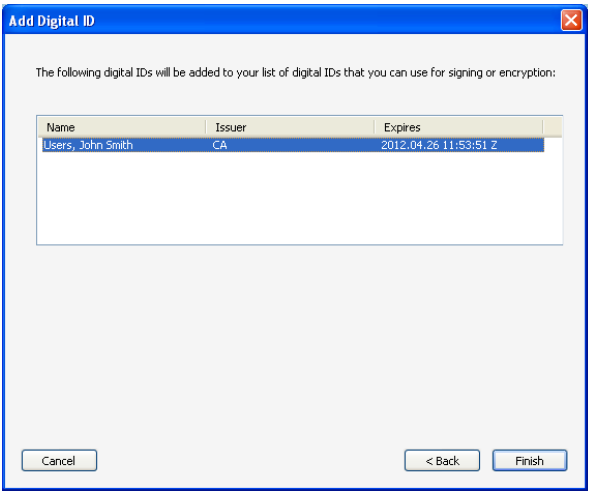


شکل ۱۵: انتخاب ماژول کیا۳

۴- در پنجره شکل ۱۶ لیست *Token*های شناسایی شده توسط *Adobe Acrobat* مشاهده می‌شود. در اینجا کیا را انتخاب می‌کنیم. در این پنجره در قسمت *Password* باید *PIN* ماژول کیا را وارد کنیم و دکمه *Next* را فشار می‌دهیم تا پنجره شکل ۱۷ ظاهر شود.



شکل ۱۶: وارد کردن PIN ماژول



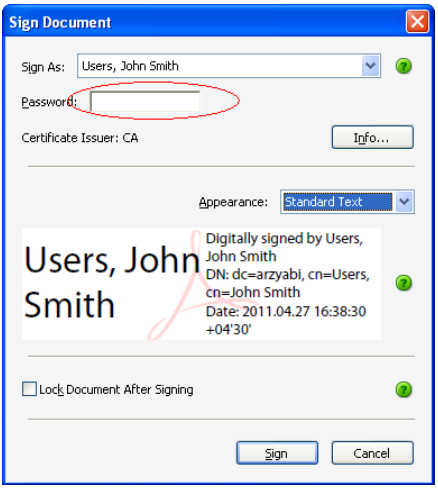
شکل ۱۷: انتخاب گواهی مورد نظر

۵- در پنجره شکل ۱۷ لیست گواهی‌های ذخیره شده روی ماژول کیا قابل مشاهده و انتخاب می‌باشند. گواهی مورد نظر را انتخاب می‌کنیم و دکمه *Finish* را فشار می‌دهیم.

۶-۲-۲ انتخاب گواهی برای امضا

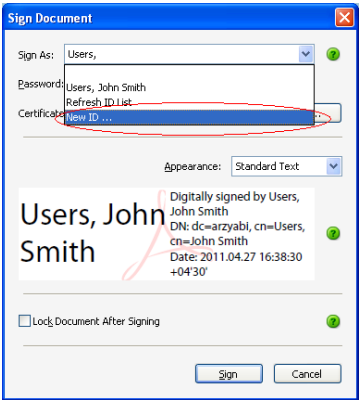
در پنجره شکل ۱۸ در قسمت *Sign As* گواهی مورد نظر را انتخاب کرده و دکمه *Sign* را فشار می‌دهیم. در این حالت با توجه به اینکه گواهی روی ماژول کیا قرار دارد در قسمت *Password*، باید *PIN* ماژول کیا را وارد کنیم. در نهایت می‌توانیم امضای دیجیتالی را بر روی قسمتی که انتخاب کرده‌ایم مشاهده نماییم.

تذکر: پس از یک بارورد کردن *PIN* ماژول کیا، مادامی که از برنامه خارج نشده و ماژول را از پورت *USB* جدا نکرده باشیم برای امضا نیازی به وارد کردن مجدد *PIN* نخواهد بود.



شکل ۱۸: وارد کردن PIN ماژول

تذکر: در حالتی که قبلا گواهی به برنامه *Adobe Acrobat* معرفی شده باشد اگر بخواهیم گواهی جدیدی معرفی نماییم باید در قسمت *Sign As* از پنجره شکل ۱۹ گزینه *New ID* را انتخاب کرده و مراحل بخش قبل را ادامه دهیم.



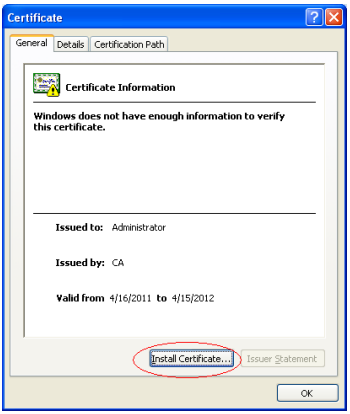
شکل ۱۹: انتخاب گواهی

۶-۳ وارسی امضا

برای اینکه برنامه *Adobe Acrobat* بتواند عملیات وارسی (*Verify*) امضای فرستنده را انجام دهد ابتدا باید گواهی مرکز *CA* در درون سیستم‌عامل گیرنده نصب شده و سپس تنظیمات لازم در برنامه *Adobe Acrobat* انجام گیرد.

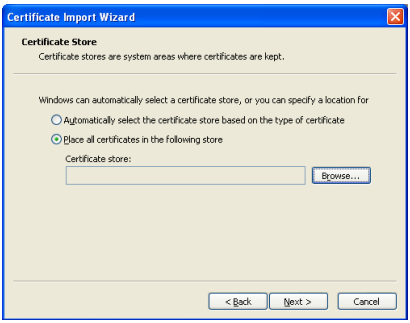
۶-۳-۱ نصب گواهی مرکز *CA* در سیستم گیرنده

۱- برای نصب گواهی مرکز *CA*، ابتدا بر روی فایل گواهی مرکز *CA* (با پسوند *.cer*) دو بار کلیک کرده و سپس در پنجره شکل ۲۰ دکمه *Install Certificate...* را فشار دهید.



شکل ۲۰: نصب گواهی ریشه

۲- در پنجره ظاهر شده (شکل ۲۱) گزینه *Place all certificates in following store* را انتخاب کرده و دکمه *Browse* را فشار دهید تا مسیر نصب مشخص گردد.



شکل ۲۱: تعیین مسیر نصب گواهی

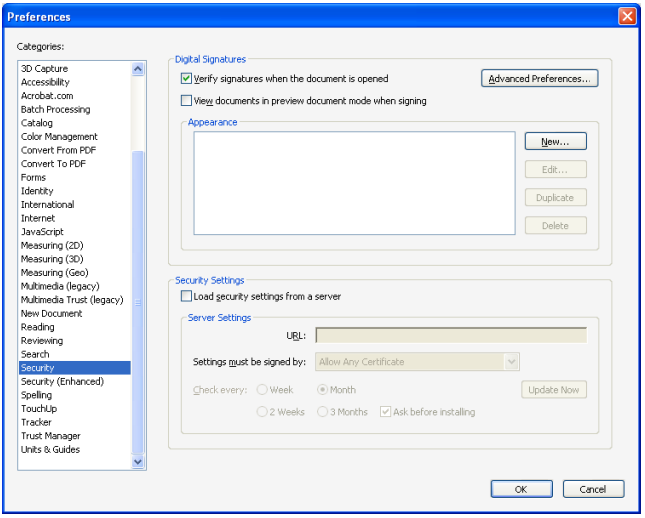
۳- در پنجره بعدی (شکل ۲۲)، باید گزینه *Trusted Root Certificate Authorities* را انتخاب نمایید.

شکل ۲۲: تعیین مسیر نصب گواهی

نکته: برای مشاهده لیست گواهی‌های نصب شده در سیستم می‌توانید در قسمت *Run* عبارت *certmgr.msc* را وارد کرده و در پنجره ظاهر شده گواهی‌های نصب شده را ببینید.

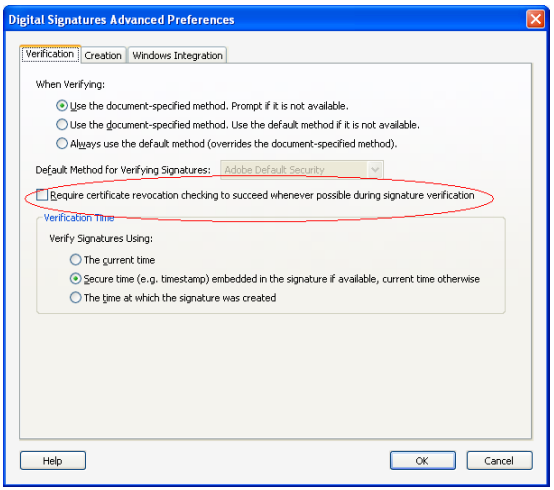
۶-۳-۲ تنظیمات برنامه *Adobe Acrobat*

۱- در پنجره اصلی برنامه منوی *Edit | Preferences* را انتخاب می‌کنیم تا شکل ۲۳ ظاهر شود. در این پنجره گزینه *Security* و درقسمت سمت راست آن گزینه *Advanced Preferences*.... را انتخاب کنید.



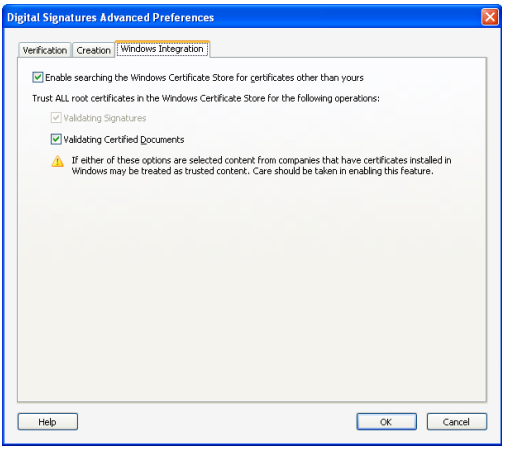
شکل ۲۳: انتخاب گزینه Security

۲- در صورتی که اتصال *Online* به مرکز *CA* برای چک گواهی‌های منقضی شده ندارید در پنجره شکل ۲٤ در برگه *Verification* گزینه *Require certificate revocation checking to succeed whenever possible during signature verification* را غیرفعال کنید.



شکل ۲٤: تعیین چک کردن گواهی‌های منقضی شده

۳- در پنجره فوق در برگه *Windows Integration* (شکل ۲۵)، گزینه *Enable searching the Certificate Store for Certificates other than yours* و همچنین گزینه *Validating Certificate Documents* را فعال کنید.



شکل ۲۵: فعال کردن گزینه‌های لازم

۴- حال با کلیک کردن بر روی محل قرار گرفتن علامت امضای دیجیتال، طی پیغامی مشخص می‌شود که آیا امضای دیجیتالی به تایید مرکز گواهی رسیده یا خیر. اگر امضا مورد تایید مرکز گواهی باشد شکل ۲۶ و در غیر این صورت شکل ۲۷ مشاهده می‌شود.

شکل ۲۶: تایید شدن امضا

شکل ۲۷: تایید نشدن امضا ۲۷