

داده ورزی سداد



بانک ملی ایران

نحوه دریافت فایل های اجرایی
به صورت امن در ویندوز 7

عنوان

صفحه

- ۱ - مقدمه ۱
- ۲ - امضای دیجیتال ۱
- ۳ - انتشار گواهی CA اختصاصی بانک ملی ۲
- ۴ - نصب مطمئن نرم افزار بر روی کامپیوتر کاربر ۲
- ۴-۱ بررسی صحت امضای فایل ۲

۱ - مقدمه

اعتماد به نرم‌افزاری که از طریق رسانه‌های ناامن مانند اینترنت منتشر می‌شود یکی از مشکلات موجود در صنعت نرم‌افزار است. در مورد نرم‌افزارهایی که به صورت بسته‌بندی عرضه می‌شوند می‌توان با استفاده از اطلاعات برند تولید کننده و فروشگاه‌های عرضه معتبر، اعتماد لازم را برای مصرف کننده ایجاد نمود. اما در مورد نرم‌افزارهایی که از طریق رسانه‌هایی مانند اینترنت منتقل می‌شوند نه تنها این امکان وجود ندارد بلکه مساله اطمینان از عدم تغییر محتوای نرم‌افزار در حین دریافت آن نیز وجود دارد. برای اینکه بتوان اینترنت را به منبعی قابل اعتماد برای نرم‌افزار تبدیل کرد باید راهکاری برای دو موضوع زیر در نظر گرفت:

۱- اطمینان از اصالت نرم‌افزار به معنی اینکه کاربر اطمینان حاصل نماید که نرم‌افزار دریافت شده به وسیله یک تولید کننده یا توزیع کننده معتبر منتشر شده است.

۲- اطمینان از تمامیت نرم‌افزار به معنی اینکه کاربر اطمینان حاصل نماید که محتوای نرم‌افزار از زمان انتشار آن تاکنون تغییری نکرده است.

راه‌حلی که برای این موارد وجود دارد استفاده از امضای دیجیتال کد به وسیله توسعه دهنده یا توزیع کننده است.

هدف از این نوشتار معرفی امضای دیجیتال کد برای نرم‌افزاری می‌باشد که قرار است به وسیله بانک ملی ایران توزیع شود و اعتماد لازم را برای کاربران این بانک را فراهم آورد.

۲ - امضای دیجیتال

امضای دیجیتال به وسیله یک الگوریتم رمز کلید عمومی قابل انجام است. در عمل الگوریتم رمز کلید عمومی برای امضاء اسناد بزرگ کارایی لازم را ندارد و امضاء اینگونه اسناد با این روش زمانگیر خواهد بود. برای صرفه جویی در زمان هاش (*hash*) سند گرفته شده و به جای امضاء سند، هاش آن امضاء می‌شود.

برای امضای دیجیتال نرم‌افزار می‌توان نسخه اجرایی نرم‌افزار و یا برنامه نصب آن را امضا نمود.

۳ - انتشار گواهی CA اختصاصی بانک ملی

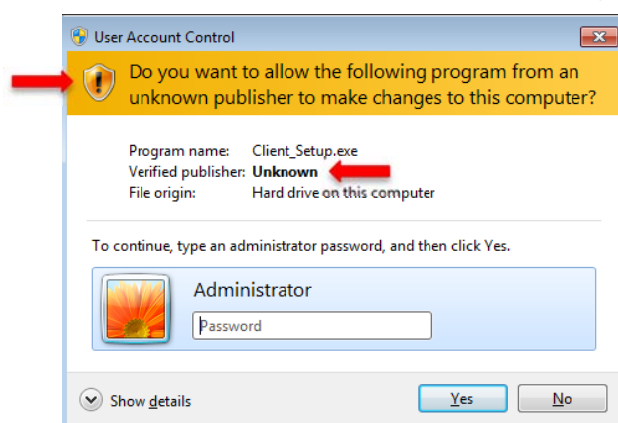
گواهی ریشه CA اختصاصی بانک ملی می بایست توسط بخش پشتیبانی شرکت داده ورزی سداد، بر روی کامپیوترهای کلیه شعب و ادارات نصب گردد.

۴ - نصب مطمئن نرم افزار بر روی کامپیوتر کاربر

پس از اینکه گواهی CA بر روی دستگاه شما نصب شد، از طریق سامانه اعلام شده اقدام به دریافت فایل مورد نظر نموده و سپس با توجه به موارد مطروحه در بند ۱-۴ اقدام به نصب نرم افزار نمایید.

۴-۱ بررسی صحت امضای فایل

هنگام اجرای فایل نصب نرم افزار، در حالی که گواهی CA اختصاصی بانک ملی ایران روی سیستم کاربر نصب نشده باشد یا نرم افزار توسط یک تولید کننده یا توزیع کننده معتبر امضاء نشده باشد پنجره شکل ۱ به کاربر نشان داده می شود.



شکل ۱

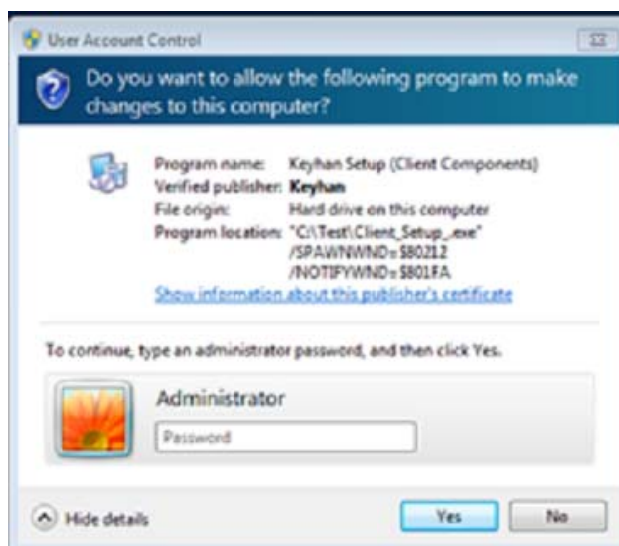
چنانچه کاربر هنگام نصب نرم افزار با پیغام شکل ۱ مواجه شود (در صورت اطمینان از نصب گواهی ریشه اختصاصی بانک ملی)، این امر نشان دهنده آن است که فایل مذکور مورد تایید نمی باشد، در این صورت کاربر می بایست از نصب نرم افزار اکیداً خودداری نماید، در غیر این صورت بدیهی است مسئولیت عواقب و مشکلات ناشی از نصب نرم افزار غیر مطمئن بر عهده کاربر می باشد.

در حالتی که گواهی CA بر روی سیستم نصب شده و این نرم افزار توسط یک تولید کننده یا توزیع کننده معتبر امضاء شده باشد، پنجره ای مطابق شکل ۲ برای کاربر به نمایش در می آید.

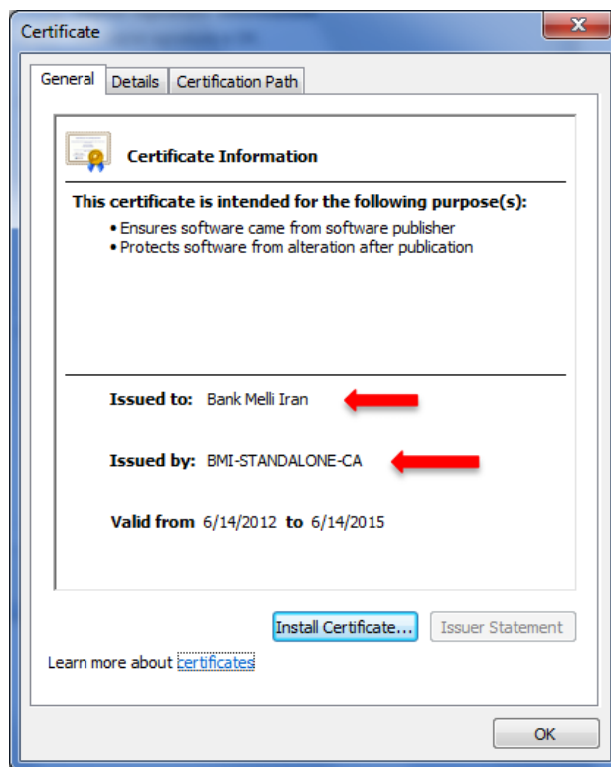


شکل ۲

در صورت کلیک بر روی گزینه *Show details* پنجره ای مانند شکل ۳ ظاهر شده و با کلیک بر روی گزینه *show information about this publisher's certificate* اطلاعات مربوط به گواهینامه دیجیتال قابل مشاهده می باشد (شکل ۴).



شکل ۳



شکل ۴

با استناد به اطلاعات مشاهده شده در شکل ۲ و ۴ کاربر می تواند اطمینان حاصل می نماید که فایل نصب را از منبعی قابل اطمینان و معتبر دریافت نموده است و نسبت به نصب آن اقدام نماید.