بانک ملی ایران

داده ورزی سداد

نحوه دریافت فایل های اجرایی
به صورت امن در ویندوز XP

عنوان **صفحه**

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 می باشد 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

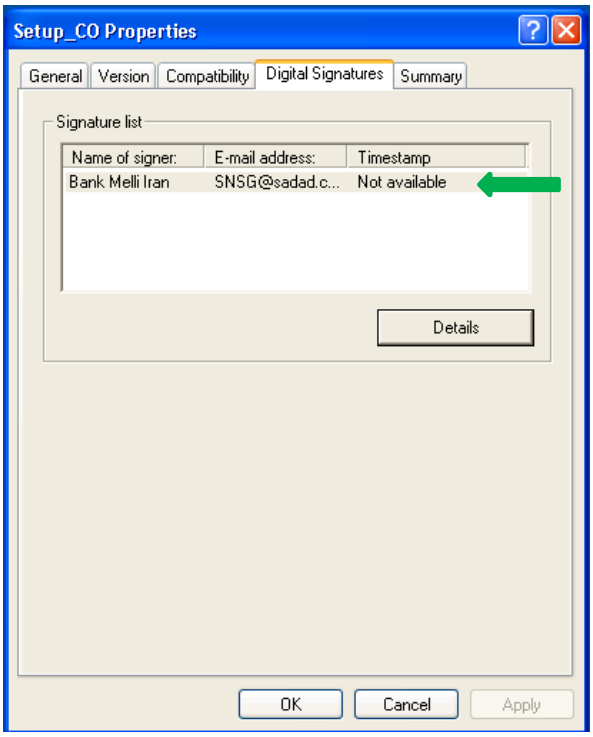
گواهی ریشه *CA* اختصاصی بانک ملی می بایست توسط بخش پشتیبانی شرکت داده ورزی سداد، بر روی کامپیوترهای کلیه شعب و ادارات نصب گردد.

۴ - نصب مطمئن نرم‌افزار 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 ٤-١ اقدام به نصب نرم افزار نمایید.

۴-۱ بررسی صحت امضای فایل

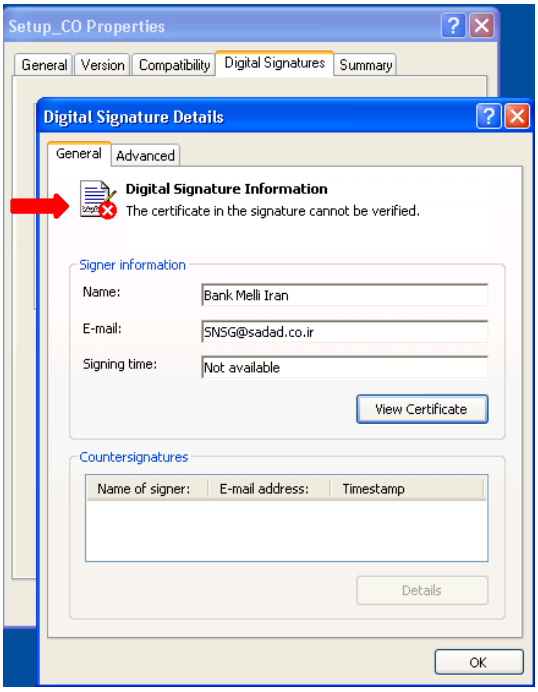
پس از دریافت فایل، آن را انتخاب نموده و بر روی آن کلیک راست نمایید و از منوی ظاهر شده گزینه *properties* را انتخاب نمایید.چنانچه فایل امضاء شده باشد،بخش جدیدی به نام *Digital Signature* به منوی *properties* اضافه شده و در قسمت *signature list* اطلاعات مربوط به امضاء کننده فایل نمایش داده میشود. (شکل ۱).



شکل ۱

در پنجره نمایش داده شده(شکل ۱) روی دکمه *Details* کلیک کنید تـا پنجـره ای مطـابق شـکل ۲ نمایش داده شود. این پنجره جزئیات مربوط به گواهینامه ای که فایل با آن امضاء شده اسـت را بـه شـما نشان می دهد.

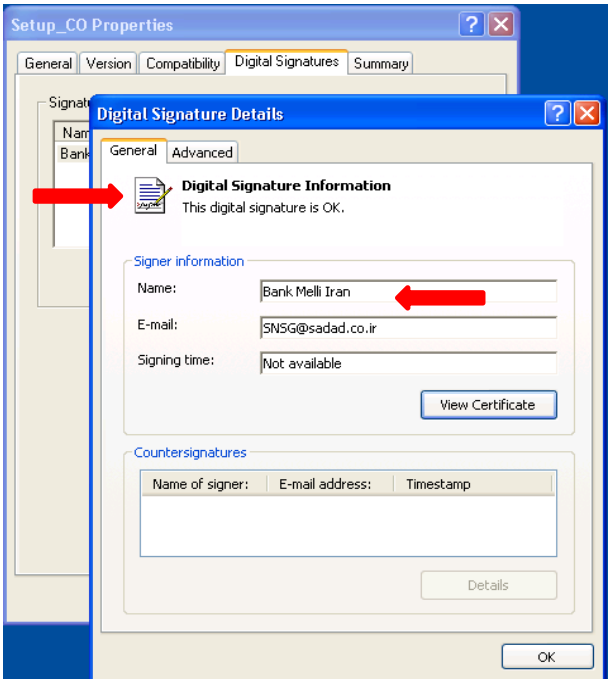
چنانچه گواهی *CA* اختصاصی بانک ملی ایران روی سیستم کاربر نصب نشده ویا نرم افزار توسـط یک تولید کننده یا توزیع کننده معتبر امضاء نشده باشد پنجـره ای مطـابق شـکل ۲ بـه کـاربر نشـان داده می‌شود.



شکل شماره ۲

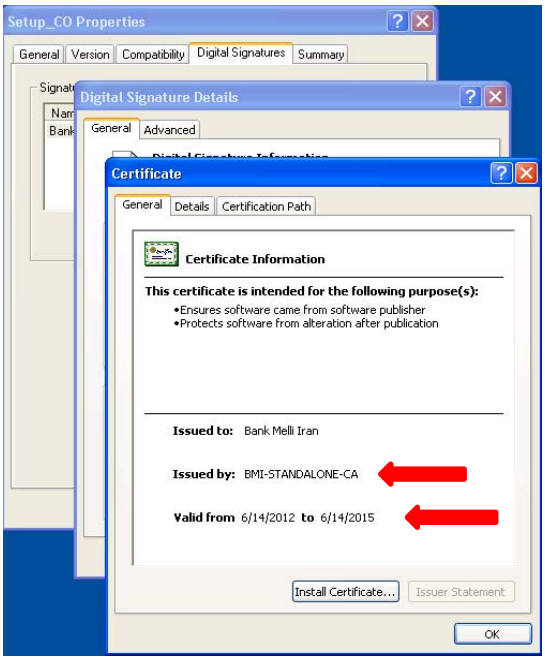
مشاهده پیغام خطا(شکل ۲)، نشان دهنده آن است که فایل مذکور **مورد تایید نمی باشد**. در این صورت کاربر می بایست از نصب نرم افزار **اکیداً خودداری نماید**، در غیر این صورت بـدیهی اسـت مسئولیت عواقب و مشکلات ناشی از نصب نرم افزار غیر مطمئن بر عهده کاربر می باشد.

چنانچه گـواهی *CA* اختصاصـی بانـک ملـی بـر روی دسـتگاه شـما نصـب گردیـده و ایـن نـرم افزار توسط یک تولید کننده یـا توزیـع کننـده معتبـر امضـاء شـده باشـد، پنجـره مطـابق شـکل شـماره ۳ نمایش داده خواهد شد.



شکل ۳

با کلیک بر روی گزینه *View Certificate* در شکل ۳، پنجره شکل ٤ نمایش داده میشود، در این پنجره اطلاعات مربوط به گواهینامه دیجیتال بانک ملی قابل مشاهده می باشد.



شکل ٤

کاربر با استناد به پنجره های نمایش داده شده در شکل ۳ و٤، اطمینان حاصل می‌نماید که فایل نصب را از منبعی قابل اطمینان و معتبر دریافت نموده است و می تواند نسبت به نصب آن اقدام نماید.