تقویت ایمنی ویندوز۷ با سیستم رمزنگاری فایل EFS

از داده‌های‌تان حفاظت کنید

داستان‌های فراوان و روزافزون هک‌شدن پی‌سی‌ها، یا مورد تهاجم قرارگرفتن پی‌سی‌ها سبب گشته است که بسیاری از کاربران از خود بپرسند که «چگونه می‌توانم برای داده‌هایم امنیت به وجود آورم؟» اگر از **ویندوز۷** نگارش Professional و Ultimate بهره می‌گیرید، یک محافظ داده‌ها مشهور به EFS در سیستم خود دارید. EFS سرواژهٔ عبارت زیر است:

Encrypting File System

که به معنی «سیستم رمزنگاری فایل» است.

> ***یادآوری: این برنامه در ویندوز۷ نگارش‌های Windows 7 Starter، Windows 7 Home Basic، و Windows 7 Home Premium به طور کامل پشتیبانی نشده است.***

با EFS می‌توانید به **ویندوز۷** دستور بدهید که از فناوری رمزگذاری چندلایه‌ای خود برای رمزنگاری فایل‌های داده‌ای، پوشه‌ها، یا دیسک سیستم استفاده کند. (EFS **فایل‌های سیستمی** یا دیسک‌هایی را که برای عملیات شما ضروری‌اند، یا روی سیستم اثرگذار هستند رمزنگاری نمی‌کند.) هرگاه فایلی را **رمزنگاری** (encrypt) کنید، عملیات «رمزگشایی/باز–رمزنگاری» برای کاربرانی که آن فایل را باز می‌کنند به صورت پنهان انجام می‌گیرد. با وجود این، هر کس دیگری که بخواهد فایل رمزنگاری‌شده را باز کند، آن را از طریق ایمیل به پی‌سی دیگری ارسال کند، یا آن را در دیسکی کپی کند که رمزنگاری را پشتیبانی نمی‌کند یک پیام خطا خواهد دید. این امکان برای داده‌های شما امنیت خوبی فراهم می‌سازد. با این همه، EFS نوشدارو نیست. یک فناوری فریبنده و پیچیده است، و کاربران باید با احتیاط فراوان از آن بهره بگیرند، در غیر این صورت ممکن است اطلاعات خود را از دست بدهند.

مبانی EFS

استفاده از فناوری EFS آسان است. اما، چند مانع ممکن است روی توانایی (یا میل) شما در استفاده از EFS اثر بگذارد.

• **ساختار دیسک.** EFS نمی‌تواند دیسک‌ها، فایل‌ها، یا پوشه‌های **فشرده‌شده** (compressed) را رمزنگاری کند. در نتیجه، EFS، پیش از آن که فایل‌ها را رمزنگاری کند، به طور خودکار فشرده‌سازی را غیرفعال می‌کند (فایل‌ها را **نافشرده** می‌کند).

اگر از فشرده‌سازی استفاده می‌کنید و فضای آزاد دیسک سخت شما ناچیز است، پیش از آن که رمزنگاری فایل‌ها یا پوشه‌ها را آغاز کنید، بعضی از فایل‌ها را حذف کنید، یا یک دیسک سخت با ظرفیت بیشتر بخرید.

EFS فقط دیسک‌هایی را رمزنگاری می‌کند که از **سیستم فایل** بومی **ویندوز۷**، یعنی سیستم فایل **NTFS**، بهره می‌گیرند.

• **معیارهای امنیتی.** اگر **بخش کاربری** (user profile) خود را به **گذرواژه** مجهز نکنید حفاظتی که EFS فراهم می‌سازد بی‌ارزش می‌شود. برای اطمینان از این که در صورت فراموشی گذرواژه می‌توانید فایل‌های خود را بازیابی کنید، یک **دیسک بازگردان گذرواژه** بسازید و آن را در جایی مطمئن قرار دهید. (اگر از یک حساب administrator برای بازسازی گذرواژه فراموش‌شده استفاده کنید دستیابی فایل‌های EFS خود را از دست خواهید داد.) **نکتهٔ یادآور** (hint) گذرواژه را استفاده نکنید، چون برای همهٔ کسانی که می‌توانند وارد بخش کاربری شما بشوند قابل رؤیت است و می‌توانند با آن، گذرواژه شما را کشف کنند.

• **محافظ دستیابی فایل.** EFS برای رمزنگاری و رمزبرداری فایل‌های شما، از یک **کلید خصوصی** ذخیره‌شده در بخش کاربری شما استفاده می‌کند. اگر بخش کاربری شما خراب یا حذف شود، **کلید خصوصی** را از دست خواهید داد. بازسازی بخش کاربری یا نصب مجدد **ویندوز۷** مسئلهٔ دستیابی را حل نخواهد کرد. اگر می‌خواهید از EFS استفاده کنید، باید چند اقدام احتیاطی را انجام دهید. در غیر این صورت، اگر دستیابی بخش کاربری خود را از دست بدهید، مجبورید برای بازیابی فایل‌های خود به شرکت‌های حرفه‌ای بازیابی داده‌ها بروید و هزینهٔ هنگفتی را متحمل شوید.

پیش‌گیری

مایکروسافت به جامعه کاربران فنی (TechNet) خود هشدار داده است که «در بعضی از وضعیت‌ها EFS ممکن است درست عمل نکند. بعضی از مسائل EFS به راه‌حل‌های پیچیده و سطح بالا نیاز دارند.» در نتیجه، مطمئن‌ترین راه برای محافظت از داده‌های رمزنگاری‌شده تهیهٔ یک نسخهٔ پشتیبان از داده‌ها و قراردادن آن در مکانی امن (جایی به جز پی‌سی) است.

نسخهٔ پشتیبان را رمزنگاری نکنید، مگر آن که در مورد رمزبرداری آن مطمئن باشید. افزون بر این، باید از **بخش کاربری** (user profile) خود نیز نسخهٔ پشتیبان تهیه کنید. (تهیهٔ یک نسخهٔ پشتیبان کامل سیستم این کار را انجام می‌دهد.)

رمزنگاری[1] یکی از عناصر بنیادین ایمن‌سازی سیستم است، در نتیجه، شگفت‌انگیز نیست اگر رمزنگاری بخشی از سیستم‌عامل باشد (هر چند، امکانات رمزنگاری در نگارش‌های Windows 7 Starter، Windows 7 Home Basic، و Windows 7 Home Premium محدود است). در حقیقت، EFS[2] از **ویندوز۲۰۰۰** به بعد، به عنوان یک خصوصیت تعبیه‌شده در **سیستم‌فایل**[3] NTFS[4] حضور داشته است که **ویندوز۷، ویستا، اکس‌پی،** و **ویندوز۲۰۰۰** بر آن بنا می‌شوند. **ویندوز۷** در نگارش‌های Professional، Enterprise، و Ultimate، یک سیستم امنیتی اضافی، به نام **BitLocker**، فراهم می‌سازد که وقتی با EFS ترکیب شود یک بستهٔ قدرتمند رمزنگاری را فراهم می‌سازد (هر چند، BitLocker اختصاصاً برای کاربران لپ‌تاپ طراحی شده است). در اینجا ما فقط به EFS توجه کرده‌ایم.

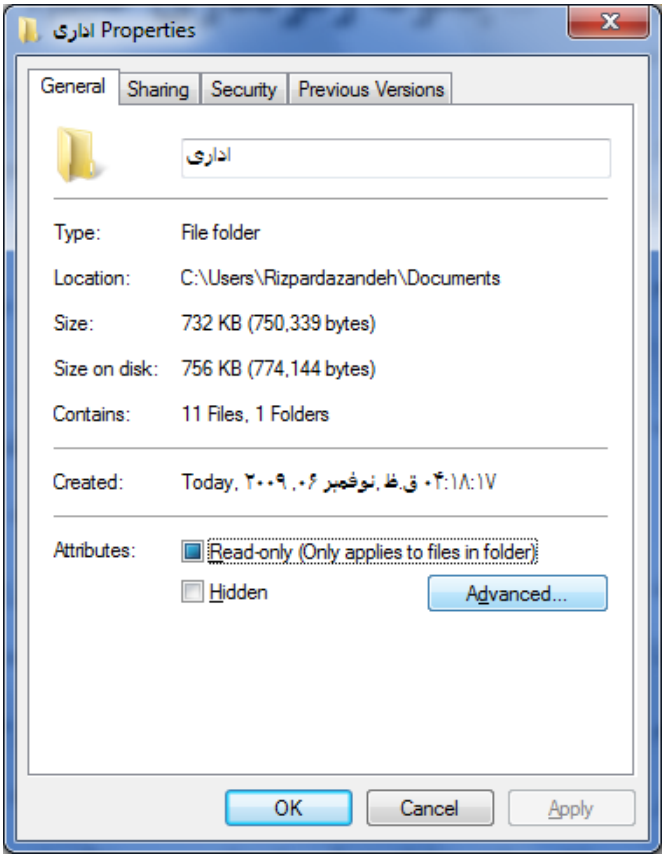
علت این که EFS در ویندوز گنجانده شده است آن است که یک سیستم رمزنگاری داده‌های قدرتمند در خود سیستم‌عامل تعبیه شود، تا در نتیجه هم به خرید یک برنامهٔ مستقل رمزنگاری نیاز نباشد، و هم جلوی مسائلی گرفته شود که برنامه‌های افزودنی مستقل می‌توانند بر روی چنین عملیات مهمی به وجود بیاورند. EFS به همراه NTFS کار می‌کند و روی **والیوم‌های**[5] FAT یا FAT32 ***کار نمی‌کند؛*** در حقیقت، اگر یک پوشه یا فایل را از یک پارتیشن NTFS در یک پارتیشن FAT32/FAT کپی کنید، از آن فایل به طور خودکار رمزگشایی می‌شود. در جهت عکس، یک پوشه یا فایلی که رمزنگاری نشده است به محض آن که به یک پوشهٔ رمزنگاری‌شده انتقال یابد رمزنگاری می‌شود. علاوه بر رمزنگاری براساس فایل به فایل، همهٔ فایل‌های داخل یک پوشه را به طور خودکار با رمزنگاری‌کردن خود پوشه می‌توانید رمزنگاری کنید _ یک روش آسان، و کارآمد.

> **یک هشدار ملایم:** *پیش از رمزنگاری فایل‌های مهم خود، کل این عملیات را روی یک پوشهٔ بلااستفاده تمرین کنید (به ویژه بخش حذف‌کردن گواهینامهٔ خود را همان‌گونه‌که در زیر پیشنهاد شده است حتماً تمرین کنید). آسان‌ترین روش، ساخت یک کپی از یک پوشهٔ موجود است؛ هنگام تمرین باید مراقب باشید که فقط روی نگارش کپی‌شده کار می‌کنید.*

[1] encryption
[2] Encrypting File System
[3] file system
[4] NT file system
[5] volume

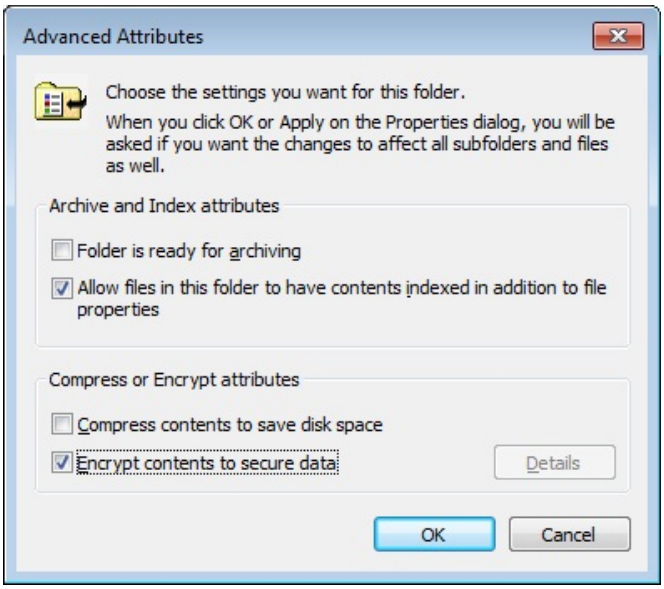
□ رمزنگاری آسان است

ویندوز۷ رمزنگاری فایل را از طریق صفحهٔ Properties برای فایل یا پوشه‌ای که می‌خواهید رمزنگاری شود انجام می‌دهد. به پوشهٔ انتخابی خود در Windows Explorer بروید، روی آن کلیک–راست کنید، و Properties را انتخاب کنید.

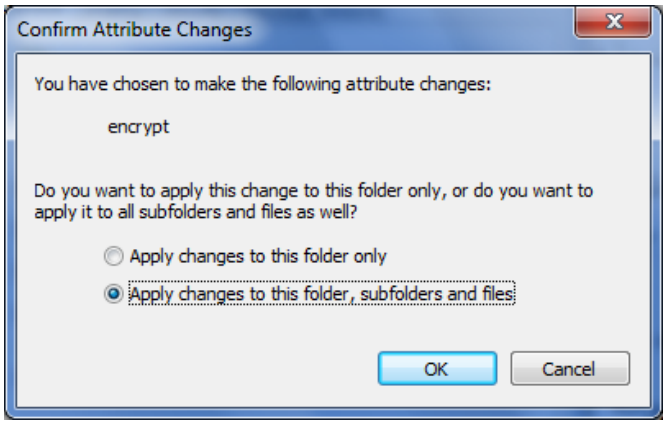


دربرگهٔ General از منوی Properties نتیجه، روی دکمهٔ Advanced کلیک کنید.

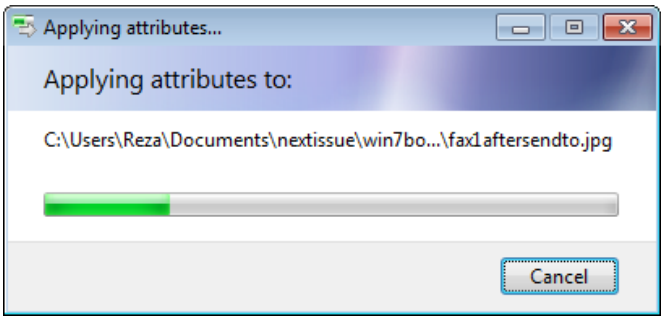
در اینجا، مربع کنار گزینهٔ Encrypt contents to secure data را تیک‌دار کنید و سپس روی OK کلیک کنید. توجه داشته باشید که با آن که گزینه‌های فشرده‌سازی و رمزنگاری در کنار هم هستند هر دو گزینه را همزمان نمی‌توانید انتخاب کنید؛ ویندوز به فایل‌های فشرده‌شده اجازهٔ رمزنگاری‌شدن از طریق EFS را نمی‌دهد. هنگامی که یک طرح ایمن‌سازی جامع را برپا می‌کنید، این محدودیت را در ذهن داشته باشید. یا همهٔ فایل‌های فشرده‌شده را از همهٔ پوشه‌های مورد نظر خود حذف کنید، یا از یک برنامهٔ رمزنگاری دیگر عرضه‌شده در بازار استفاده کنید.



روی Apply در پنجرهٔ Properties کلیک کنید. پنجرهٔ Confirm Attribute Changes آخرین گام است، که در آن بین گزینه‌های رمزنگاری صرف پوشهٔ کنونی، یا رمزنگاری پوشه به همراه رمزنگاری همهٔ پوشه‌های فرعی آن (و همهٔ فایل‌های داخل آن پوشه‌های فرعی)، یکی را انتخاب کنید.



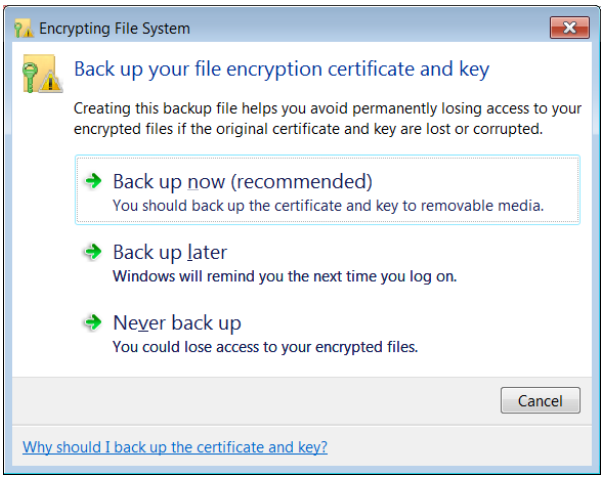
روی OK کلیک کنید، و آمادهٔ دیدن نوار پیشرفت عملیات در زمانی شوید که EFS عملیات رمزنگاری را بر روی موارد انتخابی انجام می‌دهد.



□پشتیبان‌گیری از کلیدها

ویندوز۷ برای کمک به شما در کامل‌کردن این عملیات یک کار دیگر انجام می‌دهد (که **ویندوز اکس‌پی** و سایر نگارش‌های پیشین ویندوز انجام نمی‌دادند). در لحظه‌ای که رمزنگاری را آغاز می‌کنید، یک پیام در نوار آیکن در پایین صفحهٔ اصلی ویندوز ظاهر می‌شود و از شما می‌خواهد که از **کلید** (key) رمزنگاری‌تان **پشتیبان‌گیری** کنید.

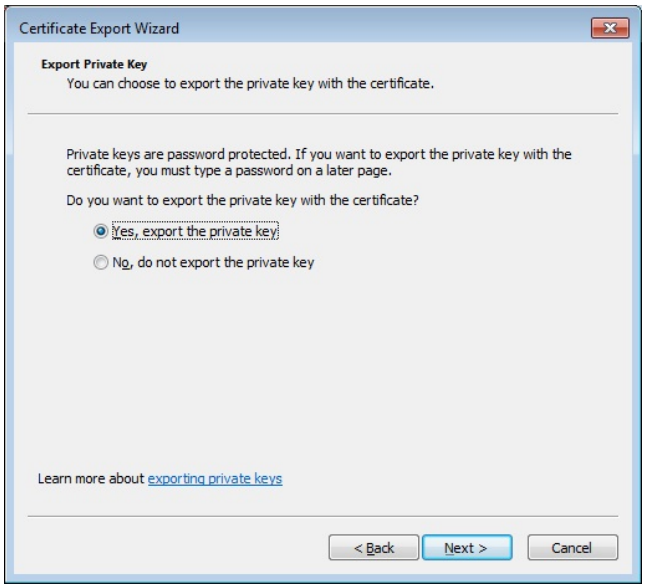
روی این پیام برای بازکردن پنجرهٔ Backup your file encryption certificate and key کلیک کنید.

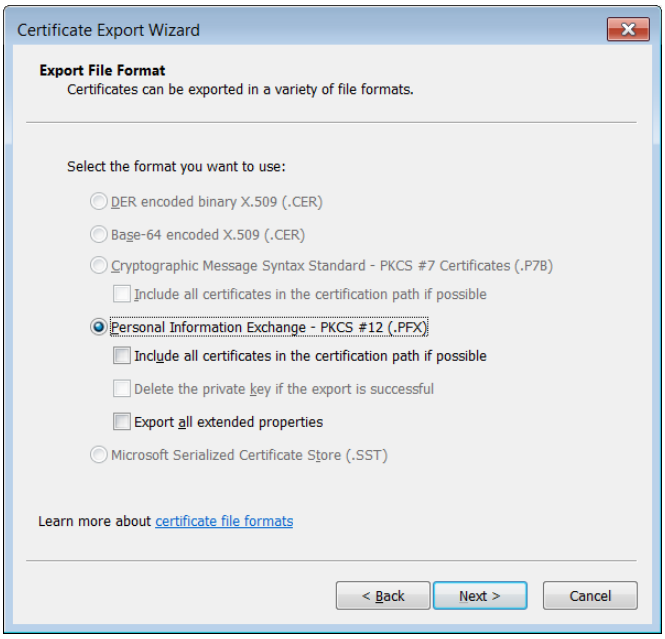


اهمیت این نسخهٔ پشتیبان در توضیحات واقع در این پنجره مشخص است _ در نتیجه، Back up now توصیه می‌شود. اما انتخاب Back up later به معنی آن است که هنگامی که بار بعد وارد حساب کاربری خود می‌شوید (log on می‌کنید)، **ویندوز۷** به شما اجازه نمی‌دهد که پشتیبان‌گیری را فراموش کنید. گزینهٔ پایانی، Never back up، فقط مخصوص خطرپذیران است: اگر از گواهینامه و کلید رمزنگاری خود پشتیبان‌گیری نکنید، و روزی مجبور به نصب مجدد **ویندوز۷** شوید، یا حساب کاربری شما آسیب ببیند، اصلاً قادر نخواهید بود که فایل‌های رمزنگاری‌شده را دستیابی کنید.

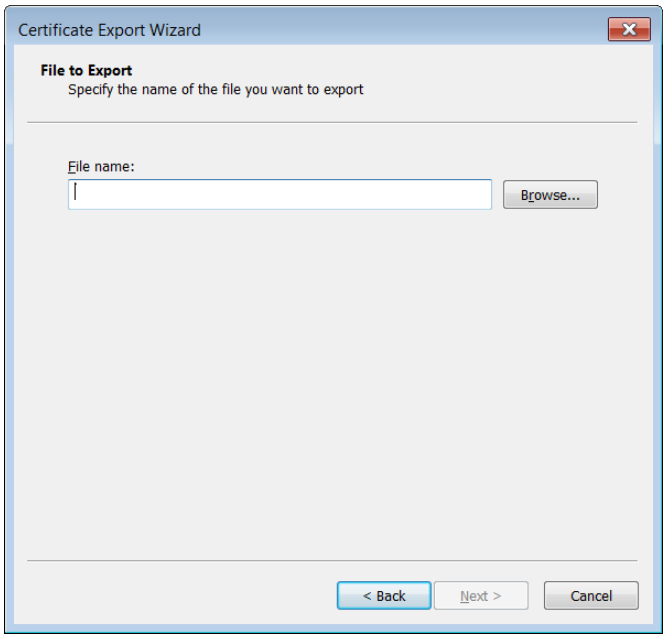
اگر روی Back up now (recommended) کلیک کنید برنامهٔ Certificate Export Wizard به اجرا در می‌آید.

روی Next کلیک کنید. در پنجرهٔ بعدی اولین گزینه را برای صدور (export) **کلید خصوصی** (private key)، انتخاب کنید، و روی Next کلیک کنید. هنگامی که برنامه انواعی از فرمت‌های رمزنگاری فایل را نمایش می‌دهد، همگی به جز یکی، Personal Information Exchange (PFX)، به رنگ خاکستری هستند، چون برنامهٔ EFS در **ویندوز۷** فقط این فرمت را پشتیبانی می‌کند.

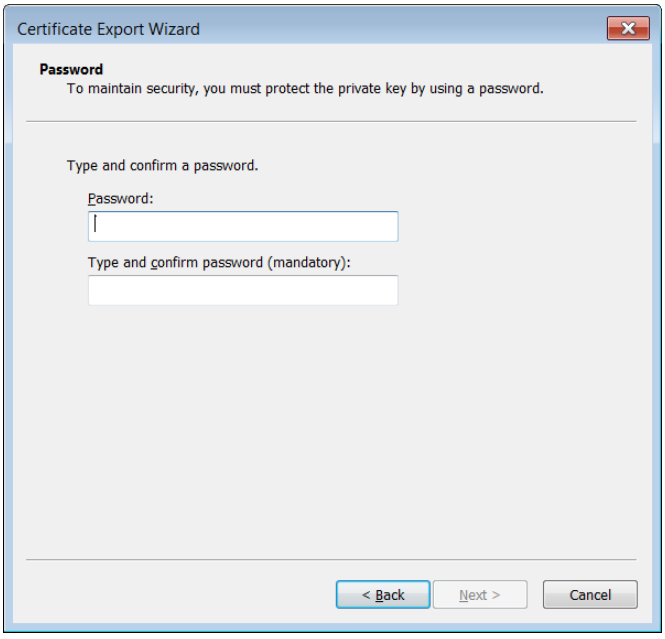




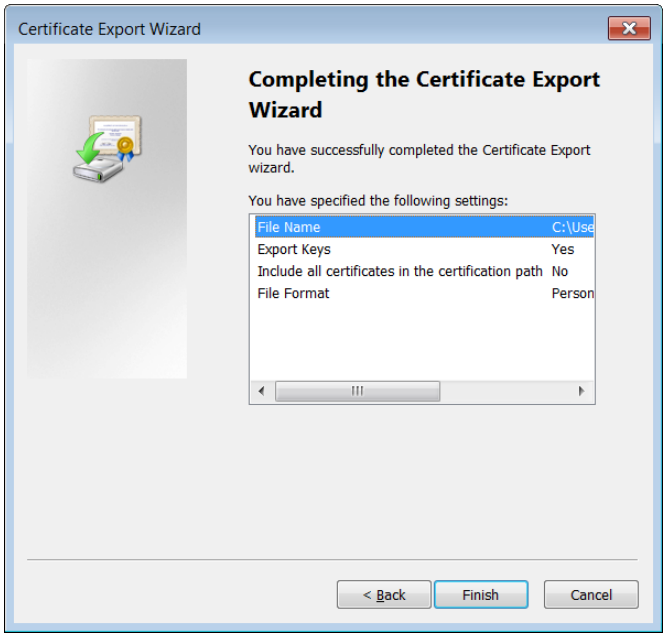
با تیک‌دارکردن اولین گزینهٔ تحت این فرمت، یعنی گزینهٔ Include all certificates in the certification path if possible به‌یک‌باره می‌توانید از همهٔ گواهینامه‌های کاربری شخصی خود پشتیبان‌گیری کنید (اگر اولین رمزنگاری شما باشد ضروری نیست). روی Next کلیک کنید.



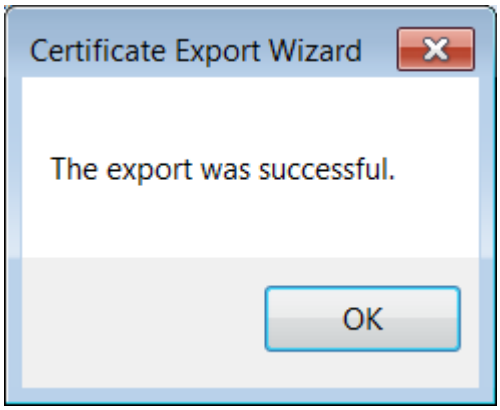
در صفحهٔ بعد، یک نام برای فایل خود تایپ کنید (هر نامی کار خواهد کرد، و **ویندوز۷** بسط «PFX.» را به طور خودکار برای آن اضافه خواهد کرد). روی دکمهٔ Browse کلیک کنید و یک مکان امن را برای ذخیرهٔ فایل گواهینامه مشخص کنید. روی Next برای نمایان‌شدن صفحهٔ موفقیت‌آمیزبودن عملیات کلیک کنید.



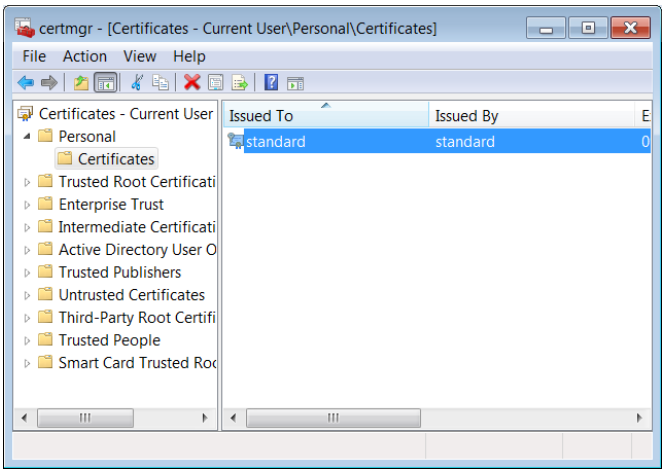
یک **گذرواژه** _ همانند همهٔ گذرواژه‌هایی که واقعاً برای تأمین امنیت داده‌ها طراحی می‌شود_ تایپ کنید. یک گذرواژهٔ آسان تایپ نکنید. در کادر بعدی دوباره همان گذرواژه را تایپ کنید.



روی Finish کلیک کنید.



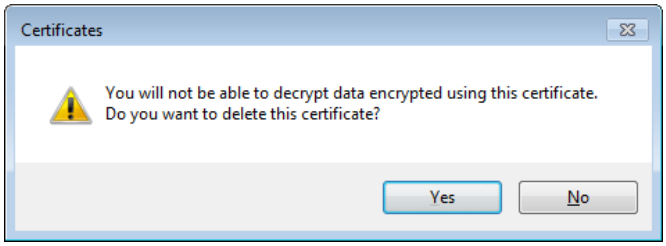
یادآوری: *اگر پشتیبان‌گیری را در این زمان انجام ندهید، این برنامه را بعداً نیز در Certificate Manager می‌توانید دستیابی کنید: عبارت* ***certmgr.msc*** *را در کادر Search در پایین منوی Start تایپ کنید. کلید Enter را بزنید. در بخش دست چپ، به Personal\Certificates بروید، سپس در بخش دست راست، همهٔ گواهینامه‌ها را انتخاب کنید و روی آنها کلیک-راست کنید، و آنگاه All Tasks | Export... را انتخاب کنید.*



□ حذف یک گواهینامه از دیسک‌سخت

پشتیبان‌گیری از گواهینامه‌ها و کلیدها در دیسک‌ها و رسانه‌های جابه‌جاپذیر بی‌مسئله نیست. بالاخره، هر کسی که به دیسک یا رسانهٔ جابه‌جاپذیر شما دسترسی پیدا کند می‌تواند اطلاعات رمزنگاری‌شدهٔ شما را دستیابی کند. باید به خوبی از این رسانه مراقبت کنید. **اما اقداماتی در برابر نفوذگرانی که از طریق اینترنت یا شبکه قصد دستیابی اطلاعات شما را دارند می‌توانید انجام بدهید. برای این کار، گواهینامه و کلید خود را از روی دیسک‌سخت حذف کنید و فقط اجازه دهید که بر روی یک رسانهٔ جابه‌جاپذیر یا جداشدنی قرار بگیرد.** البته، اگر داده‌های رمزنگاری‌شدهٔ شما بر روی یک لپ‌تاپ باشد، مجبورید رسانهٔ جداشدنی پشتیبان را همواره با خود داشته باشید تا بتوانید به داده‌های خود دسترسی پیدا کنید. در نتیجه، اگر کسی لپ‌تاپ شما و گذرواژهٔ حساب شما را بدزدد داده‌های شما را نخواهد توانست که دستیابی کند.

پس از صدور گواهینامه، رسانهٔ خارج‌شدنی خود را بررسی کنید و اطمینان یابید که فایل حاوی گواهینامه در آنجا عملاً حاضر و سالم است، سپس این رسانه را از کامپیوتر جدا کنید. Certificate Manager را باز کنید (روی دکمهٔ Start کلیک کنید، و عبارت **certmgr.msc** را در کادر Search در پایین منو تایپ کنید). در بخش دست چپ، مورد Personal را باز کنید و روی Certificates کلیک کنید تا نام کاربری خود را در سمت راست ببینید (جایی است که گواهینامه‌ای که ساخته‌اید در آن قرار دارد). روی نام کاربری خود کلیک-راست کنید و Delete را انتخاب کنید.



نگران نباشید و روی Yes کلیک کنید، چون گواهینامه بر روی رسانهٔ جداشدنی شما موجود است.

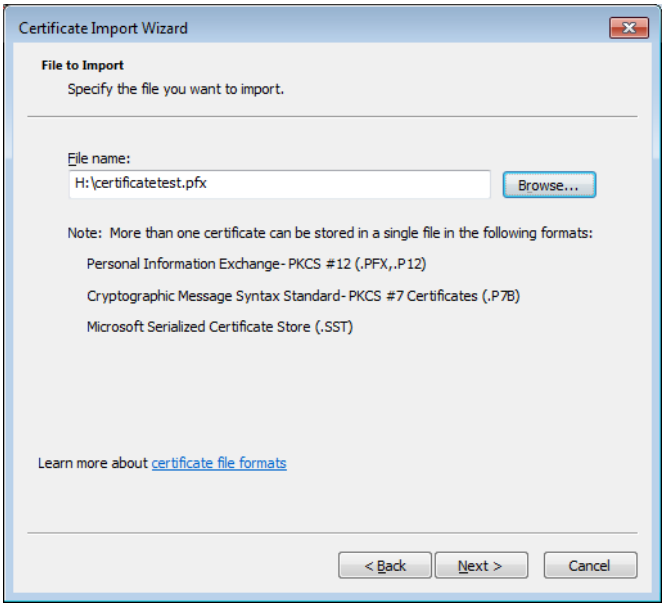
حال، از Windows Explorer برای مرور پوشهٔ رمزنگاری‌شدهٔ خود بهره بگیرید. **ویندوز۷** این پوشه و فایل‌های آن را به رنگ سبز نمایش می‌دهد. اگر بخواهید هر یک از فایل‌ها را باز کنید، یک پنجره به نمایش در می‌آید که به شما می‌گوید که اجازهٔ این کار را ندارید.

این پیام هشدار به معنی آن است که کامپیوتر شما برای رمزگشایی فایل‌ها حاوی گواهینامه متناظر با نام کاربری شما نیست. لازم است که گواهینامه‌ای را که به رسانهٔ جداشدنی صادر کرده‌اید برای سیستم خود بازگردانی کنید.

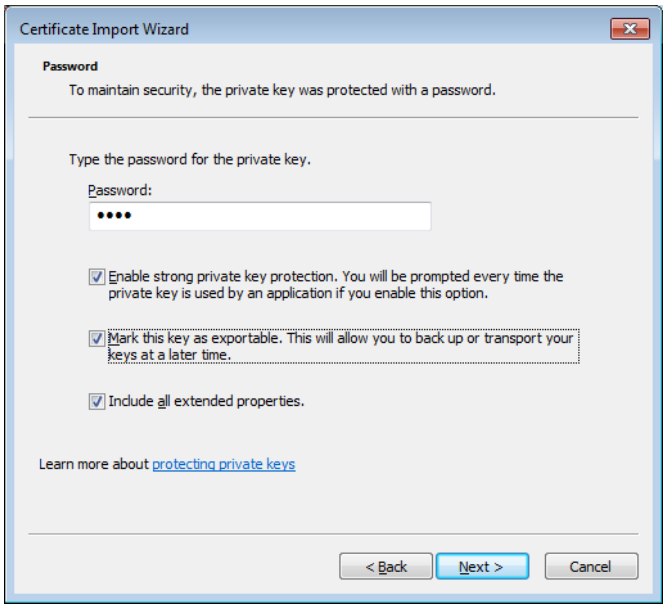
برای این کار، رسانهٔ جداشدنی را به کامپیوتر خود وصل کنید (یا اگر دیسک باشد در دیسکران قرار دهید)، Certificate Manager را

باز کنید، و روی مورد Personal در بخش دست چپ کلیک–راست کنید. All Tasks | Import را برای بارکردن Certificate Import Wizard انتخاب کنید.

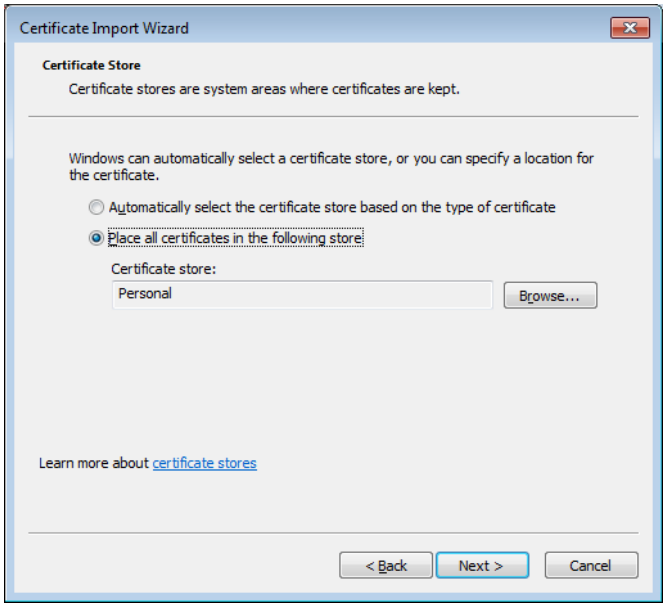
روی Next کلیک کنید و فایل حاوی گواهینامه را در رسانهٔ جداشدنی خود بیابید (در پنجره‌ای که به نمایش در می‌آید نوع فایل پیش‌فرض مورد استفاده CER و CRT است، در نتیجه، روی پیکان «file types» کلیک کنید و نوع فایل PFX را انتخاب کنید). فایل صادرشدهٔ خود را انتخاب کنید و روی Open کلیک کنید.



روی Next کلیک کنید، گذرواژه‌ای را که برای این فایل اختصاص داده‌اید تایپ کنید و روی Next کلیک کنید.



در صفحهٔ Certificate Store، برای بازگرداندن گواهینامه به ناحیهٔ حساب شخصی خود، انتخاب پیش‌فرض را بپذیرید.



روی Next کلیک کنید و سپس روی Finish کلیک کنید. به Windows Explorer بازگردید و فایل داده‌ای خود را باز کنید.

اگر اجرای عملیات رمزنگاری، با عمل حذف گواهینامه‌ها از دیسک‌سخت و بازگردانی گواهینامه‌ها از رسانهٔ جداشدنی همراه شود فایل‌های داده‌ای خصوصی خود را همواره می‌توانید خصوصی نگه دارید. **اما حتماً گواهینامهٔ خود را در دو یا سه رسانهٔ مجزا پشتیبان‌گیری کنید تا اطمینان یابید که اگر یکی از رسانه‌ها خراب یا گم شود بازهم خواهید توانست داده‌های‌تان را دستیابی کنید.**□