مرکز صدور گواهی الکترونیکی پارس‌ساین

راهنمای استفاده از گواهی الکترونیکی در نرم‌افزار

Microsoft Office Word 2007

تدوین‌کننده: شرکت امن‌افزار گستر شریف

شمارهٔ سند.....SSW_UG_PKI_91105_1

تاریخ..... ۰۵/مهر/۱۳۹۱

نگارش.....۱.۲

آدرس: تهران، خیابان آزادی، خیابان حبیب‌الله، خیابان قاسمی غربی، شمارهٔ ۳۷، طبقه پنجم

تلفن: ۲۰-۶۱۹۷۵۵۰۰ (۰۲۱) **فاکس**: ۶۶۰۹۰۲۹۹ (۰۲۱) **سایت اینترنتی**: www.parssignca.ir

حق طبع و نشر

فهرست مطالب

۱ مقدمه

نرم‌افزار Microsoft Word یکی از محبوب‌ترین واژه‌پردازها برای نوشتن اسناد می‌باشد. با استفاده از گواهی الکترونیکی می‌توان اسنادی که با استفاده از این نرم‌افزار تدوین می‌شود را امضای دیجیتال نمود. با این کار، موارد زیر تضمین می‌شود:

- **اصالت سند**[1]: با استفاده از امضای دیجیتال روی سند، می‌توان اطمینان حاصل نمود که سند تنها توسط فرد مورد نظر (یعنی امضاکننده) امضا شده است نه فرد دیگر.
- **عدم انکار**[2]: با استفاده از امضای دیجیتال روی سند، می‌توان اثبات نمود که سند توسط چه فردی امضا شده است؛ به عبارت دیگر، امضاکننده‌ی یک سند، نمی‌تواند امضای سند توسط وی را انکار نماید.
- **تمامیت**[3]: با استفاده از امضای دیجیتال می‌توان اطمینان حاصل نمود که یک سند پس از امضای آن تغییر داده نشده است؛ زیرا در صورت هرگونه تغییر در محتوای سند پس از امضای آن، امضای روی سند نامعتبر می‌گردد.

در این سند، نحوه استفاده از گواهی الکترونیکی در نرم‌افزار Microsoft Word 2007 را تشریح می‌کنیم.

۲ فرضیات این سند

در این سند، نحوه استفاده از گواهی الکترونیکی، بر اساس سناریوی فرضی زیر در نظر گرفته شده است:

«نام مالک گواهی، نام فرضی PKI_Tester است که از یک مرکز میانی صدور گواهی الکترونیکی فرضی به نام ParsSign Online CA 3 یک "گواهی الکترونیکی امضا" با سطح اطمینان یک دریافت نموده است. مرکز ریشه گواهیِ مرکزِ ParsSign Online CA 3، مرکز فرضی ParsSign ROOT CA می‌باشد. در اینجا، مالک گواهی PKI_Tester از گواهی خود برای امضای یک سند تدوین‌شده با نرم‌افزار Microsoft Word 2007 استفاده می‌نماید.»

بنابراین، خواننده به منظور استفاده از این سند در سناریوی واقعی، باید به موارد زیر دقت نماید:

[1] Authenticity
[2] Non-repudiation
[3] Integrity

- نام صادرکننده گواهی، به جای "ParsSign Online CA 3" مرکز "ParsSign Private Intermediate Bronze CA -G2" می‌باشد؛ یعنی فیلد Issuer گواهی، مقدار "ParsSign Private Intermediate Bronze CA -G2" دارد.
- نام صادرکننده گواهیِ مرکز صدور گواهی، به جای "ParsSign ROOT CA" مرکز "Islamic Republic of Iran Root CA" می‌باشد؛ یعنی فیلد Issuer این گواهی، مقدار "Islamic Republic of Iran Root CA " باشد.
- در سناریوی واقعی به جای PKI_Tester، نام فرد مالک گواهی الکترونیکی ذکر می‌گردد؛ یعنی نامی که در فیلد Subject گواهی قید شده است.

از این‌رو، برای استفاده از این سند در سناریوی واقعی، در ادامه سند، به جای "ParsSign Online CA 3" باید "ParsSign Private Intermediate Bronze CA -G2"، به جای "ParsSign ROOT CA" باید "Islamic Republic of Iran Root CA"، و به جای PKI_Tester باید نام مالک گواهی را مشاهده نمایید.

۳ مراحل پیش‌نیاز

قبل از استفاده از یک گواهی در نرم‌افزار Word 2007 باید مراحل زیر را انجام دهیم:

۱. **نصب گواهی‌های الکترونیکی مراکز صدور گواهی روی سیستم؛**
۲. **نصب راه‌انداز[1] توکن پارس‌کی (در صورت نیاز)؛**
۳. **نصب فراهم‌کننده‌ی سرویس رمزنگاری[2] پارس‌کی (ParsKey CSP).**

برای امضا نمودن اسناد Word، مراحل سه‌گانه فوق الزامی می‌باشد، اما برای بررسی صحت امضای اسناد در نرم‌افزار Word، تنها مرحله اول الزامی بوده و نیازی به مراحل دوم و سوم نمی‌باشد.

۳-۱ نصب گواهی‌های الکترونیکی مراکز صدور گواهی روی سیستم

به منظور استفاده از یک گواهی الکترونیکی صادرشده توسط مرکز صدور گواهی الکترونیکی پارس‌ساین، باید گواهی الکترونیکی این مرکز و گواهی الکترونیکی مرکز دولتی صدور گواهی الکترونیکی ریشه را

[1] Driver
[2] Cryptography Service Provider (CSP)

دریافت و روی سیستم نصب نماییم. برای آگاهی از نحوه انجام این کار، به سند "راهنمای نصب گواهی‌های الکترونیکی مراکز صدور گواهی در سیستم‌عامل ویندوز" مراجعه نمایید.

۳-۲ نصب راه‌انداز توکن پارس‌کی

در این سند فرض بر این است که گواهی الکترونیکی و زوج کلید خصوصی مالک گواهی (کاربر)، روی توکن سخت‌افزاری پارس‌کی ذخیره شده است.

- در صورتی که از توکن‌های سری B پارس‌کی (جدیدترین سری توکن پارس‌کی) استفاده می‌نماییم، نیازی به نصب راه‌انداز توکن نمی‌باشد.
- در صورتی که از توکن‌های سری A پارس‌کی استفاده می‌نماییم، برای استفاده از توکن ابتدا باید راه‌انداز آن را روی سیستم نصب نماییم. برای آگاهی از نحوه نصب راه‌انداز توکن پارس‌کی به سند "راهنمای نصب راه‌انداز توکن پارس‌کی" مراجعه نمایید.

۳-۳ نصب فراهم‌کننده سرویس رمزنگاری پارس‌کی

به منظور استفاده از توکن پارس‌کی در نرم‌افزار Word، باید فراهم‌کننده سرویس رمزنگاری پارس‌کی روی سیستم نصب گردد. برای آگاهی از نحوه نصب این نرم‌افزار به سند "راهنمای نصب فراهم‌کننده سرویس رمزنگاری پارس‌کی" مراجعه نمایید.

۴ استفاده از گواهی الکترونیکی در نرم‌افزار Word 2007

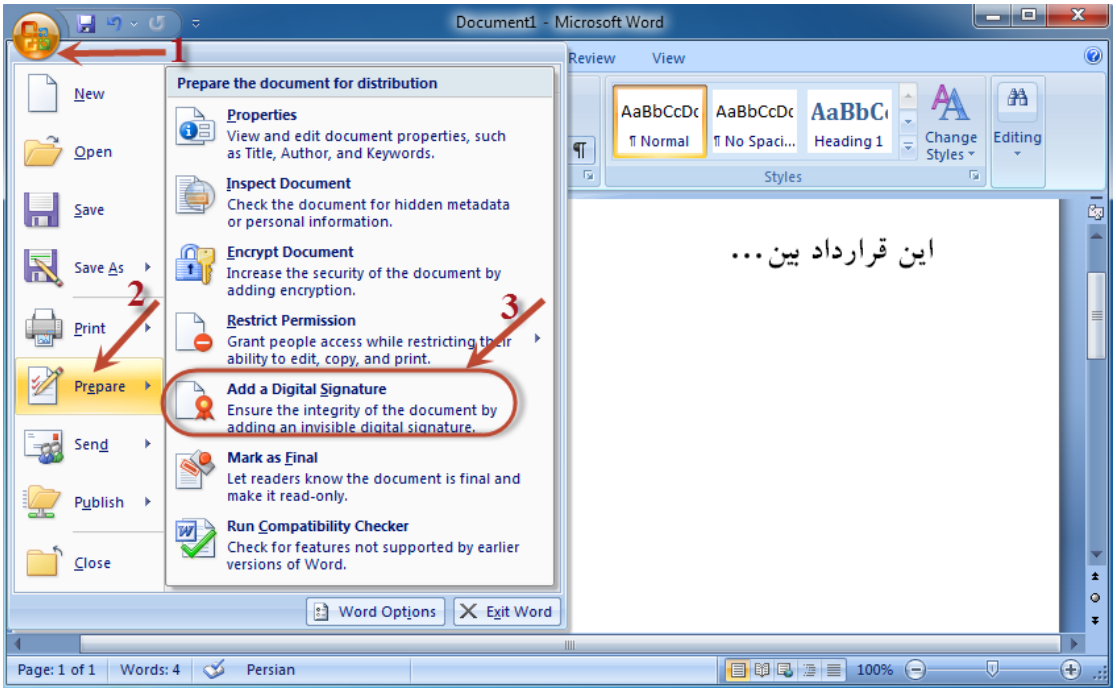
در نرم‌افزار Word 2007 از کلید خصوصی ذخیره‌شده روی توکن، به منظور امضای سند استفاده می‌شود؛ در واقع، سند با استفاده از کلید خصوصی متناظر با گواهی امضا می‌گردد.

۴-۱ امضای سند

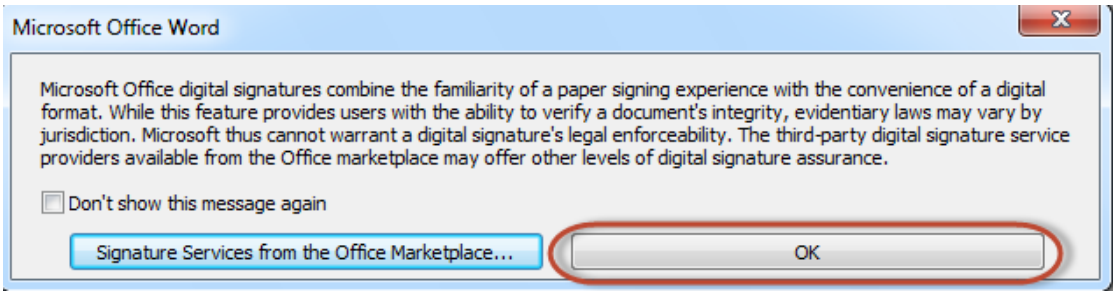
مراحل امضای یک سند در نرم‌افزار Word 2007 به صورت زیر می‌باشد:

۱. متن سند مورد را در نرم‌افزار Word می‌نویسیم.
۲. پس از اتمام نگارش متن، توکن خود را به درگاه USB سیستم متصل می‌نماییم.

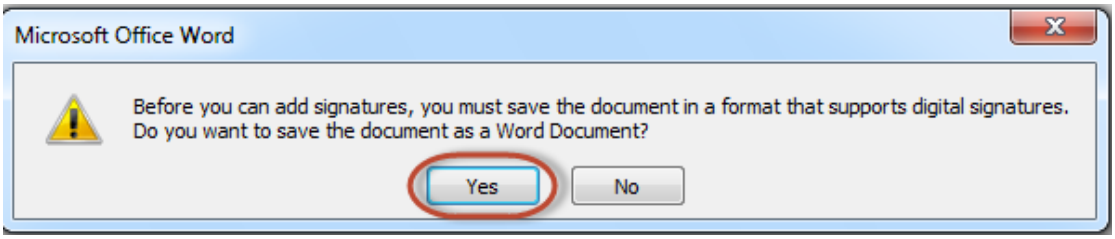
۳. مانند شکل زیر، روی دکمه Office کلیک می‌نماییم. سپس از منوی Prepare، گزینه Add a Digital Signature را انتخاب می‌نماییم.



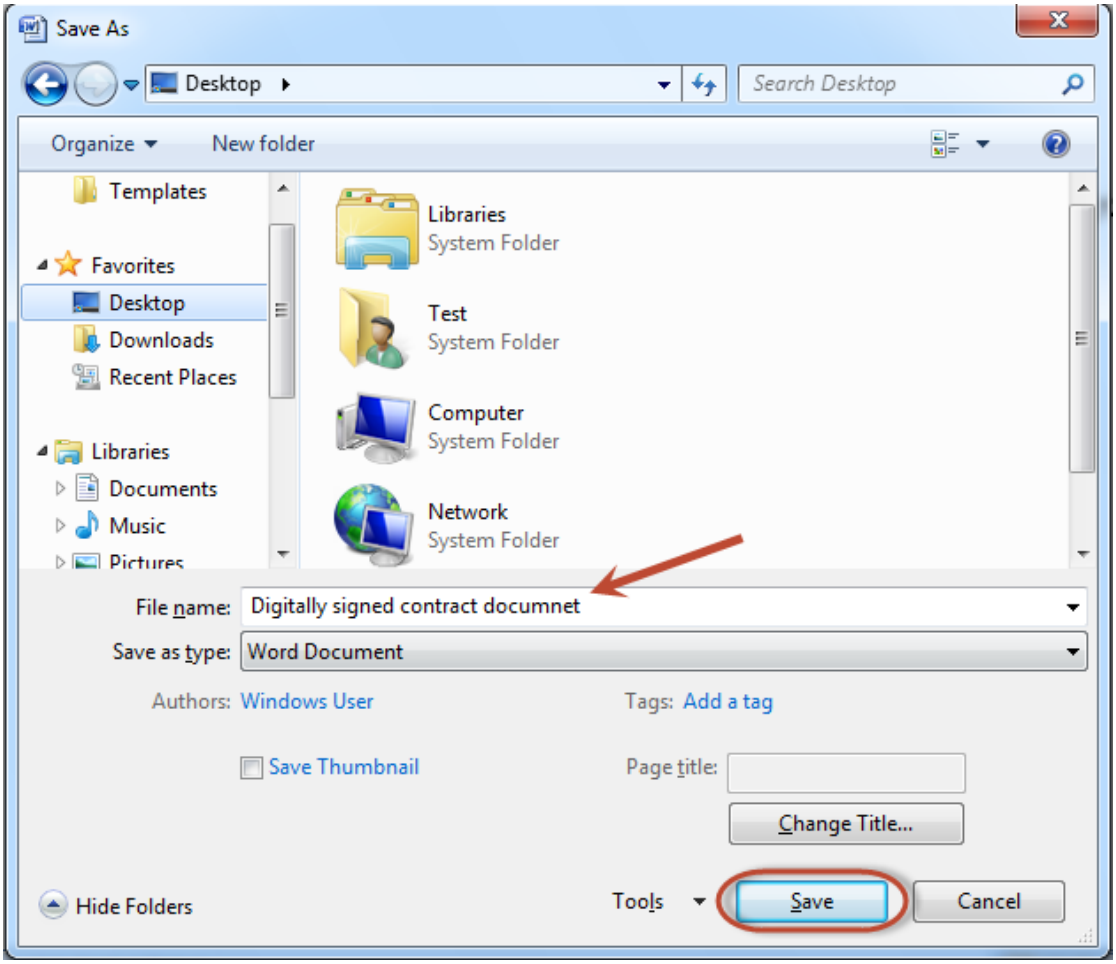
۴. در پنجره ظاهرشده (شکل زیر)، روی دکمه OK کلیک می‌نماییم.



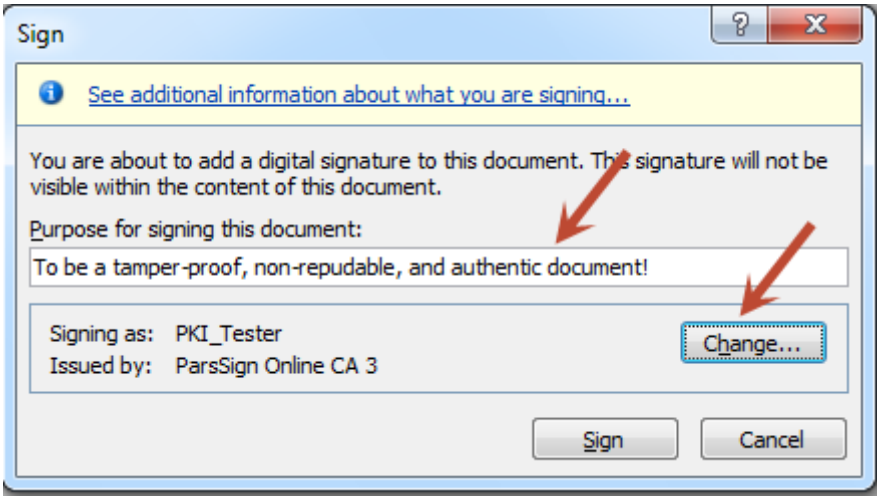
۵. قبل از امضای یک سند، باید آن را در فرمتی ذخیره نماییم که از امضای دیجیتال پشتیبانی نماید. برای این منظور، پس از مرحله قبل، پنجره زیر ظاهر می‌گردد که در آن روی دکمه YES کلیک می‌نماییم.



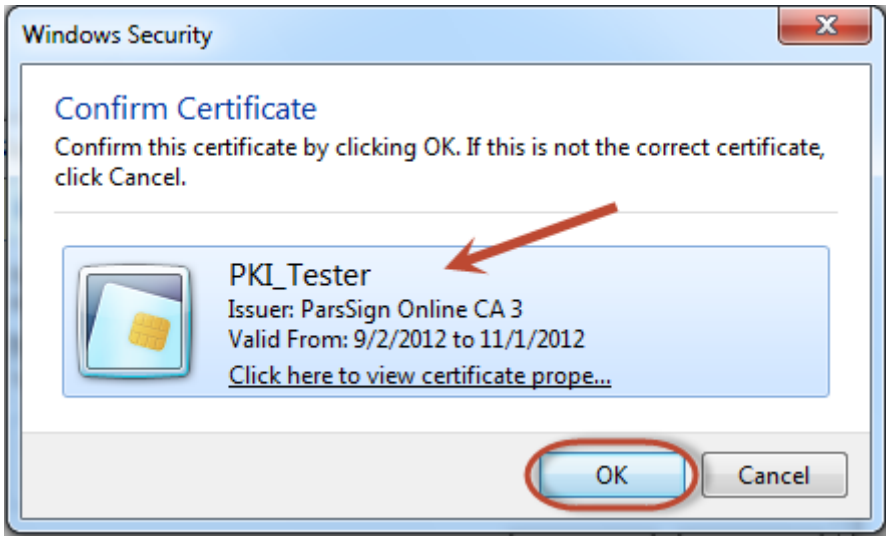
۶. در پنجره ظاهرشده (شکل زیر)، محل ذخیره‌سازی و نامی دلخواه برای سند امضاشده مشخص نموده و روی دکمه Save کلیک می‌نماییم.



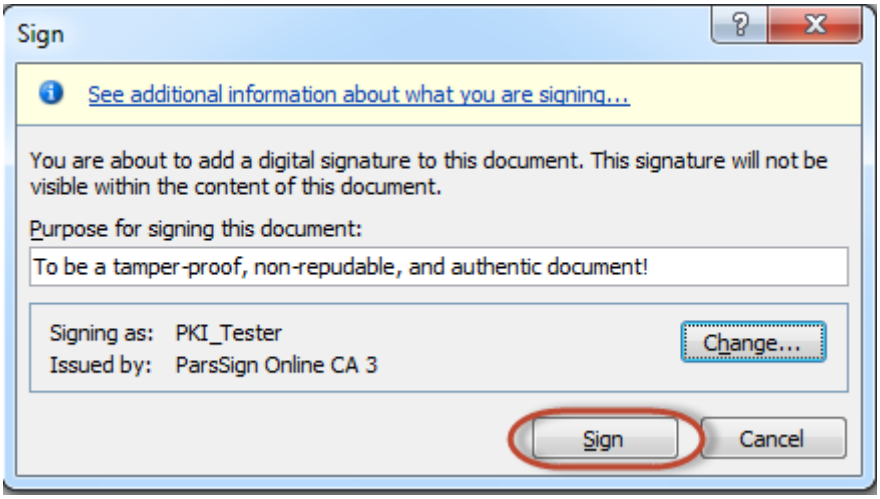
۷. در پنجره ظاهرشده (شکل زیر)، متنی دلخواه را به عنوان دلیل امضای سند وارد می‌کنیم. دقت کنید، این متن در زمان بررسی صحت امضا، به عنوان دلیل امضای سند ظاهر می‌گردد.



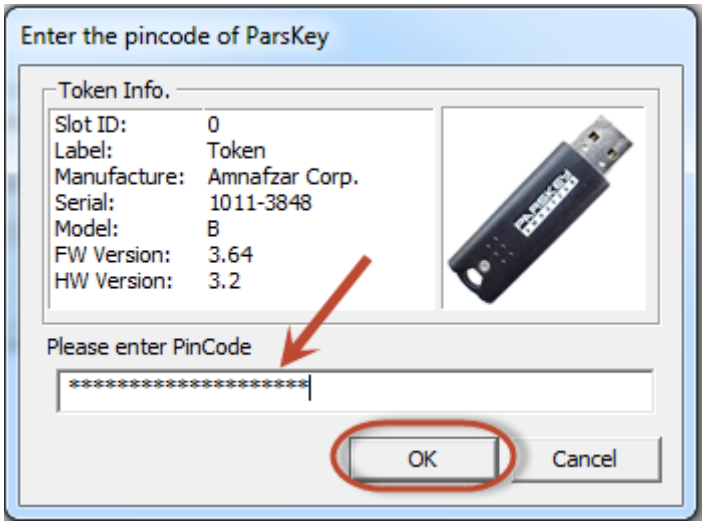
در این پنجره، گواهی الکترونیکی پیش‌فرض جهت امضا نمایش داده شده است. در صورت تمایل به استفاده از گواهی دیگر، روی دکمه Change کلیک می‌نماییم تا کادر محاوره‌ای انتخاب گواهی (شکل زیر) ظاهر شده و گواهی مورد نظر را انتخاب نماییم. در این کادر، تمام گواهی‌هایی که کلید خصوصی متناظر آن‌ها در توکن وجود دارد نمایش داده می‌شود؛ گواهی مورد نظر را انتخاب نموده و روی دکمه OK کلیک می‌نماییم (دقت کنید، در مثال ما در شکل زیر، تنها یک گواهی در توکن وجود دارد).



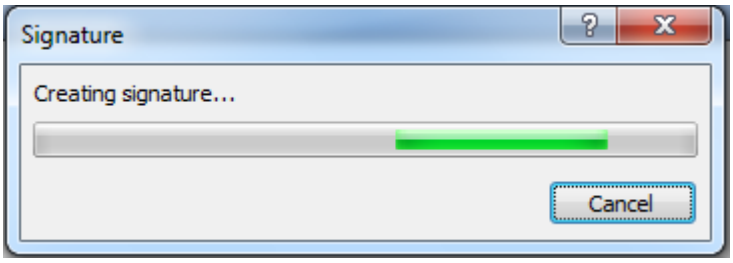
۸. پس از انتخاب گواهی، در شکل زیر روی دکمه Sign کلیک می‌نماییم.



۹. در پنجره ظاهرشده (شکل زیر)، پین‌کد توکن را وارد نموده و روی دکمه OK کلیک می‌نماییم.

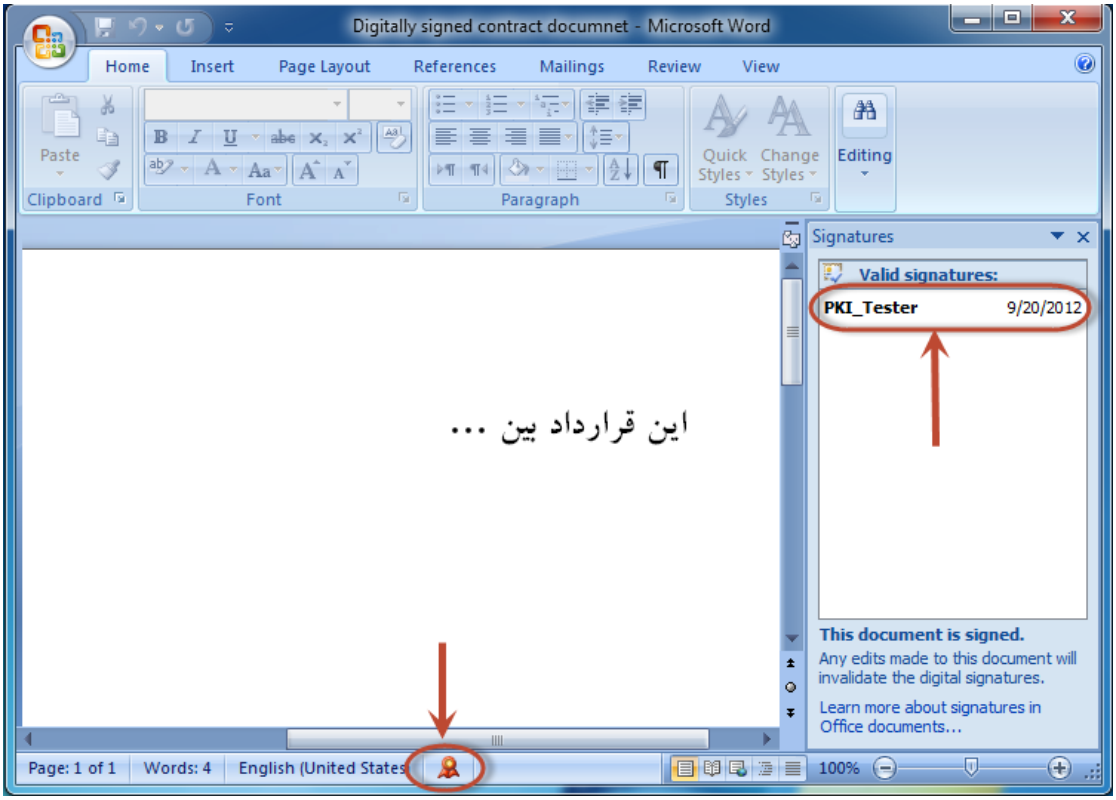


۱۰.پس از مرحله قبل، پنجره زیر ظاهر می‌گردد که نشاندهنده فرایند امضای سند می‌باشد. بستگی به حجم سند امضاشونده، فرایند امضای سند ممکن است اندکی طول بکشد.



۱۱.پس از اتمام موفق عملیات امضا، پیام زیر ظاهر می‌گردد که در آن روی دکمه OK کلیک می‌نماییم.

۱۲.پس از اتمام عملیات امضا، آیکن امضا در نوار پایین سند ظاهر می‌شود (مانند شکل زیر).



۱۳.با کلیک‌کردن روی آیکن امضا، پنل امضا در سمت راست سند ظاهر می‌شود (مانند شکل بالا) که در آن می‌توان گواهی امضاکنندگان این سند را مشاهده نمود.

نکته: یک سند می‌تواند توسط چندین فرد امضا گردد. رویه امضای چندگانه، شبیه مراحل فوق می‌باشد، بدین ترتیب که در هر مرحله، از گواهی یکی از افراد برای امضای سند استفاده می‌گردد.

توجه: پس از امضای یک سند، آن سند غیر قابل ویرایش می‌گردد. جهت ویرایش مجدد سند، امضای آن باید حذف شود (برای این منظور، به بخش ۴-۳ مراجعه نمایید).

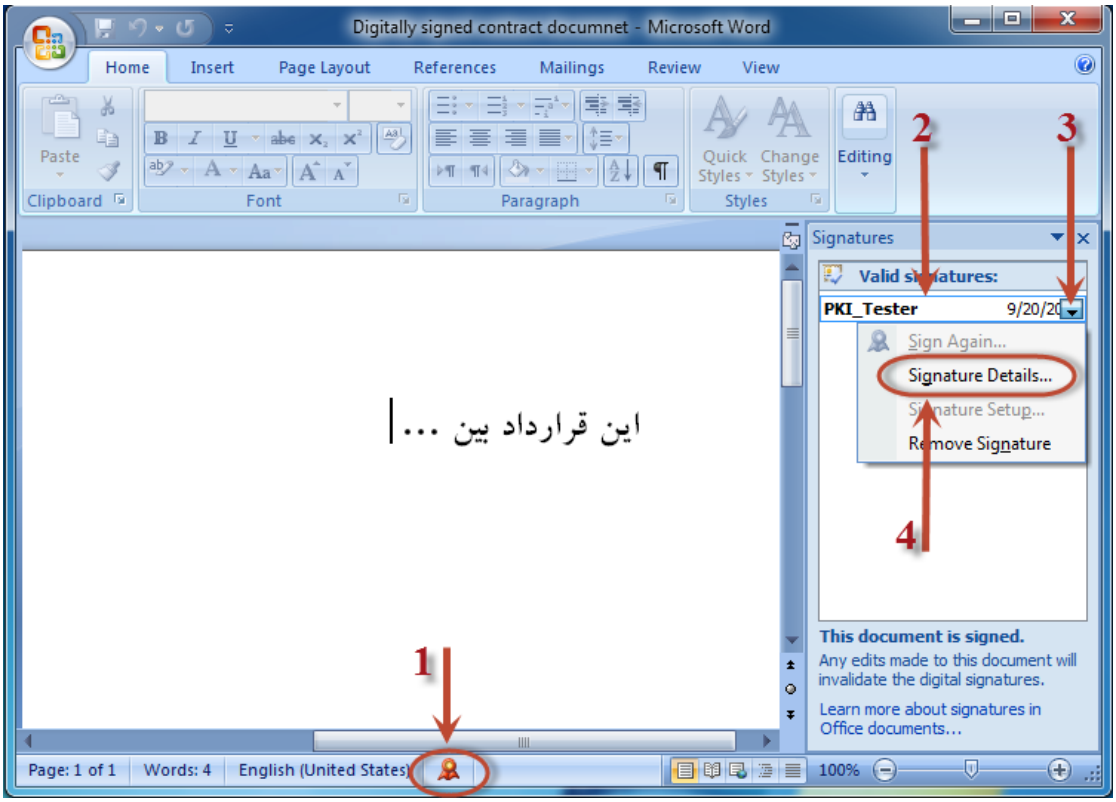
۲-۴ بررسی صحت امضای سند

وقتی یک سند امضاشده در اختیار داریم، برای بررسی صحت امضای آن به صورت زیر عمل می‌نماییم:

۱. سند مورد نظر را توسط نرم‌افزار Word باز می‌نماییم.

۲. مانند شکل زیر، در نوار پایین سند، روی آیکن امضا کلیک می‌نماییم.

۳. در پنل امضای بازشده در سمت راست سند، روی نام امضاکننده کلیک نموده و در لیست بازشونده‌ی آن، روی گزینه Signature Details کلیک می‌نماییم.



۴. در پنجره ظاهرشده (شکل زیر)، جزئیات امضا از جمله صحت آن نشان داده شده است. برای نمونه، شکل زیر نشان‌دهنده صحت امضای روی سند است. برای بررسی گواهی فرد امضاکننده می‌توانیم روی دکمه View کلیک نماییم. برای بررسی جزئیات امضا می‌توانیم روی See the additional signing information that was collected کلیک نماییم. در پایان، روی دکمه Close کلیک می‌نماییم.

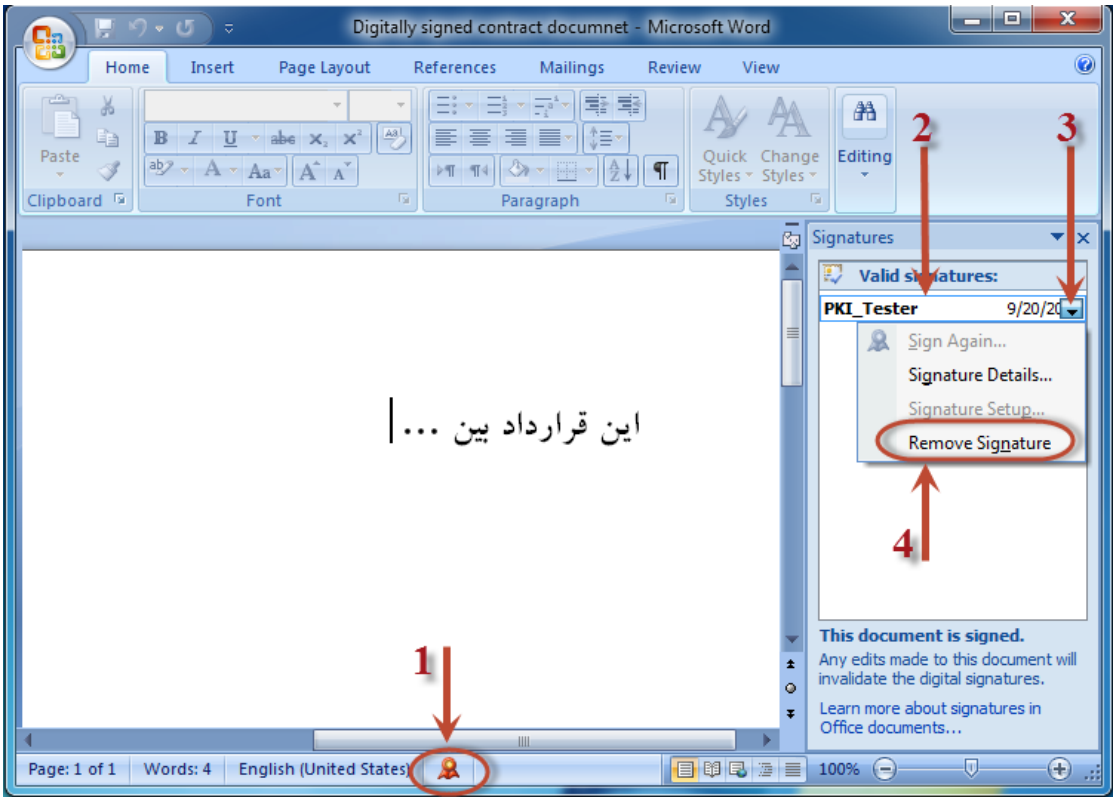
۳-۴ حذف امضای سند

توجه: عمل حذف امضای سند، عملی برگشت‌ناپذیر است و با حذف یک امضا در نرم‌افزار Word، نمی‌توان عملیات حذف امضا را خنثی (Undo) نمود.

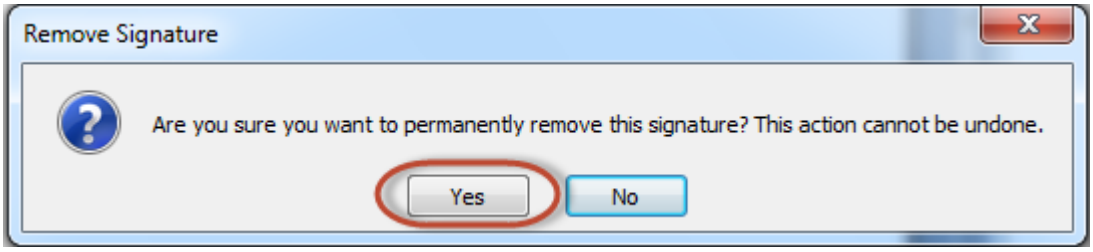
برای حذف امضا باید به صورت زیر عمل نماییم:

۱. سند مورد نظر را توسط نرم‌افزار Word باز می‌نماییم.

۲. مانند شکل زیر، در نوار پایین سند، روی آیکن امضا کلیک می‌نماییم. در پنل امضای بازشده در سمت راست، روی نام امضاکننده کلیک نموده و در لیست بازشونده‌ی آن، روی Remove Signature کلیک می‌نماییم.



۳. در پنجره بازشده (شکل زیر)، در صورت کلیک روی دکمه Yes، امضای روی سند حذف می‌گردد.



۴. پیام زیر مبنی بر حذف موفق امضای سند ظاهر می‌گردد. در پایان، روی دکمه OK کلیک می‌نماییم.