

مركز صدور گواهی الكترونيکی پارسساين

# راهنمای استفاده از گواهی الکترونیکی در نرمافزار

## **Microsoft Office Word 2007**

**تدوینکنندہ**: شرکت امنافزار گستر شریف

SSW_UG_PKI_91	شىمارەً سىند1_105
۵۰/مهر / ۱۳۹۱	تاريخ
۱.۲	نگارش

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

تلفن: ۲۰–۶۱۹۷۵۵۰ (۲۱) فاکس: ۶۶۰۹۰۲۹۹ (۲۱۰) سایت اینترنتی: www.parssignca.ir

#### حق طبع و نشر

این سند در تاریخ ۱۳۹۱/۰۶/۱۳ توسط شرکت امنافزار گستر شریف به منظور تهیهٔ بخشی از اسناد «مرکز صدور گواهی الکترونیکی پارسساین» تدوین گردیده است. تمامی حقوق این اثر متعلق به «شرکت امنافزار گستر شریف» میباشد و هرگونه نسخهبرداری از آن، اعم از کپی، نسخهبرداری الکترونیکی و یا ترجمهٔ تمام یا بخشی از آن منوط به کسب اجازهٔ کتبی از صاحب اثر است.

فهرست مطالب		
	مقد	۱
ضيات اين سند	فرظ	۲
حل پیش نیاز	مرا	٣
نصب گواهیهای الکترونیکی مراکز صدور گواهی روی سیستم۲	۳_۱	,
نصب راهانداز توکن پارسکی	۲-۳	,
نصب فراهمکننده سرویس رمزنگاری پارس کی	۳–۳	,
نفاده از گواهی الکترونیکی در نرمافزار WORD 2007۳	است	۴
امضای سند	1-4	
بررسی صحت امضای سند۹	۲-۴	
حذف امضای سند	۳_۴	

#### 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 : با استفاده از امضای دیجیتال روی سند، می توان اطمینان حاصل نمود که سند تنها توسط فرد مورد نظر (یعنی امضاکننده) امضا شده است نه فرد دیگر.
- عدم انکار<sup>۲</sup>: با استفاده از امضای دیجیتال روی سند، می توان اثبات نمود که سند توسط چه فردی امضا شده است؛ به عبارت دیگر، امضاکنندهی یک سند، نمی تواند امضای سند توسط وی را انکار نماید.
- تمامیت <sup>7</sup>: با استفاده از امضای دیجیتال می توان 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 می گردد.

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 مرکز ParsSign Online CA 3، مرکز فرضی ParsSign ROOT CA میباشد. در اینجا، مالک گواهی PKI\_Tester از گواهی خود برای امضای یک سند تدوین شده با نرمافزار مالک گواهی Microsoft Word 2007

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

<sup>&</sup>lt;sup>1</sup> Authenticity

<sup>&</sup>lt;sup>2</sup> Non-repudiation

<sup>&</sup>lt;sup>3</sup> Integrity

- TerrsSign Online CA 3" مركز "ParsSign Online CA 3" مركز
   تام صادركننده گواهی، به جای "ParsSign Private Intermediate Bronze CA -G2" میباشد؛ یعنی فیلد Issuer گواهی، مقدار
   "ParsSign Private Intermediate Bronze CA -G2" دارد.
- نام صادركننده گواهیِ مركز صدور گواهی، به جای "ParsSign ROOT CA" مركز
   نام صادركننده گواهیِ مركز صدور گواهی، به جای "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 می گردد؛ یعنی نامی که
   در فیلد Subject گواهی قید شده است.

"ParsSign Online CA 3" از این رو، برای استفاده از این سند در سناریوی واقعی، در ادامه سند، به جای "ParsSign ROOT CA" باید باید "ParsSign ROOT CA", به جای "ParsSign Private Intermediate Bronze CA -G2" 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:

- د. نصب گواهی های الکترونیکی مراکز صدور گواهی روی سیستم؛
  - ۲. نصب راهانداز ۲ توکن پارسکی (در صورت نیاز)؛
- ۳. نصب فراهم کننده یسرویس رمزنگاری<sup>۲</sup> پارس کی (ParsKey CSP).

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

## ۱–۳ نصب گواهی های 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

<sup>&</sup>lt;sup>1</sup> Driver

<sup>&</sup>lt;sup>2</sup> Cryptography Service Provider (CSP)

### ۲-۳ نصب راهانداز توکن پارس کی

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 نمی باشد.
- در صورتی که از توکنهای سری A پارس کی استفاده مینماییم، برای استفاده از توکن ابتدا باید راهانداز آن را روی سیستم نصب نماییم. برای آگاهی از نحوه نصب راهانداز توکن پارس کی به سند "راهنمای نصب راهانداز توکن پارس کی" مراجعه نمایید.

## ۳-۳ نصب فراهم کننده سرویس رمزنگاری پارس کی

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.

#### ۱-۴ 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.

© Copyright Amnafzar Co.

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.

Microsoft Office Word	×
Microsoft Office digital signatures combine the familiarity of a pa format. While this feature provides users with the ability to verit jurisdiction. Microsoft thus cannot warrant a digital signature's le providers available from the Office marketplace may offer other	per signing experience with the convenience of a digital y a document's integrity, evidentiary laws may vary by gal enforceability. The third-party digital signature service levels of digital signature assurance.
Don't show this message again	
Signature Services from the Office Marketplace	ОК
ی ذخیره نماییم که از امضای دیجیتال پشتیبانی نماید.	۵. قبل از امضای یک سند، باید آن را در فرمتو
زیر ظاهر میگردد که در آن روی دکمه YES کلیک	برای این منظور، پس از مرحله قبل، پنجره
	مىنماييم.

Microsoft (	Office Word
<u> </u>	Before you can add signatures, you must save the document in a format that supports digital signatures. Do you want to save the document as a Word Document?
	Yes No

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

🗐 Save As			×
🔾 🗢 💻 Deskto	p ►	✓  Search Desktop	٩
Organize 🔻 Nev	v folder		0
👔 Templates	Libraries System Folder		
Desktop			
Downloads	System Folder		E
🖳 Recent Places			
4 ᇘ Libraries	Computer System Folder		
Documents	Network		
Pictures	- System Folder		-
File <u>n</u> ame:	Digitally signed contract documnet		-
Save as <u>t</u> ype:	Word Document		•
Authors: \	Windows User	Tags: Add a tag	
Ū	Save Thumbnail	Page <u>t</u> itle:	
		<u>_</u>	
Alide Folders		Too <u>l</u> s • Save Cano	el

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 می گردد.

Sign	? <mark>x</mark>
See additional information about what you are signing	
You are about to add a digital signature to this document. This sign visible within the content of this document. Purpose for signing this document:	ature will not be
To be a tamper-proof, non-repudable, and authentic document!	
Signing as: PKI_Tester Issued by: ParsSign Online CA 3	Change
Sign	Cancel

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 می شود؛ گواهی مورد نظر را انتخاب نموده و روی دکمه OK کلیک می نماییم (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.

Sign		? ×
See add	ditional information about wha	at you are signing
You are abou visible within	t to add a digital signature to the content of this document.	this document. This signature will not be
Purpose for s	igning this document:	
To be a tamp	er-proof, non-repudable, and	d authentic document!
Signing as:	PKI_Tester	Change
Issued by:	ParsSign Online CA 3	
		Sign Cancel

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

E	nter the pincod	e of ParsKe	у			
Γ	- Token Info					
	Slot ID: Label: Manufacture: Serial: Model: FW Version: HW Version:	0 Token Amnafzar C 1011-3848 B 3.64 3.2	orp.		- Start	
	Please enter Pir	nCode 🖌				
	********	*******				
	,		$\subset$	ОК	Ca	ncel

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

Signature	? ×
Creating signature	
	Cancel

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





١٢. پس از اتمام عمليات امضا، آيكن امضا در نوار پايين سند ظاهر مي شود (مانند شكل زير).

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 می تواند 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 می گردد.

**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 می توانیم روی دکمه View کلیک نماییم. برای بررسی جزئیات امضا می توانیم روی See the additional signing information that was collected کلیک نماییم. در پایان، روی دکمه Close

Signature Details
Valid signature - This signature and the signed content have not been modified since the signature was applied.
Purpose for signing this document: To be a tamper-proof, non-repudable, and authentic documnet!
Signing as: PKI_Tester Issued by: ParsSign Online CA 3
See the additional signing information Close

#### ۴-۳ حذف امضای سند

**توجه**: عمل حذف امضای سند، عملی برگشتناپذیر است و با حذف یک امضا در نرمافزار Word، نمی توان 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 می نماییم. در پنل امضای بازشده در سمت راست، روی نام امضاکننده کلیک نموده و در لیست بازشوندهی آن، روی Remove Signature کلیک می نماییم.



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

Remove Signature	٢.
Are you sure you want to permanently remove this signature? This action cannot be undon	e.
Yes No	

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

Signature	Removed
1	The signature has been removed and the document has been saved.
	ОК