

مركز صدور گواهى الكترونيكى پارسساين

# راهنمای استفاده از گواهی الکترونیکی در نرمافزار PuTTY

**تدوینکنندہ**: شرکت امنافزار گستر شریف

ىمارە سىند SSW_UG_PKI_91160_1	ش
<b>ریخ</b> ۱۳۹۲/فروردین /۱۲	تا
ئارش	نگ

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

تلفن: ۲۰–۸۱۷۵۵۰۰ (۲۱۱) فاکس: ۶۶۰۹۰۲۹۹ (۲۱۰) سایت اینترنتی: www.parssignca.ir

## حق طبع و نشر

این سند در تاریخ ۱۳۹۱/۰۸/۰۳ توسط شرکت امنافزار گستر شریف به منظور تهیهٔ بخشی از اسناد «مرکز صدور گواهی میانی پارس ساین» 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

۱	مقدمه	۱
۲	فرضيات سند	۲
۲	نحوه استفاده از نرمافزار PUTTY SC	٣
۲	۳–۱ تنظیمات نرمافزار PuTTY SC	
۴	۳–۲ تنظیمات سرور	
۶	نحوه استفاده از نرمافزار PUTTY-CAC	۴
۶	۴-۱ تنظیمات نرمافزار PuTTY-CAC	
۶	۴−۱−۱ استفاده از کتابخانه PKCS #11	
۸	۲-۱-۴ استفاده از کتابخانه CAPI	
١٠	۴–۲ تنظیمات سرور	
•••	برقراری ارتباط SSH با استفاده از توکن	۵

#### ۱ مقدمه

PuTTY، نرمافزاری سبک و در عین حال قدرتمند است؛ از این نرمافزار برای اتصال از راه دور به سیستم از طریق پروتکلهای Telent، SSH و Rlogin استفاده می شود. یکی از کاربردهای مهم نرمافزار، اتصال از راه دور به سیستم از طریق SSH می باشد. در کاربرد عادی نرمافزار هنگام اتصال SSH به سیستم، احراز هویت بر اساس گذرواژه انجام می شود. مکانیزمی امن تر از مکانیزم گذرواژه، احراز هویت دو فاکتوره <sup>۲</sup> مبتنی بر کلید عمومی است که در آن، علاوه بر گذرواژه از یک سخت افزار به نام توکن امنیتی<sup>۳</sup> نیز استفاده می شود. در زیر، مکانیزم احراز هویت دو فاکتوره با مکانیزم احراز هویت مبتنی گذرواژه مقایسه شده است:

- در احراز هویت مبتنی بر گذرواژه، امنیت سیستم تنها وابسته به یک فاکتور یعنی گذرواژه میباشد.
   اگر گذرواژه افشا شود (مثلاً حمله کننده ای با استفاده از حمله Brute-force آن را به دست آورد)،
   امنیت سیستم به مخاطره می افتد.
- در احراز هویت دو فاکتوره، برای دسترسی به سیستم، علاوه بر گذرواژه باید توکن نیز وجود داشته باشد. به عبارت دیگر، اگر گذرواژه افشا یا توکن سرقت شود، حمله کننده با در اختیار داشتن یکی از این دو نمی تواند به سیستم دسترسی داشته باشد. از این رو، امنیت سیستم وابسته به دو فاکتور می باشد؛ گذرواژه و توکن.
- در احراز هویت دو فاکتوره، گذرواژه دسترسی به کلید خصوصی روی توکن، روی سرور یا کلاینت ذخیره نمی شود (تنها چیزی که روی سرور ذخیره می شود، کلید عمومی است که افشای آن هیچ مخاطره امنیتی ندارد)، از اینرو احتمال افشای گذرواژه کم است. در حالی که در احراز هویت مبتنی بر گذرواژه، گذرواژه در سرور ذخیره می شود که احتمال به مخاطره افتادن آن وجود دارد.
- در احراز هویت مبتنی بر گذرواژه، به ازای هر سیستم باید یک گذرواژه به خاطر بسپاریم (زیرا انتخاب یک گذرواژه برای تمام سیستمها به لحاظ امنیتی توصیه نمی شود و با افشای گذرواژه در یک سیستم، امنیت سیستمهای دیگر نیز به خطر می افتد). علاوه بر این، مدیریت گذرواژه ها نیز در آن دشوار است و با افزایش تعداد سیستمها و کاربران، این کار دشوارتر نیز می شود. در حالیکه در احراز هویت دو

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

<sup>&</sup>lt;sup>2</sup> Two-factor authentication

<sup>&</sup>lt;sup>3</sup> Security Token

فاکتوره، چنین الزامی وجود نداشته و با استفاده یک گذرواژه می توان به هر تعداد دلخواهی سیستم ارتباط SSH برقرار کرد (زیرا گذرواژه روی سرور یا کلاینت ذخیره نمی شود). در این سند، نحوه از استفاده از نرمافزار PuTTY و برقراری ارتباط SSH با استفاده از احراز هویت دوفاکتوره را شرح می دهیم. برای استفاده از احراز هویت دو فاکتوره، باید از نرمافزار PuTTY SC استفاده گردد. تنها تفاوت SC PuTTY با PuTTY مقابلیت پشتیبانی از توکن است. نرمافزار PuTTY-CAC، نیز عملکردی مشابه PuTTY SC دارد (احراز هویت دو فاکتوره با استفاده از توکن)، با این تفاوت که

PuTTY-CAC علاوه بر پشتیبانی از کتابخانه PKCS #11، از PKCS علاوه بر پشتیبانی از CAPI) Microsoft's Cryprographic API) نیز پشتیبانی میکند. در ادامه نحوه استفاده از هر دو نرمافزار توضیح داده می شود.

## ۲ فرضیات سند

در این سند، فرضیات زیر در نظر گرفته شده است:

- سیستمعامل سروری که میخواهیم روی آن SSH کنیم، CentOS میباشد.
  - برچسب توکنی که در مثالها استفاده مینماییم، My\_Token میباشد.
  - برچسب گواهی که در مثالها استفاده مینماییم، PKI\_Tester میباشد.

# ۳ نحوه استفاده از نرمافزار PuTTY SC

- مراحل انجام كار به صورت زير ميباشد:
  - ۱. تنظیمات نرمافزار PuTTY SC؛
    - ۲. تنظیمات سرور.

# PuTTY SC تنظیمات نرمافزار ۱-۳

تنظیمات نرمافزار به صورت زیر میباشد:

۱. دانلود نرمافزار PuTTY SC: برای دانلود نرمافزار به آدرس زیر مراجعه نمایید:

http://www.joebar.ch/puttysc/

- ۲. دانلود کتابخانه ۹۱۱ PKCS پارس کی: برای استفاده از توکن پارس کی در نرمافزار PKCS، باید کتابخانه ۹۱۱ PKCS توکن به نرمافزار معرفی گردد. برای دانلود این کتابخانه به بخش "دانلود" از سایت مرکز میانی پارس ساین به آدرس www.parssignca.ir مراجعه نمایید.
   توجه: در صورتی که نرمافزار ParsKey Utility روی سیستم نصب باشد، این کتابخانه در مسیر /System32 موجود بوده و نیازی به دانلود آن نیست.
- ۳. تنظیمات اتصال SSH همانند تنظیمات عادی PuTTY، در صفحه اصلی نرمافزار (بخش Session)، آدرس IP سرور و شماره درگاه<sup>۱</sup> SSH را وارد مینماییم. در شکل زیر، ۱۹۲.۱۶۸.۲۰۰ آدرس IP سرور و ۲۲ شماره درگاه SSH میباشد.

Reputty Configuration	×
Category: Session Logging Teminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Colours Connection Proxy Telnet Rlogin SSH Serial	Basic options for your PuTTY session         Specify the destination you want to connect to         Host Name (or IP address)         92.168.20.20         (92.168.20.20)         (22)         Connection type:         Raw         Telnet         Raw         Telnet         Raw         Telnet         Rogin         Save         Saved Sessions         CentOS-VM+token         Default Settings         Load         Save         Delete     Close window on exit:           Always       Never
About	Open Cancel

۴. تنظیمات SSH در نرمافزار: در منوی سمت چپ نرمافزار، به بخش SSH میرویم. در زیرمنوی بازشده، روی Pkcs11 کلیک نموده و تنظیمات زیر را انجام میدهیم:

© Copyright Amnafzar Co.

- ۱. در بخش Authentication Methods، تیک گزینه Use Windows event log را فعال میکنیم.
- ۲. در بخش Authentication Methods، تیک گزینه Attempt "PKCS#11 smartcard" auth (SSH-2) را فعال میکنیم.
- .PKCS#11 library for authentication گزینه Authentication Parameters، روبروی گزینه PKCS#11 library for authentication, در بخش Browse کلیک نموده و در پنجره جدید بازشده، محل فایل کتابخانه parskey11.dll را مشخص می کنیم.
- ۴. توکن خود را به سیستم متصل مینماییم. سپس، روبروی گزینه Token label، روی فِلش کلیک نموده و برچسب توکن خود را انتخاب مینماییم. همچنین روبروی گزینه Certificate label، روی فِلش کلیک نموده و برچسب گواهی خود (که روی توکن ذخیره شده) را انتخاب مینماییم.

Reputty Configuration	x
Category:	
Bell /	Options controlling PKCS11 SSH authentication
⊡. Window	Authentication methods
- Appearance	Use Windows event log
Behaviour	4 CAttempt "PRCS#11 smartcard" auth (SSH-2)
Iranslation	Authentication parameters
Colours	PKCS#11 library for authentication:
	5 (C:\Windows\System32\parskey11.dl) Browse
Data	Token label: My_Token 6
Telnet	Certificate label: PKI Tester 7
Rlogin E	
i ssh 1	
Kex	
2 (Pkcs11)	
-X11	
Bugs	
Serial	
About	Open Cancel

## ۲-۳ تنظیمات سرور

به منظور استفاده از احراز هویت دو فاکتوره در اتصال SSH، باید تنظیمات لازم در سرور انجام شود. برای این منظور، به صورت زیر عمل مینمایید. نکته: در صورتی که چنین فایلی وجود نداشته باشد، آن را ایجاد مینماییم. نکته: برای به دست آوردن مقدار کلید عمومی به صورت زیر عمل مینماییم:

- ۱. پس از انجام تنظیمات بخش ۳–۱، روی دکمه Open کلیک مینماییم (دقت کنید سرور باید روشن و قابل دسترسی بوده و SSH آن نیز فعال باشد. در غیر این صورت، امکان به دست آوردن کلید عمومی در مرحله بعد وجود نخواهد داشت).
- Control Panel > Administrative Tools > Computer Managemnet ۲. در ویندوز، به بخش Event Viewer > Windows Logs > Application میرویم. در پنجرهی بازشده، به بخش source آن puttysc است را پیدا کرده و روی آن کلیک می رویم. در این بخش، top این رویداد، به بخش Details رفته و مقدار روبروی عبارت puttysc: info sc:

ssh-rsa AAAAB3NzaC1yc2EAAAA.....ZHkknlDE7jhQ==

۲. مجوزهای ssh. و authorized\_keys را به ترتیب 700 و 600 قرار میدهیم:

#chmod 700 \$HOME/.ssh #chmod 600 \$HOME/.ssh/authorized\_keys . فایل پیکربندی SSH، را با یک ویرایشگر متن مثل vim باز می نماییم:

#vim /etc/ssh/sshd\_config

۴. در این فایل، باید گزینههای زیر وارد شود:

Protocol 2

PubkeyAuthentication yes

AuthorizedKeysFile .ssh/authorized\_keys

نکته: در صورتی که بخواهیم احراز هویت فقط با استفاده از مکانیزم دوفاکتوره فعال باشد، می توانیم احراز هویت بر اساس گذرواژه را غیر فعال نماییم. برای این کار، باید گزینه زیر را در فایل پیکربندی قرار دهیم:

PasswordAuthentication no

۵. در پایان، فایل پیکربندی را ذخیره نموده و سرویس sshd را راهاندازی مجدد می نماییم:

#/etc/init.d/sshd restart

## ۴ نحوه استفاده از نرمافزار PuTTY-CAC

برای نرمافزار PuTTY-CAC، دو روش برای استفاده از توکن وجود دارد:

- با استفاده از کتابخانه PKCS #11؛
- با استفاده از فراهمکننده سرویس رمزنگاری (CSP)؛

مراحل انجام کار به صورت زیر میباشد:

۱. تنظیمات نرمافزار PuTTY-CAC؛

۲. تنظیمات سرور.

تنظيمات سرور، مشابه بخش ٣-٢ ميباشد. از اينرو، در ادامه تنها تنظيمات نرمافزار را توضيح ميدهيم.

## PuTTY-CAC تنظیمات نرمافزار ۱-۴

#### PKCS #11 استفاده از کتابخانه 11-۱-۴

تنظیمات نرمافزار به صورت زیر میباشد:

۱. دانلود نرمافزار PuTTY-CAC: برای دانلود نرمافزار به آدرس زیر مراجعه نمایید:

<u>http://www.risacher.org/putty-cac/</u> ۲. دانلود کتابخانه PKCS #11 پارس کی: برای استفاده از توکن پارس کی در نرمافزار PKCS، باید کتابخانه PKCS توکن به نرمافزار معرفی گردد. برای دانلود این کتابخانه به بخش "دانلود" از سایت مرکز میانی پارس ساین به آدرس www.parssignca.ir مراجعه نمایید.

**توجه**: در صورتی که نرمافزار ParsKey Utility روی سیستم نصب باشد، این کتابخانه در مسیر \ParsKey System32 موجود بوده و نیازی به دانلود آن نیست.

۳. تنظیمات اتصال SSH: همانند روال عادی SSH، آدرس IP سرور، شماره درگاه SSH، را وارد می نماییم. در شکل زیر، SSH می اشد.

Reputty Configuration	
Category: Session Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial	Basic options for your PuTTY session         Specify the destination you want to connect to         Host Name (or IP address)       3 Port         192.168.20.20       22         Connection type:       22         Raw       Telnet       Rlogin       SSH         Saved Sessions       Serial         CentOS-VM+token       Load         Default Settings       Load         CentOS-VM+token       Save         Delete       Only on clean exit
About	Open Cancel

- ۴. تنظیمات SSH در نرمافزار: در منوی سمت چپ نرمافزار، به بخش SSH میرویم. در زیرمنوی بازشده، روی Pkcs11 کلیک نموده و تنظیمات زیر را انجام میدهیم:
  - ۱. در بخش Authentication Methods، تیک گزینه Use Windows event log را فعال میکنیم.

گزينه	تيک	Authentication	Methods	بخش	۲. در
		Attem را فعال ميكنيم.	pt "PKCS#11 sma	rtcard" auth (S	SH-2)

© Copyright Amnafzar Co.

- PKCS#11 library for authentication گزینه Authentication Parameters. در بخش PKCS#11 library for authentication را روی دکمه Browse کلیک نموده و در پنجره جدید بازشده، محل فایل کتابخانه Parskey11.dll را مشخص میکنیم.
- ۴. توکن خود را به سیستم متصل مینماییم. سپس، روبروی گزینه Token label، روی فِلش کلیک نموده و برچسب توکن خود را انتخاب مینماییم. همچنین روبروی گزینه Certificate label، روی فِلش کلیک نموده و برچسب گواهی خود (که روی توکن ذخیره شده) را انتخاب مینماییم.



#### ۲-۱-۴ استفاده از کتابخانه CAPI

تنظیمات نرمافزار به صورت زیر میباشد:

۱. دانلود نرمافزار PuTTY-CAC: برای دانلود نرمافزار به آدرس زیر مراجعه نمایید:

<u>http://www.risacher.org/putty-cac/</u> ۲. **دانلود فراهم کننده سرویس رمزنگاری (CSP) پارس کی**: برای استفاده از توکن پارس کی در نرمافزار باید فراهم کننده سرویس رمزنگاری پارس کی (ParsKey CSP) روی سیستم نصب (Parskey CSP) گردد. برای دانلود این نرمافزار به بخش "دانلود" از سایت مرکز میانی پارسساین به آدرس www.parssignca.ir مراجعه نمایید.

۳. تنظیمات اتصال SSH: همانند روال عادی SSH، آدرس IP سرور، شماره درگاه SSH را وارد . مینماییم. در شکل زیر، ۱۹۲.۱۶۸.۲۰.۲۰ آدرس IP سرور و ۲۲ شماره درگاه SSH می باشد.

R PuTTY Configuration	×
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Colours Connection Proxy Telnet Rlogin SSH	Basic options for your PuTTY session         Specify the destination you want to connect to         Host Name (or IP address)       3 Port         192.168.20.20       22         Connection type:       22         Raw       Telnet       Rlogin         Saved Sessions       Serial         CentOS-VM+token       Load         Default Settings       Load         Save       Delete
Serial	Close window on exit: Always Never Only on clean exit
About	Open Cancel

- ۴. تنظیمات SSH در نرمافزار: در منوی سمت چپ نرمافزار، به بخش SSH میرویم. در زیرمنوی بازشده، روی CAPI کلیک نموده و تنظیمات زیر را انجام میدهیم:
- ۰. در بخش Authentication Methods تیک گزینه

Attempt "CAPI Certificate" (Key only) auth (SSH-2) را فعال ميكنيم.

۲. توکن خود را به سیستم متصل مینماییم.

<sup>1</sup> Port

© Copyright Amnafzar Co.

- ۳. در بخش Authentication Parameters، روبروی گزینه Store، روی فِلش کلیک نموده و User\MY (Personal Certificate) را انتخاب مینماییم.
- ۴. سپس، روبروی گزینه Cert، روی دکمه Browse کلیک نموده و گواهی خود (که روی توکن ذخیره شده) را انتخاب مینماییم.
   نکته: کلید عمومی متناظر گواهی، در بخش SSH keystring نوشته می شود، که از آن می توان برای



#### ۲-۴ تنظیمات سرور

تنظيمات سرور، مشابه بخش ٣-٢ ميباشد.

**نکته**: وقتی از نرمافزار PuTTY-CAC استفاده مینماییم، مقدار کلید عمومی، مقداری است که هنگام معرفی توکن به نرمافزار طبق بخش ۴–۱، در بخش SSH keystring نشان داده می شود. این مقدار، شبیه عبارت زیر است: ssh-rsa AAAAB3NzaC1yc2EAAAA.....ZHkknlDE7jhQ==

# ۵ برقراری ارتباط SSH با استفاده از توکن

پس از انجام تنظیمات بخشهای ۳–۱ و ۳–۲ میتوانیم با استفاده از توکن با سرور ارتباط SSH برقرار نماییم. برای این کار به صورت زیر عمل مینماییم:

- ۱. نرمافزار PuTTY SC را باز نموده و طبق بخش ۳–۱ تنظیمات لازم را انجام میدهیم.
   ۱. نرمافزار PuTTY SC را ذخیره نماییم
   نکته: برای راحتی، می توان پس از انجام تنظیمات، در صفحه اصلی نرمافزار، session را ذخیره نماییم
   تا در دفعات بعد نیاز به تکرار تنظیمات نباشد.
  - ۲. روی دکمه Open کلیک مینماییم.
- ۳. پنجرهای مشابه شکل زیر ظاهر می گردد که در آن، روبروی عبارت login as، نام کاربری و روبروی
  ۳. پنجرهای مشابه شکل زیر ظاهر می گردد که در آن، روبروی عبارت login as، نام کاربری و روبروی
  ۳. پنجرهای HIN Code، پینکد (PIN Code) توکن خود را وارد نماییم. بدینسان،
  ۱۳. اتصال SSH برقرار می شود.

PuTTY (inactive)	
login as: root Authenticating with public key "PKI_Tester" Passphrase for smartcard "My_Token":	*