مرکز صدور گواهی الکترونیکی پارس‌ساین

راهنمای استفاده از گواهی الکترونیکی در نرم‌افزار

PuTTY

تدوین‌کننده: شرکت امن‌افزار گستر شریف

شمارهٔ سند.....SSW_UG_PKI_91160_1

تاریخ..... ۱۱/فروردین/۱۳۹۲

نگارش..... ۱.۱

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

PuTTY، نرم‌افزاری سبک و در عین حال قدرتمند است؛ از این نرم‌افزار برای اتصال از راه دور به سیستم از طریق پروتکل‌های SSH، Telent، و Rlogin استفاده می‌شود. یکی از کاربردهای مهم نرم‌افزار، اتصال از راه دور به سیستم از طریق SSH می‌باشد. در کاربرد عادیِ نرم‌افزار هنگام اتصال SSH به سیستم، احراز هویت بر اساس گذرواژه[1] انجام می‌شود. مکانیزمی امن‌تر از مکانیزم گذرواژه، احراز هویت دو فاکتوره[2] مبتنی بر کلید عمومی است که در آن، علاوه بر گذرواژه از یک سخت‌افزار به نام توکن امنیتی[3] نیز استفاده می‌شود. 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 حمله‌کننده‌ای با استفاده از حمله Brute-force آن را به دست آورد)، امنیت سیستم به مخاطره می‌افتد.
- 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، حمله‌کننده با در اختیار داشتن یکی از این دو نمی‌تواند به سیستم دسترسی داشته باشد. از این‌رو، **امنیت سیستم وابسته به دو فاکتور می‌باشد**؛ گذرواژه و توکن.
- در احراز هویت دو فاکتوره، گذرواژه دسترسی به کلید خصوصی روی توکن، روی سرور یا کلاینت ذخیره نمی‌شود (تنها چیزی که روی سرور ذخیره می‌شود، 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 می‌شود 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 نمی‌شود و با افشای گذرواژه در یک سیستم، امنیت سیستم‌های دیگر نیز به خطر می‌افتد). علاوه بر این، مدیریت گذرواژه‌ها نیز در آن دشوار است و با افزایش تعداد سیستم‌ها و کاربران، این کار دشوارتر نیز می‌شود. در حالیکه در احراز هویت دو

[1] Password
[2] Two-factor authentication
[3] Security Token

فاکتوره، چنین الزامی وجود نداشته و با استفاده یک گذرواژه می‌توان به هر تعداد دلخواهی سیستم ارتباط SSH برقرار کرد (زیرا گذرواژه روی سرور یا کلاینت ذخیره نمی‌شود).

در این سند، نحوه از استفاده از نرم‌افزار PuTTY و برقراری ارتباط SSH با استفاده از احراز هویت دوفاکتوره را شرح می‌دهیم. برای استفاده از احراز هویت دو فاکتوره، باید از نرم‌افزار PuTTY SC استفاده گردد. تنها تفاوت PuTTY SC با PuTTY، قابلیت 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 Microsoft's Cryprographic API (CAPI) نیز پشتیبانی می‌کند. در ادامه نحوه استفاده از هر دو نرم‌افزار توضیح داده می‌شود.

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 کار به صورت زیر می‌باشد:

۱. تنظیمات نرم‌افزار PuTTY SC؛
۲. تنظیمات سرور.

۳-۱ تنظیمات نرم‌افزار PuTTY SC

تنظیمات نرم‌افزار به صورت زیر می‌باشد:

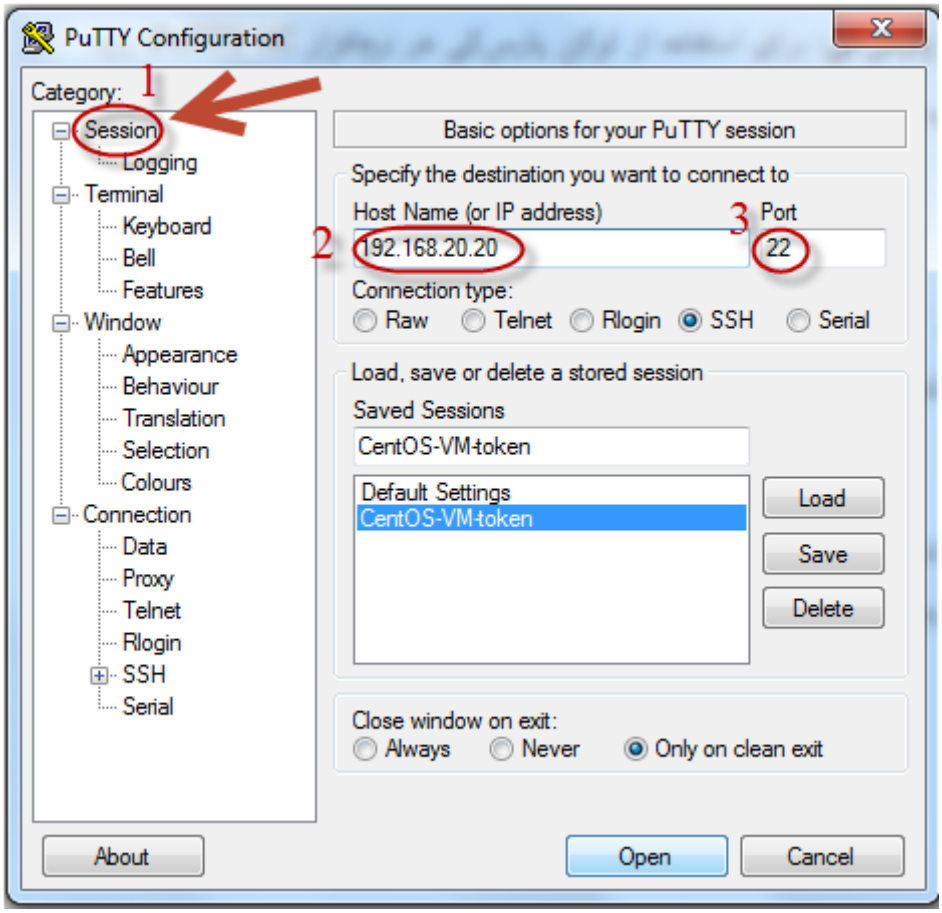
۱. **دانلود نرم‌افزار PuTTY SC**: برای دانلود نرم‌افزار به آدرس زیر مراجعه نمایید:

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

۲. **دانلود کتابخانه PKCS #11 پارس‌کی:** برای استفاده از توکن پارس‌کی در نرم‌افزار PuTTY SC، باید کتابخانه PKCS #11 توکن به نرم‌افزار معرفی گردد. برای دانلود این کتابخانه به بخش "دانلود" از سایت مرکز میانی پارس‌ساین به آدرس www.parssignca.ir مراجعه نمایید.

توجه: در صورتی که نرم‌افزار ParsKey Utility روی سیستم نصب باشد، این کتابخانه در مسیر C:\Windows\System32\ و با نام Parskey11.dll موجود بوده و نیازی به دانلود آن نیست.

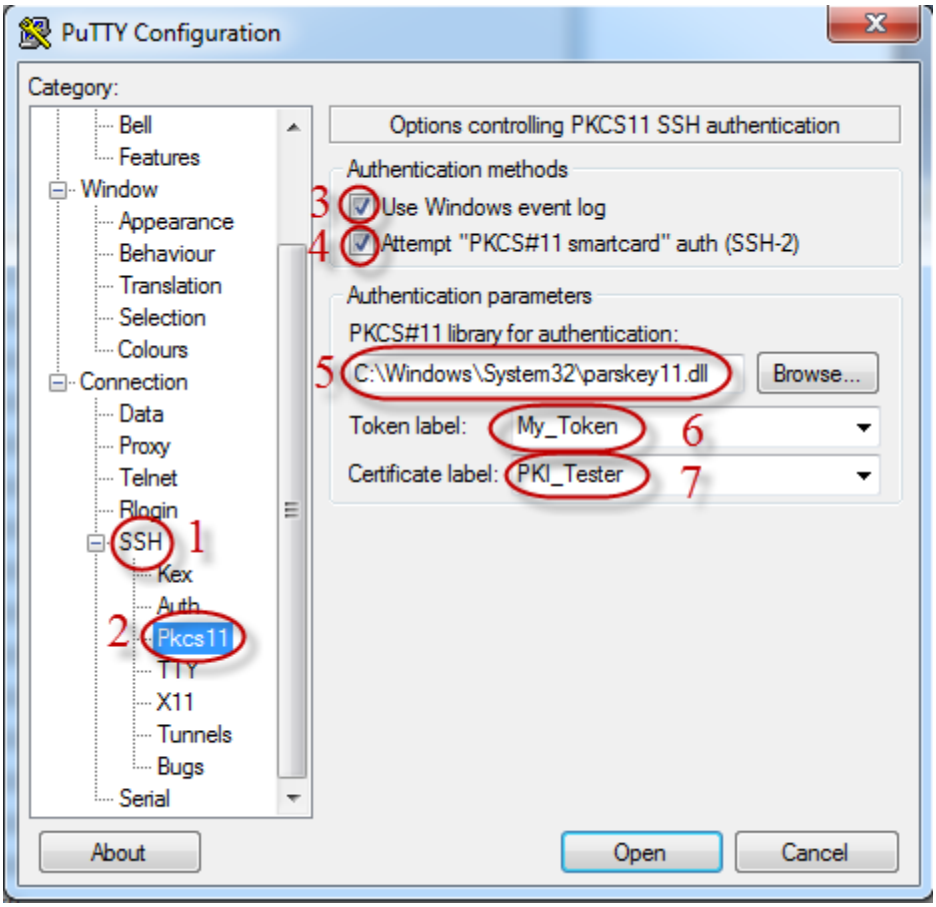
۳. **تنظیمات اتصال SSH:** همانند تنظیمات عادی PuTTY، در صفحه اصلی نرم‌افزار (بخش Session)، آدرس IP سرور و شماره درگاه[1] SSH را وارد می‌نماییم. در شکل زیر، ۱۹۲.۱۶۸.۲۰.۲۰ آدرس IP سرور و ۲۲ شماره درگاه SSH می‌باشد.



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:

[1] Port

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.
۳. در بخش Authentication Parameters، روبروی گزینه PKCS#11 library for authentication، 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.



۳-۲ 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.

۱. فایل زیر را با یک ویرایشگر متن مثل vim باز نموده و مقدار کلید عمومی را در آن وارد می‌نماییم:

```
#vim $HOME/.ssh/authorized_keys
```

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).

۲. در ویندوز، به بخش Control Panel > Administrative Tools > Computer Managemnet می‌رویم. در پنجره‌ی بازشده، به بخش Event Viewer > Windows Logs > Application می‌رویم. در این بخش، eventی که source آن puttysc است را پیدا کرده و روی آن کلیک می‌نماییم. در بخش اطلاعات این رویداد، به بخش Details رفته و مقدار روبروی عبارت puttysc: info sc: را کپی می‌نماییم. این مقدار، شبیه عبارت زیر است:

```
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
```

۳. فایل پیکربندی SSH، را با یک ویرایشگر متن مثل vim باز می‌نماییم:

```
#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، می‌توانیم 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 می‌نماییم:

```
#/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.

تنظیمات سرور، مشابه بخش ۳-۲ می‌باشد. از این‌رو، در ادامه تنها تنظیمات نرم‌افزار را توضیح می‌دهیم.

۴-۱ تنظیمات نرم‌افزار PuTTY-CAC

۴-۱-۱ استفاده از کتابخانه PKCS #11

تنظیمات نرم‌افزار به صورت زیر می‌باشد:

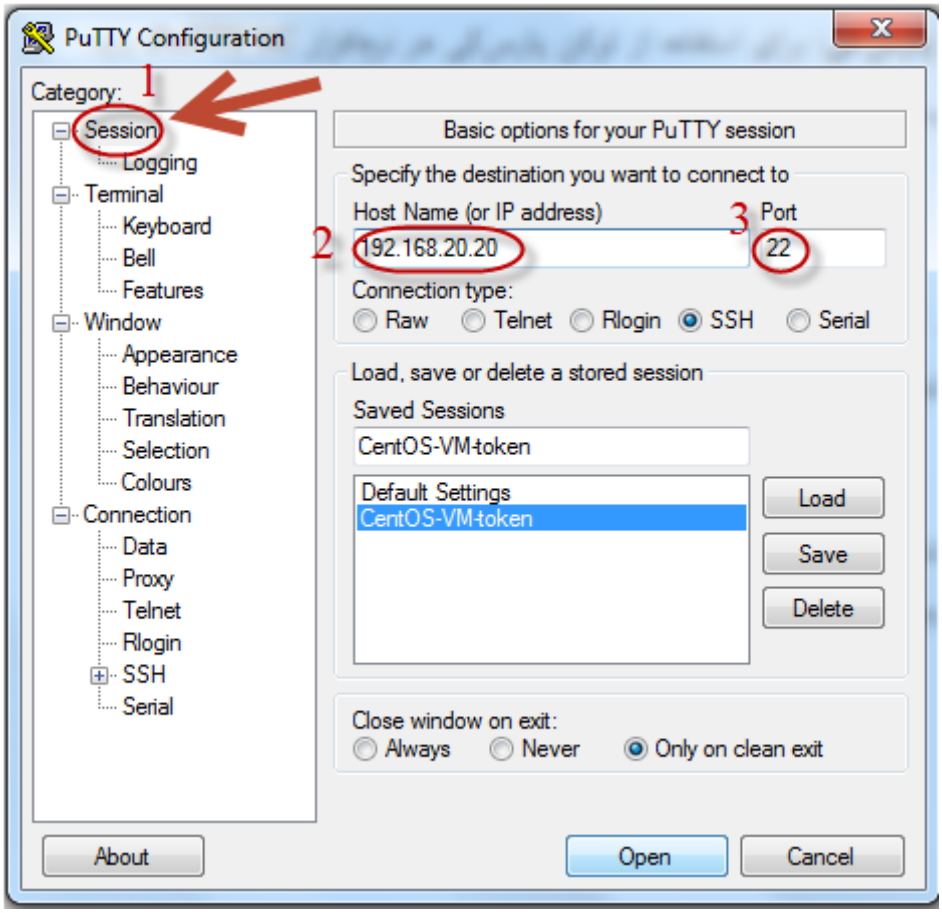
۱. **دانلود نرم‌افزار PuTTY-CAC:** برای دانلود نرم‌افزار به آدرس زیر مراجعه نمایید:

http://www.risacher.org/putty-cac/

۲. **دانلود کتابخانه PKCS #11 پارس‌کی:** برای استفاده از توکن پارس‌کی در نرم‌افزار PuTTY SC، باید کتابخانه PKCS #11 توکن به نرم‌افزار معرفی گردد. برای دانلود این کتابخانه به بخش "دانلود" از سایت مرکز میانی پارس‌ساین به آدرس www.parssignca.ir مراجعه نمایید.

توجه: در صورتی که نرم‌افزار ParsKey Utility روی سیستم نصب باشد، این کتابخانه در مسیر C:\Windows\System32\ و با نام Parskey11.dll موجود بوده و نیازی به دانلود آن نیست.

۳. **تنظیمات اتصال SSH:** همانند روال عادی SSH، آدرس IP سرور، شماره درگاه[1] SSH، را وارد می‌نماییم. در شکل زیر، ۱۹۲.۱۶۸.۲۰.۲۰ آدرس IP سرور و ۲۲ شماره درگاه SSH می‌باشد.



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:

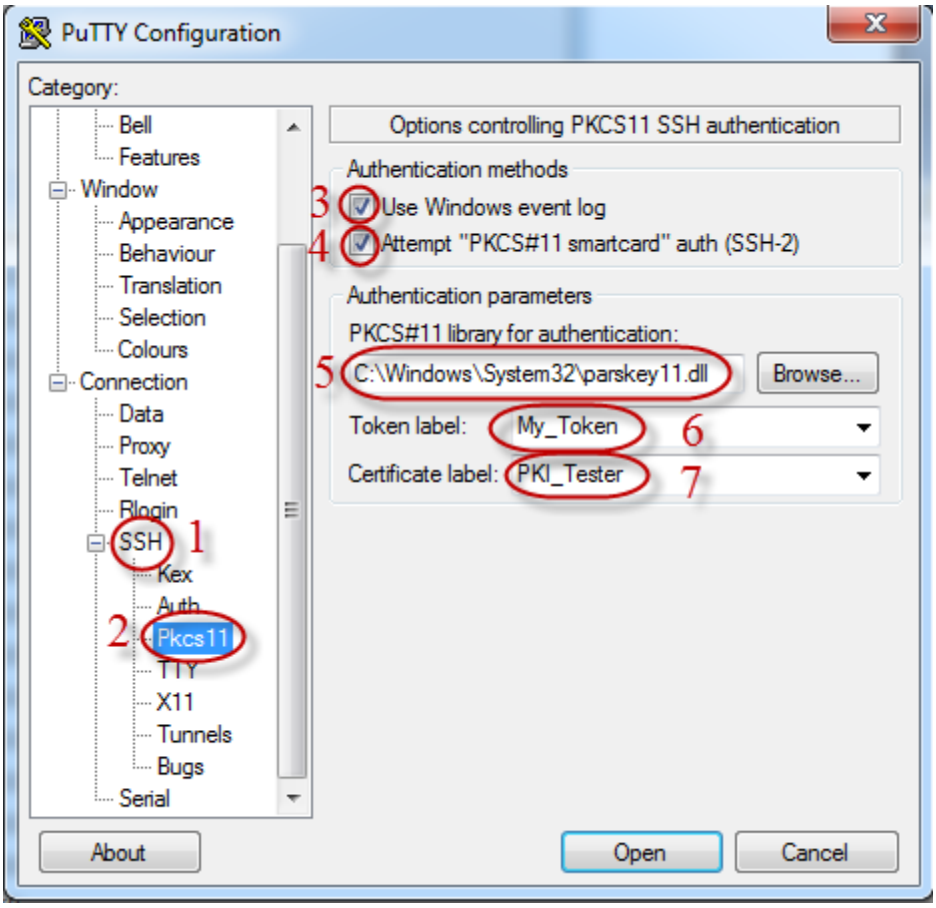
۱. در بخش Authentication Methods، تیک گزینه Use Windows event log را فعال می‌کنیم.

۲. در بخش Authentication Methods، تیک گزینه Attempt “PKCS#11 smartcard” auth (SSH-2) را فعال می‌کنیم.

[1] Port

۳. در بخش Authentication Parameters، روبروی گزینه PKCS#11 library for authentication، 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.



۴-۱-۲ استفاده از کتابخانه CAPI

تنظیمات نرم‌افزار به صورت زیر می‌باشد:

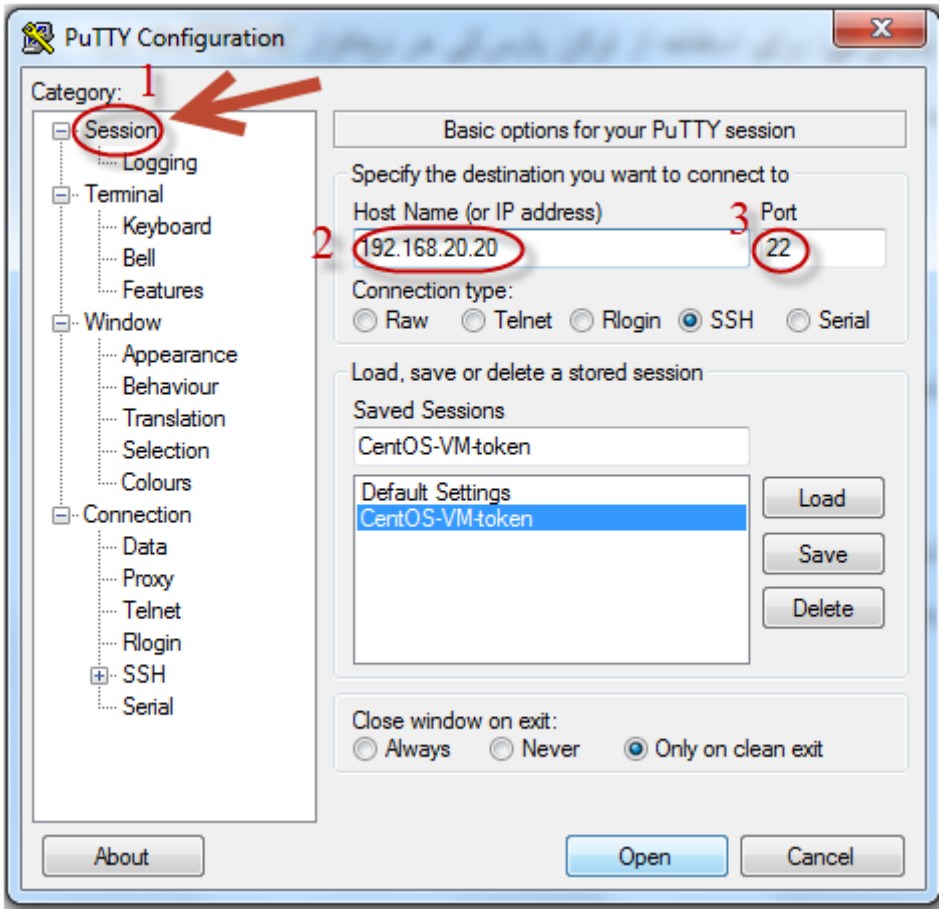
۱. **دانلود نرم‌افزار PuTTY-CAC:** برای دانلود نرم‌افزار به آدرس زیر مراجعه نمایید:

http://www.risacher.org/putty-cac/

۲. **دانلود فراهم‌کننده سرویس رمزنگاری (CSP) پارس‌کی:** برای استفاده از توکن پارس‌کی در نرم‌افزار PuTTY-CAC، باید فراهم‌کننده سرویس رمزنگاری پارس‌کی (ParsKey CSP) روی سیستم نصب

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[1] SSH، را وارد می‌نماییم. در شکل زیر، ۱۹۲.۱۶۸.۲۰.۲۰ آدرس IP سرور و ۲۲ شماره درگاه SSH می‌باشد.



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:

۱. در بخش Authentication Methods، تیک گزینه Attempt "CAPI Certificate" (Key only) auth (SSH-2) را فعال می‌کنیم.

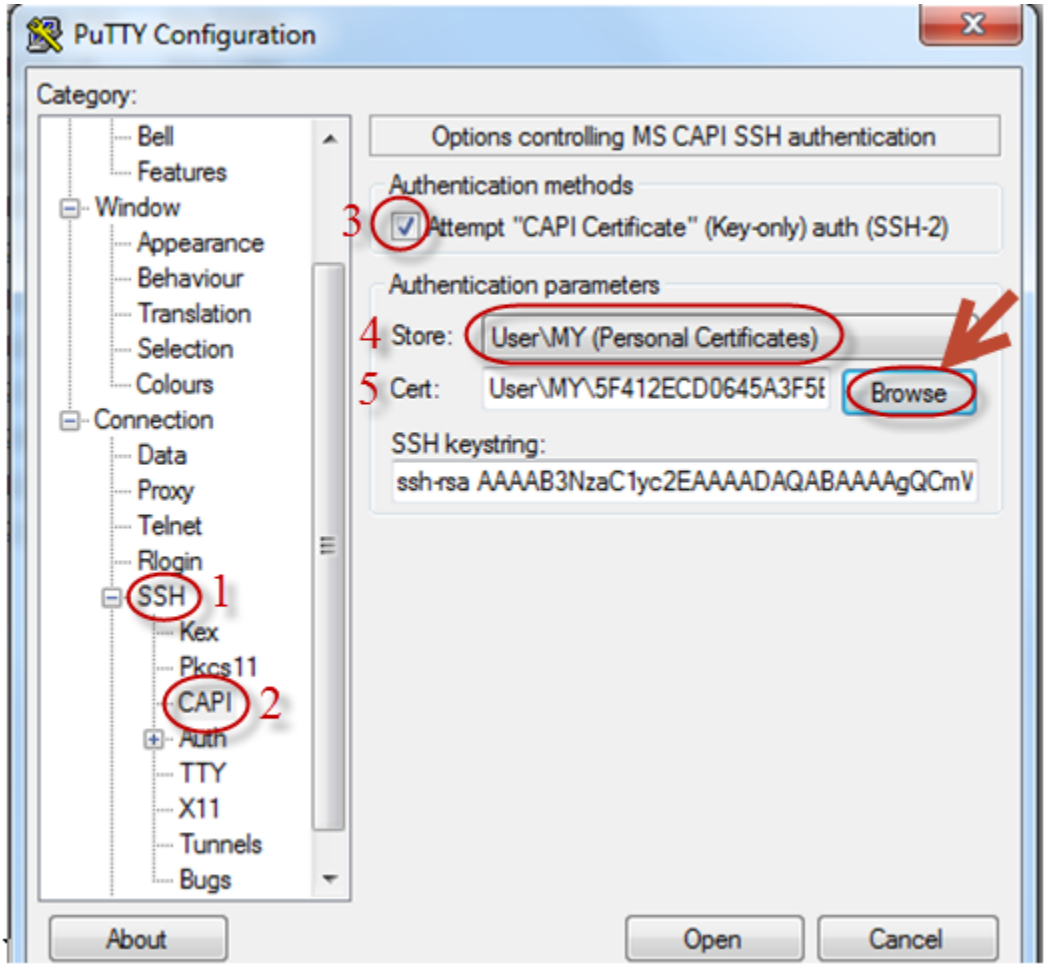
۲. توکن خود را به سیستم متصل می‌نماییم.

[1] Port

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 می‌شود، که از آن می‌توان برای انجام تنظیمات در سمت سرور استفاده نمود.



۲-۴ تنظیمات سرور

تنظیمات سرور، مشابه بخش ۳-۲ می‌باشد.

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 می‌شود. 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.

نکته: برای راحتی، می‌توان 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 می‌گردد که در آن، روبروی عبارت login as، نام کاربری و روبروی Passphrase for smartcard "My_Token"، پین‌کد (PIN Code) توکن خود را وارد نماییم. بدین‌سان، اتصال SSH برقرار می‌شود.