Remove SSL Key Passphrase (.p12)

By default, ssl certificates are created using a password. For example, OpenVPN keys (.p12 files) always have a passphrase in them.

However, when automating connections, such as ensuring an OpenVPN connection is created on boot, requires the private key passphrase to be removed.

I got tired of the almost 10 commands to do this, so I wrote the following Perl script. If you don't want to run a Perl script, simply copy/paste the commands (it is just a list of commands to run).

This should be executed as:

```
removeP12Passphrase.pl /full/path/to/key.p12 'passphrase'
```

The original encrypted key will be stoed as key.p12.save, then the key will be removed. It will ask for a passphrase two times, and just pressing Enter will give it a blank passphrase.

NOTE: if you enter a passphrase, it will simply encrypt it with the new one.

removeP12Passphrase.pl

```
#! /usr/bin/perl -w

use Cwd 'abs_path';

my $keyfile = shift;
my $passphrase = shift;

$keyfile = abs_path( $keyfile );

die "the first parameter should be the full path to your p12 file"
unless -e $keyfile;
die "the second parameter should be the password to your p12 file"
unless $passphrase;

sub runCommand {
   my $command = shift;
   qx/$command/;
  if ($? == -1) {
      die "$command\nfailed to execute: $!\n";
  }
  elsif ($? & 127) {
      die sprintf( "$command\n died with signal %d, %s coredump\n",
          ($? & 127),  ($? & 128) ? 'with' : 'without' );
  }
  else {
     die sprintf( "$command\n exited with value %d\n", $? >> 8) if $?
>> 8;
```

```
  }
}

chdir '/tmp';
&runCommand( "cp '$keyfile' '$keyfile.save'" );
&runCommand( "openssl pkcs12 -clcerts -nokeys -in '$keyfile' -out
certificate.crt -password pass:'$passphrase' -passin pas:'$passphrase'"
);
&runCommand( "openssl pkcs12 -cacerts -nokeys -in '$keyfile' -out ca-
cert.ca -password pass:'$passphrase' -passin pass:'$passphrase'" );
&runCommand( "openssl pkcs12 -nocerts -in '$keyfile' -out private.key -
password pass:'$passphrase' -passin pass:'$passphrase' -passout
pass:joe" );
&runCommand( "openssl rsa -in private.key -out 'NewKeyFile.key' -passin
pass:joe" );
&runCommand( "cat 'NewKeyFile.key' > PEM.pem" );
&runCommand( "cat 'certificate.crt' >> PEM.pem" );
&runCommand( "cat 'ca-cert.ca' >> PEM.pem" );
&runCommand( "openssl pkcs12 -export -nodes -CAfile ca-cert.ca -in
PEM.pem -out '$keyfile'" );

1;
```

From:
https://kb.unixservertech.com/ - **Unix Server Tech Knowledge Base**

Permanent link:
https://kb.unixservertech.com/other/encryption/ssl_key_passphrase

Last update: **2016/12/10 05:39**