pfSense - Feature #1257

Handle encypted CA private keys

02/06/2011 09:32 AM - Brad Langhorst

Status:	New	**Start date:**	02/06/2011
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Certificates	**Estimated time:**	0.00 hour
Target version:			

Description

when i export a certificate using
http://192.168.3.1/system_certmanager.php

i get an empty file.

the private key downloads just fine.

History

#1 - 02/06/2011 09:38 AM - Brad Langhorst

upon further investigation, i see that the crt was not saved.

here's a bit of the config file.

```
&lt;descr&gt;&lt;![CDATA[walden]]&gt;&lt;/descr&gt;
                &lt;caref&gt;4d460d3298bb2&lt;/caref&gt;
                &lt;crt/&gt;
                &lt;prv&gt;I REMOVED THIS ONE THE OTHER ONE IS BLANK&lt;/prv&gt;
        &lt;/cert&gt;
```

#2 - 02/06/2011 09:41 AM - Brad Langhorst

the title of this bug should be "certificate file is not properly generated or saved." using internal cert auth

#3 - 02/07/2011 09:06 AM - Jim Pingle

- Status changed from New to Rejected

I can't replicate this - I can make certificates several different ways on current snapshots and they are complete inside of the config.

You might want to make a thread on the forum with more detail about exactly how you are creating the certificates, there may be something else going on, but the certificate generation code appears to be working properly.

#4 - 02/08/2011 01:35 PM - Brad Langhorst

Seems to be related to importing of a certificate authority.

To isolate a bit... I created an internal certificate authority and generated a cert.
This one looks fine.

I still cannot create certs when i choose the pre-existing cert authority that I created outside of pfsense
(using openssl/tinyca2)

I looked for some kind of log to show what commands php is trying to run, but didn't find one.
How can i help debug this problem?

#5 - 02/08/2011 01:38 PM - Jim Pingle

When you imported the CA, did you import both the cert and private key of the CA?

All of the certificates are made in certs.inc. The code is laid out pretty well there, shouldn't be hard to see what commands are run.

#6 - 02/08/2011 01:49 PM - Brad Langhorst

One more clarification...
I just checked and see that the private key is encrypted, so cert signing must fail since it never asks for a password.

I can think of a few possible solutions

- ask for a password before attempting to sign a new cert (my favorite option)
- don't allow encrypted private keys (probably not a great idea), and reject an invalid key during import
- don't allow creation of new certs if no usable key is available for the selected cert

Certificate generation works if I paste in the unencrypted ca key, though this strikes me as a poor security practice.
At minimum, I think the user should be notified if the a new cert cannot be generated.

#7 - 02/08/2011 02:31 PM - Jim Pingle

- Subject changed from exported certificate files are empty to Handle encypted CA private keys

- Status changed from Rejected to New

- Target version deleted (2.0)

- Affected Architecture set to All

Not sure if this will make 2.0 or not. It may have to wait for 2.1 at this point, it may end up a documented limitation for 2.0 because it works fine for certificates made and managed in the GUI.

#8 - 06/14/2016 05:30 PM - Chris Buechler

- Tracker changed from Bug to Feature

#9 - 04/04/2019 02:55 PM - Peter Feichtinger

I made a preliminary PR that adds support for encrypted private keys to the CA, certificate, and user managers.
Would love to get some feedback: https://github.com/pfsense/pfsense/pull/4062