Prelude Manager - Bug #222

TLS Certificate generation takes ages

05/06/2007 07:21 PM - admin admin

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:	wontfix		

Description

When generating the TLS certificate using prelude-adduser, the generation of the certificate takes between 2 and 30 minutes, depending on the kernel and gnutls version. warning.png
Tracing the processes shows that, for an unknown reason, [[GnuTLS]] is using /dev/random instead of /dev/urandom (both exist on the test system)
This is more a [[GnuTLS]] problem, yet maybe there is a function which can be called to set the random parameters ?

History

#1 - 05/14/2007 01:53 PM - Yoann VANDOORSELAERE

- Status changed from New to Closed

- Resolution set to wontfix

Unfortunately, the problem lie in Gcrypt and there is currently no way of working it around except from generating activity on the machine where key generation occur:

```
dd if=/dev/zero of=/tmp/tmp.blah
```

Is reported to work well.
There are ongoing discussions on way of improving this issue on the [[GnuTLS]] mailing list, and we hope that a solution will be adopted in the near future.

#2 - 01/05/2009 11:43 PM -

In order to accelerate the generation process, one can recur to the instructions on: https://trac.prelude-ids.org/wiki/Misc/Entropy

In a debian system:

```
aptitude install rng-tools
 vi /etc/default/rng-tools
```

Add the following lines to the configuration file

```
HRNGDEVICE=/dev/urandom
 RNGDOPTIONS="-W 80% -t 20"
```

Start the entropy generator:

/etc/init.d/rng-tools start

The RSA private key generation should happen very quickly. BUT, as the /dev/urandom is not a real rng, of course there are all the problems related to the randomness of the generated numbers, entropy, etc. Beware! If you don't know what is it, then don't do it.

#3 - 01/05/2009 11:57 PM - admin admin

Now, correctly formatted (sorry!)
In order to accelerate the generation process, one can recur to the instructions on https://trac.prelude-ids.org/wiki/Misc/Entropy

In a debian system:

```
aptitude install rng-tools
vi /etc/default/rng-tools
```

Add the following lines to the configuration file

```
HRNGDEVICE=/dev/urandom
RNGDOPTIONS="-W 80% -t 20"
```

Start the entropy generator:

```
/etc/init.d/rng-tools start
```

The RSA private key generation should happen very quickly. BUT, as the /dev/urandom is not a real rng, of course there are all the problems related to the randomness of the generated numbers, entropy, etc. Beware! If you don't know what is it, then don't do it.

#4 - 04/29/2009 12:20 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude Manager

- Category deleted (3)