strongSwan - Feature #221

pki --gen and Hosts with Low Entropy

06.09.2012 11:07 - Dmitry Korzhevin

Status:	Closed	**Start date:**	06.09.2012
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:			
Target version:	5.0.1		
Resolution:			

Description

Please, add option to choose, which random data surce use to gen key:

Now, pki --gen can use only /dev/random, but you could add option to choose /dev/urandom also.

Associated revisions

Revision 7b68cd92 - 10.09.2012 17:07 - Martin Willi

Add strongswan.conf runtime options for /dev/[u]random files

Fixes #221.

History

#1 - 10.09.2012 17:13 - Martin Willi

- Status changed from New to Closed

- Assignee set to Martin Willi

I don't think it is a good idea to get random bytes from /dev/urandom for private key generation.

But if /dev/random does not work for you, you can ./configure strongSwan *--with-random-device=/dev/urandom*. Or, with the referenced patch, set the strongswan.conf option *libstrongswan.plugins.random.random* to */dev/urandom.*