



Full credit is given to the above companies including the Operating System (OS) that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'Crypt::URandom.3pm'

\$ man Crypt::URandom.3pm

Crypt::URandom(3pm) User Contributed Perl Documentation Crypt::URandom(3pm)

NAME

Crypt::URandom - Provide non blocking randomness

VERSION

This document describes Crypt::URandom version 0.36

SYNOPSIS

```
use Crypt::URandom();

my $random_string_50_bytes_long = Crypt::URandom::urandom(50);
```

OR

```
use Crypt::URandom qw( urandom );

my $random_string_50_bytes_long = urandom(50);
```

DESCRIPTION

This Module is intended to provide an interface to the strongest available source of non-blocking randomness on the current platform. Platforms currently supported are anything supporting /dev/urandom and versions of Windows greater than or equal to Windows 2000.

SUBROUTINES/METHODS

"urandom"

This function accepts an integer and returns a string of the same size filled with random data. The first call will initialize the native cryptographic libraries (if necessary) and load all the required Perl libraries

DIAGNOSTICS

"No secure alternative for random number generation for Win32 versions older than W2K"

The module cannot run on versions of Windows earlier than Windows 2000 as there is no

cryptographic functions provided by the operating system.

"Could not import CryptAcquireContext"

The module was unable to load the CryptAcquireContextA function from the advapi32 dynamic library. The advapi32 library cannot probably be loaded.

"CryptAcquireContext failed"

The module was unable to call the CryptAcquireContextA function from the advapi32 dynamic library.

"Could not import CryptGenRandom"

The module was unable to load the CryptGenRandom function from the advapi32 dynamic library.

"Could not import SystemFunction036"

The module was unable to load the SystemFunction036 function from the advapi32 dynamic library.

"The length argument must be supplied and must be an integer"

The get method must be called with an integer argument to describe how many random bytes are required.

"CryptGenRandom failed"

The Windows 2000 CryptGenRandom method call failed to generate the required amount of randomness

"RtlGenRand failed"

The post Windows 2000 RtlGenRand method call failed to generate the required amount of randomness

"Only read n bytes from path"

The /dev/urandom device did not return the desired amount of random bytes

"Failed to read from path"

The /dev/urandom device returned an error when being read from

"Failed to open path"

The /dev/urandom device returned an error when being opened

CONFIGURATION AND ENVIRONMENT

Crypt::URandom requires no configuration files or environment variables.

DEPENDENCIES

If the platform is Win32, the Win32::API module will be required. Otherwise no other modules other than those provided by perl will be required

INCOMPATIBILITIES

None reported.

BUGS AND LIMITATIONS

No bugs have been reported.

Please report any bugs or feature requests to "bug-crypt-urandom@rt.cpan.org", or through the web interface at <<http://rt.cpan.org>>.

AUTHOR

David Dick "<ddick@cpan.org>"

ACKNOWLEDGEMENTS

The Win32::API code for interacting with Microsoft's CryptoAPI was stolen with extreme gratitude from Crypt::Random::Source::Strong::Win32 by Max Kanat-Alexander

LICENSE AND COPYRIGHT

Copyright (c) 2011, David Dick "<ddick@cpan.org>". All rights reserved.

This module is free software; you can redistribute it and/or modify it under the same terms as Perl itself.

DISCLAIMER OF WARRANTY

BECAUSE THIS SOFTWARE IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE SOFTWARE, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE SOFTWARE "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU. SHOULD THE SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE SOFTWARE AS PERMITTED BY

THE ABOVE LICENCE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE SOFTWARE TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.