

NAME

life_cycle-rand – The RAND algorithm life-cycle

DESCRIPTION

All random number generator (RANDs) go through a number of stages in their life-cycle:

start

This state represents the RAND before it has been allocated. It is the starting state for any life-cycle transitions.

newed

This state represents the RAND after it has been allocated but unable to generate any output.

instantiated

This state represents the RAND when it is set up and capable of generating output.

uninstantiated

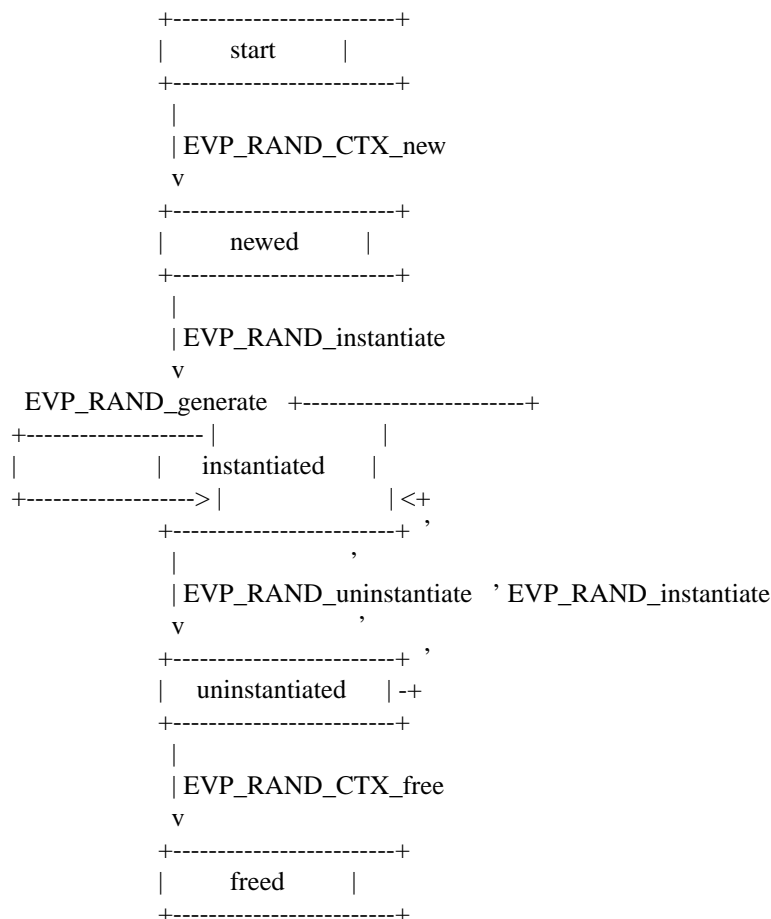
This state represents the RAND when it has been shutdown and it is no longer capable of generating output.

freed

This state is entered when the RAND is freed. It is the terminal state for all life-cycle transitions.

State Transition Diagram

The usual life-cycle of a RAND is illustrated:

**Formal State Transitions**

This section defines all of the legal state transitions. This is the canonical list.

Function Call	-----	Current State	-----
		start	newed
		newed	instantiated
		instantiated	uninstantiated
		uninstantiated	freed

EVP RAND_CTX_new	newed			
EVP RAND_instantiate	instantiated			
EVP RAND_generate		instantiated		
EVP RAND_uninstantiate		uninstantiated		
EVP RAND_CTX_free	freed	freed	freed	freed
EVP RAND_CTX_get_params	newed	instantiated	uninstantiated	freed
EVP RAND_CTX_set_params	newed	instantiated	uninstantiated	freed
EVP RAND_CTX_gettable_params	newed	instantiated	uninstantiated	freed
EVP RAND_CTX_settable_params	newed	instantiated	uninstantiated	freed

NOTES

At some point the EVP layer will begin enforcing the transitions described herein.

SEE ALSO

provider-rand (7), **EVP RAND** (3).

HISTORY

The provider RAND interface was introduced in OpenSSL 3.0.

COPYRIGHT

Copyright 2021 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the “License”). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.