



**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 'life\_cycle-rand.7ssl'***

***\$ man life\_cycle-rand.7ssl***

LIFE\_CYCLE-RAND(7SSL)                      OpenSSL                      LIFE\_CYCLE-RAND(7SSL)

**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**

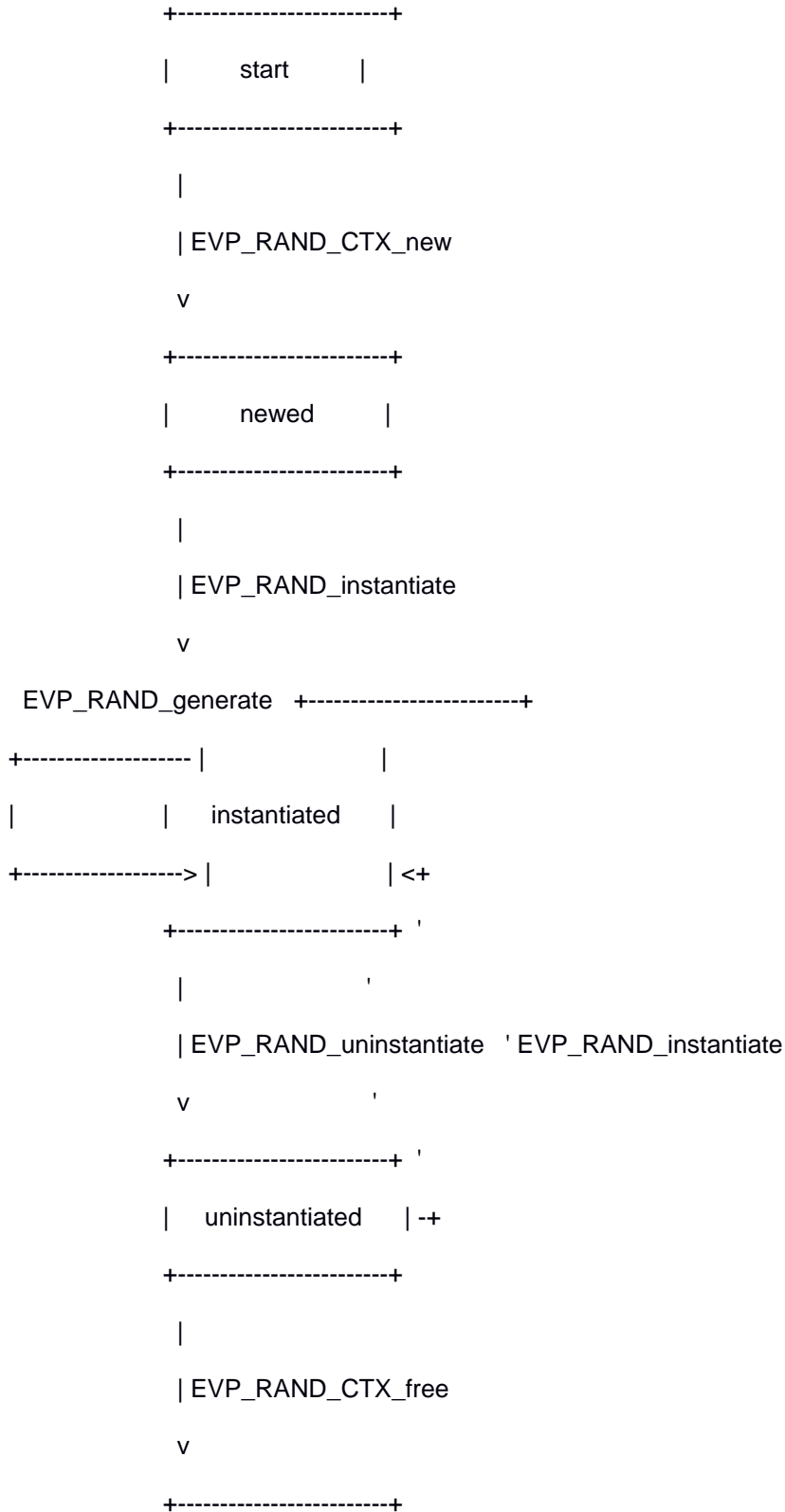
This state represents the RAND when it has been shutdown and it is no longer capable of generating output.

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:



```

|   freed   |
+-----+

```

## Formal State Transitions

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

Function Call	-----	Current State	-----
		start	newed instantiated 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>.

