NAME

life_cycle-mac - The MAC algorithm life-cycle

DESCRIPTION

All message authentication codes (MACs) go through a number of stages in their life-cycle:

start

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

newed

This state represents the MAC after it has been allocated.

initialised

This state represents the MAC when it is set up and capable of processing input.

updated

This state represents the MAC when it is set up and capable of processing additional input or generating output.

finaled

This state represents the MAC when it has generated output.

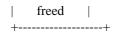
freed

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

State Transition Diagram

The usual life-cycle of a MAC is illustrated:

```
start
  | EVP_MAC_CTX_new
 newed
 +----+
  | EVP_MAC_init
+> | initialised | <+
| +-----
| | EVP_MAC_update | EVP_MAC_init
    EVP_MAC_init | +----- |
|| updated |-+
i I I I
| | EVP_MAC_final | EVP_MAC_finalXOF
+- | finaled |
 +----+
  | EVP_MAC_CTX_free
 +----+
```



Formal State Transitions

This section defines all of the legal state transitions. This is the canonical list. ----- Current State -----Function Call start newed initialised updated finaled freed EVP_MAC_CTX_new newed EVP_MAC_init initialised initialised initialised EVP_MAC_update updated updated EVP_MAC_final finaled EVP_MAC_finalXOF finaled EVP_MAC_CTX_free freed freed freed freed freed newed initialised updated newed initialised updated EVP_MAC_CTX_get_params EVP_MAC_CTX_set_params EVP_MAC_CTX_gettable_params newed initialised updated EVP_MAC_CTX_settable_params newed initialised updated

NOTES

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

SEE ALSO

provider-mac (7), EVP_MAC (3).

HISTORY

The provider MAC 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.