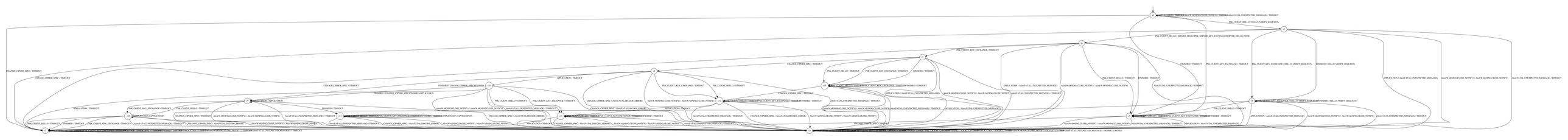

s0 APPLICATION / TIMEOUTAlert(WARNING,CLOSE_NOTIFY) / TIMEOUTAlert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT

s1

CHANGE_CIPHER_SPEC / TIMEOUT

s2

PSK_CLIENT_HELLO / HELLO_VERIFY_REQUEST+

s5

FINISHED / TIMEOUT PSK_CLIENT_KEY_EXCHANGE / TIMEOUT

PSK_CLIENT_HELLO / TIMEOUTPSK_CLIENT_KEY_EXCHANGE / TIMEOUTCHANGE_CIPHER_SPEC / TIMEOUTFINISHED / TIMEOUTAPPLICATION / TIMEOUTAlert(WARNING,CLOSE_NOTIFY) / TIMEOUTAlert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT

CHANGE_CIPHER_SPEC / TIMEOUT

s3

APPLICATION / Alert(FATAL,UNEXPECTED_MESSAGE) Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY) Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT

s4

PSK_CLIENT_KEY_EXCHANGE / HELLO_VERIFY_REQUEST+ FINISHED / HELLO_VERIFY_REQUEST+

s6

PSK_CLIENT_HELLO / SERVER_HELLO|PSK_SERVER_KEY_EXCHANGE|SERVER_HELLO_DONE

PSK_CLIENT_HELLO / SOCKET_CLOSEDPSK_CLIENT_KEY_EXCHANGE / SOCKET_CLOSEDCHANGE_CIPHER_SPEC / SOCKET_CLOSEDFINISHED / SOCKET_CLOSEDAPPLICATION / SOCKET_CLOSEDAlert(WARNING,CLOSE_NOTIFY) / SOCKET_CLOSEDAlert(FATAL,UNEXPECTED_MESSAGE) / SOCKET_CLOSED

CHANGE_CIPHER_SPEC / TIMEOUT APPLICATION / Alert(FATAL,UNEXPECTED_MESSAGE) Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY) Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT

PSK_CLIENT_KEY_EXCHANGE / HELLO_VERIFY_REQUEST+FINISHED / HELLO_VERIFY_REQUEST+

PSK_CLIENT_HELLO / TIMEOUT

CHANGE_CIPHER_SPEC / TIMEOUT Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY) Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT APPLICATION / Alert(FATAL,UNEXPECTED_MESSAGE)

PSK_CLIENT_HELLO / TIMEOUTPSK_CLIENT_KEY_EXCHANGE / TIMEOUTFINISHED / TIMEOUT

CHANGE_CIPHER_SPEC / TIMEOUT APPLICATION / Alert(FATAL,UNEXPECTED_MESSAGE) Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY) Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT

PSK_CLIENT_HELLO / TIMEOUT FINISHED / TIMEOUT

s7

PSK_CLIENT_KEY_EXCHANGE / TIMEOUT

APPLICATION / Alert(FATAL,UNEXPECTED_MESSAGE) Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY) Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT

s8

CHANGE_CIPHER_SPEC / TIMEOUT

s15

PSK_CLIENT_HELLO / TIMEOUT PSK_CLIENT_KEY_EXCHANGE / TIMEOUT FINISHED / TIMEOUT

s9 CHANGE_CIPHER_SPEC / Alert(FATAL,DECODE_ERROR) Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY) Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT

FINISHED / CHANGE_CIPHER_SPEC|FINISHED s10

APPLICATION / TIMEOUT

s11

PSK_CLIENT_KEY_EXCHANGE / TIMEOUT PSK_CLIENT_HELLO / TIMEOUT

Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY) Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT CHANGE_CIPHER_SPEC / Alert(FATAL,DECODE_ERROR)

APPLICATION / APPLICATION

s12

PSK_CLIENT_KEY_EXCHANGE / TIMEOUT PSK_CLIENT_HELLO / TIMEOUT

s14

APPLICATION / TIMEOUT FINISHED / TIMEOUT Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY) Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT CHANGE_CIPHER_SPEC / Alert(FATAL,DECODE_ERROR)

FINISHED / CHANGE_CIPHER_SPEC|FINISHED|APPLICATION

s13

PSK_CLIENT_HELLO / TIMEOUT PSK_CLIENT_KEY_EXCHANGE / TIMEOUT

Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT CHANGE_CIPHER_SPEC / Alert(FATAL,DECODE_ERROR) Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY)

PSK_CLIENT_HELLO / TIMEOUTPSK_CLIENT_KEY_EXCHANGE / TIMEOUTFINISHED / TIMEOUT

APPLICATION / TIMEOUT

PSK_CLIENT_HELLO / TIMEOUT FINISHED / TIMEOUT PSK_CLIENT_KEY_EXCHANGE / TIMEOUT Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT CHANGE_CIPHER_SPEC / Alert(FATAL,DECODE_ERROR) Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY)

APPLICATION / APPLICATION

APPLICATION / TIMEOUT CHANGE_CIPHER_SPEC / Alert(FATAL,DECODE_ERROR) Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY) Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT

PSK_CLIENT_HELLO / TIMEOUTPSK_CLIENT_KEY_EXCHANGE / TIMEOUTFINISHED / TIMEOUT

Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT CHANGE_CIPHER_SPEC / Alert(FATAL,DECODE_ERROR) Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY)

PSK_CLIENT_HELLO / TIMEOUTPSK_CLIENT_KEY_EXCHANGE / TIMEOUTFINISHED / TIMEOUTAPPLICATION / APPLICATION

Alert(WARNING,CLOSE_NOTIFY) / Alert(WARNING,CLOSE_NOTIFY) Alert(FATAL,UNEXPECTED_MESSAGE) / TIMEOUT APPLICATION / Alert(FATAL,UNEXPECTED_MESSAGE)

CHANGE_CIPHER_SPEC / TIMEOUT

PSK_CLIENT_HELLO / TIMEOUTPSK_CLIENT_KEY_EXCHANGE / TIMEOUTFINISHED / TIMEOUT