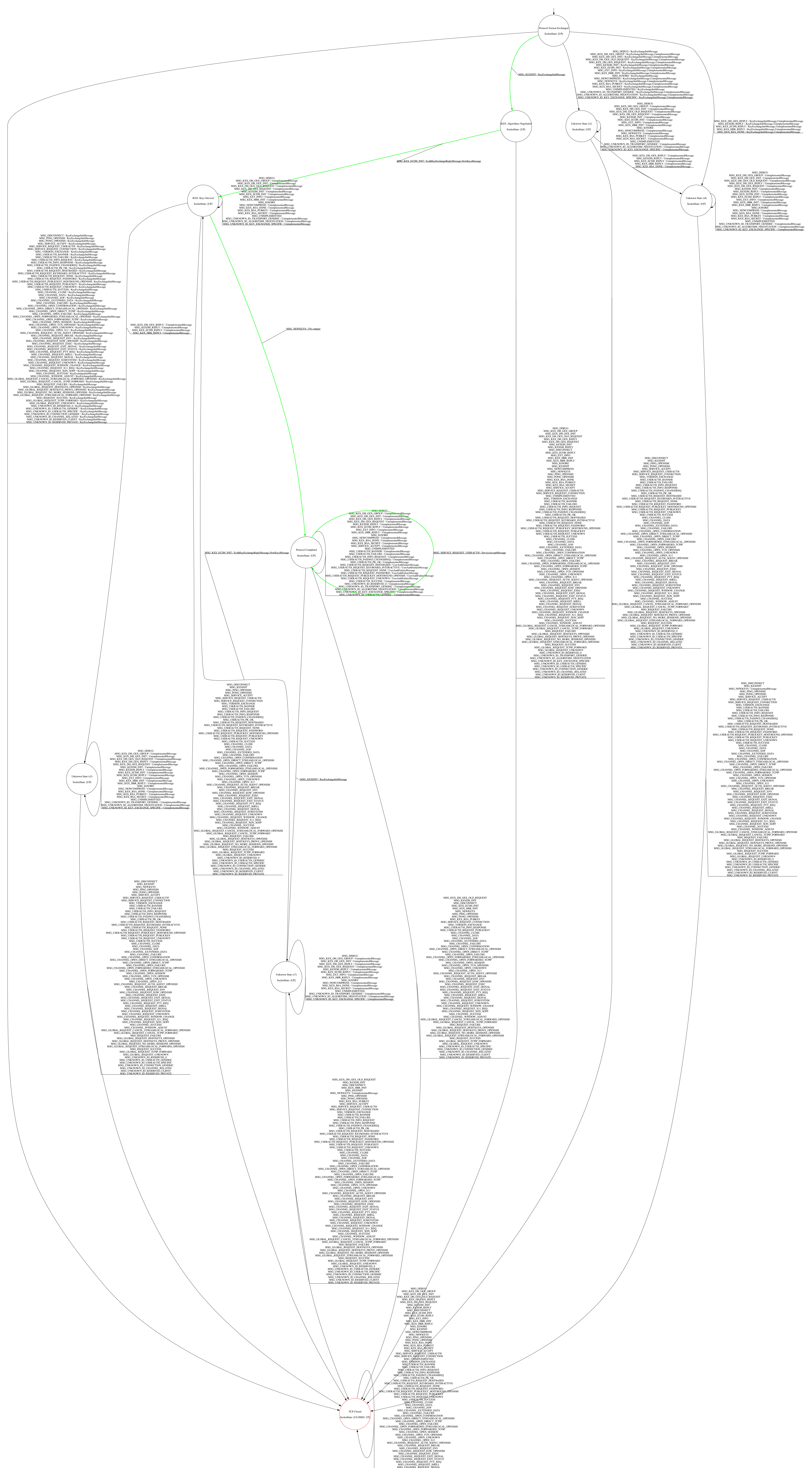

Server/Client: Dropbear 2025.87
Protocol Stage: TRANSPORT
KEX Algorithm: ecdh-sha2-nistp256
Strict KEX enabled: true

Messages used during testing:
MSG_DEBUG
MSG_KEX_DH_GEX_GROUP
MSG_KEX_DH_GEX_INIT
MSG_KEX_DH_GEX_OLD_REQUEST
MSG_KEX_DH_GEX_REPLY
MSG_KEX_DH_GEX_REQUEST
MSG_KEXDH_INIT
MSG_KEXDH_REPLY
MSG_DISCONNECT
MSG_KEX_ECDH_INIT
MSG_KEX_ECDH_REPLY
MSG_EXT_INFO
MSG_KEX_HBR_INIT
MSG_KEX_HBR_REPLY
MSG_IGNORE
MSG_KEXINIT
MSG_NEWCOMPRESS
MSG_NEWKEYS
MSG_PING_OPENSSH
MSG_PONG_OPENSSH
MSG_KEX_RSA_DONE
MSG_KEX_RSA_PUBKEY
MSG_KEX_RSA_SECRET
MSG_SERVICE_ACCEPT
MSG_SERVICE_REQUEST_USERAUTH
MSG_SERVICE_REQUEST_CONNECTION
MSG_UNIMPLEMENTED
MSG_VERSION_EXCHANGE
MSG_USERAUTH_BANNER
MSG_USERAUTH_FAILURE
MSG_USERAUTH_INFO_REQUEST
MSG_USERAUTH_INFO_RESPONSE
MSG_USERAUTH_PASSWD_CHANGEREQ
MSG_USERAUTH_PK_OK
MSG_USERAUTH_REQUEST_HOSTBASED
MSG_USERAUTH_REQUEST_KEYBOARD_INTERACTIVE
MSG_USERAUTH_REQUEST_NONE
MSG_USERAUTH_REQUEST_PASSWORD
MSG_USERAUTH_REQUEST_PUBLICKEY_HOSTBOUND_OPENSSH
MSG_USERAUTH_REQUEST_PUBLICKEY
MSG_USERAUTH_REQUEST_UNKNOWN
MSG_USERAUTH_SUCCESS
MSG_CHANNEL_CLOSE
MSG_CHANNEL_DATA
MSG_CHANNEL_EOF
MSG_CHANNEL_EXTENDED_DATA
MSG_CHANNEL_FAILURE
MSG_CHANNEL_OPEN_CONFIRMATION
MSG_CHANNEL_OPEN_DIRECT_STREAMLOCAL_OPENSSH
MSG_CHANNEL_OPEN_DIRECT_TCPIP
MSG_CHANNEL_OPEN_FAILURE
MSG_CHANNEL_OPEN_FORWARDED_STREAMLOCAL_OPENSSH
MSG_CHANNEL_OPEN_FORWARDED_TCPIP
MSG_CHANNEL_OPEN_SESSION
MSG_CHANNEL_OPEN_TUN_OPENSSH
MSG_CHANNEL_OPEN_UNKNOWN
MSG_CHANNEL_OPEN_X11
MSG_CHANNEL_REQUEST_AUTH_AGENT_OPENSSH
MSG_CHANNEL_REQUEST_BREAK
MSG_CHANNEL_REQUEST_ENV
MSG_CHANNEL_REQUEST_EOW_OPENSSH
MSG_CHANNEL_REQUEST_EXEC
MSG_CHANNEL_REQUEST_EXIT_SIGNAL
MSG_CHANNEL_REQUEST_EXIT_STATUS
MSG_CHANNEL_REQUEST_PTY_REQ
MSG_CHANNEL_REQUEST_SHELL
MSG_CHANNEL_REQUEST_SIGNAL
MSG_CHANNEL_REQUEST_SUBSYSTEM
MSG_CHANNEL_REQUEST_UNKNOWN
MSG_CHANNEL_REQUEST_WINDOW_CHANGE
MSG_CHANNEL_REQUEST_X11_REQ
MSG_CHANNEL_REQUEST_XON_XOFF
MSG_CHANNEL_SUCCESS
MSG_CHANNEL_WINDOW_ADJUST
MSG_GLOBAL_REQUEST_CANCEL_STREAMLOCAL_FORWARD_OPENSSH
MSG_GLOBAL_REQUEST_CANCEL_TCPIP_FORWARD
MSG_REQUEST_FAILURE
MSG_GLOBAL_REQUEST_HOSTKEYS_OPENSSH
MSG_GLOBAL_REQUEST_HOSTKEYS_PROVE_OPENSSH
MSG_GLOBAL_REQUEST_NO_MORE_SESSIONS_OPENSSH
MSG_GLOBAL_REQUEST_STREAMLOCAL_FORWARD_OPENSSH
MSG_REQUEST_SUCCESS
MSG_GLOBAL_REQUEST_TCPIP_FORWARD
MSG_GLOBAL_REQUEST_UNKNOWN
MSG_UNKNOWN_ID_RESERVED_0
MSG_UNKNOWN_ID_TRANSPORT_GENERIC
MSG_UNKNOWN_ID_ALGORITHM_NEGOTIATION
MSG_UNKNOWN_ID_KEY_EXCHANGE_SPECIFIC
MSG_UNKNOWN_ID_USERAUTH_GENERIC
MSG_UNKNOWN_ID_USERAUTH_SPECIFIC
MSG_UNKNOWN_ID_CONNECTION_GENERIC
MSG_UNKNOWN_ID_CHANNEL_RELATED
MSG_UNKNOWN_ID_RESERVED_CLIENT
MSG_UNKNOWN_ID_RESERVED_PRIVATE