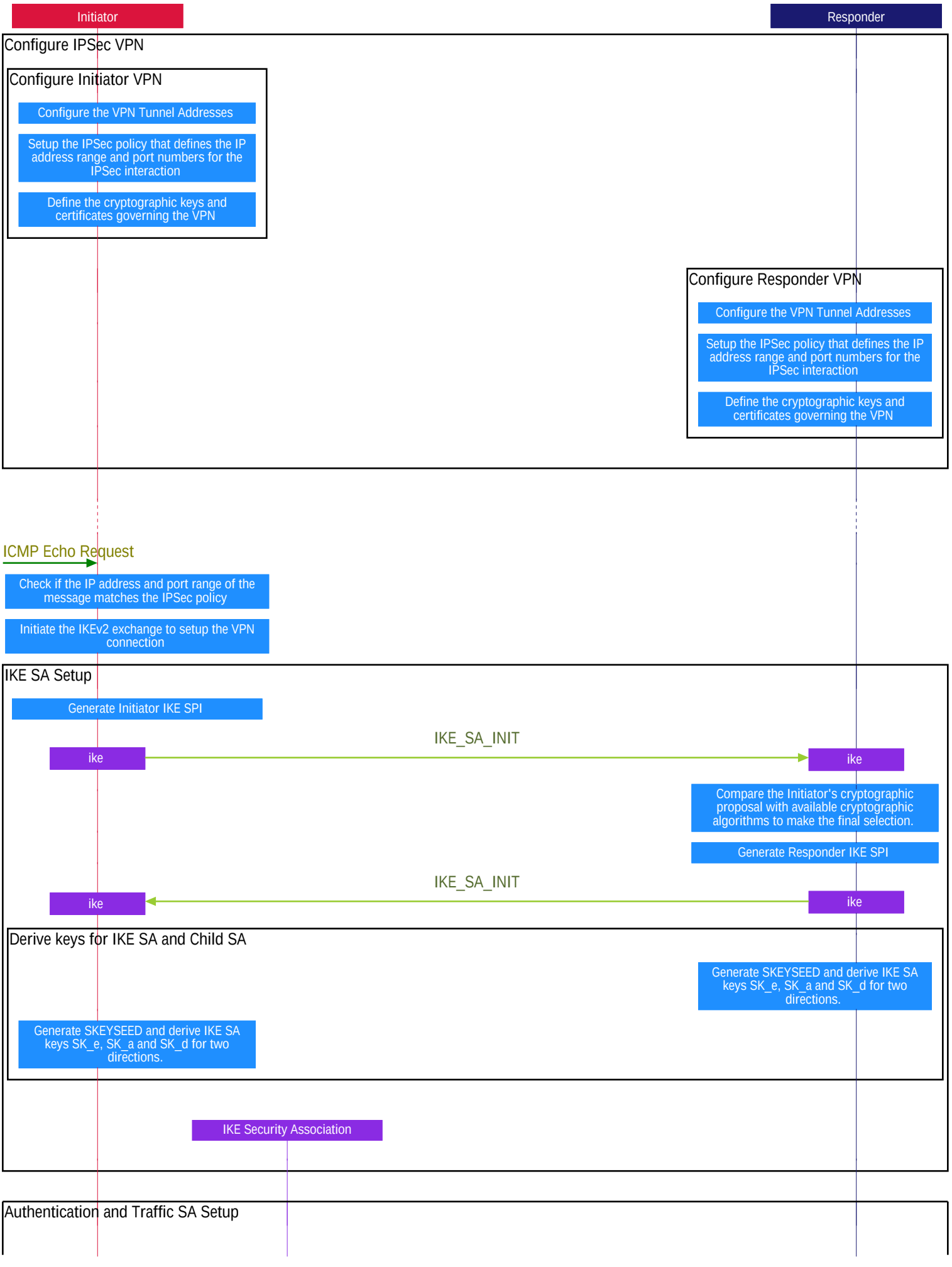
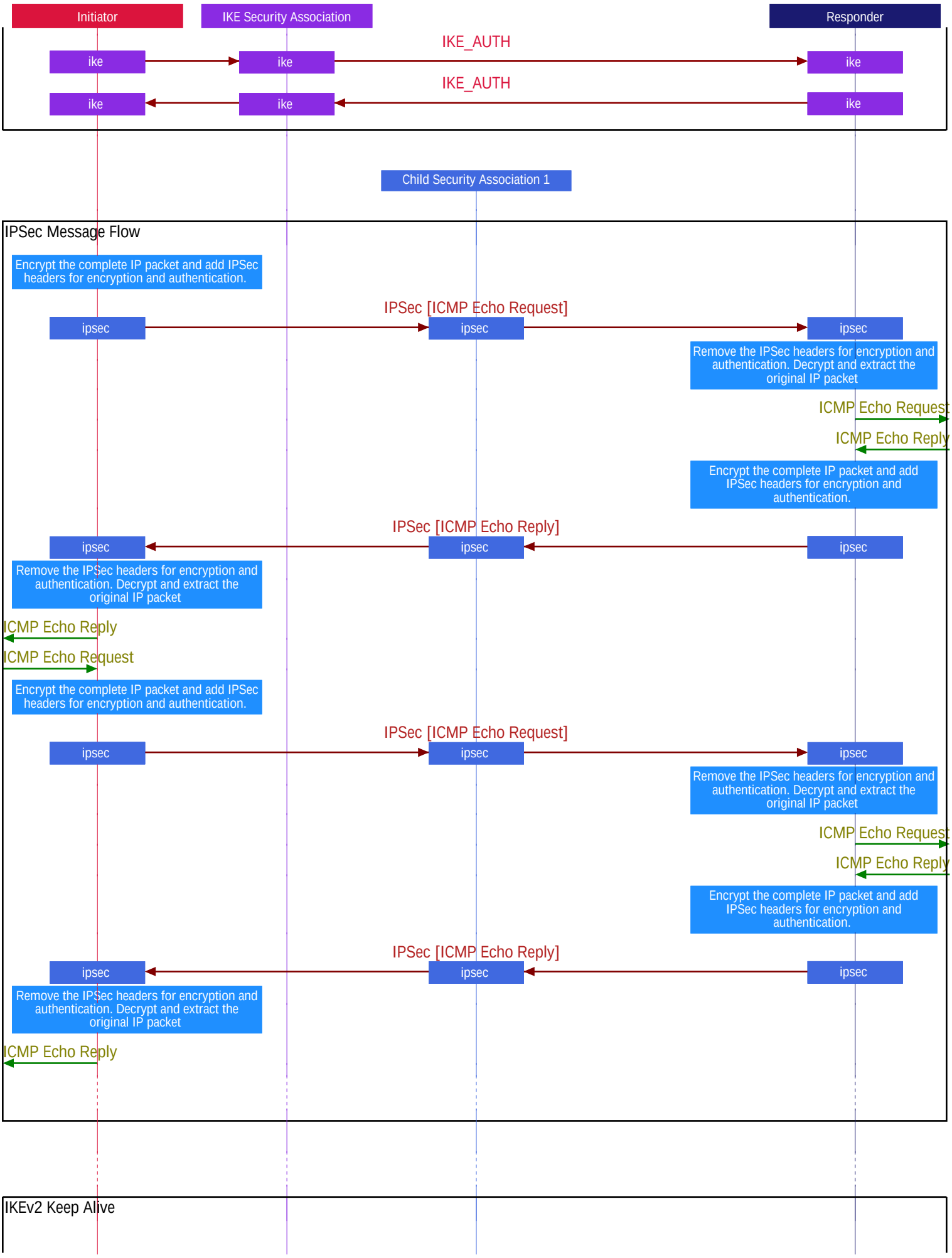
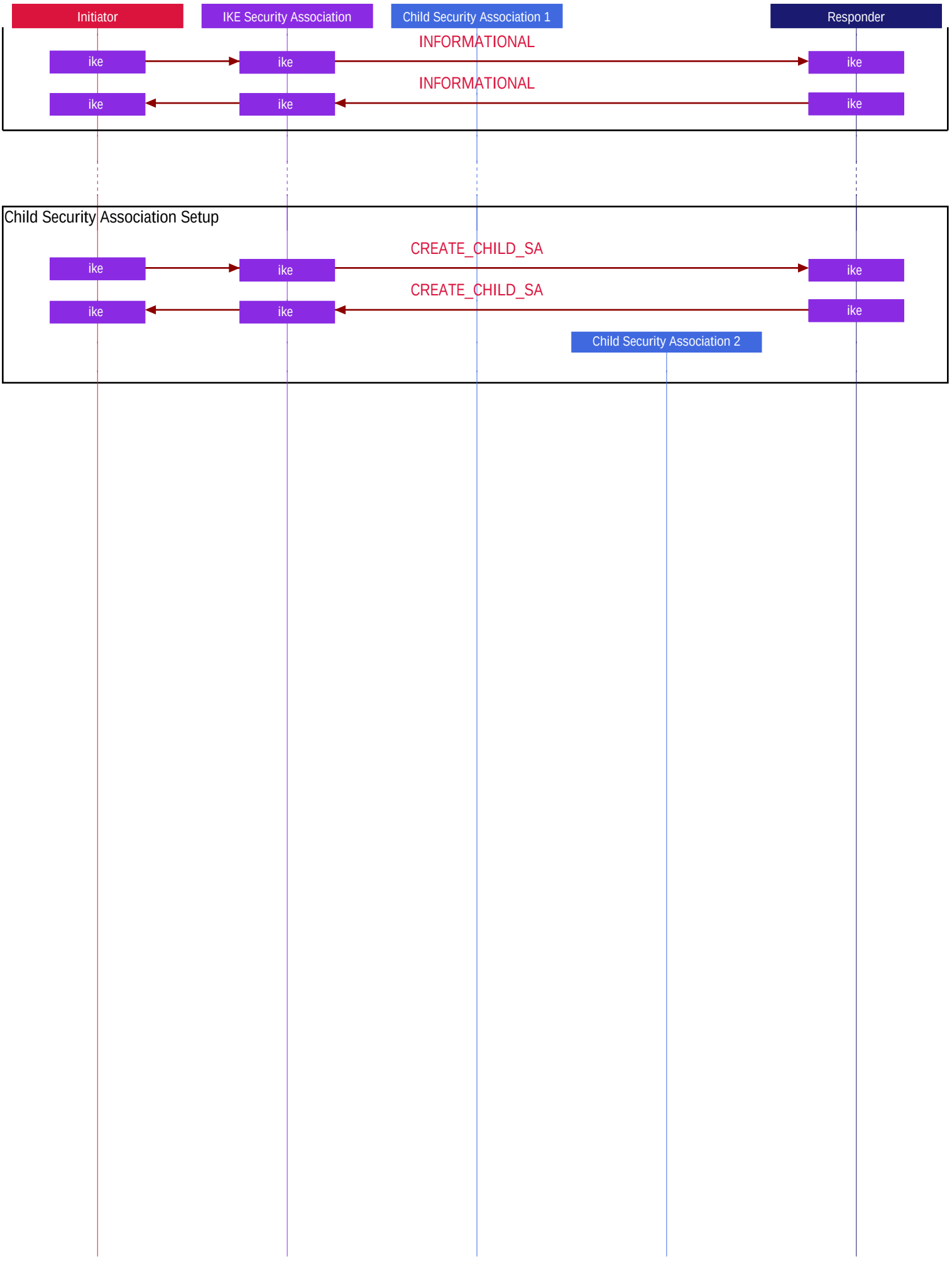

Initiator
Responder
Configure IPSec VPN
Configure Initiator VPN
Configure the VPN Tunnel Addresses
Setup the IPSec policy that defines the IP address range and port numbers for the IPSec interaction
Define the cryptographic keys and certificates governing the VPN
Configure Responder VPN
Configure the VPN Tunnel Addresses
Setup the IPSec policy that defines the IP address range and port numbers for the IPSec interaction
Define the cryptographic keys and certificates governing the VPN
ICMP Echo Request
Check if the IP address and port range of the message matches the IPSec policy
Initiate the IKEv2 exchange to setup the VPN connection
IKE SA Setup
Generate Initiator IKE SPI
IKE_SA_INIT
ike
ike
Compare the Initiator's cryptographic proposal with available cryptographic algorithms to make the final selection.
Generate Responder IKE SPI
IKE_SA_INIT
ike
ike
Derive keys for IKE SA and Child SA
Generate SKEYSEED and derive IKE SA keys SK_e, SK_a and SK_d for two directions.
Generate SKEYSEED and derive IKE SA keys SK_e, SK_a and SK_d for two directions.
IKE Security Association
Authentication and Traffic SA Setup


Initiator
IKE Security Association
Responder
IKE_AUTH
ike
ike
ike
IKE_AUTH
ike
ike
ike
Child Security Association 1
IPSec Message Flow
Encrypt the complete IP packet and add IPSec headers for encryption and authentication.
IPSec [ICMP Echo Request]
ipsec
ipsec
ipsec
Remove the IPSec headers for encryption and authentication. Decrypt and extract the original IP packet
ICMP Echo Request
ICMP Echo Reply
Encrypt the complete IP packet and add IPSec headers for encryption and authentication.
IPSec [ICMP Echo Reply]
ipsec
ipsec
ipsec
Remove the IPSec headers for encryption and authentication. Decrypt and extract the original IP packet
ICMP Echo Reply
ICMP Echo Request
Encrypt the complete IP packet and add IPSec headers for encryption and authentication.
IPSec [ICMP Echo Request]
ipsec
ipsec
ipsec
Remove the IPSec headers for encryption and authentication. Decrypt and extract the original IP packet
ICMP Echo Request
ICMP Echo Reply
Encrypt the complete IP packet and add IPSec headers for encryption and authentication.
IPSec [ICMP Echo Reply]
ipsec
ipsec
ipsec
Remove the IPSec headers for encryption and authentication. Decrypt and extract the original IP packet
ICMP Echo Reply
IKEv2 Keep Alive


Initiator
IKE Security Association
Child Security Association 1
Responder
INFORMATIONAL
ike
ike
ike
INFORMATIONAL
ike
ike
ike
Child Security Association Setup
CREATE_CHILD_SA
ike
ike
ike
CREATE_CHILD_SA
ike
ike
ike
Child Security Association 2