Options for ECDH handshake using eOAM

Glen Kramer, Broadcom

Option 1: 4 attributes / 8 OAMPDUs

eOAM Attributes / TLVs

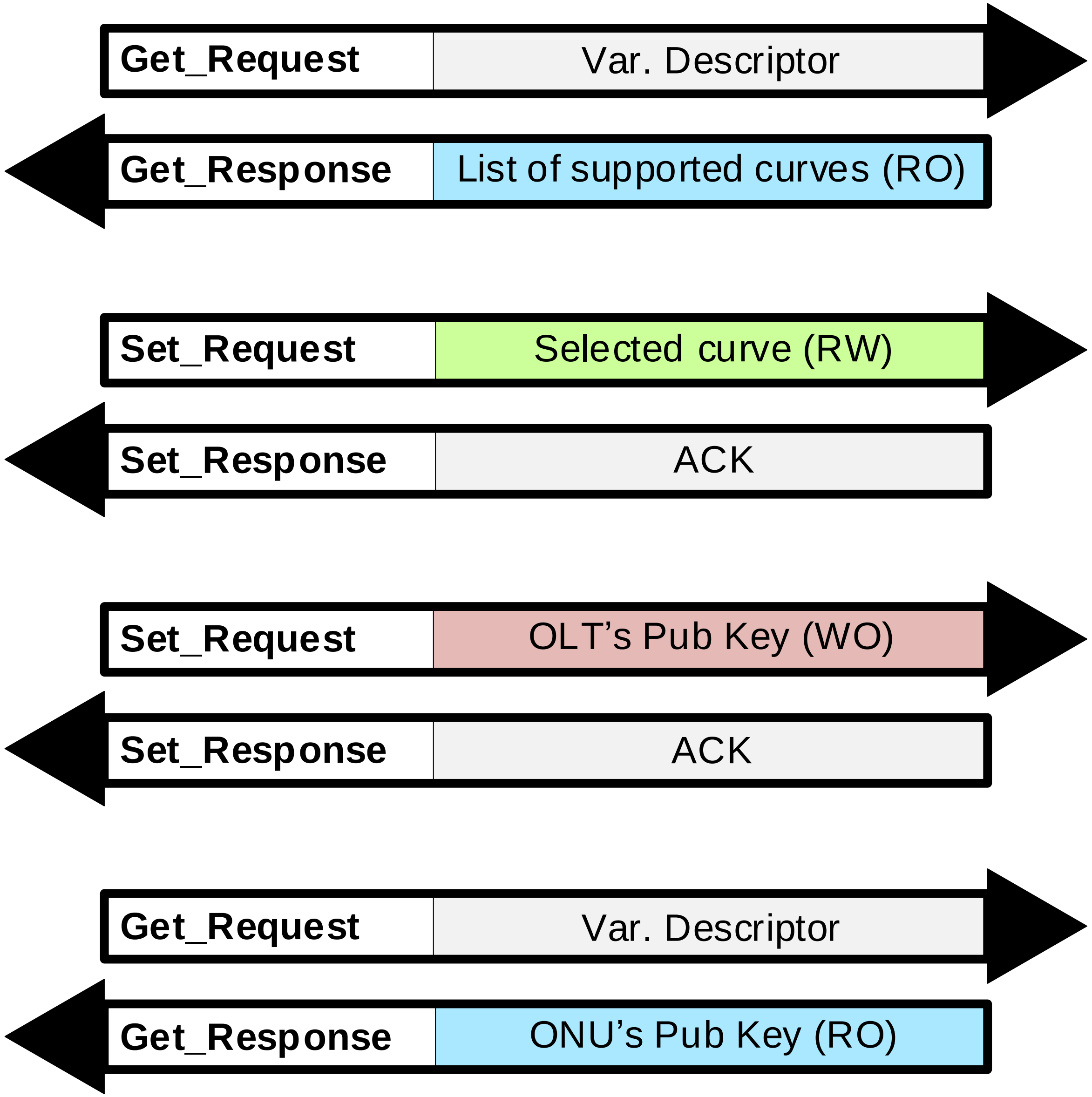
List of supported curves (RO)

Selected curve (RW)

OLT’s Pub Key (WO)

ONU’s Pub Key (RO)

- ❑ Each attribute is set/get using a separate Request/Response exchange
- ❑ Too many messages?
- ❑ OLT public key and ONU public key attributes are related, but will be defined in different sub-clauses (attributes vs. actions)
- ❑ Message order needs to be enforced via an explicit requirement



Get_Request Var. Descriptor

Get_Response List of supported curves (RO)

Set_Request Selected curve (RW)

Set_Response ACK

Set_Request OLT’s Pub Key (WO)

Set_Response ACK

Get_Request Var. Descriptor

Get_Response ONU’s Pub Key (RO)

Option 2: 4 attributes / 6 OAMPDUs

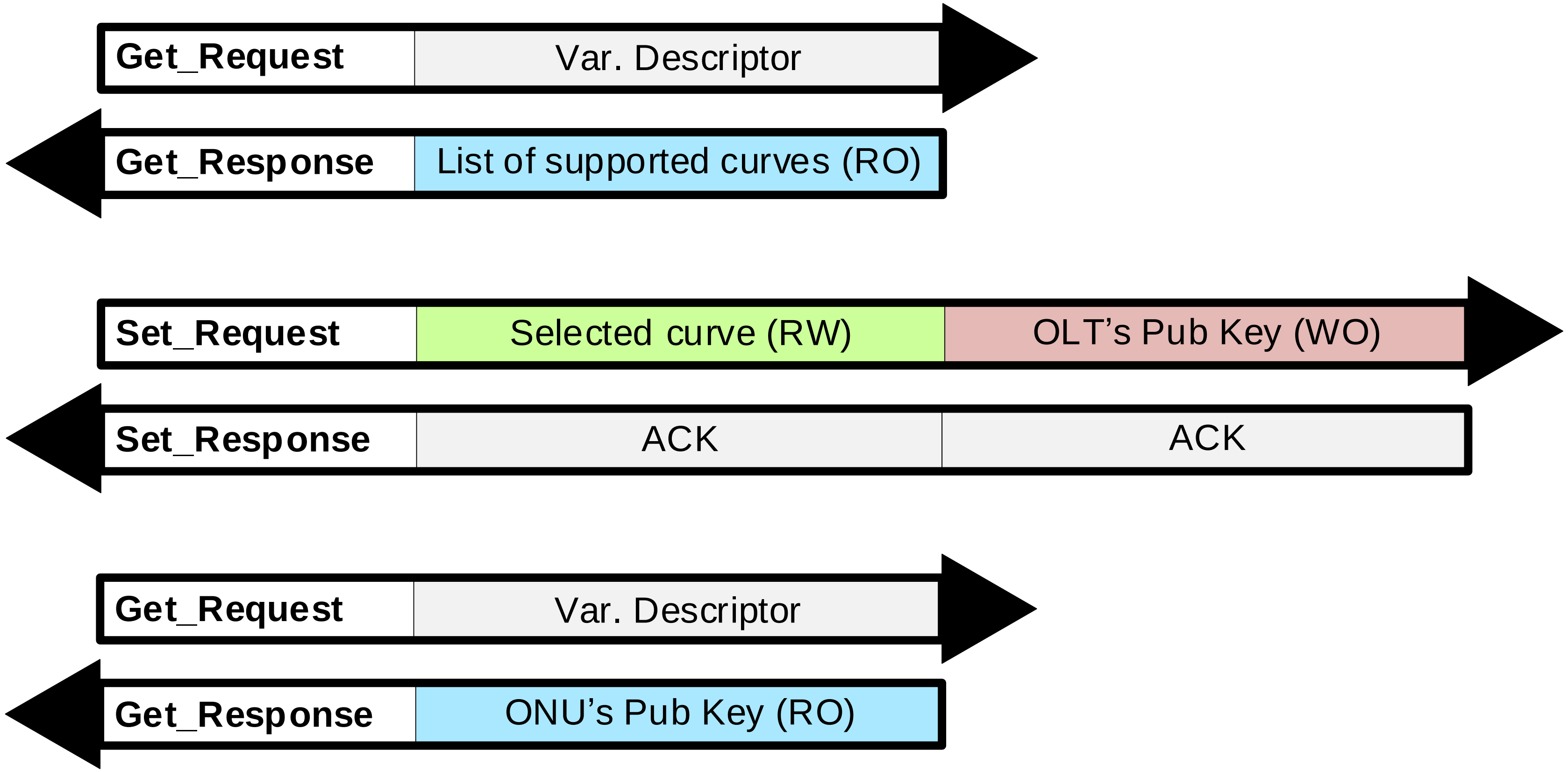
eOAM Attributes / TLVs

List of supported curves (RO)

Selected curve (RW)

OLT’s Pub Key (WO)

ONU’s Pub Key (RO)



Get_Request | Var. Descriptor

Get_Response | List of supported curves (RO)

Set_Request | Selected curve (RW) | OLT’s Pub Key (WO)

Set_Response | ACK | ACK

Get_Request | Var. Descriptor

Get_Response | ONU’s Pub Key (RO)

- Can put two TLVs into one OAMPDU
- OLT public key and ONU public key attributes are related, but will be defined in different sub-clauses (attributes vs. actions)
- Message order needs to be enforced via an explicit requirement

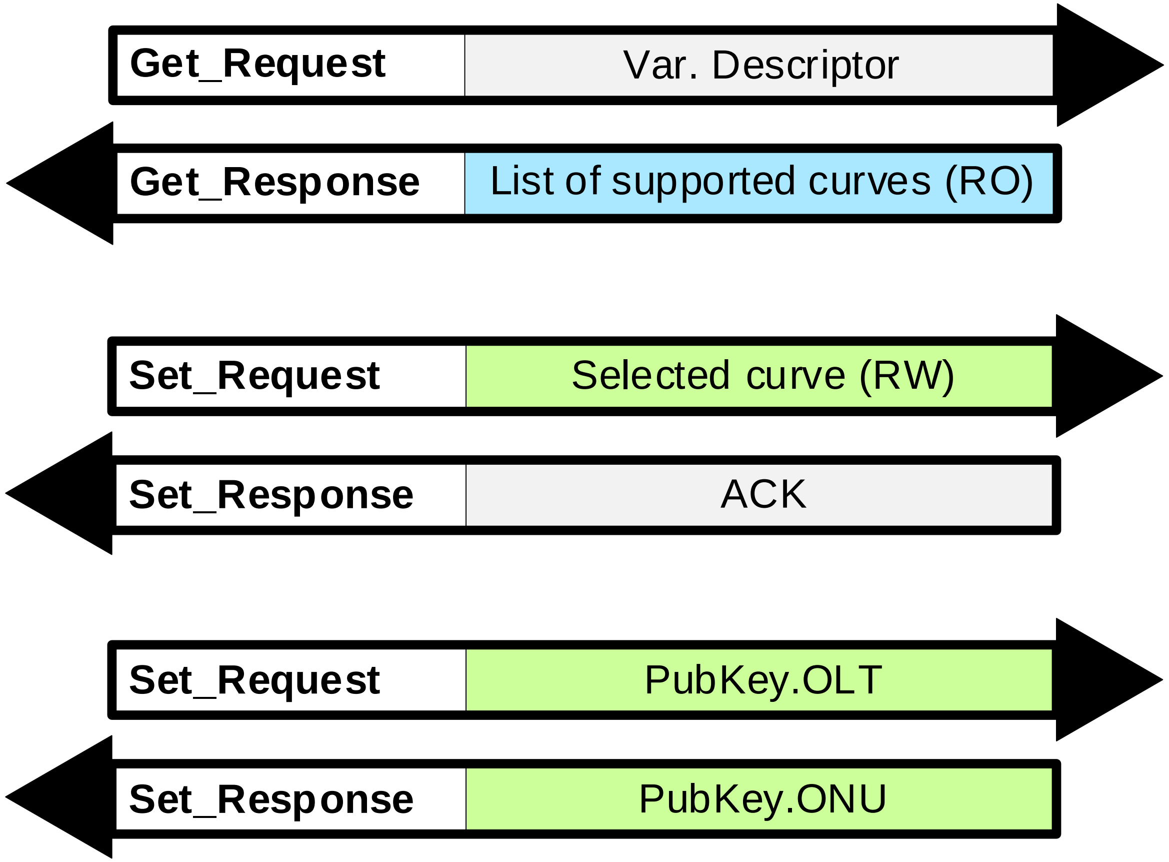
Option 3: 3 attributes / 6 OAMPDUs

eOAM Attributes / TLVs

List of supported curves (RO)

Selected curve (RW)

PubKey (RW)	.OLT (WO)
	.ONU (RO)



Get_Request | Var. Descriptor

Get_Response | List of supported curves (RO)

Set_Request | Selected curve (RW)

Set_Response | ACK

Set_Request | PubKey.OLT

Set_Response | PubKey.ONU

- ❑ Related OLT and ONU public keys are grouped together into one compound attribute consisting of two sub-attributes
  - .OLT (write only)
  - .ONU (read-only)
- ❑ Full variable container is used in both Set_Request and Set_Response
- ❑ Message order needs to be enforced via an explicit requirement

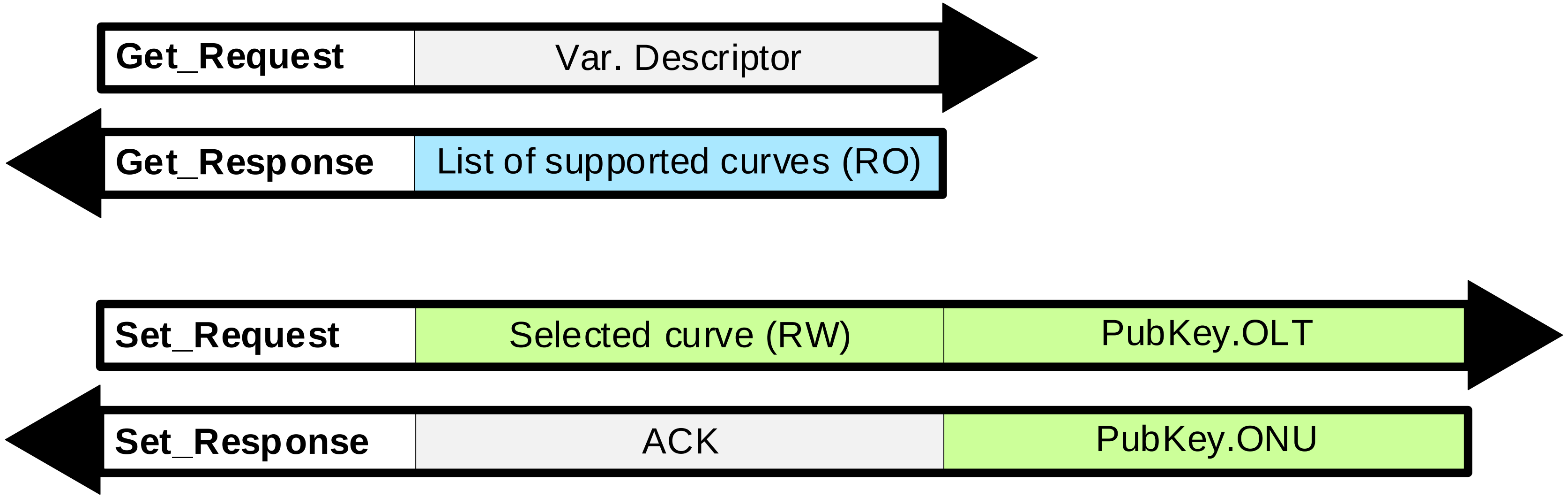
Option 4: 3 attributes / 4 OAMPDUs

eOAM Attributes / TLVs

List of supported curves (RO)

Selected curve (RW)

PubKey (RW)	.OLT (WO)
	.ONU (RO)



Get_Request | Var. Descriptor

Get_Response | List of supported curves (RO)

Set_Request | Selected curve (RW) | PubKey.OLT

Set_Response | ACK | PubKey.ONU

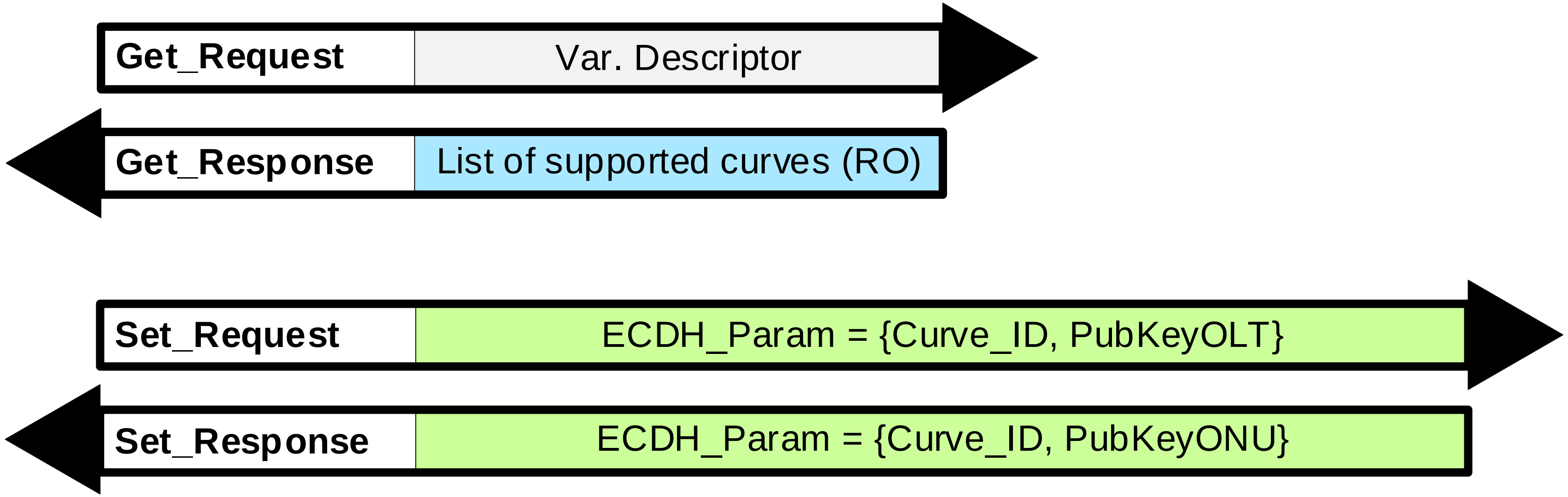
- Related OLT and ONU public keys are grouped together into one compound attribute consisting of two sub-attributes
  - .OLT (write only)
  - .ONU (read-only)
- Set_Request OAMPDU includes two Variable Container TLVs
- Set_Response OAMPDU includes one Response Code TLV and one full Variable Container TLV
- Message order is implicitly enforced by TLV order in the OAMPDU

Option 5: 2 attributes / 4 OAMPDUs

eOAM Attributes / TLVs

List of supported curves (RO)

ECDH Param.	.Curve_ID (RW)
	.PubKeyOLT (WO)
	.PubKeyONU (RO)



Get_Request Var. Descriptor

Get_Response List of supported curves (RO)

Set_Request ECDH_Param = {Curve_ID, PubKeyOLT}

Set_Response ECDH_Param = {Curve_ID, PubKeyONU}

- All ECDH negotiation parameters are grouped together into one compound attribute consisting of 3 sub-attributes
  - .SelectedCurve (read/write)
  - .OLT (write only)
  - .ONU (read-only)
  - TLV includes only Curve_ID and PubKey (identical TLV format in Request and Response)
- Set_Request OAMPDU includes one Variable Container TLVs
- Set_Response OAMPDU includes one Variable Container TLV
- Message order is implicitly enforced by the attribute definition

Thank you