## 11.3 Initial Key establishment

Once the OLT and the ONU have established communication using an MLID channel, they engage in an exchange of keying material to allow for mutual derivation of an initial symmetric encryption key used for secure communication. This ephemeral key exchange, illustrated in Figure 11-xx, enables Perfect Forward Secrecy (PTS), since encryption keys are not derived from persistent secrets used for peer authentication.

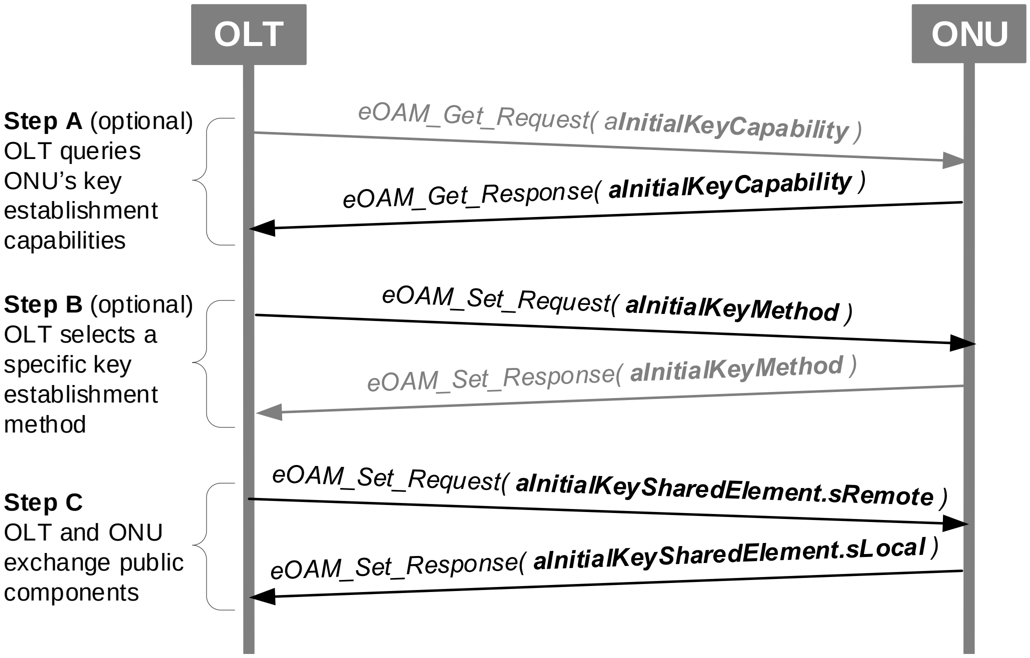
OLT
ONU
**Step A** (optional)
OLT queries
ONU's key
establishment
capabilities
eOAM_Get_Request( aInitialKeyCapability )
eOAM_Get_Response( aInitialKeyCapability )
**Step B** (optional)
OLT selects a
specific key
establishment
method
eOAM_Set_Request( aInitialKeyMethod )
eOAM_Set_Response( aInitialKeyMethod )
**Step C**
OLT and ONU
exchange public
components
eOAM_Set_Request( aInitialKeySharedElement.sRemote )
eOAM_Set_Response( aInitialKeySharedElement.sLocal )

**Figure 11-xx – Initial Key establishment protocol**

The key exchange is performed using a key establishment method negotiated between the OLT and ONU using three steps:

- In Step A, the OLT queries the ONU's supported key establishment methods using the *aInitialKeyCapability* attribute (see **Error! Reference source not found.**). This step is optional and is only performed if the OLT/NMS intends to use one of the non-mandatory methods.

- In Step B, the OLT selects a specific key establishment method using the *aInitialKeyMethod* attribute (see **Error! Reference source not found.**). The selected method can be any of the methods reported by the ONU in Step A, or one or mandatory methods, if Step A was omitted. Step B is optional and is only performed if the OLT/NMS intends to use the non-default method. The default key establishment method is `iana_tls_groups/secp256r1`.

- In Step C, the OLT and the ONU exchange their key components using the *aInitialKeySharedElement* attribute (see 14.4.5.3). The structure of the key components (also referred to as a public key) depends on the selected key establishment method. Both the *eOAM_Set_Request* message and the *eOAM_Set_Response* message carry the *Initial Key Shared Element* TLVs.

As with many OAMPDU attributes, compliant OLT implementation may choose to combine the *aInitialKeyMethod* attribute and *aInitialKeySharedElement* attribute into a single *eOAM_Set_Request* OAMPDU. A compliant ONU implementation may choose to combine the *aInitialKeyMethod* attribute and *aInitialKeySharedElement* attribute into a single *eOAM_Set_Response* OAMPDU.

11.

Once both parties have the other party’s key components, they mutually derive the initial key according to the selected key establishment method. The initial key is then activated according to the process defined in **Error! Reference source not found.**.

Once the initial key is activated, communication between the ONU and OLT is private – ensuring that other ONUs cannot observe communication between the parties. However the authenticity of the parties and the initial key is not established until the authentication process described in **Error! Reference source not found.** is successfully completed.

1.

11.