11 Security-oriented mechanisms

11.1 Introduction

11.2 Overview of SIEPON.4 security architecture

11.2.2 Encryption entity

11.2.3 Location of encryption/decryption functions

11.2.4 Latency requirements

11.2.5 Establishment of security mechanisms

The process of adding a new ONU to a PON follows a series of defined steps, ensuring secure ONU integration and subsequent operation. Figure 11-1 illustrates these steps:

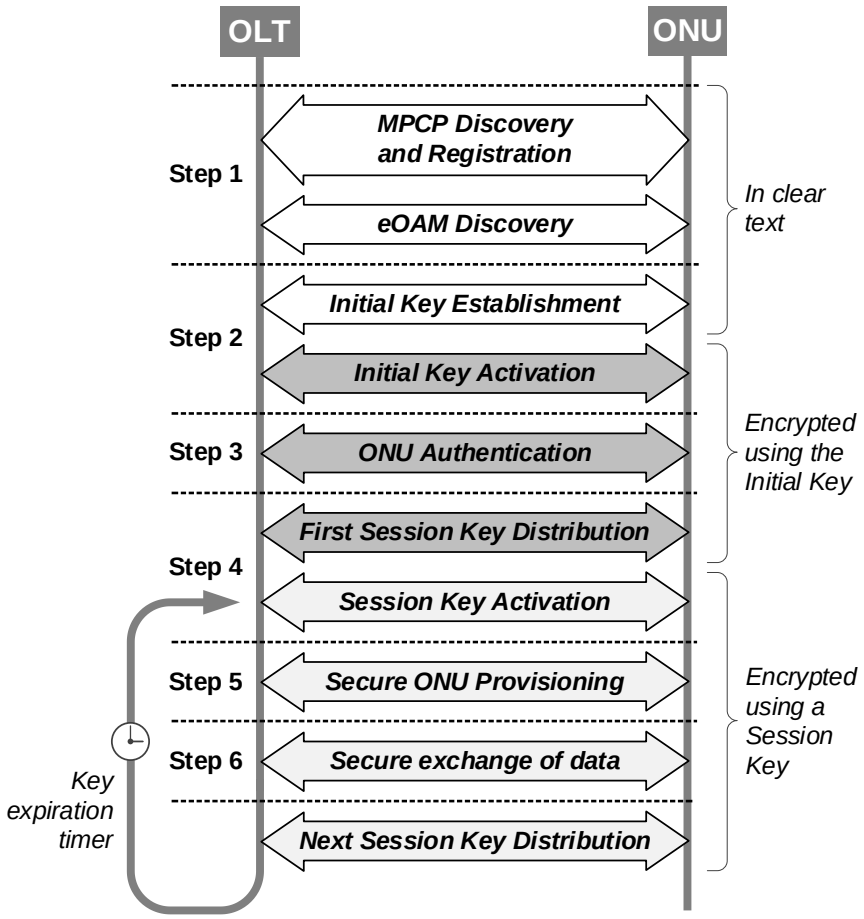

Figure 11-1–Sequence of steps to establish secure ONU operation

Step 1 - ONU Discovery and Registration: Upon completion of the boot/restart sequence, the ONU completes the MPCP and eOAM discovery processes as specified in **Error! Reference source not found.**. At this time, ONU gets assigned two logical links: PLID for exchanging the GATE and REPORT MPCPDUs and MLID for exchanging the OAM control messages (OAMPDUs). The MPCP and OAM discoveries are performed in the clear, i.e., using unencrypted MPCP and OAM messages.

Step 2 – Establishment of the initial key: Once the OLT and the ONU have established an MLID, they exchange keying material used for mutual derivation of an initial symmetric cryptographic key that enables private communication between the ONU and OLT and perfect forward secrecy (PFS). This is described in detail in 0.

Step 3 – Authentication: Upon establishment of the initial key, the ONU and OLT proceed with authentication using the method defined in 0. This step ensures that the ONU is a trusted entity within the network and that the initial key is authentic.

Step 4 – Secure distribution and activation of session keys: The OLT/NMS distributes the new session key to the ONU using the session key distribution protocol (see 11.5). The messages exchanged under the session key distribution protocol are encrypted using the initial key obtained in Step 2 above. After the encryption key is distributed to the ONU, the OLT initiates a switch to the new key (i.e., key activation by both the OLT and the ONU), using the procedure described in 0.

Step 5 – Secure provisioning of additional logical links: With the encryption of the PLID and MLID of the given ONU established, the NMS can proceed with provisioning of the additional bidirectional and unidirectional (multicast) logical links for this ONU. The additional logical links are provisioned using the extended action *acConfigLlid* (see **Error! Reference source not found.**).

Note that no additional encryption configuration steps are needed for the newly-provisioned bidirectional links. These links automatically begin operating with the ONU's currently active session encryption key. However, this is not the case for the newly provisioned unidirectional (multicast) logical links. As explained in 11.5.3, each of multicast logical link uses a unique encryption key that is shared among all members of this multicast group. Therefore, before the ONU is able to process the data frames received on the multicast logical link, it needs to obtain the specific encryption key for that multicast group. The multicast keys are distributed using the same extended action *acConfigEncrKey* (see **Error! Reference source not found.**) as is used for the unicast keys.

The control messages that provision additional logical links (*acConfigLlid* actions) and the messages that convey encryption keys for the multicast LLIDs (*acConfigEncrKey* action) are securely exchanged between the OLT and an ONU via the encrypted MLID link.

Step 6 - Exchange of encrypted data and control messages: With the session keys distributed by the OLT and additional ULIDs provisioned for carrying the subscriber data, the OLT and the ONU can securely exchange data frames over the PON. The data frames are encrypted using the session key to ensure confidentiality and integrity during transmission. The cryptographic method is defined in 0. The OLT can also provide credential and trust store updates to the ONU for future authentication as described in 0.