11 Security-oriented mechanisms

11.1 Introduction

[omitted]

11.2 Overview of SIEPON.4 security architecture

[omitted]

11.3 Authentication of the ONU

[omitted]

11.4 Initial key establishment

Once the ONU and OLT have completed the authentication exchange, the initial AES-128 encryption key shall be established by both parties from the least-significant 128 bits (16 octets) of the MSK, which is derived from the TLS 1.3 ephemeral session key as described in RFC-9190 section 2.3.

The initial key is used by the OLT to encrypt the MLID channel for distribution of a new session key to the ONU. See section 11.5 for details on the session key distribution protocol.