Contents

IEEE Standard for Service Interoperability in Ethernet Passive Optical Networks (SIEPON.4)

1 Normative References

Add the following references:

[SECv3.0] Data-Over-Cable Service Interface Specifications, Security Specification, CM-SPSECv3.0-C01-171207, December 7, 2017, Cable Television Laboratories, Inc.

2 Definitions, acronyms, and abbreviations

2.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[1]

25/10G-EPON: An EPON architecture supporting a maximum sustained throughput of 25 Gb/s in the downstream direction and 10 Gb/s in the upstream direction (asymmetric rate).

25/25G-EPON: An EPON architecture supporting a maximum sustained throughput of 25 Gb/s in both downstream and upstream directions (symmetric rate).

2.2 Acronyms and abbreviations

(Add these acronyms)

SAK	Security Association Key

[1] *IEEE Standards Dictionary Online* is available at http://ieeexplore.ieee.org/.

11 Security-oriented mechanisms

11.1 Introduction

Clause 11 introduces the security-related mechanisms, focusing in particular on various aspects of ONU authentication (see 11.2) and data encryption (see 11.3), achieved in an interoperable manner.

11.1.1 Threat model

The security threat model in PONs encompasses various risks and vulnerabilities that need to be addressed to ensure a secure and reliable network infrastructure:

- **Broadcast of downstream data**:
  One of the inherent vulnerabilities in PONs is the broadcast nature of downstream data transmission. As downstream data is broadcasted to all ONUs attached to the OLT's PON port, a malicious user who gains control of an ONU or attaches an un-authorized device could intercept and access downstream data intended for all connected users. This poses a significant risk to the confidentiality and privacy of user data.

- **Impersonation and service theft**:
  Due to the nature of upstream data transmission in PONs, where data can originate from any ONU attached to the ODN, a malicious user with control over an ONU could forge packets to impersonate a different ONU. This "theft of service" attack allows the attacker to masquerade as a legitimate ONU, potentially gaining unauthorized access to network resources or services.

- **Infrastructure Tampering**:
  An attacker could compromise the security of the PON infrastructure by physically tampering with street cabinets, spare ports, or fiber cables. By connecting a malicious device at various points within the network, the attacker could intercept and manipulate network traffic. Depending on the location of the malicious device, it could impersonate the OLT, allowing unauthorized access and control over the network, or impersonate an ONU to intercept and tamper with data.

- **Packet Replay and Bit-Flipping Attacks**:
  In PONs, a malicious user who successfully captures network packets transmitted on the PON could store and replay them at a later time. This replay attack poses a threat to data integrity and can lead to unauthorized access or service disruption. Additionally, an attacker could conduct bit-flipping attacks, altering the content of transmitted packets, potentially compromising the integrity and accuracy of the data.

11.1.2 Security mechanisms

The physical security and tamper-proof installation of the ODN, optical splitters, and ONUs can enhance the overall security of the PON infrastructure. By implementing physical security measures, such as secure enclosures, access controls, and tamper-evident mechanisms, the risk of unauthorized access or tampering can be significantly reduced. The recommended physical security measures are outlined in 11.6.

However, the specific threat landscape of PON installations requires deployment of specific security measures, such as robust authentication protocols, encryption mechanisms, network monitoring systems, and intrusion detection systems, to mitigate the identified threats effectively. By adopting a comprehensive and multi-layered security approach, PON operators can ensure the confidentiality, integrity, and authenticity of data transmitted over the network, even in scenarios where physical security measures are compromised or absent.

11.2 Overview of SIEPON.4 security architecture

11.2.1 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:

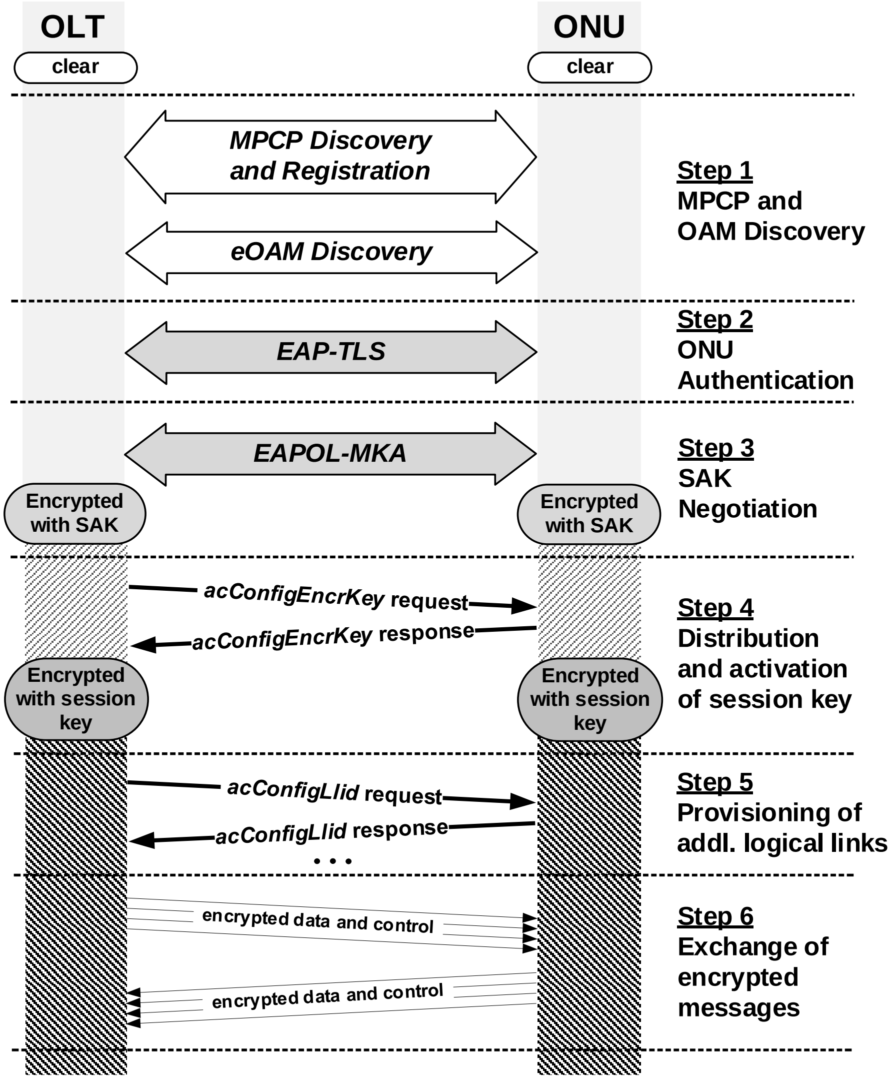

Figure 15-1 – Sequence of steps to establish secure ONU operation

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 13.3.1. 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 - ONU Authentication: Upon successful discovery and registration, the ONU proceeds with authentication. The OLT and the ONU employ the authentication method defined in 11.3 to ensure that the ONU is a trusted entity within the network.

Step 3 - Exchange of the initial Security Association Key: Once the ONU's identity is confirmed, the OLT and the ONU engage in an exchange of an initial cryptographic key for secure communication. This exchange utilizes the EAPOL-MKA protocol (see IEEE 802.1X, xxx). Through EAPOL-MKA, the OLT and the ONU establish a Security Association Key (SAK), which serves as the shared secret for encrypting and decrypting subsequent PON control frames (MPCPDUs exchanged on PLID logical link, and OAMPDUs exchanged on MLID logical link).

Step 4 – Secure distribution and activation of session keys: The OLT/NMS distributes the new session key to the ONU using the extended action *acConfigEncrKey* (see 14.x.x). The MLID envelope carrying the OAMPDU with the *acCofigEncKey*, and possible other OAMPDUs as well, is encrypted using the SAK obtained in Step 3 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 11.5.3.

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 *aConfigLlid* (see 14.6.2.8).

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 encryption key. However, this is not the case for the newly-provisioned unidirectional (multicast) logical links. As explained in TBD, 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 the that multicast group. The multicast keys are distributed using the same extended action *acConfigEncrKey* (TBD) 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 encryption method is defined in 11.4.

11.2.2 Encryption of bidirectional and unidirectional logical links

As explained in 4.5.1, all logical links of an ONU (whether provisioned or assigned during registration) are categorized as either bidirectional or unidirectional. The ONU is capable of receiving data from all provisioned logical links, while it can only transmit data through bidirectional links.

The traffic on all bidirectional links terminated at a specific ONU is encrypted using a single ONU-wide encryption key. When a key switch event occurs, it affects all bidirectional links, although for 50G-EPON ONUs, this event may happen at different times on different channels.

The unidirectional logical links are typically provisioned as point-to-multipoint (P2MP) links and carry downstream multicast traffic. Each envelope transmitted by the OLT is delivered to multiple ONUs. Therefore, the encryption key used to encrypt the multicast traffic needs to be shared among all ONUs that are part of the multicast group. Consequently, each unidirectional LLID at the ONU is provisioned to use a unique key that is distinct from the ONU-wide key used by all bidirectional LLIDs.

11.2.3 Location of the encryption function

11.3 ONU authentication

(THIS ENTIRE SECTION IS TAKEN FROM DPOE SECv2.0. IT MUST BE RE-WRITTEN)

The DPoE Network uses device identity and authentication procedures functionally equivalent to DOCSIS. The DPoE Network uses existing DOCSIS protocols for all interfaces from the DPoE Network to the OSS for back office compatibility. However, the protocols and procedures for device authentication within the DPoE Network (from the OLT to the ONU across the TU interface) are different from those in DOCSIS. All of the TU interface protocols are distinct from the subscriber interfaces (C and S) and the OSS and NSI interfaces (D and M). Because none of these protocols are visible to the subscriber or the service provider, the DPoE specifications do not affect existing products, services, or operations for service providers. These specifications are for interoperability between DPoE Network elements (the OLT or ONU).

11.3.1 ONU MAC Address Identity

DOCSIS uses the DOCSIS CM MAC address as the identity of the CM. The identity is not implicitly trusted, but is the basic identify for all DOCSIS service OAMP. OLT MUST use the EPON ONU MAC address as the identity of the ONU.

When a ONU is powered on, each logical link reports its MAC address to the OLT through the MPCP discovery process as defined in **Error! Reference source not found.**.

The OLT MUST support verification of the ONU's identity as authorized for the particular OLT port on which it is discovered. The OLT MUST NOT admit an authorized ONU on a different OLT port. The OLT MUST NOT admit an unauthorized ONU from accessing the network from any location. The OLT MAY use characteristics of the ONU in addition to the MAC address and OLT port, such as round-trip time, to deny access to ONU that are unexpectedly relocated.

The first ONU to register with a particular MAC address and pass authentication MUST be the only ONU with that MAC address allowed by the OLT on the OLT port. Duplicate ONU MAC addresses MUST NOT be allowed by the OLT.

11.3.2 ONU Authentication

The OLT assumes that the ONU identity cannot be trusted until the ONU has been authenticated. Authentication of the device is a prerequisite for later software download, device configuration, service configuration, and service operation. The DPoE Network emulates the behavior of the DOCSIS system, although the implementation within the DPoE Network across the TU interface differs in terms of packet formats. To external systems across the D interface, the ONU device authentication (based on the MAC address and certificates) operates as specified **Error! Reference source not found.**, **Error! Reference source not found.**, and **Error! Reference source not found.**.

The OLT MUST validate the ONU certificate using the procedures and criteria defined in **Error! Reference source not found.** and deny service to ONUs presenting invalid certificates. The OLT MUST verify that the MAC address in the ONU device certificate is the same as the source MAC address in the Ethernet frame it received from the ONU as part of ONU device certificate validation.

The length of time to authenticate a ONU SHOULD NOT exceed 300 seconds. (data doesn’t start for 5 minutes?)

11.3.3 Use of EAP-TLS for ONU Authentication

The packet format used to retrieve ONU certificates is EAP-TLS as defined in **Error! Reference source not found.**. This is a method of the EAP authentication framework, defined in **Error! Reference source not found.**. EAP is conveyed in Ethernet frames according to the EAP Over LAN (EAPOL) format as defined in [802.1X]. The summary of these specifications in this section is for informative purposes only.

Normative requirements for use of these specifications are signaled below with the usual upper-case keywords.

A typical message sequence for EAP-TLS in downstream-only mode is shown in Figure 1.

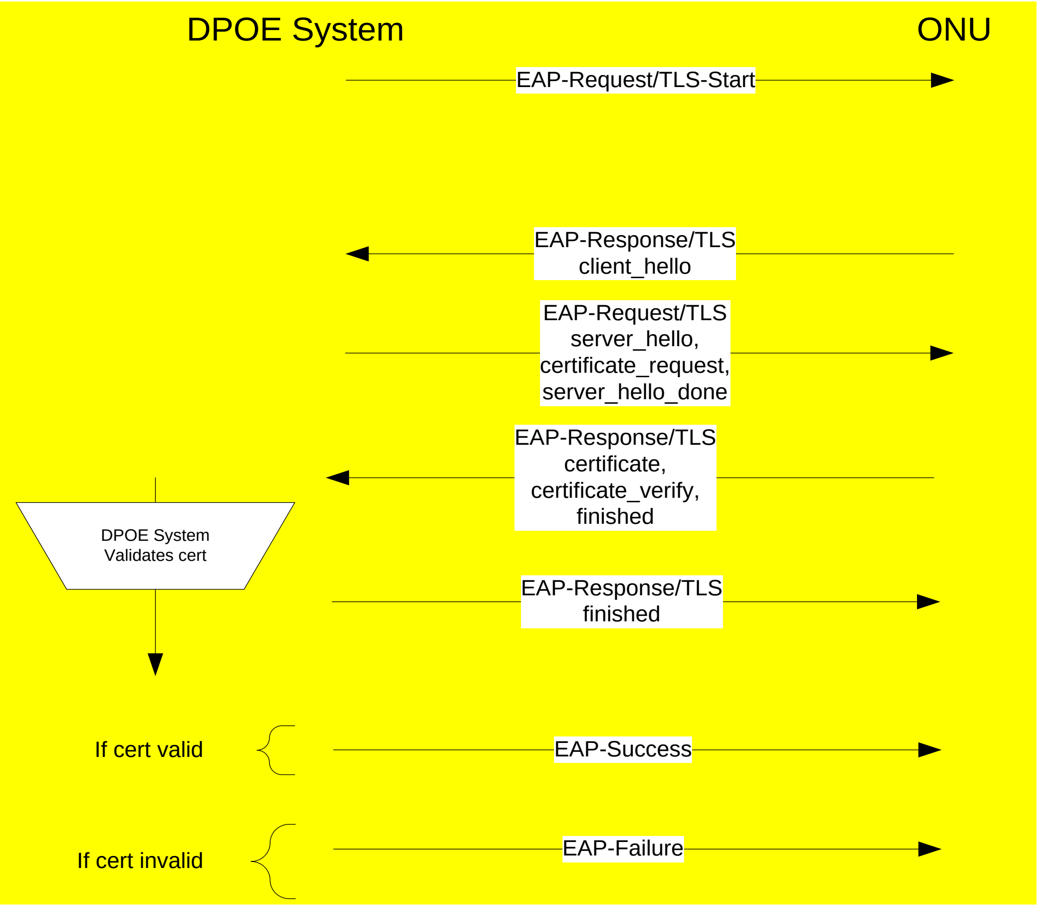
DPOE System
ONU
EAP-Request/TLS-Start
EAP-Response/TLS client_hello
EAP-Request/TLS server_hello, certificate_request, server_hello_done
EAP-Response/TLS certificate, certificate_verify, finished
DPOE System Validates cert
EAP-Response/TLS finished
If cert valid
EAP-Success
If cert invalid
EAP-Failure

Figure 1 - EAP-TLS Message Sequence

The EAP-TLS frame format is summarized in Figure 2.

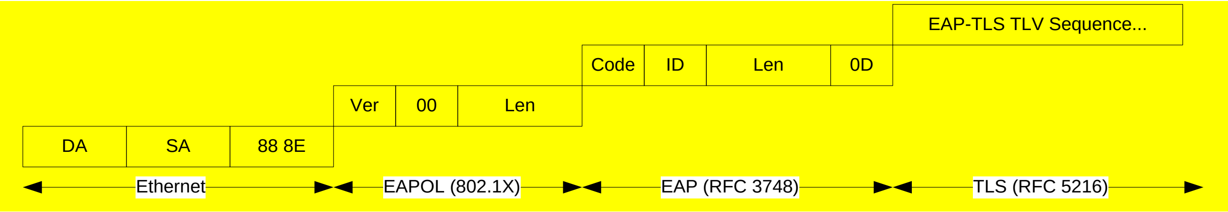

Figure 2 - EAP-TLS Frame Format

DA Ethernet Destination Address

SA	Ethernet Source Address
88 8E	EtherType assigned to EAPOL
Ver	EAPOL Version
Type	EAPOL Type (0x00, "EAP")
Len	Length of EAPOL Packet Body to follow
Code	EAP Packet Type Code (1-4, Request / Response / Success / Failure)
ID	Arbitrary ID number that matches Reponses to Requests
Len	Length of packet to follow
Type	EAP authentication method (0x0D, "TLS")

EAP-TLS in turn encapsulates the TLS protocol (**Error! Reference source not found.**). TLS exchanges T LS Records of various types that actually contain the data for key exchanges, authentication, and so on, as described earlier. TLS Records are a series of TLVs that can in theory be very long (2^24 bytes). The primary function of EAP-TLS in the protocol layering is to fragment a single TLS record (which is agnostic to maximum packet sizes) across multiple EAP frames (as EAP itself does not support fragmentation). The OLT MUST support EAP-TLS fragmentation as defined in RFC 5216. The ONU MUST support EAP-TLS fragmentation as defined in RFC 5216. In DPoE, the TLS record most likely to be fragmented is the ONU certificate response, which contains two X.509 certifications and could be a few thousand bytes long. Figure 3 shows a Flags field and TLS Len value for a fragmented TLS record containing a certificate message.

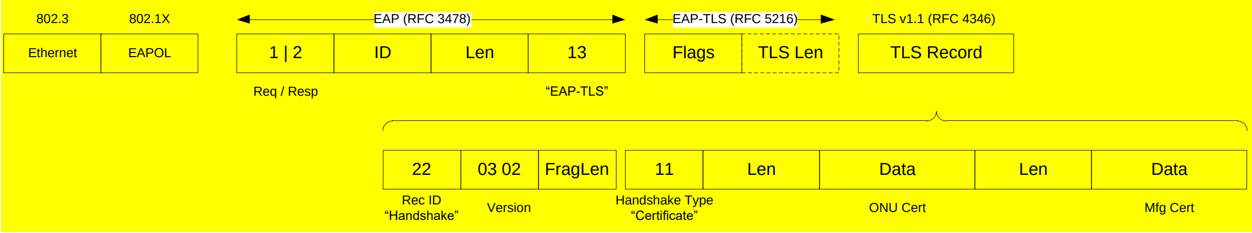

Figure 3 - EAP-TLS Frame Format 2

EAP-TLS frames always have a Flags field which indicates whether there is a 32-bit length field in this frame, and whether more frames with fragments of the current TLS record are expected. Only the frame containing the beginning of a particular TLS record has a TLS Len field; subsequent frames do not have the TLS Len field. All frames except the last frame containing a particular TLS Record have the "More Fragments" flag set; the final frame has the flag clear. A frame with a TLS Record that fits entirely in one frame has the More Fragments flag cleared (as it is the last frame), and also has the Length Present flag set (as it is also the first frame).

There are many length values in the entire frame, one at each protocol layer, each one measuring a slightly different sequence of bytes. The EAP-TLS length, shown as "TLS Len" in Figure 3 - EAP-TLS Frame Format 2 indicates the length of the entire TLS record across all fragments. The length inside the TLS record, shown as "Frag Len", indicates the length of this particular fragment only. Finally, the lengths inside the Handshake type Certificate TLV, shown as "Len" above, indicate the total length of the individual certificate that follows, whether fragmented or not. Appendix **Error! Reference source not found.** shows an example Certificate response fragmented across two Ethernet frames.

11.3.3.1 EAPOL Notes

The presence of a ONU is already well known to the OLT due to MPCP Registration and OAM Discovery, and so the Authenticator-Initiated option of EAPOL is used. A ONU MUST NOT send an EAPOL-Start frame to initiate Supplicant-Initiated Authentication.

Similarly, ONU deregistration is handled by MPCP. The ONU MUST NOT send an EAPOL-Logoff message before deregistering.

11.3.3.2 EAP Notes

The identity of a ONU is its MAC address. So, the OLT MUST NOT send an EAPOL-Request/Identity to the ONU to request its identity. Authentication begins with the OLT sending an EAP-Request/TLS-Start PDU to the ONU.

EAP-Success or Failure is determined by the OLT validation of the ONU certificate as described in Section **Error! Reference source not found.**, **Error! Reference source not found.**.

11.3.3.3 TLS Notes

The following notes describe changes to the TLS standard to support DPoE:

CipherSuite and Compression Negotiation

DPoE does not support CipherSuite and compression method negotiation. The key exchange and encryption algorithms to be used for DPoE are defined in this specification. The OLT MUST ignore the CipherSuite and compression fields in the ClientHello message. The ONU SHOULD NOT send any CipherSuites or compression methods in the ClientHello message. The ONU MUST ignore the CipherSuite and compression fields in the ServerHello message.

OLT Authentication

The OLT is assumed trusted and therefore is not authenticated. The OLT MUST NOT send a Certificate message to the ONU for server authentication.

ONU Authentication

ONU device authentication is supported by sending certificates to the OLT for validation. The OLT MUST send a CertificateRequest message to the ONU. The ONU MUST include a Certificate and CertificateVerify message in its response. The Certificate message sent by the ONU MUST contain the ONU device certificate and the CableLabs DPoE Mfr CA certificate. The CertificateVerify message contains hash values of the concatenation of all handshake messages, sent or received. For downstream-only mode those handshake messages are: ClientHello, ServerHello, CertificateRequest, ServerHelloDone, and Certificate. For bi-directional mode those handshake messages are: ClientHello, ServerHello, ServerKeyExchange, CertificateRequest, ServerHelloDone, Certificate, and ClientKeyExchange.

Key Exchange

TLS message requirements for exchanging keys depend upon the encryption mode. For downstream-only mode the ServerKeyExchange message and the ClientKeyExchange message are not used since the encryption keys have already been exchanged. The OLT MUST NOT send a ServerKeyExchange message when operating in downstream-only encryption mode. The ONU MUST NOT send a ClientKeyExchange message when operating in downstream-only encryption mode.

In bi-directional encryption mode both the ServerKeyExchange and ClientKeyExchange messages are used. The OLT MUST use a 2048 bit RSA public and private key pair for supporting exchange of the pre-master secret with ONU devices. The OLT's RSA public key MUST be sent to the ONU in the ServerKeyExchange message. After the ONU creates the premaster secret it MUST encrypt it using the

OLT’s public key and send it to the OLT in the ClientKeyExchange message. The OLT can then decrypt the pre-master secret using its private key. The CAK is derived from the pre-master secret.

ChangeCipherSpec Messages

The ChangeCipherSpec message is used by the client and server to indicate they are ready to begin L4 encryption of traffic (as in SSL). In DPoE there is another key exchange that occurs after EAP-TLS messaging to setup the traffic encryption key. Therefore, the ChangeCipherSpec messages do not apply. The OLT MUST NOT send a ChangeCipherSpec message. The ONU MUST NOT send a ChangeCipherSpec message.

Finished Messages

Finished messages are sent by the client and server to indicate that the TLS message exchange is complete. Since DPoE traffic encryption keys may not be exchanged until after EAP-TLS messaging the finished messages may not be encrypted. Downstream-only methods encrypt the channel before the TLS authentication sequence, and so all messages would be encrypted at L2. Bidirectional methods begin L2 encryption after the entire TLS sequence is complete. The OLT MUST NOT include hash results, a MAC value, or apply L4 encryption to the Finished message. The ONU MUST NOT include hash results, a MAC value, or apply L4 encryption to the Finished message. The Finished messages used with DPoE are thus zero length.

11.4 Data encryption and integrity protection

11.4.1 Introduction

11.4.2 Location of the encryption sub-layer

11.4.3 Encrypted envelope format

11.4.4 Cryptographic method

11.4.4.1 Encryptor function

11.4.4.2 Decryptor function

11.4.4.3 Initialization Vector (IV) construction

11.4.4.3.1 MPCP jitter correction

11.5 Encryption key management

11.5.1 Initial Security Association Key exchange

11.5.2 Key distribution protocol

11.5.3 Key activation protocol

11.5.4 Key storage in the OLT

11.5.5 Key storage in the ONU

11.5.6 Key lifetime

11.6 Physical protection of security data in the ONU

(THIS SECTION NEEDS REVIEW AND SANITY CHECK)

The physical protection measures outlined in this sub-clause collectively ensure the secure storage and protection of certificates and keys within ONUs in PON networks, safeguarding against unauthorized access and potential security breaches.

11.6.1 Secure Non-Volatile Storage

ONUs shall implement the requirements outlined in [SECv3.0] for secure non-volatile storage of certificates and their associated public/private keys. This ensures that sensitive cryptographic information remains protected from unauthorized disclosure and modification.

11.6.2 Protection against Unauthorized Access

ONUs should employ measures to prevent unauthorized access to the ONU certificate private key, particularly in production devices. One recommended approach is to restrict or block physical access to the memory that contains the private key. This prevents unauthorized individuals from using debugger tools to read the key.

11.6.3 Use of One-Time-Programmable (OTP) Memory

To enhance security and make it more challenging to replicate a valid ONU, ONUs should use one-time-programmable (OTP) memory for storing certificates and keys. OTP memory is designed to prevent alteration or cloning of the stored data, thereby bolstering the overall security of the ONU.

11.6.4 Compliance with FIPS-140-2 Security Requirements

The ONU shall meet the security requirements specified in the Federal Information Processing Standard (FIPS) 140-2 for all instances of permanent private and public key storage. FIPS-140-2 provides a rigorous set of cryptographic security standards, ensuring the confidentiality and integrity of the stored keys.

11.6.5 Compliance with FIPS-140-2 Security Level 1

The ONU shall also comply with FIPS-140-2 Security Level 1. This level requires minimal physical protection and shall be achieved through the use of production-grade enclosures. The enclosures for ONUs shall meet production-grade quality standards, including standard passivation sealing. The circuitry within the ONU shall be implemented as a production-grade multi-chip embodiment, typically in the form of an IC printed circuit board. The ONU itself should be contained within a metal or hard plastic enclosure, which may include doors or removable covers.