Contents

Style Definition: TOC 2

3 Definitions, acronyms, and abbreviations

3.1 Definitions

…

Encryption entity: A distinct logical element within a communication system that is responsible for maintaining the confidentiality of data exchanged within the communication system. In SIEPON.4 system, each ONU and each multicast group (i.e., multicast LLID) constitue a separate encryption entity. Each encryption entity encrypts data using its unique session key.

Initial Key: The 128 or 256-bit symmetric encryption key mutually derived by an ONU and OLT in order to commence the encryption process. The initial key is used for a short period of time to perform authentication and distribute the first session key to the ONU.

Session Key: The 128 or 256-bit symmetric encryption key used to encrypt traffic between an OLT and ONU. The session key is distributed periodically by the OLT to the ONU via existing encrypted MLID channels. A unique session key is provided to each encryption entity in the SIEPON.4 system.

DHE: Diffie-Hellman Exchange. A form of cryptographic network exchange that allows a shared secret to be established by two parties in a way that is not derivable by observers.

Deleted: the

Deleted: it takes

Deleted: e the ONU and to

Deleted: -bit

Deleted: the

Deleted: each

Deleted: s

Deleted: are

Deleted: s

Formatted: Font: Not Bold

11 Security-oriented mechanisms

11.1 Introduction

11.2 Overview of SIEPON.4 security architecture

11.3 Establishment of the initial key

Once the OLT and the ONU have established communication using an MLID channel, they engage in an exchange of key material to allow for mutual derivation of the initial symmetric encryption key used for secure communication.

As illustrated in Figure 11-4, the initial key is only in effect long enough to perform the ONU/mutual authentication (step 3) and to distribute the first session key (step 4). Once the first session key is distributed by the OLT and activated by OLT and the ONU, the initial key is discarded by both parties.

A common approach to establish a shared symmetric key is to use a Diffie–Hellman key exchange method (DHE) – which allows a shared secret to be privately established by two parties that is not derivable by observers – and then using the shared secret from the DHE to calculate the shared symmetric key. Several such methods are allowed by this clause to determine the initial key. The initial key establishment method negotiation and Diffie-Hellman key exchange is illustrated in Figure 11-5.

11.3.1 Mandatory DHE methods

The OLT and the ONU shall support DHE key initialization methods based on named elliptic curves *secp256r1* (see SECG-SEC2, 2.4.2) and *x25519* (see RFC 7748, 4.1).

11.3.2 Optional DHE methods

The OLT and the ONU should support DHE key initialization methods based on named elliptic curves *secp384r1* (see SECG-SEC2, 2.5.1) and *x448* (see RFC 7748, 4.2). The OLT and the ONU also may support *secp512r1* (see SECG-SEC2, 2.6.1).

11.3.3 Initial key exchange protocol

The DHE method determination and component exchange for establishing the initial key is illustrated in Figure 11-5.

Deleted: ing

Deleted: <#>A common approach to establish a shared key is to use Elliptic Curve Diffie-Hellman (ECDH) key exchange methods, which allow a common key to be established by two parties, but not be determined by observers. Several such methods are allowed by this clause. The initial key establishment method negotiation and Diffie-Hellman key exchange is defined in 11.3.3.¶
As illustrated in Figure 11-4, the initial key is only in effect long enough to perform the ONU/mutual authentication (step 3) and to distribute the first session key (step 4). Once the first session key is distributed by the OLT and is activated by the OLT and the ONU, the initial key is discarded by both parties.¶

Deleted: <#>**key establishment methods**

Deleted: the

Deleted: ECDH

Deleted: establishment

Deleted: key establishment

Deleted: the

Deleted: ECDH

Deleted: establishment

Deleted: Key

Deleted: Figure 11-5

Deleted: The negotiation of the ECDH key establishment method and the exchange of keying material consists of three steps illustrated in Figure 11-5.

Deleted: 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 11-5, enables perfect forward secrecy, since encryption keys are not derived from persistent secrets used for peer authentication.

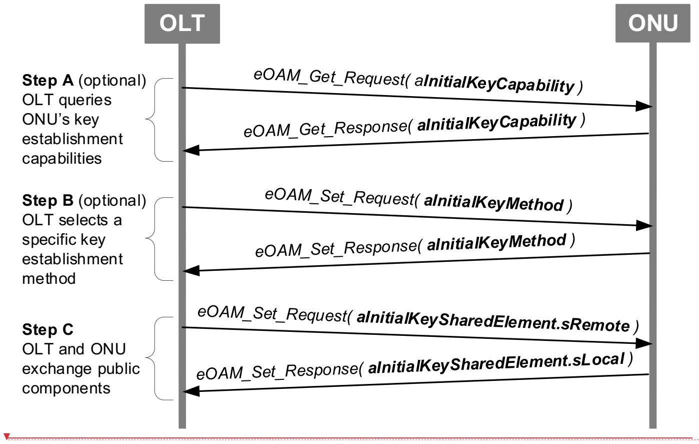

OLT
ONU
Step A (optional) OLT queries ONU's key establishment capabilities
eOAM_Get_Request(aInitialKeyCapability)
eOAM_Get_Response(aInitialKeyCapability)
Step B (optional) OLT selects a specific key establishment method
eOAM_Set_Request(aInitialKeyMethod)
eOAM_Set_Response(aInitialKeyMethod)
Step C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

Figure 11-5–Initial Key establishment protocol

The Diffie-Hellman exchange is performed using a DHE method negotiated between the OLT and ONU using three steps:

- In Step A, the OLT queries the ONU's supported DHEs using the *aInitialKeyDHECapability* attribute (see 14.4.5.1).. This step is optional for the OLT and is only necessary if the OLT/NMS intends to use a non-mandatory method.

- In Step B, the OLT selects a specific DHE method and initial key type using the *aInitialKeyMethod* attribute (see 14.4.5.2 - Attribute *aInitialKeyMethod*). The selected method can be any of the methods reported by the ONU in Step A or any mandatory method.

- In Step C, the OLT and the ONU exchange their DHE components using the *aInitialKeyDHESharedElement* attribute (see 14.4.5.3 – Attribute *aInitialKeyDHESharedElement*). The makeup of the key components (also referred to as public keys) 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.

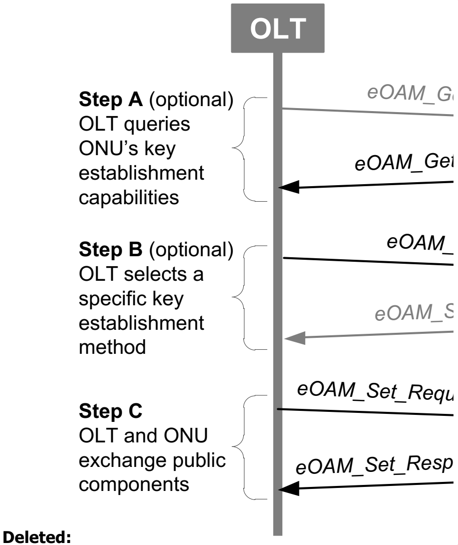
Once the OLT and ONU have completed the DHE, they shall both derive shared secret data and calculate the initial key from the shared secret data according to the *aInitialKeyMethod* attribute (see 14.4.5.2).

After 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 of the initial encryption key is not established until the authentication process described in 11.4 is successfully completed.

Note that a compliant OLT implementation may choose to combine the *aInitialKeyMethod* attribute and *aInitialKeyDHESharedElement* attribute into a single *eOAM_Set_Request* OAMPDU. A compliant ONU implementation may choose to combine the *aInitialKeyMethod* attribute and *aInitialKeyDHESharedElement* attribute into a single *eOAM_Set_Response* OAMPDU.

11.3.4 Symmetric key derivation using HKDF

The initial encryption key can be derived using the HMAC-based Extract-and-Expand Key Derivation Function (HKDF) defined in RFC-5869 with the following parameters:


OLT
Step A (optional) OLT queries ONU's key establishment capabilities
eOAM_G
eOAM_Ge
Step B (optional) OLT selects a specific key establishment method
eOAM_
eOAM_S
Step C OLT and ONU exchange public components
eOAM_Set_Requ
eOAM_Set_Resp

Deleted:

Deleted: <#>The key exchange is performed using a key establishment method negotiated between the OLT and ONU using three steps:¶

Deleted: <#>In Step step A, the OLT queries the ONU's supported key establishment methods using the *aInitialKeyCapability* attribute (see 14.4.5.1). This step is optional and is only performed necessary if the OLT/NMS intends to use one of the non-mandatory methods. ¶
In Step step B, the OLT selects a specific key establishment method using the *aInitialKeyMethod* attribute (see 14.4.5.2). The selected method can be any of the methods reported by the ONU in Step step A, or one or mandatory methods, if Step 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, A compliant OLT implementation may choose to combine the *aInitialKeyMethod* attribute and *aInitialKeySharedElement* attribute into a single ... [1]

Deleted: <#>both parties have exchanged key components, both

Deleted: <#>the other party's key components, they mutually derive the initial key

Deleted: <#>according to the selected key establishment method

Deleted: <#>

Deleted: <#>and then calculate the initial encryption key from the shared secret using HKDF with the SHA-256 HMAC (see RFC-5869). The initial key is then activated according to the process defined in 11.6.

Formatted: Font: Not Italic

Deleted: Once

- Input data: Shared secret data calculated from the selected DHE method

- Hash: SHA-256

- Info data: *“SIEPON.4 INITIAL KEY” encoded in 7-bit ASCII (0x534945504f4e20494e495449414c204b4559)*

- *Salt data: None*

The data retrieved from the HKDF depends upon the key type. See section 14.4.5.2 (Attribute *aInitialKeyMethod*) for details.

Formatted: Normal

Page 4: [1] Deleted Craig Pratt 11/28/23 11:56:00 PM