11 Security-oriented mechanisms

11.1 Introduction

[omitted]

11.2 Overview of SIEPON.4 security architecture

[omitted]

11.3 Authentication of the ONU

Before an ONU is allowed access to the operator's network and symmetric encryption keys established for secure communication between the OLT and the ONU, the ONU's identity needs to be determined and verified. The authenticated ONU identity can then be used by the NMS to reliably establish what level of access the ONU is granted. This subclause defines how this authentication is performed.

11.3.1 ONU identity

The SIEPON.4 system uses the ONU MAC address associated with the ONU's PON port as the identity of the ONU (see 14.4.1.2). The ONU identity cannot be trusted until the ONU has successfully completed the Authentication procedure (see 11.3.4).

When an ONU is powered on, it reports its MAC address to the OLT through the MPCP Discovery process, as defined in IEEE 802.3, clause 144.

The OLT shall use the ONU MAC address associated with PON port as the identity of the ONU.

11.3.2 Network Access Control

The OLT shall initiate the ONU Authentication procedure immediately after the completion of OAM/eOAM discovery. At this time, the ONU's access to the network is restricted; it has only two "system" logical links assigned to it: PLID used for providing connectivity (carries GATE and REPORT MPCPDUs) and MLID used for ONU management (carries OAMPDUs). The ONU cannot support any data services at this time.

Before provisioning data services to the ONU, the OLT shall authenticate the ONU identity and verify that the ONU is authorized to operate on the given network. If port-based access control is enabled, the OLT shall verify that given ONU is authorized for the particular OLT PON port on which it is discovered.

The OLT may consult NMS/AAA servers to determine the ONU's authorization to access the network resources. The mechanism of communication with the NMS/AAA servers or the nature of information passed between the OLT and the servers is outside the scope of this standard.

The OLT shall deny service provisioning to the following categories of ONUs:

- An ONU that failed authentication,
- An ONU whose identity matches that of another authenticated ONU,
- An authenticated ONU that is unauthorized to connect to the network from any location,
- An authenticated and authorized ONU that has been discovered on a PON port different from the one on which it is authorized.

The OLT may analyze various ONU parameters, capabilities, and operational characteristics of the ONU in addition to the ONU identity and PON port to determine its access to the PON and connected resources. For example, the OLT may compare the ONU's round-trip time to the previous measurement,deny access to the ONU that has unexpectedly relocated and/or require the ONU to repeat the onboarding process.

11.3.3 ONU Authentication Credentials

The ONU may be authenticated using the built-in credential (the Device Authentication Credential) or an operator-provided credential (the Network Authentication Credential). In either case, the ONU identity is attested via the built-in keypair (the Device Authentication Keypair). When properly used, these credentials provide the ability for an NMS to cryptographically verify the identity of the ONU attempting to access the PON and determine what access the ONU is granted.

11.3.3.1 The Device Authentication Keypair (DAK) Requirements

The Device Authentication Keypair (DAK) facilitates robust identification and authentication of ONUs on the PON network.

All SIEPON.4 ONUs and OLTs shall have a unique DAK of type *Curve P-384* (see FIPS 186-4, D.2.4). The keypair shall be generated in accordance to NIST ST SP 800-57 Part 1R5 section 8.1.5.1. The DAK shall persist across device power cycles and factory resets.

Requirements for securing the DAK private key can be found in section 11.10 (Physical protection of security data in the ONU).

11.3.3.2 Credential Identification and Selection

In order to provide the NMS/OLT the ability to select the particular ONU credential to use for authentication, the TLS 1.3 CertificateRequest extension "SIEPON.4 Credential Type" is defined in the IEEE namespace as OID 1.3.111.2.1904.4.1.1 with the following definition:

```
enum {undefined(0), dac(1), nac(2), reserved(3..255)} SIEPON4CredentialType;
```

11.3.3.3 The Device Authentication Credential (DAC) Requirements

The DAC is a data structure containing the DAK public key, metadata identifying the PON device (including the *aOnuId* attribute), and a cryptographic signature(s) used to verify the authenticity of the DAC. The DAC shall be formatted and authenticated in accordance to X.509v3 (see X.509/RFC-6818). Specifically,

- Shall contain the SIEPON4CredentialType extension with a value of "1" (dac). (see section 11.3.3.2 [Credential identification and selection])
- For ONUs, the Subject Common Name (CN) field shall conform with the PrintableString definition as described in RFC-5280 and shall contain the *aOnuId* attribute value encoded into 12 hexadecimal digits preceded by the string "SIEPON4_ONU_". For example, "`CN=SIEPON4_ONU_0A7FB49E2CF1`" (see RFC-4648 section 8)
- The public key field shall contain the DAK public key of the device encoded according to RFC-5480 section 2.1.
- The DAC must be signed using the device's DAK private key producing an ECDSA signature with a SHA-256, SHA-384, or SHA-512 HMAC according to RFC-5480 section 2.1.
- The DAC may also be signed using a device manufacturer's CA private key producing an ECDSA signature with a SHA-256, SHA-384, or SHA-512 HMAC according to RFC-5480 section 2.1.
- The Key Usage Extension shall indicate the certificate's public key usage is "Digital Signature" and "Key Encipherment". (see RFC-5280, section 4.2.1.12).
- The size shall not exceed 1491 bytes.
- The certificate shall not include any extensions marked "critical" unless required by RFC-5280 or required above.

Every ONU shall present a DAC during the authentication process (see 11.3.4 [The authentication procedure]). An example DAC is provided in Annex 11A, x.x.

11.3.3.4 The Network Authentication Credential (NAC) Requirements

The Network Authentication Credential (NAC) is a data structure containing an end-entity certificate (see RFC-5280) containing the DAK public key, operator-defined metadata, and a cryptographic signature used to verify the authenticity of the NAC. The NAC should be formatted and authenticated in accordance to RFC-5280. Specifically,

— The public key field of the NAC leaf certificate should contain the DAK public key of the device encoded according to RFC-5480 section 2.1.

— Should contain the SIEPON4CredentialType extension with a value of “2 (nac)”. (see section 11.3.3.2 [Credential identification and selection])

— The total size of the NAC should not exceed 1491 octets.

— Should be signed using an ECC Named Curve as defined in section 2.1.1.1.

The network operator may create a NAC for an ONU to contain network operator-defined metadata. The NAC shall be signed using an operator-defined Certificate Authority (CA) – enabling the ONU to be validated using a network operator-defined Public Key Infrastructure (PKI) system. For example, a network operator may create an NAC containing a unique serial number, alternate operator-defined identify for the ONU, identify the customer or management entity associated with the ONU, the ONU’s assigned service level, and/or the network locale the ONU can operate within. Note that any PKI system is expected to incorporate a robust certificate renewal and revocation system to ensure that ONUs do not operate with expired NACs and to enable ONUs to be disabled on-demand. An example NAC is provided in Annex 11A, x.y.

Once an ONU is authenticated, a network operator may create, install, renew, or revise a NAC on the ONU at any time using the *eOAM_Install_NAC_Request* eOAMPDU (see 13.4.6.7.1). Intermediate CA certificates and the root CA can also be uploaded along with the NAC so long as the total size of the certificate chain does not exceed the maximum NAC length. NAC creation is facilitated by the *eOAM_Retrieve_DAC_Request* eOAMPDU (see 13.4.6.7.3), which allows for on-demand retrieval of the ONU’s DAC, containing the DAK public key.

11.3.3.5 Network Authentication Credential (NAC) Intermediate Certificates

The Network Authentication Credential (NAC) may reference intermediate certificates which a NMS way want to include with the NAC certificate for the purposes of authenticating the NAC. For example, intermediate certs can be included to enable the authentication of NACs signed by intermediate CAs with AAA servers which only have root certificates in their trust store. NAC intermediate certificates shall be formatted and authenticated in accordance to RFC-5280. Specifically, to limit the size of intermediate certificates, NAC intermediate certificates

— Should contain an ECC public key as defined in RFC-5280 and utilize a Named Curve as defined in section 2.1.1.1.

— Should be signed using an ECC Named Curve as defined in section 2.1.1.1.

11.3.4 The Authentication Procedure

Authentication in SIEPON.4 is accomplished using EAP-TLS 1.3 [see RFC-9190] with the OLT operating as the ”EAP Authenticator”/“EAP-TLS Server” and the ONU operating as the ”EAP Supplicant”/“EAP-TLS Client” (see RFC-3748). By utilizing TLS 1.3 as described in this clause, the TLS handshake is encrypted and authenticated using an ephemeral key that provides a shared secret to both parties while ensuring privacy and perfect forward secrecy (PFS). The shared secret is then used to derive the SIEPON.4 initial traffic encryption key, as described in 11.4 [Initial Key Establishment].

In order to perform EAP-based authentication, the OLT and ONU exchange EAPOL (Extensible Authentication Protocol over LAN) frames over the MLID (see IEEE 802.1X, Clause 11,). Additionally, the EAP authentication process shall be performed according to the following guidelines:

— The OLT and ONU shall support EAP-TLS 1.3 as defined in RFC-9190 and use EAP type EAP-TLS (type 13) in all EAP-Request and EAP-Response messages. EAP-Request/Response for Identity (type 1) are not to be supported by the ONU or OLT and the ONU shall return an EAP-Response/Nak to any EAP-Request/Identity messages.

— The OLT and ONU shall only advertise TLS 1.3 in their respective TLS `ClientHello` and `ServerHello` messages (exchanged via EAP), as defined in RFC-8446. The `legacy_version` field shall be set to `0x0303` and the `supported_versions` extension shall include TLS 1.3 (`versions` value `0x0304`).

— The OLT and ONU may utilize any TLS 1.3 supported and negotiated DHE key exchange method. Session resumption using PSK-based key exchange methods are not defined for use in SIEPON.4 at this time but may be supported in the future.

— In order to support ONU authentication, the OLT shall issue and the ONU shall honor the CertificateRequest message, as described in TLS 1.3 Section 4.3.2.

— The ONU shall support TLS 1.3 OID Filters extension as described in TLS 1.3 (RFC-8446 section 4.2.5). The NMS/OLT may use this to perform credential selection, When a SIEPON4CredentialType is present in the TLS 1.3 CertificateRequest OID Filters extension (see RFC-8446 section 4.2.5), the filter shall only be considered matched against an ONU credential if the ONU has an authentication certificate containing the SIEPON4CredentialType extension with the same value as the one in the CertificateRequest.

— If the ONU is not configured with a NAC, or the DAC is matched via the TLS CertificateRequest OID Filter (see section 11.3.3.2[credential identification and selection]), the ONU shall include the DAC in its TLS 1.3 Certificate message as the "end-entity" certificate in the `certificate_list`. Requirements for the DAC can be found in section 11.3.2.

— If the ONU is configured with an NAC, and the DAC is not explicitly selected via a TLS CertificateRequest OID Filter (see section 11.3.3.2 [credential identification and selection]), then the ONU shall include the NAC in its TLS 1.3 Certificate message as the `end-entity` certificate with any intermediate certificates following the NAC in the `certificate_list`. Requirements for the NAC and associated intermediate certificates can be found in sections 11.3.3.4 and 11.3.3.5, respectively.

— If the ONU is not configured with a credential that is explicitly selected via the TLS CertificateRequest OID Filter (see section 11.3.6 [credential identification and selection]), the ONU shall abort the handshake with an "unsupported_certificate" alert.

An OLT can initiate the EAP authentication process at a time of its choosing by issuing an EAP-Request with an EAP-Type of EAP-TLS (type `13`). The OLT shall not initiate another EAP authentication session until any ongoing authentication session has been completed with either Success or Failure, per EAP section 2.1 (see RFC-3748).

11.3.5 ONU onboarding

Identification and authorization are necessary prerequisites for reliable and robust access control. In SIEPON.4, the authentication of the ONU enables the NMS to robustly identify ONUs and determine what customer or management entity each ONU is associated with and, by extension, what level of network access the ONU is granted.

While the initial association and authentication of an ONU with a NMS customer or management entity is out of scope for this clause, SIEPON.4 enables a number of methods for onboarding an ONU. Here are some examples of onboarding methods and what facilities in this subclause support the method(s):

— The ONU's DAK public key or public key fingerprint can be retrieved from the ONU, be associated with a customer or management entity and have a NAC installed prior to delivery.
— The ONU's DAK public key or public key fingerprint can be scanned/retrieved from the ONU and associated with a customer or management entity at the time of installation by either a technician or customer, facilitated by the use of a smart device with Internet access.
— An ONU can be allowed to complete the authentication process without a prior association and provided access to a limited-access network to allow the technician/user to complete the association process via an operator-provided web site. In this case the public key can be retrieved from the DAC or via the *aOnuNakPublicKey* attribute (see 14.4.5.1 [aOnuNakPublicKey]).
— An activation/association passphrase can be generated from the NMS for a customer or management entity and delivered with an ONU. An ONU can be allowed to complete the authentication process without a prior association, queried by the OLT using a *Get_Request* eOAMPDU for the *aOnuActivationPassphrase* attribute prompting the customer/technician for the passphrase, and returning the supplied value by issuing a *Get_Response* eOAMPDU with the *aOnuActivationPassphrase* attribute. (see [14.4.1.x]).

In any onboarding method, a NAC can be installed into or updated on the ONU after initial authentication and session key establishment to provide a network-specific identity during subsequent authentication exchanges. A NAC can contain access group rules, service groups, VLAN IDs, or any other NMS or non-NMS data the operator wishes to associate with the ONU. The NMS can explicitly trust data contained in the NAC after validating the signature and other metadata.

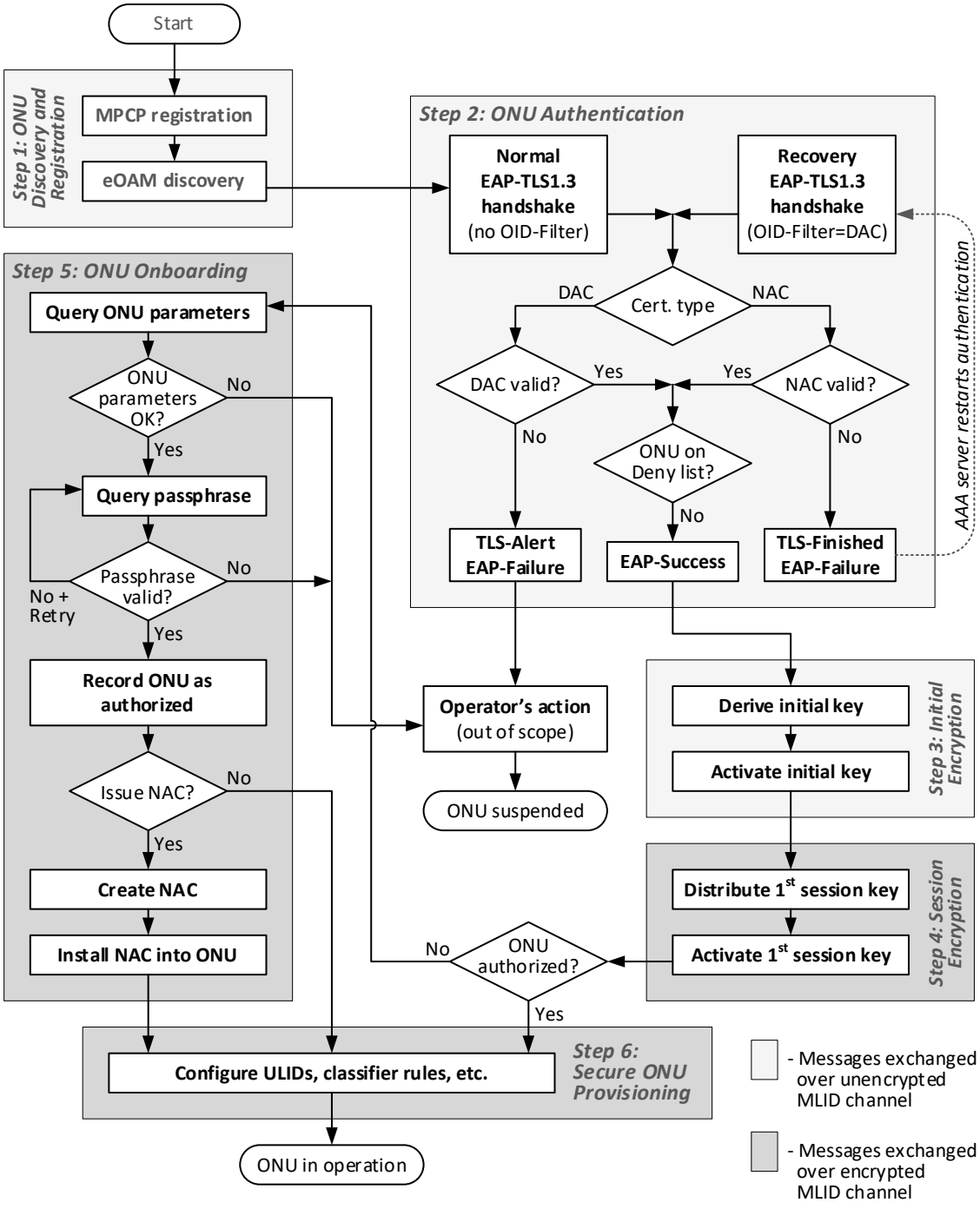

Figure 11-x: Illustration of ONU Authentication and onboarding procedures

In cases where a NAC is not installed on an ONU, and the DAC is used for ONU authentication, only the DAC/DAK public key (or public key fingerprint) can be used to identify the ONU and provide robust access control.