11 Security-oriented mechanisms

11.1 Overview of threats and mitigation measures

11.2 ONU identity and access management

11.2.1 ONU identity

11.2.2 ONU authentication

11.2.2.1 ONU authentication credentials

11.2.2.1.1 The Device Authentication Keypair (DAK) requirements

11.2.2.1.2 Credential Identification and Selection

11.2.2.1.3 The Device Authentication Credential (DAC) Requirements

The DAC is a data structure containing the DAK public key, metadata identifying the ONU device (including the *aOnuId* attribute), and a cryptographic signature(s) used to verify the authenticity of the DAC. The DAC shall neet the following requirements:

— Formatted in accordance to X.509v3 (see X.509/RFC-6818).

— Contains the *SIEPON4CredentialType* extension with a value of 1 (see 11.2.2.1.2).

— The Subject Common Name (CN) field conforms to the PrintableString definition as described in RFC-5280 and contains the *aOnuId* attribute value encoded into 12 hexadecimal digits preceded by the string "SIEPON4_ONU_". For example, "`CN=SIEPON4_ONU_58D08F123456`" (see RFC-4648, section 8).

— The public key field contains the DAK public key of the device encoded according to RFC-5480, section 2.1.

— The DAC be is 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 Key Usage Extension indicates the certificate's public key usage is "Digital Signature" and "Key Encipherment". (see RFC-5280, section 4.2.1.12).

~~— The total size of the DAC does not exceed 1489 octets.~~

— The certificate does not include any extensions marked "critical", except the *BasicConstraints* extension.

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.

An example DAC is provided in Annex 11A.

11.2.2.1.4 The Network Authentication Credential (NAC) Requirements

The Network Authentication Credential (NAC) is 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 network operator may create a NAC for an ONU to contain network operator-defined metadata. The NAC is 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, an 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. An example NAC is provided in Annex 11A.

A NAC may be pre-installed into an ONU before the ONU's deployment/installation, or it may be installed remotely after the ONU has successfully authenticated using the built-in DAC (see 11.2.2.1.3).

To ensure that ONUs do not operate with expired NACs, a network operator may revoke the existing NAC and/or install a new NAC in the ONU at any time using the *eOAM_Install_NAC_Request* eOAMPDU (see 13.4.6.7.1.1). Intermediate CA certificates and the root CA can also be uploaded along with the NAC as long as the total size of the certificate chain does not exceed the specified maximum NAC length. NAC creation is facilitated by the *eOAM_Retrieve_DAC_Request* eOAMPDU (see 13.4.6.7.3.1), which allows for on-demand retrieval of the ONU's DAC, containing the DAK public key.

The OLT shall not generate the *eOAM_Install_NAC_Request* eOAMPDU(s) containing the NAC that

- Is not formatted in accordance with the RFC-5280
- ~~Has size exceeding 1489 octets~~
- Is not signed using an ECC Named Curve as defined in RFC-5480, section 2.1.1.1.

The ONU shall set the field `CertificateStatus` in the final *eOAM_Install_NAC_Response* eOAMPDU (see 13.4.6.7.1.2) to the value ~~`Invalid Format` (~~0x03~~)~~ "Invalid format", if the received NAC

- Is not formatted in accordance with the RFC-5280
- Contains a public key that does not match the ONU's DAK public key
- Does not contain the SIEPON4CredentialType extension with a value of 2 (see 11.2.2.1.2).

An example NAC is provided in Annex 11A.

11.2.2.1.5 Network Authentication Credential (NAC) Intermediate Certificates

The Network Authentication Credential (NAC) may reference intermediate certificates. The NMS may install the intermediate certificates together with the NAC certificate into an ONU for the purposes of authenticating the NAC. For example, intermediate certificates can be included to enable the authentication of NACs signed by intermediate CAs with AAA servers that only have root certificates in their trust store. NAC intermediate certificates are formatted and authenticated in accordance to RFC-5280.

~~Note that the~~The OLT ~~is able to include~~installs the intermediate certificates together with the NAC certificate using~~in the~~ one or more *eOAM_Install_NAC_Request* eOAMPDUs~~ (see ~~, as specified in 13.4.6.7.1~~) only if the total size of the encoded certificate chain (i.e., the NAC certificate and all the intermediate certificates) does not exceed 1489 octets~~.