11.3 Establishment of the initial key

11.3.1 Key establishment methods

The OLT and ONUs may use various methods for establishing the initial key, while ensuring the perfect forward secrecy. A common approach to establish an initial key is to use Elliptic-curve Diffie–Hellman (ECDH) methods. Several such methods are named in the IANA TLS Supported Groups registry

11.3.1.1 Mandatory key establishment methods

The OLT and the ONU shall support the ECDH key establishment methods based on named elliptic curves *secp256r1* (see SECG-SEC2, 2.4.2) and *x25519* 21 (see RFC 7748, 4.1).

11.3.1.2 Optional key establishment methods

The OLT and the ONU should support the ECDH key establishment 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).

11.3.2 Initial key lifetime

The initial key is an *ephemeral* key that is active for only a short period of time. As illustrated in Figure 11-4, the initial key is used to perform the ONU/mutual authentication (step 3) and to distribute the first session key (a portion of step 4). Once the first session key is activated, the initial key is discarded by both the OLT and the ONU.

~~11.3.1~~11.3.3 Initial ~~Key~~ key exchange protocol

The current text in D1.6, 11.3 goes here as is