Add normative references:

SECG-SEC2, Certicom Research, "*SEC 2: Recommended Elliptic Curve Domain Parameters*", Standards for Efficient Cryptography 2 (SEC 2), Version 2.0, January 2010, available at http://www.secg.org/sec2-v2.pdf.

IETF RFC 7748 (January 2016 1989), *Elliptic Curves for Security*, Langley, A., Hamburg, M., Turner, S., available at https://www.rfc-editor.org/rfc/rfc7748.

This text (or similar) needs to go into section 11.4.

The ONU shall support the ECDHE key establishment methods based on named elliptic curves ***secp256r1*** and ***x25519.*** The ONU should support the ECDHE key establishment methods based on named elliptic curves ***secp384r1*** and ***x448.***

14 Management entities

14.1 Introduction

14.2 Branch 0xDA “identification”

14.3 Branch 0x07 “basic attributes”

14.4 Branch 0xDB “extended attributes”

14.4.1 ONU management

14.4.2 Bridging

14.4.3 Statistics and counters

14.4.4 Alarms

14.4.5 Encryption

14.4.5.1 Attribute *aInitialKeyMethods* (0xDB/0x04-01)

This attribute represents the list of key establishment methods (KEM) supported by the given ONU. Each KEM is identified by a 16-bit KEM ID value. There could be various organizations providing their own KEM definitions and KEM ID enumerations.

The *aInitialKeyMethods* attribute consists of the following sub-attributes: *sKemCount*, *sKemId[sKemCount]*, and *sKemDomainId[sKemCount]*.

Sub-attribute *aInitialKeyMethods.sKemCount*:

Syntax: Unsigned integer
Range: 0x02 to 0xFF
Remote access: Read-Only
Description: This sub-attribute represents the number of KEMs supported by the ONU.

Sub-attribute *aInitialKeyMethods.sKemDomainId[sKemCount]*:

Syntax: Enumeration
Remote access: Read-Only
Description: Each element of this array identifies the KEM domain, i.e., an organization that defines and maintains the KEM ID enumeration system. The following KEM domain ID values are defined:

`tls_groups`: indicates that the corresponding *sKemId[i]* is defined by the IANA *TLS Supported Groups* registry (see [IANA TLS Groups]) .

All other values are reserved for future use.

Sub-attribute *aInitialKeyMethods.sKemId[sKemCount]*:

Syntax: Enumeration
Remote access: Read-Only
Description: Each element of this array identifies a KEM supported by the ONU. The *sKemId[i]* value is interpreted within the context of its specified KEM domain. The following KEM ID values are defined within the `tls_groups` KEM domain:

`kem_secp256r1`: identifies the named elliptic curve ***secp256r1*** (see SECG-SEC2, 2.4.2);
`kem_secp384r1`: identifies the named elliptic curve ***secp384r1*** (see SECG-SEC2, 2.5.1);
`kem_secp512r1`: identifies the named elliptic curve ***secp512r1*** (see SECG-SEC2, 2.6.1);
`kem_x25519`: identifies the named elliptic curve ***x25519*** (see RFC 7748, 4.1);
`kem_x448`: identifies the named elliptic curve ***x448*** (see RFC 7748, 4.2);

The *aInitialKeyMethods* attribute is associated with the ONU object (see 14.2.1). The Variable Container TLV for the *aInitialKeyMethods* attribute shall be as specified in Table 14-xx.

Table 14-xx—*Initial Key Methods* TLV (0xDB/0x04-01)

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier
2	Leaf	0x04-01	Leaf identifier
1	Length	1+3×*N*	The size of TLV fields following the `Length` field
1	KemCount	*N*	Value of the *sKemCount* sub-attribute
1	KemDomainId[0]	Varies	Value of the *sKemDomainId[0]* sub-attribute, encoded as follows: `tls_groups`: 0x01
2	KemId[0]	Varies	Value of the *sKemId[0]* sub-attribute encoded as follows: `kem_secp256r1`: 0x00-17 (23) `kem_secp384r1`: 0x00-18 (24) `kem_secp512r1`: 0x00-19 (25) `kem_x25519`: 0x00-1D (29) `kem_sx448`: 0x00-1E (30)
…	…	…	…
1	KemDomainId[*N*-1]	Varies	Value of the *sKemDomainId[N-1]* sub-attribute. (Refer to *KemDomainId[0]* field for encoding.)
2	KemId[*N*-1]	Varies	Value of the *sKemId[N-1]* sub-attribute. (Refer to *KemId[0]* field for encoding.)

14.4.5.2 Attribute *aInitialKeyParameters* (0xDB/0x04-02)

This attribute represents a set of parameters exchanged between the OLT and the ONU in order to derive the initial encryption key (see TBD). The set of parameters includes a selection of a specific key establishment method (KEM) and an associated *shared element* of a format specific to the selected KEM.

The *aInitialKeyParameters* attribute consists of the following sub-attributes: *sSelectedKemDomainId*, *sSelectedKemId*, *sRemoteSharedElement*, and *sLocalSharedElement*.

Sub-attribute *aInitialKeyParameters.sSelectedKemDomainId*:
Syntax: Enumeration
Remote access: Write-Only
Description: This sub-attribute identifies the domain of the selected KEM, i.e., an organization that defines and maintains the KEM ID enumeration system. Refer

to sub-attribute *aInitialKeyMethods.sKemDomainId[sKemCount]* for more information (see 14.4.5.1).

Sub-attribute *aInitialKeyMethods.sSelectedKemId*:

Syntax: Enumeration
Remote access: Write-Only
Description: This sub-attribute identifies the selected KEM. The *sSelectedKemId* value is interpreted within the context of the specified KEM domain (*sSelectedKemDomainId*). Refer to the sub-attribute *aInitialKeyMethods.sKemId[sKemCount]* (14.4.5.1) for the names and descriptions of the allowed enumerated code-points.

Sub-attribute *aInitialKeyParameters.sRemoteSharedElement*:

Syntax: KEM-dependent structure (see description below)
Remote access: Write-Only
Description: This sub-attribute represents the KEM shared (public) element received from the OLT. The structure of the shared element depends on the selected KEM:

`kem_secp256r1`:
The *sRemoteSharedElement* represents a point on the associated elliptic curve. The point is in uncompressed format and is represented by
sRemoteSharedElement.X – 256-bit X coordinate,
sRemoteSharedElement.Y – 256-bit Y coordinate.

`kem_secp384r1`:
The *sRemoteSharedElement* represents a point on the associated elliptic curve. The point is in uncompressed format and is represented by
sRemoteSharedElement.X – 384-bit X coordinate,
sRemoteSharedElement.Y – 384-bit Y coordinate.

`kem_secp512r1`:
The *sRemoteSharedElement* represents a point on the associated elliptic curve. The point is in uncompressed format and is represented by
sRemoteSharedElement.X – 512-bit X coordinate,
sRemoteSharedElement.Y – 512-bit Y coordinate.

`kem_x25519`:
The *sRemoteSharedElement* is a 32-octet string.

`kem_x448`:
The *sRemoteSharedElement* is a 56-octet string.

Sub-attribute *aInitialKeyParameters.sLocalSharedElement*:

Syntax: Same as *sRemoteSharedElement*:
Remote access: Read-Only
Description: This sub-attribute represents the KEM shared (public) element generated by the ONU and queried by the OLT. The structure of the *sLocalSharedElement* is the same as that of the *sRemoteSharedElement*.

The *aInitialKeyParameters* attribute is associated with the ONU object (see 14.2.1). In the *Set_Request* OAMPDU, the Variable Container TLV for the *aInitialKeyParameters* attribute shall be as specified in Table 14-xx1.

Table 14-xx1—*Initial Key Parameters* TLV (0xDB/0x04-02) in *Set_Request* OAMPDU

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier

Size (octets)	Field (name)	Value	Notes
2	Leaf	0x04-02	Leaf identifier
1	Length	Varies	The size of TLV fields following the `Length` field
1	SelectedKemDomainId	0x01	Value of the *sSelectedKemDomainId* sub-attribute, encoded as follows: `tls_groups`: 0x01
2	SelectedKemId	Varies	Value of the *sSelectedKemId* sub-attribute.
Varies	SharedElement	Varies	This field carries the value of *sRemoteSharedElement* sub-attribute. The size and format of this field depends on the selected KEM (*SelectedKemDomainId* / *SelectedKemId*): — For `tls_group/kem_secp256r1` refer to Table 14-xx3. — For `tls_group/kem_secp384r1` refer to Table 14-xx4. — For `tls_group/kem_secp512r1` refer to Table 14-xx5. — For `tls_group/kem_x25519` refer to Table 14-xx6. — For `tls_group/kem_x448` refer to Table 14-xx7.

In the *Set_Response* OAMPDU, the Variable Container TLV for the *aInitialKeyParameters* attribute shall be as specified in Table 14-xx2.

Table 14-xx2—*Initial Key Parameters* TLV (0xDB/0x04-02) in *Set_Response* OAMPDU

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier
2	Leaf	0x04-02	Leaf identifier
1	Length	Varies	The size of TLV fields following the `Length` field
Varies	SharedElement	Varies	This field carries the value of *sLocalSharedElement* sub-attribute. The size and format of this field is the same as that of the *SharedElement* field in Table 14-xx1.

Table 14-xx3—*SharedElement* field format for KEM *secp256r1* (`tls_groups/kem_secp256r1`)

Size (octets)	Field (name)	Notes
32	EcPoint_X	X coordinate of a point on elliptic curve *secp256r1*
32	EcPoint_Y	Y coordinate of a point on elliptic curve *secp256r1*

Table 14-xx4—*SharedElement* field format for KEM *secp384r1*
(`tls_groups/kem_secp384r1`)

Size (octets)	Field (name)	Notes
48	EcPoint_X	X coordinate of a point on elliptic curve *secp384r1*
48	EcPoint_Y	Y coordinate of a point on elliptic curve *secp384r1*

Table 14-xx5—*SharedElement* field format for KEM *secp512r1*
(`tls_groups/kem_secp512r1`)

Size (octets)	Field (name)	Notes
64	EcPoint_X	X coordinate of a point on elliptic curve *secp512r1*
64	EcPoint_Y	Y coordinate of a point on elliptic curve *secp512r1*

Table 14-xx6—*SharedElement* field format for KEM *x25519*
(`tls_groups/kem_x25519`)

Size (octets)	Field (name)	Notes
32	SharedElement_x25519	U-value of a point on the elliptic curve

Table 14-xx7—*SharedElement* field format for KEM *x448*
(`tls_groups/kem_x448`)

Size (octets)	Field (name)	Notes
56	SharedElement_x448	U-value of a point on the elliptic curve

14.4.5.3 Attribute *aEncryptionMode* (0xDB/0x04-03)