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 *aInitialKeyCapability* (0xDB/0x04-01)

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

The *aInitialKeyCapability* attribute consists of the following sub-attributes: *sCount*, *sRegistry[sCount]*, and *sIdentifier[sCount]*.

Sub-attribute *aInitialKeyCapability.sCount*:

Syntax: Unsigned integer
Range: 0x02 to 0xFF
Remote access: Read-Only
Description: This sub-attribute represents the number of KEMs supported by the ONU. The minimum value of 2 denotes the two KEMs that are mandatory to support (see 11.4.TBD).

Sub-attribute *aInitialKeyCapability.sRegistry[sCount]*:

Syntax: Enumeration
Remote access: Read-Only
Description: Each element of this array identifies the registry that defines and maintains the enumeration system of the KEM identifiers. The following *Registry* values are defined:

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

All other values are reserved for future use.

Sub-attribute *aInitialKeyCapability.sIdentifier[sCount]*:

Syntax: Enumeration
Remote access: Read-Only
Description: Each element of this array identifies a KEM supported by the ONU. The *sIdentifier[i]* value is interpreted within the context of its specified registry. The

following identifier values are defined within the `iana_tls_groups` registry:

`secp256r1`: identifies the named elliptic curve ***secp256r1*** (see SECG-SEC2, 2.4.2);

`secp384r1`: identifies the named elliptic curve ***secp384r1*** (see SECG-SEC2, 2.5.1);

`secp512r1`: identifies the named elliptic curve ***secp512r1*** (see SECG-SEC2, 2.6.1);

`x25519`: identifies the named elliptic curve ***x25519*** (see RFC 7748, 4.1);

`x448`: identifies the named elliptic curve ***x448*** (see RFC 7748, 4.2);

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

Table 14-xx—*Initial Key Capability* 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	Count	*N*	Value of the *sCount* sub-attribute
1	Registry[0]	Varies	Value of the *sRegistry[0]* sub-attribute, encoded as follows: `iana_tls_groups`: 0x01
2	Identifier[0]	Varies	Value of the *sIdentifier[0]* sub-attribute encoded as follows: `secp256r1`: 0x00-17 (23) `secp384r1`: 0x00-18 (24) `secp512r1`: 0x00-19 (25) `x25519`: 0x00-1D (29) `x448`: 0x00-1E (30)
…	…	…	…
1	Registry[*N*-1]	Varies	Value of the *sRegistry[N-1]* sub-attribute. (Refer to *Registry[0]* field for encoding.)
2	Identifier[*N*-1]	Varies	Value of the *sIdentifier[N-1]* sub-attribute. (Refer to *Identifier[0]* field for encoding.)

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

This attribute represents the selected key establishment method (KEM) to be used to derive the initial encryption key (see 11.4.TBD). The selected KEM is one of the KEMs supported by both the OLT and the ONU (see the attribute *aInitialKeyCapability* in 14.4.5.1). The *aInitialKeyMethod* attribute consists of the following sub-attributes: *sRegistry* and *sIdentifier*.

Sub-attribute *aInitialKeyMethod.sRegistry*:

Syntax: Enumeration
Default value: `iana_tls_groups`
Remote access: Read/Write

Description: This sub-attribute identifies the registry maintaining the enumeration system that includes the KEM identifier. Refer to sub-attribute *aInitialKeyCapability.sRegistry[sCount]* for more information (see 14.4.5.1).

Sub-attribute *aInitialKeyMethod.sIdentifier*:

Syntax: Enumeration
Default value: `secp256r1`
Remote access: Read/Write
Description: This sub-attribute identifies the selected KEM. The *sIdentifier* value is interpreted within the context of the specified KEM registry (*sRegistry*). Refer to the sub-attribute *aInitialKeyCapability.sIdentifier[sCount]* (14.4.5.1) for the names and descriptions of the allowed enumerated code-points.

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

Table 14-xx1—*Initial Key Method* TLV (0xDB/0x04-02)

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier
2	Leaf	0x04-02	Leaf identifier
1	Length	0x03	The size of TLV fields following the `Length` field
1	Registry	0x01	Value of the *sRegistry* sub-attribute, encoded as follows: `iana_tls_groups`: 0x01
2	Identifier	Varies	Value of the *sIdentifier* sub-attribute.
32	SharedElement_x25519	U-value of a point on the elliptic curve	

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

This attribute represents public components (e.g., points on an elliptic curve) exchanged between the OLT and the ONU in order to derive the initial encryption key (see 11.4.TBD). The initial key derivation procedure requires one shared element to be conveyed by the OLT to the ONU and another such element to be conveyed by the ONU to the OLT. The format of the shared element is specific to the selected key establishment method (see the attribute *aInitialKeyMethod* in 15.4.5.2). The *aInitialKeySharedElement* attribute consists of the following sub-attributes: *sRemote* and *sLocal*.

Sub-attribute *aInitialKeySharedElement.sRemote*:

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

If *aInitialKeyMethod* `== {iana_tls_groups; secp256r1}` then the *sRemote* represents a point on the associated elliptic curve. The point is in uncompressed format and is represented by
sRemote.X – 256-bit X coordinate,
sRemote.Y – 256-bit Y coordinate.

If *aInitialKeyMethod* `== {iana_tls_groups; secp384r1}`, then the *sRemote* represents a point on the associated elliptic curve. The

point is in uncompressed format and is represented by
sRemote.X – 384-bit X coordinate,
sRemote.Y – 384-bit Y coordinate.

If *aInitialKeyMethod* == `{iana_tls_groups; secp512r1}`, then the *sRemote* represents a point on the associated elliptic curve. The point is in uncompressed format and is represented by
sRemote.X – 512-bit X coordinate,
sRemote.Y – 512-bit Y coordinate.

If *aInitialKeyMethod* == `{iana_tls_groups; x25519}` then the *sRemote* is a 32-octet string.

If *aInitialKeyMethod* == `{iana_tls_groups; x448}`, then the *sRemote* is a 56-octet string.

The ONU shall respond with the "Bad Parameters" code 0x86 (see 13.4.7) to an attempt to write a value of size or format incompatible with the current value of the *aInitialKeyMethod* attribute.

Sub-attribute *aInitialKeySharedElement.sLocal*:

Syntax: Same as *sRemote*
Remote access: Read-Only
Description: This sub-attribute represents the shared (public) element generated by the ONU to be conveyed to the OLT. The structure of the *sLocal* sub-attribute is the same as that of the *sRemote* sub-attribute.

The *aInitialKeySharedElement* attribute is associated with the ONU object (see 14.2.1).

The *aInitialKeySharedElement* attribute is accessed via the *Set_Request* OAMPDU, which carries the value of *sRemote* sub-attribute and *Set_Response* OAMPDU, which carries the value of *sLocal* sub-attribute. The *sLocal* sub-attribute may not be read without also writing the *sRemote* sub-attribute in the same operation. The ONU shall respond with the "Unsupported Attribute/Action" code 0xA1 (see 13.4.7) to a *Get_Request* OAMPDU attempting to only read the *sLocal* sub-attribute value.

The Variable Container TLV for the *aInitialKeySharedElement* attribute shall be as specified in Table 14-xx2 through Table 14-xx6.

Table 14-xx2—*Initial Key Shared Element* TLV (0xDB/0x04-03) when *aInitialKeyMethod* == {`iana_tsl_groups;secp256r1`}

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier
2	Leaf	0x04-03	Leaf identifier
1	Length	0x40	The size of TLV fields following the `Length` field
32	SharedElementX	Varies	In *Set_Request* OAMPDU, this field carries the value of *sRemote.X* sub-attribute. In *Set_Response* OAMPDUs, this field carries the value of *sLocal.X* sub-attribute.
32	SharedElementY	Varies	In *Set_Request* OAMPDU, this field carries the value of *sRemote.Y* sub-attribute. In *Set_Response* OAMPDUs, this field carries the value of *sLocal.Y* sub-attribute.

Table 14-xx3—*Initial Key Shared Element* TLV (0xDB/0x04-03)
when *aInitialKeyMethod* == {`iana_tsl_groups:secp384r1`}

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier
2	Leaf	0x04-03	Leaf identifier
1	Length	0x60	The size of TLV fields following the `Length` field
48	SharedElementX	Varies	In *Set_Request* OAMPDU, this field carries the value of *sRemote.X* sub-attribute. In *Set_Response* OAMPDUs, this field carries the value of *sLocal.X* sub-attribute.
48	SharedElementY	Varies	In *Set_Request* OAMPDU, this field carries the value of *sRemote.Y* sub-attribute. In *Set_Response* OAMPDUs, this field carries the value of *sLocal.Y* sub-attribute.

Table 14-xx4—*Initial Key Shared Element* TLV (0xDB/0x04-03)
when *aInitialKeyMethod* == {`iana_tsl_groups:secp512r1`}

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier
2	Leaf	0x04-03	Leaf identifier
1	Length	0x00	The size of TLV fields following the `Length` field. The value 0x00 encodes TLV length of 128 octets (see 13.4.3.2)
64	SharedElementX	Varies	In *Set_Request* OAMPDU, this field carries the value of *sRemote.X* sub-attribute. In *Set_Response* OAMPDUs, this field carries the value of *sLocal.X* sub-attribute.
64	SharedElementY	Varies	In *Set_Request* OAMPDU, this field carries the value of *sRemote.Y* sub-attribute. In *Set_Response* OAMPDUs, this field carries the value of *sLocal.Y* sub-attribute.

Table 14-xx5—*Initial Key Shared Element* TLV (0xDB/0x04-03)
when *aInitialKeyMethod* == {`iana_tsl_groups:x25519`}

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier
2	Leaf	0x04-03	Leaf identifier
1	Length	0x20	The size of TLV fields following the `Length` field (see 13.4.3.2)
32	SharedElement	Varies	In *Set_Request* OAMPDU, this field carries the value of *sRemote* sub-attribute. In *Set_Response* OAMPDUs, this field carries the value of *sLocal* sub-attribute.

Table 14-xx6—*Initial Key Shared Element* TLV (0xDB/0x04-03) when *aInitialKeyMethod* == {`iana_tsl_groups;x448`}

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier
2	Leaf	0x04-03	Leaf identifier
1	Length	0x38	The size of TLV fields following the `Length` field (see 13.4.3.2)
56	SharedElement	Varies	In *Set_Request* OAMPDU, this field carries the value of *sRemote* sub-attribute. In *Set_Response* OAMPDUs, this field carries the value of *sLocal* sub-attribute.

14.4.5.4 Attribute *aEncryptionMode* (0xDB/0x04-04)