International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.987.3

Amendment 1
(06/2012)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Digital sections and digital line system – Optical line systems for local and access networks

10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence layer (TC) specification

Amendment 1

Recommendation ITU-T G.987.3 (2010) – Amendment 1

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
General	G.900–G.909
Parameters for optical fibre cable systems	G.910–G.919
Digital sections at hierarchical bit rates based on a bit rate of 2048 kbit/s	G.920–G.929
Digital line transmission systems on cable at non-hierarchical bit rates	G.930–G.939
Digital line systems provided by FDM transmission bearers	G.940–G.949
Digital line systems	G.950–G.959
Digital section and digital transmission systems for customer access to ISDN	G.960–G.969
Optical fibre submarine cable systems	G.970–G.979
Optical line systems for local and access networks	**G.980–G.989**
Access networks	G.990–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T G.987.3

10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence layer (TC) specification

Amendment 1

Summary

Amendment 1 to Recommendation ITU-T G.987.3 (2010) contains additional details and clarifications for the security clause of the Recommendation, introduces the optional features of PON-ID management and extended rogue optical network unit (ONU) mitigation capabilities, defines additional golden vectors and provides regular specification maintenance.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G.987.3	2010-10-07	15
1.1	ITU-T G.987.3 (2010) Amd.1	2012-06-22	15

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T G.987.3

10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence layer (TC) specification

Amendment 1

1) Scope

This amendment to ITU-T G.987.3 (2010) contains additional details and clarifications for the security clause of the Recommendation, introduces the optional features of PON-ID management and extended rogue optical network unit (ONU) mitigation capabilities, defines additional golden vectors and provides regular maintenance of the text.

2) XG-PON security clarifications

2.1) Modified clause 15

Replace clause 15 of Recommendation ITU-T G.987.3 with the following:

15 XG-PON security

This clause discusses threat models characteristic for the XG-PON operating environment, and specifies authentication, data integrity, and privacy protection aspects of the system.

15.1 Threat model for XG-PON

XG-PON security is intended to protect against the following threats:

a) Since downstream data is broadcast to all ONUs attached to the XG-PON OLT, a malicious user capable of replacing or re-programming an ONU would be capable of receiving all downstream data intended for all connected users.

b) Since upstream data received by the optical line terminal (OLT) can originate from any ONU attached to the XG-PON optical distribution network (ODN), a malicious user capable of replacing or re-programming an ONU could forge packets so as to impersonate a different ONU (i.e., theft of service).

c) An attacker could connect a malicious device at various points on the infrastructure (e.g., by tampering with street cabinets, spare ports, or fibre cables). Such a device could intercept and/or generate traffic. Depending on the location of such a device, it could impersonate an OLT or alternatively it could impersonate an ONU.

d) A malicious user in any of the above scenarios could record packets transmitted on the passive optical network (PON) and replay them back onto the PON later, or conduct bit-flipping attacks.

Passive optical networks (PONs) are deployed in a wide variety of scenarios. In some cases, the ODN, the optical splitter, or even the ONUs may be installed in a manner considered to be physically secure or tamper-proof.

To accommodate these scenarios in an economical manner, activation of some of the XG-PON security features is optional, as indicated in the clauses below.

15.2 Authentication

The XG-PON system supports several mechanisms for authentication. The first mechanism is based on the registration ID. It is executed in the course of ONU activation and may be repeated throughout the duration of the activation cycle, i.e., until the ONU's next entry into the Initial state (O1). The registration-based authentication mechanism provides a basic level of authentication of the ONU to the OLT. It does not provide authentication of the OLT to the ONU. Support of the registration-based authentication mechanism is mandatory in all XG-PON devices. The two other authentication mechanisms provide secure mutual authentication to both OLT and ONU. One of them is based on an ONU management and control interface (OMCI) message exchange (see Annex C). The other is based on an IEEE 802.1X message exchange and provides a wide range of extensible features (see Annex D). Support for OMCI-based and IEEE 802.1X-based authentication mechanisms is mandatory for implementation at the component level, but optional from an equipment specification perspective. In other words, the transmission convergence (TC) layer implementation will have the capability to support both secure mutual authentication methods, but equipment constructed using these TC-layer implementations may choose not to support them.

It is within the discretion of an operator to require support of one or both secure mutual authentication mechanisms at the equipment specification stage, and to employ any or none of the authentication methods, including the basic registration-based authentication, when the system is in service.

Upon authentication failure, the OLT may undertake measures to restore functionality and to prevent a potential security breach, which may include repeating authentication using the same or an alternative mechanism, blocking upstream and downstream traffic, deactivating or disabling the offending ONU, or executing the rogue ONU diagnostic procedures.

15.2.1 Registration ID-based authentication

The registration ID-based authentication mechanism can provide authentication of ONU to OLT, but not vice versa. Its support is mandatory for all XG-PON systems. To maintain full functionality, this method requires:

- that a registration ID be assigned to a subscriber at the management level;
- that the registration ID be provisioned into the OLT and be communicated to field personnel or to the subscriber directly;
- that the ONU supports a method for entering the registration ID in the field (specification of such a method being beyond the scope of this Recommendation);
- that field personnel or the subscriber in fact enter the registration ID into the ONU.

15.2.1.1 The OLT perspective

The OLT must support the possibility to perform ONU authentication based on the reported registration ID (details of this procedure are operator-specific), as well as to execute the MSK and derived shared key calculation procedure based on the reported registration ID (see clause 15.3).

The OLT requests the Registration ID from the ONU in the following situations:

- In the course of ONU activation, by issuing a ranging grant;
- As a final handshake upon completion of a secure mutual authentication procedure, by sending a Request_Registration message to the ONU;
- At any time throughout the ONU's activation cycle at its own discretion, by sending a Request_Registration message to the ONU.

If at the time of Registration ID receipt from the ONU, there is no valid secure mutual association (SMA) between the OLT and the ONU (i.e., in the course of ONU activation, or if secure mutual authentication has not been executed or has failed), the OLT:

- must compute the master session key (MSK) and derived shared keys based on the reported Registration ID;
- may perform authentication of the ONU based on the reported Registration ID.

It is up to the operator to specify whether registration-based authentication is performed and how the result is used. Failure of registration-based authentication shall not prevent the OLT from issuing an equalization delay to the ONU (i.e., the ONU is nevertheless allowed to enter the Operation state (O5)) or from maintaining management level communication with the ONU, but may have an effect on how the OLT further handles the ONU and, in particular, on subsequent provisioning of services.

Registration-based authentication is not performed and the registration-based MSK and derived shared keys are not calculated, if at the time of the Registration ID report there exists a valid SMA between the OLT and the ONU.

Once the OLT transmits a Request_Registration message to the ONU while expecting to use the reported Registration ID for shared key derivation, it refrains from sending to that ONU other PLOAM or OMCI messages with ONU-specific MIC (see clauses 15.3.2 and 15.3.3) until after the Registration ID is received and the registration-based MSK and derived shared keys are calculated.

Once the OLT completes calculation of the registration-based MSK and derived shared keys for a particular ONU, it immediately commits those keys as active.

At the start of the ONU's activation cycle, the OLT discards any active registration-based MSK and derived shared keys.

15.2.1.2 The ONU perspective

The ONU must be able to perform calculation of the MSK and derived share keys based on the Registration ID.

The ONU computes the registration-based MSK and derived shared keys upon power up (initially, using the well-known default registration ID (see clause 11.3.4.2)), and each time the Registration ID changes. The computed values are stored for future use. As the registration-based key set may be required at any time, the ONU may benefit by storing the registration-based MSK and derived shared keys separately from the MSK and derived shared keys based on secure mutual authentication.

ONU reports Registration ID to the OLT in the following situations:

- In the course of ONU activation, in response to a ranging grant;
- At any time during the ONU's activation cycle, in response to a Request_Registration message.

The events that cause registration-based key re-computation are asynchronous to the physical layer operations, administration and maintenance (PLOAM) channel events. The ONU is expected to have the registration-based MSK and derived shared keys available at the time it reports its Registration ID to the OLT.

If there is no valid SMA between the OLT and the ONU, the ONU commits the set of shared keys based the reported Registration ID immediately upon sending the Registration PLOAM message.

The ONU retains the Registration ID and the stored registration-based MSK and derived shared keys between activation cycles and between power cycles.

15.2.2 Secure mutual authentication options

Two secure mutual authentication mechanisms are defined: OMCI-based authentication (Annex C), and IEEE 802.1X-based authentication (Annex D). These mechanisms authenticate the OLT to the ONU as well as the ONU to the OLT. The support of both secure mutual authentication mechanisms is optional on the system level.

If secure mutual authentication is supported by the system and is employed by the operator, the OLT initiates the secure mutual authentication procedure using an appropriate mechanism upon completion of the ONU activation procedure before user data traffic is transmitted, and subsequently may initiate re-authentication at any time, subject to the operator's policies and discretion.

In the course of execution of a secure mutual authentication procedure, the OLT and the ONU compute the secure Master Session Key and a set of secure shared keys applicable for specific management and operation tasks.

Both the OLT and the ONU discard the MSK and derived shared keys obtained in the course of secure mutual authentication at the start of the ONU's activation cycle along with the other TC layer parameters.

15.3 Key derivation

The mathematical details of the MSK and derived shared key calculation are shared by the OLT and the ONU.

The ONU computes the registration-based MSK and derived shared keys upon power up (initially using the well-known default registration ID (see clause 11.3.4.2)), and each time the Registration ID changes.

The OLT computes the registration-based MSK and derived shared keys under the following conditions:

a) each time the ONU reports its registration ID to the OLT in response to a ranging grant in the course of ONU activation, regardless of whether or not the reported registration ID is used for authentication, and what the outcome of the registration-based authentication procedure is;

b) each time the ONU reports its registration ID to the OLT in response to the Request_Registration PLOAM message, but only when there is no valid mutual security association between OLT and ONU.

Both the OLT and the ONU compute the secure MSK and derived shared keys each time a secure mutual authentication procedure using either the OMCI-based or the IEEE 802.1X-based mechanism is executed.

15.3.1 Cryptographic method

The secure key derivation procedure employs the cipher-based message authentication code (CMAC) algorithm specified in [NIST SP800-38B] with the advanced encryption standard (AES) encryption algorithm [NIST FIPS-197] as the underlying block cipher.

The AES-CMAC function takes as its inputs:

– block cipher key *K*;

– the information message *M*; and

– the bit length of the output *Tlen*,

and produces the message authentication code T of length $Tlen$ as an output. The notation for invocation of the AES-CMAC function is:

$$T = \text{AES-CMAC}(K, M, Tlen) \tag{15-1}$$

For the purposes of this Recommendation, the block size of the underlying block cipher and the bit length of the AES key are 128 bits. This version of the block cipher is referred to herein as AES-128.

15.3.2 Master session key

The master session key (MSK) is a 128-bit value that is shared between the OLT and the given ONU as a result of an authentication procedure and which serves as a starting point for the derivation of all of the other secret keys used in subsequent secure communications.

For the registration-based key derivation, the MSK is obtained from the ONU registration ID:

$$MSK = \text{AES-CMAC}((0\text{x}55)_{16}, Registration\_ID, 128) \tag{15-2}$$

Here $(0\text{x}55)_{16}$ denotes a default key composed of the hex pattern 0x55 repeated 16 times, and *Registration_ID* is the 36-byte value transmitted in the Registration PLOAM message. Note that the Registration PLOAM message may carry either an ONU-specific *Registration_ID*, or a well-known default value.

When the key derivation is triggered by the success of secure mutual authentication, the procedure to obtain the MSK depends on the specific authentication mechanism.

15.3.3 Derived shared keys

The session key (SK) binds the MSK to the context of the security association between the OLT and ONU. The SK, which is used for subsequent key derivations, is obtained using the following formula:

$$SK = \text{AES-CMAC } (MSK, (\text{SN} \mid \text{PON-TAG}\mid 0\text{x}53657373696\text{f}6\text{e}4\text{b}), 128) \tag{15-3}$$

where the information message, which is 24 bytes long, is a concatenation of three elements: the ONU serial number (SN) as reported in octets 5 to 12 of the upstream Serial_Number_ONU PLOAM message (clause 11.3.4.1), the PON-TAG as reported in octets 26 to 33 of the downstream Profile PLOAM message (clause 11.3.3.1), and the hexadecimal representation of the ASCII string "SessionK".

The OMCI integrity key (OMCI_IK) is used to generate and verify the integrity of OMCI messages. The OMCI_IK is derived from the SK by the following formula:

$$OMCI\_IK = \text{AES-CMAC } (SK , 0\text{x}4\text{f}4\text{d}4349496\text{e}746567726974794\text{b}6579, 128) \tag{15-4}$$

Here the information message parameter of the AES-CMAC function is 128 bits long, and is the hexadecimal representation of the ASCII string "OMCIIntegrityKey".

The PLOAM integrity key (PLOAM_IK) is used to generate and verify the integrity of XGTC layer unicast PLOAM messages. The PLOAM_IK is derived from the SK by the following formula:

$$PLOAM\_IK = \text{AES-CMAC } (SK , 0\text{x}504\text{c}4\text{f}414\text{d}496\text{e}7465677274794\text{b}6579, 128) \tag{15-5}$$

Here the information message parameter of the AES-CMAC function is 128 bits long, and is the hexadecimal representation of the ASCII string "PLOAMIntegrityKey".

For downstream broadcast PLOAM messages and for unicast PLOAM messages exchanged in the course of ONU activation prior to availability of the Registration-based MSK, the default PLOAM_IK value is used, which is equal to $(0\text{x}55)_{16}$, the subscript indicating the multiplicity of repetition of the specified hex pattern.

The key encryption key (KEK) is used to encrypt/decrypt and protect/verify the integrity of the data encryption key that is carried in the PLOAM channel. The KEK is derived from the SK by the following formula:

$$KEK = \text{AES-CMAC}\ (SK\ , \text{0x4b6579456e6372797074696f6e4b6579}, 128) \qquad (15\text{-}6)$$

Here the information message parameter of the AES-CMAC function is 128 bits long, and is the hexadecimal representation of the ASCII string "KeyEncryptionKey".

15.4 XGEM payload encryption system

XGEM payloads can be encrypted for transmission to provide data privacy in the presence of a potential eavesdropping threat.

15.4.1 Cryptographic method

The algorithm used for XG-PON encapsulation method (XGEM) payload encryption is the AES-128 [NIST FIPS-197] cipher, used in Counter mode (AES-CTR), as described in [NIST SP800-38A]. The AES-CTR algorithm applies a forward cipher with a secret key known only to the OLT and ONU (or ONUs – in the case of a broadcast key) to a sequence of input counter blocks to produce a sequence of output blocks that are exclusive-OR-ed with the plaintext XGEM payload. The sequence of counter blocks is initialized for each XGEM frame payload field to a value called "initial counter block" and is incremented using a standard incrementing function applied to the entire counter block (see section B.1 of [NIST SP800-38A]). To decrypt the ciphertext, for each XGEM frame, the forward cipher with the same secret key is applied to a sequence of input counter blocks initialized to the same initial counter block value. The output blocks are exclusive-OR-ed with the blocks of ciphertext XGEM payload to restore the plaintext XGEM payload.

15.4.2 Secret key selection

XGEM payload encryption may apply to any unicast transmission in the downstream and upstream directions, and to one specified multicast service stream for downstream broadcast transmission. The OLT ensures that, at all times, there is a PON-wide broadcast key pair which is used for broadcast XGEM Port-ID or Port-IDs, and that there is a unicast key pair for each ONU which is used for all XGEM Port-IDs that belong to that ONU. See clause 15.5 for the key exchange and activation mechanism that, at all times, allows to select a valid key for each supported key pair.

The key pair to be used for XGEM payload encryption depends on the XGEM Port-ID. Given the XGEM Port-ID (unicast or broadcast), the sender selects the specific key of the appropriate key pair, according to the rules of clause 15.5, and provides an indication of the selected key in the XGEM header.

Each XGEM frame header, as defined in clause 9.1.2, contains a 2-bit field designated as the key index, carrying an indication whether or not the particular XGEM frame payload is encrypted and if so, which of the encryption keys was used. The following code points are defined for the key index field:

- 00 – XGEM frame payload is unencrypted;
- 01 – XGEM frame payload is encrypted using the first encryption key;
- 10 – XGEM frame payload is encrypted using the second encryption key;
- 11 – Reserved.

15.4.3 Initial counter block

The 128-bit initial counter block value for a particular XGEM frame is determined by the values of superframe counter (SFC) and intra-frame counter (IFC) associated with the given XGEM frame.

In the downstream direction, the SFC value is contained in the PSBd field of the PHY frame in which the given downstream XGEM frame is transmitted. In the upstream direction, the SFC value is contained in the PSBd field of the PHY frame that specifies the upstream PHY burst in which the given upstream XGEM frame is transmitted. For the purpose of the initial counter block construction, the MSB of the SFC value is omitted, and the 50-bit field is used.

To obtain the IFC value of the given XGEM frame, the following block enumeration procedure applies (see Figure 15-1).

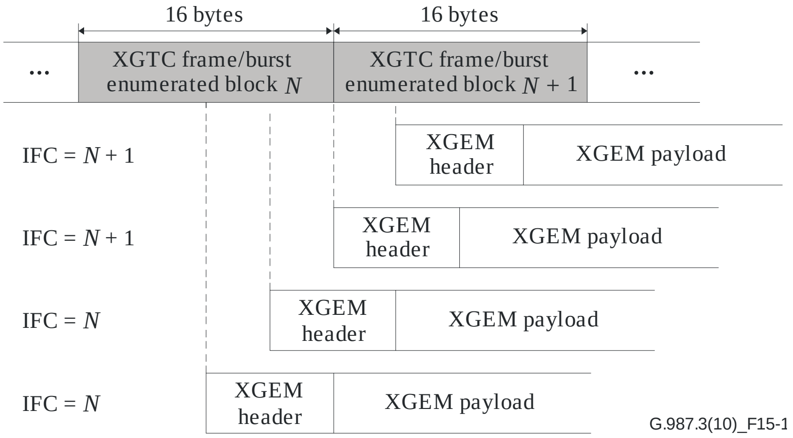


Figure 15-1 – Obtaining the intra-frame counter value for an XGEM frame

In the downstream direction, the XGTC frame of the framing sublayer (see Figure 8-1) is partitioned into 16-byte blocks, and these blocks are sequentially numbered from 0 to 8464, the last block being half-size. The size of the sequence number is 14 bits.

In the upstream direction, the XGTC burst of the framing sublayer (see Figure 8-5) is partitioned into 16-byte blocks, and these blocks are sequentially numbered from ($\lfloor$StartTime/4$\rfloor$) to ($\lfloor$StartTime/4$\rfloor$ + X), where X is the number of complete and incomplete 16-byte blocks in the XGTC burst, less 1. The size of the sequence number is 14 bits. As a reference, at 2.5G upstream, the largest StartTime is 9719. Hence, the largest number for the first block of a burst is 2429. The maximum XGTC burst size is 9720 words or 2430 blocks. Hence, the largest possible 16-byte block number in an upstream XGTC burst is 4858.

An XGEM frame appearing within the payload of a downstream XGTC frame or upstream XGTC burst can occur in one of four phase positions with respect to the 16-byte block boundary. The IFC of an XGEM frame is the sequence number of the 16-byte block to which the first 4 bytes of the XGEM header belong.

The 128-bit initial counter block for a particular downstream XGEM frame is a concatenation of SFC and IFC for the given frame obtained, as described above, concatenated with itself. The 128-bit initial counter block for a particular upstream XGEM frame is a concatenation of SFC and IFC for the given frame obtained, as described above, concatenated with the bit-complement of itself.

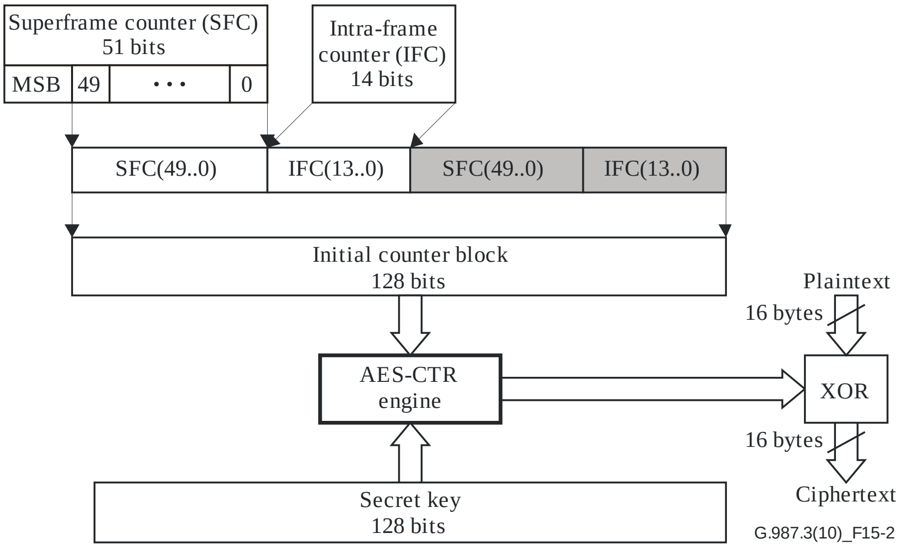


Figure 15-2 – Initial counter block construction for downstream encryption (for upstream, the shaded fields are taken in bit-complement)

NOTE – It has been shown that two SFC(49..0) values, $0b1(0)_{49}$ and $0b0(1)_{49}$, can lead to several duplicated counter blocks in the upstream and downstream directions. As these values appear at the middle of the SFC(49..0) range, the window of weaker counter blocks occurs for approximately 250 μs once in 4000 years. The potential impact can be mitigated by initializing the SFC to a small value.

15.5 Data encryption key exchange and activation mechanism

15.5.1 Overview

The data encryption configuration of an ONU is provisioned over OMCI. Each ONU advertises its security capabilities, which are required to include at least AES-128. The OLT is free to select zero or any one of the ONU's advertised capabilities; the OLT's choice then becomes binding on the ONU. For each non-default XGEM port, the OLT configures the port's encryption key ring attribute (GEM port network CTP managed entity, clause 9.2.3 of [ITU-T G.988]), which specifies whether the port is provisioned for encryption, and if so, in which direction encryption applies (downstream only or both downstream and upstream), and which data encryption key type (unicast or broadcast) should be used for the encrypted traffic. The default XGEM port has no configurable key ring, and is defined for bidirectional encryption using the unicast type key.

Provisioning a non-default XGEM port for encryption does not imply the traffic is always encrypted. The encryption status of each individual XGEM frame is determined dynamically by the sender, within the explicitly configured or pre-defined capabilities of the associated XGEM port, and is indicated in the XGEM frame header.

Whenever the default XGEM port traffic is encrypted in the downstream direction, the ONU is expected to encrypt the default XGEM port traffic upstream.

For each of two key types (unicast and broadcast), both the OLT and the ONU maintain an indexed array of two data encryption key entries. The broadcast keys are generated by the OLT and communicated to the ONUs via OMCI as described in clause 15.5.4. The unicast keys are generated and communicated upstream by the ONU upon the OLT's instructions using the PLOAM channel as described in clause 15.5.3. The value of the unicast key is not exposed to the OMCI.

The type of the data encryption key used to encrypt the payload of a particular XGEM frame on transmission is implicit in the XGEM Port-ID. The Key_Index field of the XGEM frame header indicates whether the payload is encrypted and, if so, which of the two data encryption keys of the given type is used. The specific key selected for encryption shall be valid at the XGEM frame transmission time, as determined by the respective key exchange protocol. The sender starts using the new data encryption key during the time interval when both keys of the respective type are valid. When no valid data encryption key is available (for example, immediately after ONU reactivation), the sender transmits XGEM frames without encryption using a Key_Index value of 0.

15.5.2 Cryptographic method

The data encryption keys are themselves transmitted between the OLT and the ONU encrypted with the AES-128 block cipher [NIST FIPS-197] which is used in Electronic Codebook mode (AES-ECB), as specified in [NIST SP800-38A]. In AES-ECB encryption, the forward AES-128 function is applied directly and independently to each block of plaintext using a secret key to produce a block of ciphertext. In AES-ECB decryption, the inverse AES-128 function is applied directly and independently to each block of ciphertext with the same secret key to restore the original block of plaintext. The notation for invocation of the AES-ECB algorithm is:

$$C = \text{AES-ECB}(K, P);$$

$$P = \text{AES-ECB}^{-1}(K, C);$$

Here P is a block of plaintext, C is a block of ciphertext, and K is the block cipher key. For the purposes of this Recommendation, both the block size and the key length are equal to 128 bits.

15.5.3 Unicast encryption

The OLT and the ONU maintain a number of logical state variables that are associated with the encryption and decryption functions, and this state information guides the exchange and activation of new key material. The OLT's state diagram is shown in Figure 15-4, and the ONU's diagram is shown in Figure 15-5. Both of the state machines run entirely in the Operation state (O5). When the ONU is activated or reactivated, the data encryption keys are invalidated and are reacquired via PLOAM exchange after the shared KEK is established.

15.5.3.1 Sequence of encryption key exchange and activation events

The process of unicast data encryption key exchange and activation is performed under the control of the OLT by means of a series of PLOAM messages. The activation process events are given below:

– The OLT begins by requesting a new unicast data encryption key from the ONU by using the Key_Control(Generate) PLOAM message that contains the key index for the new key. A single copy of the request is sent, and if there is no response, the OLT should retry the request.

– Upon receipt of the Key_Control(Generate) PLOAM message from the OLT, the ONU generates a new encryption key using a random number generator suitable for cryptographic purposes. The ONU stores the new key in its encryption control and decryption control structures (according to the specified key index). The ONU then sends the new key to the OLT using the Key_Report(NewKey) PLOAM message. The key is encrypted in the Key_Report(NewKey) PLOAM message with AES-ECB using KEK.

– When the OLT receives the Key_Report(NewKey) PLOAM message, it decrypts the new key and stores it in its logical encryption control and decryption control structures for the originating ONU, according to the specified key index.

– The OLT then sends the Key_Control(Confirm) PLOAM message that contains the key index of the newly generated key.

– When the ONU receives the Key_Control(Confirm) PLOAM message, it knows that the OLT now has the new key. Therefore, the ONU changes the new key state in the encryption control structure to active. The ONU responds with a Key_Report(ExistingKey) PLOAM message indicating the "Key_Name" of the specified key.

– If, at any time, the OLT wishes to check the ONU's key against its own (to diagnose a key mismatch situation), the OLT can issue a Key_Control(Confirm) PLOAM message for a key_index of an existing key. This triggers the ONU to respond with a Key_Report(ExistingKey) PLOAM message containing the key name.

The preceding description pertains to a normal key exchange process; however, the state diagrams in clauses 15.5.1.2 and 15.5.1.3 are the primary reference for the behaviour.

If on receipt of a Key_Report(ExistingKey) PLOAM message, the OLT discovers a discrepancy between the reported and locally computed key hashes, it should stop using the data encryption key with the specified key index and take remediation actions at its own discretion. Such actions may include, for example, reconfirmation of the key, generation of a new key, or re-authentication of the ONU.

Referring to the state diagrams of Figures 15-3 and 15-4, the notational conventions "oldkey" and "newkey" denote the two data encryption keys (with the corresponding key indices), of which the former is active before the key exchange is initiated, and the latter, after the key exchange is completed.

Note that in the course of the key exchange in the view of both the OLT and the ONU, the moment the oldkey ceases to be valid for transmit differs from the moment the oldkey ceases to be valid for receive, and the moment the newkey becomes valid for transmit differs from the moment the newkey becomes valid for receive.

For the OLT as well as for the ONU, there is a time interval when both oldkey and newkey are valid for transmit, and there is a time interval when both oldkey and newkey are valid for receive. Within the interval when both oldkey and newkey are valid for transmit, the respective sender selects a moment when it starts encrypting the outgoing XGEM frame payload with the newkey and putting the key_index of the newkey into the outgoing XGEM frame header. Once the sender switches to using the newkey for transmit, the sender should stop using and discard the oldkey for transmit. Within the interval when both oldkey and newkey are valid for receive, the receiver accepts either key_index to decrypts the incoming XGEM frame payload. Outside that interval, the receiver discards the XGEM frame payload that is encrypted with an invalid key.

It is the responsibility of the OLT to ensure that the key_index parameter of the Key_Control PLOAM messages is set correctly. In particular, the OLT should abstain from sending Key_Control(Confirm) PLOAM message for the key_index that is presently invalid at the ONU and, except for the key mismatch recovery situations, from sending Key_Control(Generate) PLOAM message for the only currently valid key_index at the ONU.

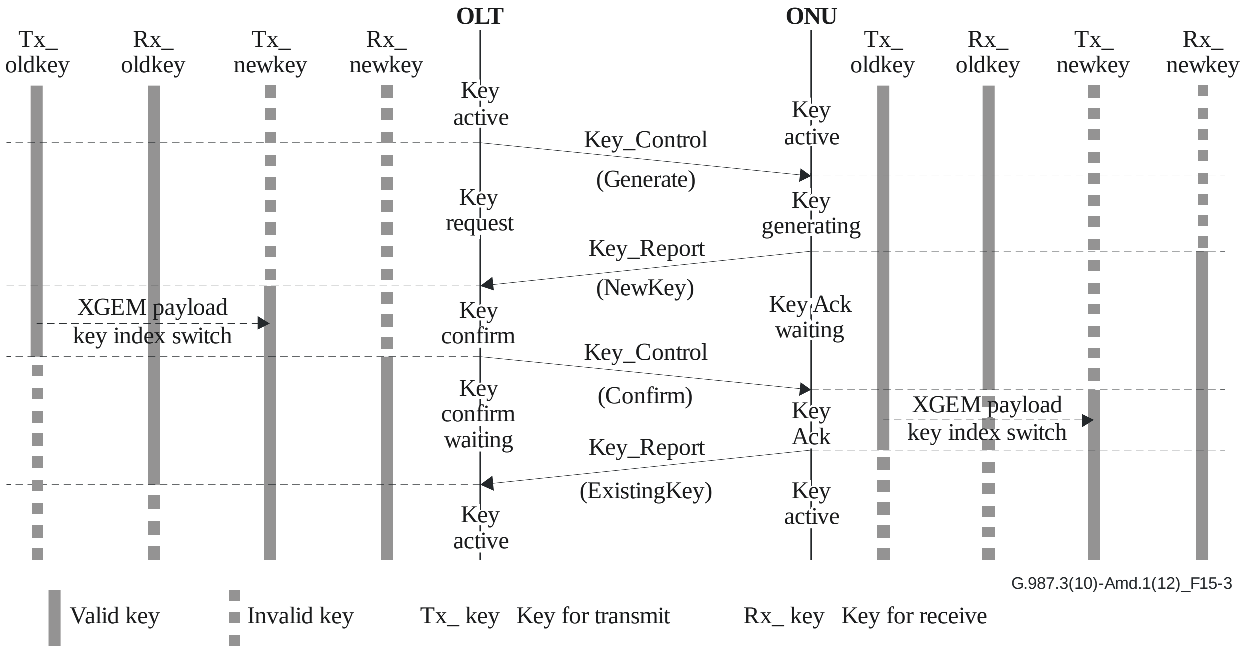


Figure 15-3 – Key validity in key exchange

15.5.3.2 OLT states and state diagram

The five OLT states of encryption key exchange and activation are defined as follows:

a) Key Inactive state (KL0)

The ONU is registered and is in state O5. There is no active key for XGEM payload encryption. No keys are valid to receive and/or transmit between the OLT and the ONU. When the OLT decides to initiate the unicast data encryption key exchange, it moves to the Key Request state (KL1).

b) Key Request state (KL1)

The OLT initiates a new key request by sending a Key_Control(Generate) PLOAM message, that instructs the ONU to generate a new key and to send it upstream. In this state, the new key is yet unknown to the OLT and, therefore, is invalid to receive and invalid to transmit. If there is an old key (i.e., an existing key), the old key remains valid to receive and valid to transmit at the OLT. Once a Key_Report(NewKey) PLOAM message is received, the OLT moves to the Key Confirm state (KL2).

If timer TK1 expires and no Key_Report(NewKey) message is received, the OLT initiates a new key request.

c) Key Confirm state (KL2)

In this state, the new key is valid to transmit and invalid to receive at the OLT. The old key (if there is an old key) is valid to receive and valid to transmit at the OLT. The OLT selects the moment to begin encrypting XGEM payload with the new key.

d) Key Confirm Waiting state (KL3)

The OLT sends a Key_Control(Confirm) PLOAM message for the specified key index. The new key becomes valid to receive and valid to transmit at the OLT. The old key (if there is an old key) remains valid to receive but becomes invalid to transmit at the OLT. Once a Key_Report(ExistingKey) PLOAM is received, the OLT moves to the Key Active state (KL4).

If timer TK2 expires and no Key_Report(ExistingKey) has been received, the OLT sends a new Key_Control(Confirm) PLOAM message.

e) Key Active state (KL4)

Once a Key_Report(ExistingKey) PLOAM message is received, the old key (if there is an old key) becomes invalid to receive and invalid to transmit. The new key is the only active key for receive and transmit between the OLT and the ONU.

If a rekey is required, the OLT moves to the Key Request state (KL1).

If a key check is required, the OLT sends a Key_Control(Confirm) PLOAM message, but no state transition occurs.

To support encryption key exchange and activation, the OLT maintains three timers:

TK1 – OLT key exchange waiting timer. Timer TK1 is used to abort an unsuccessful key exchange or key check attempt by limiting the overall time an OLT can sojourn in states KL1, KL2, and KL3. The recommended initial value of TK1 is 100 ms.

TK2 – Key waiting timer. Timer TK2 is used to abort an unsuccessful key request attempt by limiting the overall time an OLT can sojourn in state KL1. The recommended initial value of TK2 is 10 ms.

TK3 – Key confirmation waiting timer. Timer TK3 is used to abort an unsuccessful key confirmation request attempt by limiting the overall time an OLT can sojourn in state KL3. The recommended initial value of TK3 is 10 ms.

Figure 15-4 shows a graphic representation of the states of the OLT.

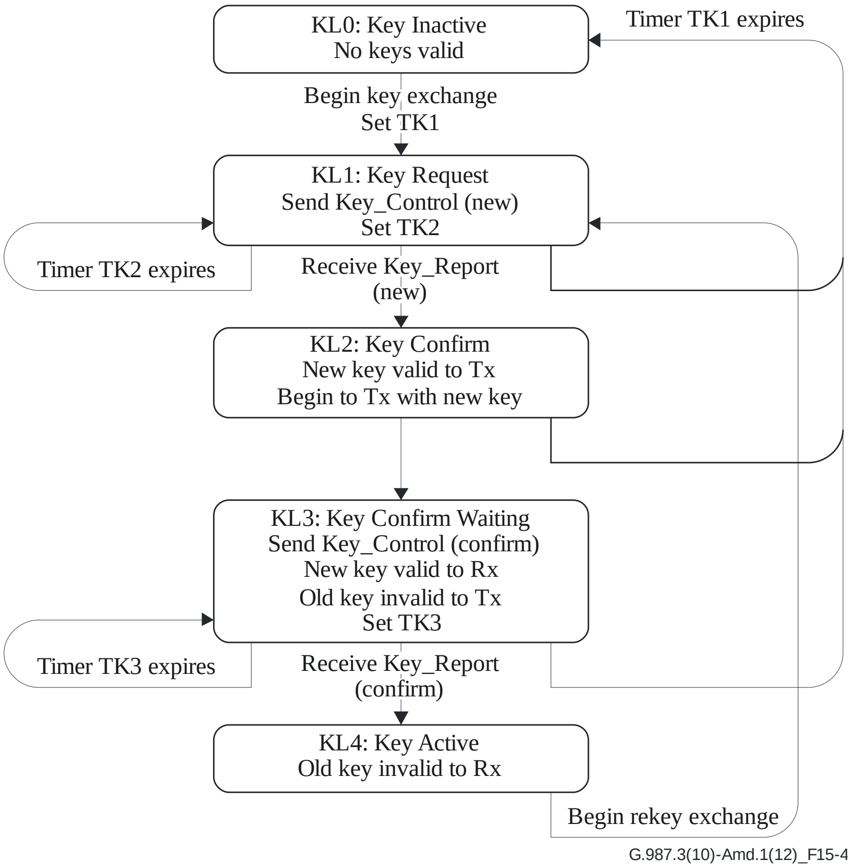


Figure 15-4 – OLT key exchange state diagram

15.5.3.3 ONU states and state diagram

The five ONU states of encryption key exchange and activation are defined as follows:

a) Key Inactive state (KN0)

The ONU is registered and is in state O5. There are no active keys for XGEM payload encryption between the OLT and the ONU. When a Key_Control(Generate) PLOAM message for a new key is received, the ONU moves to the Key Generating state (KN1).

b) Key Generating state (KN1)

The ONU generates a new key. If there is an old key, the old key is valid to receive and valid to transmit at the ONU. The new key is invalid to receive and invalid to transmit at the ONU.

c) Key Ack Waiting state (KN2)

The ONU sends a Key_Report(NewKey) PLOAM message to inform the OLT of the new key. The new key is encrypted for PLOAM transmission with AES-ECB using KEK. The new key becomes valid to receive and remains invalid to transmit at the ONU. Once a Key_Control(Confirm) PLOAM message is received, the ONU moves to the Key Ack state (KN3).

If timer TK5 expires and no Key_Control(Confirm) message is received, the ONU resends the Key_Report(NewKey) PLOAM message with the new key. If the ONU receives a new Key_Control(Generate) PLOAM message, it also resends the Key_Report(NewKey) PLOAM message. In this case it is at ONU's discretion to use a previously generated key, or to generate yet another new key.

d) Key Ack state (KN3)

In this state, the new key is valid to receive and becomes valid to transmit at the ONU. The old key (if there is an old key) remains valid to transmit but becomes invalid to receive at the ONU. The ONU begins to encrypt XGEM payload with the new key. The ONU acknowledges the OLT by sending a Key_Report(ExistingKey) PLOAM message with the Key_Name of the newly generated key. Once the Key_Report(ExistingKey) PLOAM message is sent, the ONU moves to the Key Active state (KN4).

e) Key Active state (KN4)

In this state, the new key is valid to receive and valid to transmit at the ONU. The old key (if there is an old key) becomes invalid to receive and invalid to transmit at the ONU.

Once a Key_Control(Generate) PLOAM message is received for the presently inactive key_index, the ONU moves to the Key Generating state (KN1) with the active key being referenced to as old key.

If at any time a Key_Control(Confirm) PLOAM message is received for the existing key, the ONU sends a Key_ Report(ExistingKey) PLOAM message, but no state transition occurs.

To support encryption key exchange and activation, the ONU maintains two timers:

TK4 – ONU key exchange waiting timer. Timer TK4 is used to abort an unsuccessful key exchange or key check attempt by limiting the overall time an ONU can sojourn in the set of states KN1, KN2, and KN3. The recommended initial value of TK4 is 100 ms.

TK5 – Key Ack waiting timer. Timer TK5 is used to limit the overall time an ONU can sojourn in state KN2. The recommended initial value of TK5 is 20 ms.

Figure 15-5 shows a graphic representation of the states of the ONU.

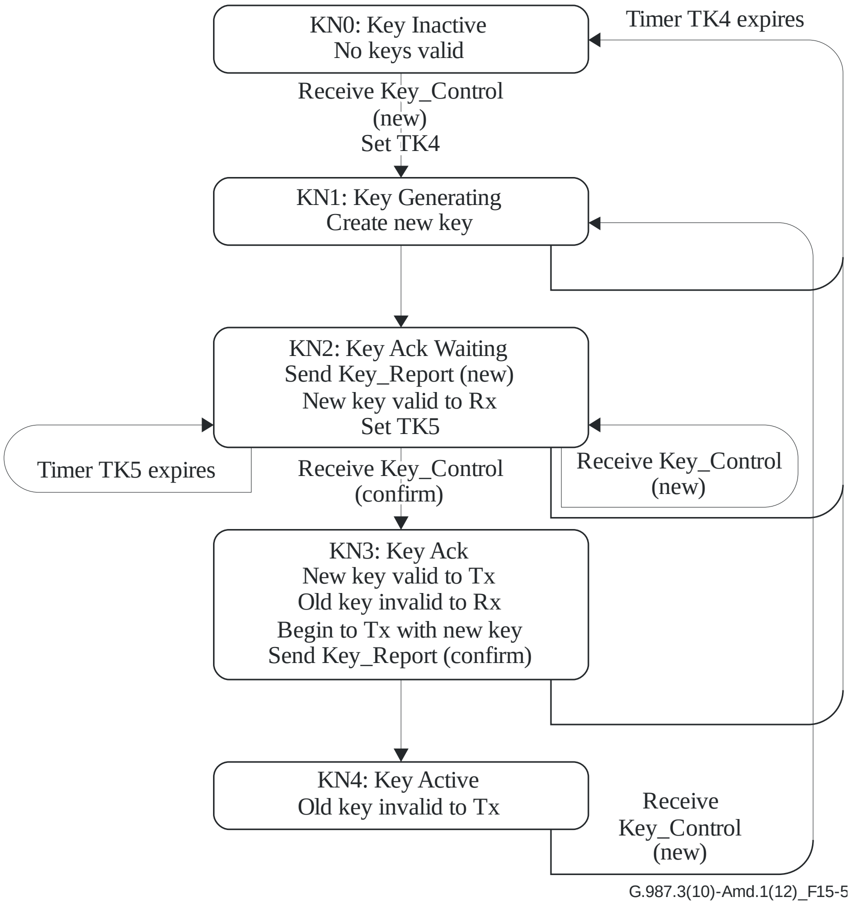


Figure 15-5 – ONU key exchange state diagram

15.5.4 Downstream multicast encryption

The key exchange process is initiated by the OLT. The OLT selects the key index to be changed. The OLT takes this key index out of use, to avoid key mismatch during the process of re-keying. The OLT generates each broadcast key using a random number generator suitable for cryptographic purposes.

Via OMCI, the OLT then writes the key to the broadcast key table attribute (see clause 9.13.11 of [ITU-T G.988]) in the MIB of each ONU that is provisioned to receive multicast traffic. The broadcast encryption key is encrypted with the AES-ECB algorithm using the KEK.

The OMCI is an acknowledged channel, so the OLT can confirm that the ONU has indeed modified the key attribute in question. Once the OLT has confirmed that all relevant ONUs have the new broadcast key, the OLT can put the key index back into service.

15.6 Integrity protection and data origin verification for PLOAM

For the PLOAM messaging channel, sender identity verification and protection against forgery is achieved with the use of the 8-byte message integrity check (MIC) field of the PLOAM message format.

15.6.1 Cryptographic method

The MIC field of the PLOAM message format is constructed using the cipher-based message authentication code (CMAC) algorithm specified in [NIST SP800-38B] with the 128-bit Advanced encryption standard (AES-128) encryption algorithm [NIST FIPS-197] as the underlying block cipher.

The parameters and the notation for invocation of the AES-CMAC function are described in clause 15.3.1.

15.6.2 MIC calculation

Given the 40 bytes of the PLOAM message content and the PLOAM integrity key PLOAM_IK, the sender and receiver can calculate the MIC field as follows:

$$PLOAM\text{-}MIC = \text{AES-CMAC}\ (PLOAM\_IK, C_{\text{dir}} \,|\, PLOAM\_CONTENT, 64) \qquad (15\text{-}7)$$

Where C_{dir} is the direction code: C_{dir} = 0x01 for downstream and C_{dir} = 0x02 for upstream, and *PLOAM_CONTENT* denotes octets 1 to 40 of the PLOAM message.

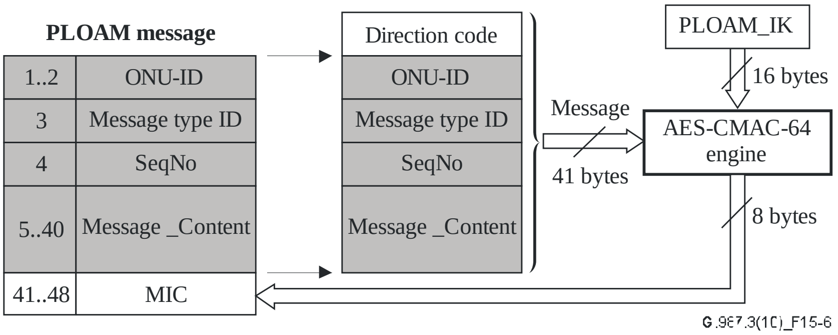


Figure 15-6 – PLOAM integrity protection

15.7 Integrity protection and data origin verification for OMCI

For the OMCC channel, the sender identity verification and protection against forgery is achieved with the use of the 4-byte message integrity check (MIC) field of the OMCI message format.

15.7.1 Cryptographic method

The MIC field of the OMCI message format is constructed using the cipher-based message authentication code (CMAC) algorithm specified in [NIST SP800-38B] with the 128-bit advanced encryption standard (AES-128) encryption algorithm [NIST FIPS-197] as the underlying block cipher.

The parameters and the notation for invocation of the AES-CMAC function are described in clause 15.3.1.

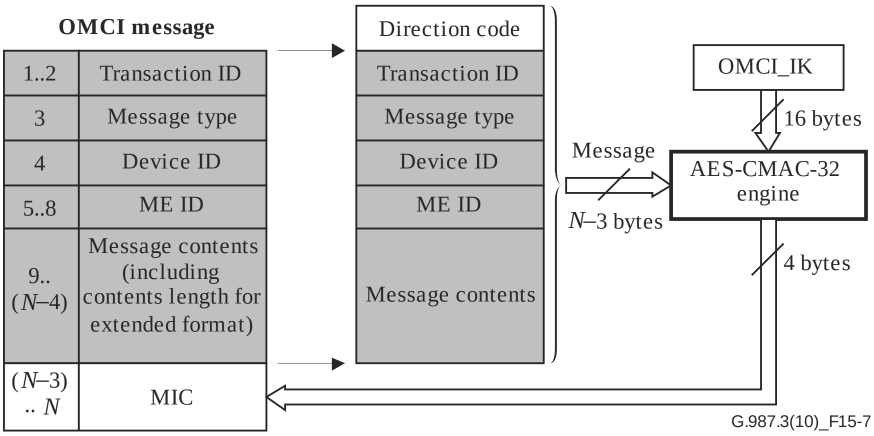


Figure 15-7 – OMCI integrity protection

15.7.2 MIC calculation

Given the content of the OMCI message and the OMCI integrity key OMCI_IK, the sender and receiver can calculate the MIC field as follows:

$$\mathit{OMCI\text{-}MIC} = \text{AES-CMAC}\,(\mathit{OMCI\_IK}, (C_{\mathrm{dir}} \mid \mathit{OMCI\_CONTENT}), 32) \qquad (15\text{-}8)$$

Where C_{dir} is the direction code: C_{dir} = 0x01 for downstream and C_{dir} = 0x02 for upstream, and *OMCI_CONTENT* refers to the OMCI message except the last 4 bytes.

15.8 Integrity and data origin verification key switching

15.8.1 Use of the default key

At the start of ONU activation, the PLOAM integrity key for the given ONU is set to the default value of $(0x55)_{16}$, which is used for PLOAM message exchange while no MSK is available. Once the ONU communicates its registration ID to the OLT, the basic MSK is established and all the derivative shared keys are obtained. The OMCI integrity key does not require an explicit default, as no OMCI exchange takes place prior to MSK establishment and no broadcast OMCC channel is supported.

The broadcast PLOAM messages, the Serial_Number_ONU (upstream) PLOAM message, the Deactivate_ONU-ID (downstream) PLOAM message, as well as the Request_Registration (downstream) and Registration (upstream) PLOAM messages are always protected by a MIC that is generated with the default PLOAM integrity key. The specified messages, therefore, can be successfully transmitted even if the OLT and ONU have not established or no longer agree on the dynamically derived keys.

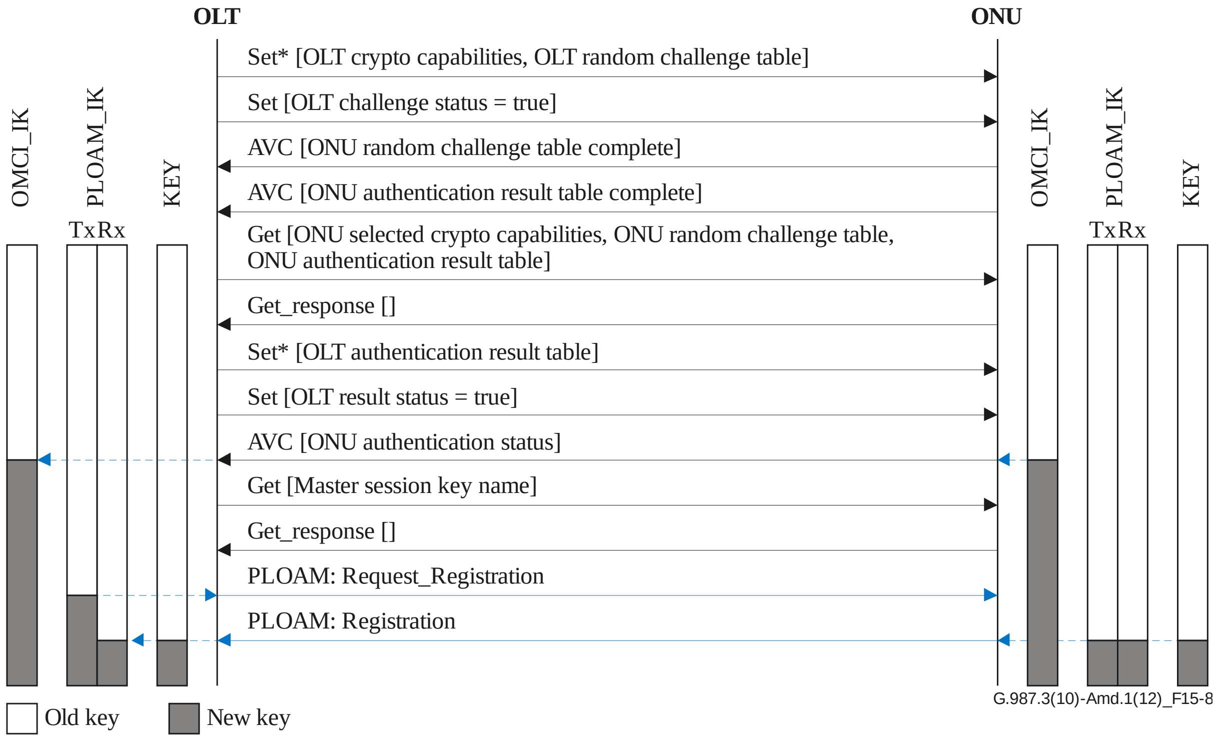
15.8.2 Key switching for OMCI-based secure mutual authentication

The following description refers to the Enhanced security control attributes and procedures specified in clause 9.13.11 of [ITU-T G.988].

The authentication is implemented as a three-step symmetric-key-based challenge-response procedure in the OMCI channel followed by a PLOAM handshake in the form of Registration ID exchange.

The OLT initiates the OMCI-based authentication at its discretion by writing the OLT random challenge table attribute. From this point to the completion of the authentication procedure, the OLT refrains from sending to the ONU any OMCI messages unrelated to authentication.

The ONU generates a random challenge of its own, computes the response to the OLT challenge, and initiates the secure MSK and derived shared key calculation procedure. Once computed, the secure keys are stored for future use.


OLT
ONU
Set* [OLT crypto capabilities, OLT random challenge table]
Set [OLT challenge status = true]
AVC [ONU random challenge table complete]
AVC [ONU authentication result table complete]
Get [ONU selected crypto capabilities, ONU random challenge table, ONU authentication result table]
Get_response []
Set* [OLT authentication result table]
Set [OLT result status = true]
AVC [ONU authentication status]
Get [Master session key name]
Get_response []
PLOAM: Request_Registration
PLOAM: Registration
OMCI_IK
PLOAM_IK
KEY
TxRx
Old key
New key
G.987.3(10)-Amd.1(12)_F15-8

NOTE – Set* indicates multiple set operations as needed to fill the table

Figure 15-8 – OMCI-based secure mutual authentication procedure. Unless explicitly specified otherwise, the messages are exchanged over the OMCI channel.

Upon receipt of the ONU's response to optical line terminal (OLT) random challenge along with the ONU random challenge table, the OLT unilaterally verifies the ONU's authentication status. If the unidirectional ONU-to-OLT authentication fails, further execution of the authentication procedure is aborted. If the unidirectional ONU-to-OLT authentication succeeds, the OLT calculates the MSK and the derivative shared keys, storing them for future use. Once the key calculation is completed, the OLT proceeds with execution of the authentication procedure by writing the OLT authentication result table and OLT result status to the ONU.

Upon receipt of the OLT's response, the ONU verifies the OLT's authentication status and fills in the ONU authentication state attribute. The ONU uses the next available default Alloc-ID grant opportunity to transmit an attribute value change (AVC) on the ONU authentication state attribute. If the unidirectional OLT-to-ONU authentication has failed, a message integrity check (MIC) on the AVC message is generated using the previously active OMCI_IK. If the unidirectional OLT-to-ONU authentication has succeeded (and thus the mutual authentication has succeeded as well), the MIC field on the AVC message is generated with the new OMCI_IK. The new OMCI_IK is committed active at the ONU.

When the OLT receives the AVC on the ONU authentication state from the ONU, it checks whether the MIC field has been generated using the old OMCI_IK or the new OMCI_IK. If the old OMCI_IK was used by the ONU, the OLT discards the previously calculated key material. If the new OMCI_IK was used by the ONU, the OLT commits the new OMCI_IK as active. The OLT then initiates a PLOAM handshake by generating a downstream Request_Registration PLOAM message to the ONU. The purpose of the handshake is to delineate the activation of the secure shared keys in case of authentication success, or to obtain the registration-based MSK and derived shared keys in case of authentication failure. The Request_Registration PLOAM message is protected, by definition, using the default PLOAM_IK. Upon transmission of the Request_Registration message, the OLT commits the new PLOAM_IK as active on transmit.

Once the ONU receives the downstream Request_Registration PLOAM message, it generates an upstream Registration PLOAM message, which is protected, by definition, using the default PLOAM_IK. Upon transmission of the Registration message, the ONU commits the new PLOAM_IK and KEK as active.

Once the OLT receives the upstream Registration PLOAM message from the ONU, it commits the PLOAM_IK and KEK as active on receive, thus completing the key switching procedure.

15.8.3 Key switching for IEEE 802.1x-based authentication

Once the IEEE 802.1x-based mutual authentication or re-authentication process has completed, the OLT and the authenticated ONU have a 200 ms grace interval to compute the new set of derived shared keys. Within this interval, a sender should either remain silent or continue to use the old integrity key and switch to the new one as soon as it detects the new key in the received message, or at the end of the grace interval, at the latest. While the new key is being computed, a receiver continues checking the received messages with the old key. When the new key becomes available, the receiver should start checking messages with both old and new keys and switch to using the new key only once the new key check is successful, or at the end of the grace interval, at the latest.

15.8.4 MIC failure considerations

If MIC failure is caused by random transmission errors, then it is likely a rare event that can be correlated with the observed bit-error ratio (BER) level. A persistent MIC failure, on the other hand, is likely caused by an integrity key mismatch at the transmitter and receiver and may indicate either a security threat or a malfunction of the authentication and key generation procedure. In case of persistent message integrity check failure, of which the OLT learns either directly (upstream MIC failure) or through the lack of expected management traffic flow from the ONU (downstream MIC failure), the OLT recognizes a loss of PLOAM channel (LOPCi) defect or a loss of OMCI channel (LOOCi) defect for a given ONU and has to select, at its discretion, the appropriate mitigation actions, which may include repeating authentication using the same or an alternative mechanism, blocking upstream and downstream traffic, deactivating or disabling the offending ONU, or executing a rogue ONU diagnostic procedure.

15.9 XG-PON systems with reduced data encryption strength

Clause 15.9.1 introduces the concept of effective key length. Clause 15.9.2 contains the conditional requirements that are mandatory only for XG-PON systems with specified effective key lengths less than 128 bits. For an ONU, the effective key length is provisioned using the effective key length attribute (see clause 9.13.11 of [ITU-T G.988]).

15.9.1 Effective key length

The standard key size used for AES data encryption in XG-PON is 128 bits. Per operator requirements, an XG-PON system may optionally employ a data encryption system of reduced strength by replacing a part of the key with a well-defined bit pattern. The number of randomly generated bits of the key is referred to as the effective key length.

15.9.2 Data encryption key format

In an XG-PON system with reduced data encryption strength, the effective key length L_{eff} is a multiple of 8 bits, and each network element responsible for data encryption key generation replaces the $(128 - L_{\mathrm{eff}})/8$ most significant octets of the 128-bit key with the value 0x55, as shown in Figure 15-9.

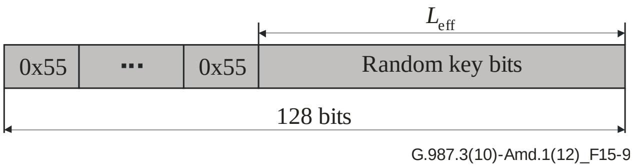


Figure 15-9 – Format of a data encryption key with reduced effective length

In an XG-PON system with reduced data encryption strength, a network element responsible for the generation of a data encryption key should be able to report the effective key length to the element management system.

2.2) Various security-related maintenance items

2.2.1) Modified clause 11.3.1 – Key_Control and Key_Report PLOAM message definitions

Modify the definitions of Key_Control PLOAM message (summary in clause 11.3.1 with format specification in clause 11.3.3.8) and Key_Report PLOAM message (summary in clause 11.3.2 with format specification in clause 11.3.4.3) as follows:

11.3.1 Downstream message summary

Table 11-2 summarizes the downstream messages.

…

0x0D	Key_Control	The OLT instructs the ONU to generate a new data encryption key or to confirm an existing data encryption key	At the OLT's discretion.	Send one Key_Report message for each 32-byte fragment of response content.

…

11.3.2 Upstream message summary

Table 11-3 summarizes the upstream messages.

…

0x05	Key_Report	To send a fragment of a new data encryption key or a hash of an existing data encryption key	In response to Key_Control message from the OLT	See clause 15.5.1 for the details of the protocol.

…

11.3.3.8 Key_Control message

Octet	Content	Description
1-2	ONU-ID	Directed or broadcast message to instruct one or all ONUs to generate new keying material or confirm their existing keys. As a broadcast message, ONU-ID = 0x03FF.
3	0x0D	Message type ID "Key_Control".
4	SeqNo	Unicast or broadcast PLOAM sequence number, as appropriate.

Octet	Content	Description
5	Reserved	Set to 0x00 by the transmitter; treated as "don't care" by the receiver.
6	0000 000C	Control: 0-Generate: The ONU shall generate a new data encryption key and send it upstream. 1-Confirm: The ONU shall send upstream a hash of the existing data encryption key (Key_Name).
7	0000 00bb	bb: Key index 01-First key of a key pair. 10-Second key of a key pair.
8	Key_Length	Required key length, bytes. The value 0 specifies a key of 256 bytes (Note).
9-40	Padding	Set to 0x00 by the transmitter; treated as "don't care" by the receiver.
41-48	MIC	Message integrity check.
NOTE – This parameter supports the long-term extensibility of the data encryption key exchange protocol. The currently specified cryptographic method for the data encryption, the AES-128 cipher (see clause 15.4) uses the fixed size key of 16 bytes.		

11.3.4.3 Key_Report message

Octet	Content	Description
1-2	ONU-ID	
3	0x05	Message type ID "Key_Report".
4	SeqNo	Repeats value from the downstream Key_Control message. If the length of the keying material requires that several Key_Report messages be sent upstream, the sequence number is the same in each of them.
5	0000 000R	Report type. R: 0-NewKey: The message contains the newly generated key or key fragment 1-ExistingKey: The message contains the cryptographic hash of an existing key.
6	0000 00bb	bb: Key index 01-First key of a key pair. 10-Second key of a key pair.
7	0000 0FFF	Fragment number, range 0..7. The first fragment is number 0 (Note).
8	Reserved	Set to 0x00 by the transmitter; treated as "don't care" by the receiver.

Octet	Content	Description
9-40	Key_Fragment	Key fragment, 32 bytes. Any padding that may be required is in the higher-numbered bytes of the message. To confirm the existing key, a single 16-byte fragment containing the cryptographic hash of the key (key name) is sent. Key_Name = AES_CMAC (KEK, encryption_key | 0x33313431353932363533353839373933, 128). For a new key, KEK_encrypted key fragment is sent. KEK_Encrypted_key_fragment = AES_ECB_128(KEK, encryption_key_fragment). (Note)
41-48	MIC	Message integrity check.
NOTE – This parameter supports the long-term extensibility of the data encryption key exchange protocol. Both the currently specified (see clause 15.4) cryptographic method for the data encryption (AES-128) and its immediate extension (AES-192 or AES-256) require a single key fragment and only one Key_Report PLOAM message to transmit the key.		

2.2.2) Modified clause 11.3.3.4 – Deactivate_ONU-ID PLOAM message description

In the table of clause 11.3.3.4, change the description of octets 41-48 to read as follows:

Message integrity check computed using the default PLOAM integrity key (see clause 15.8).

2.2.3) Modified clause 11.3.4.3 – Notation for AES-ECB procedure

In the table of clause 11.3.4.3, in the last line of the description of the octets 9-40, Key_Fragment field, replace AES_ECB_128 with AES-ECB:

KEK_Encrypted_key = AES-ECB (KEK, encryption_key).

2.2.4) Modified clause 12.2.2 – MSK and shared key discard

In clause 12.2.2, insert the words "as well as the MSK and the derived shared keys," *after the list of the TC layer configuration parameters in the third sentence of item (a) Initial state (O1), before the words* "are discarded", *and in the second sentence of item (f) Emergency stop state (O7), before the words* "are effectively discarded".

a) Initial state (O1)

The ONU originally powers up in this state and enters this state upon ONU deactivation or enabling after an emergency stop. The transmitter is turned off. The TC layer configuration parameters, including ONU-ID, default and explicitly assigned Alloc-IDs, default XGEM Port-ID, burst profiles, and equalization delay, as well as the secure MSK and the derived shared keys, are discarded.

…

f) Emergency Stop state (O7)

An ONU that receives a Disable_Serial_Number message with the 'disable' option moves to the Emergency Stop state (O7) and shuts its laser off. The TC layer configuration parameters, including ONU-ID, default and explicitly assigned Alloc-IDs, default XGEM Port-ID, burst profiles, and equalization delay, as well as the secure MSK and the derived shared keys, are effectively discarded.

2.2.5) Modified clause 14.1 – XGEM key error conditions

Modify the value of the Description entry for the XGEM key errors parameter in Table 14-1 (clause 14.1) as follows:

XGEM frames discarded because of unknown or invalid encryption key. Examples include: no unicast or broadcast key established for specified key index, key index indicating encrypted XGEM frame on an XGEM port that is not provisioned for encryption, key index indicating upstream encryption on an XGEM port that is provisioned for downstream encryption only, or invalid key index (11) This count is included in the Rx XGEM frame count.

2.2.6) Modified clause 15.7.1 – Cryptographic method

OMCI message content

In Figure 15-7 modify the parenthetic phrase after Message contents to read:

(including contents length for the extended format and the first four bytes of the trailer for the basic format)

3) Additional golden vectors

In Appendix IV, add clauses IV.9 and IV.10 with the following content.

IV.9 Upstream key reporting

```
Data_encryption_key = 0x112233445566778899AABBCCDDEEFF00

KEK = 0x6f9c99b8361768937e453b165f609710


AES-ECB (KEK, Data_encryption_key)

0x4018340d538bb3f50df3186cf075f7b6

AES-CMAC (KEK, Data_encryption_key | 0x33313431353932363533353839373933, 128)

0x3cc507bb1731c569ed7b79f8bdc376be
```

IV.10 Downstream OMCI message integrity check

```
OMCI message direction:
       Cdir = 0x01 (downstream)
OMCI_CONTENT:
       Transaction correlation identifier: 0x80 0x00
       Message type: 0x49 (GET)
       Device identifier: 0x0A (Baseline OMCI)
       Managed entity identifier: 0x01 0x00 0x00 0x00 (ONU-G)
       Message contents:
          0x00 0x80 0x00 0x00 0x00 0x00 0x00 0x00
          0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
          0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
          0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
       OMCI trailer[1:4]: 0x00 0x00 0x00 0x28
OMCI_IK = 0x184b8ad4d1ac4af4dd4b339ecc0d3370
```

```
AES-CMAC (OMCI_IK, (Cdir | OMCI_CONTENT), 32)
0x78dca53d
```

4) Regular maintenance items

4.1) Modified clause 8.2.2.1 – Encoding of BufOcc in the DBRu structure

Add the following sentence at the end of clause 8.2.2.1:

While the length *L* of an individual SDU is a natural number, the BufOcc field needs to encode two special values: 0x000000 denotes an empty buffer, and 0xFFFFFF represents an invalid measurement.

4.2) Acknowledgment PLOAM message

*Replace word "*Acknowledge*" with "*Acknowledgment*" on the following five occasions:*

(1) Clause 11.3.2, Table 11-3: Message name for Message-ID 0x09;

(2) Clause 11.3.4.4: Clause heading;

(3) Clause 11.3.4.4: Description of octet 3;

(4) Clause 14.1, Table 14-1: Description column corresponding to the row "Upstream PLOAM message count" in "PLOAM PM" section;

(5) Clause 14.1, Table 14-1: Parameter column in "PLOAM PM" section.

4.3) PLOAM message format ONU-ID field description

Insert words "Sender identity" into the Description column of the row "Octet 1-2" in clauses 11.3.4.2, 11.3.4.3, 11.3.4.4, and 11.3.4.5.

4.4) Modified clause 13.1.8 – Round-trip delay and round-trip time

In clause 13.1.8, in Equation 13-8, replace RTD_i *with* RTT_i *, and in the subsequent note, replace the words* "Here RTD_i is the round-trip delay in microseconds as measured by the OLT" by "Here RTT_i is the round-trip time, i.e., the actual offset of the start of the upstream PHY burst with respect to the start of the downstream PHY frame specifying that burst, in microseconds, as measured by the OLT."

4.5) Modified clause 14.2.1 – Acronym expansion for DFi defect

In the table of clause 14.2.1, modify the DFi type expansion as follows:

Disable failure of ONU *i*.

4.6) Modified clause 14.2.1 – Semantics of LOOCi defect.

In the table of clause 14.2.1, in the description of the LOOCi defect, remove words " and/or protocol violations".

4.7) Clauses 16.2 and 16.3 – Power management state transition diagram clarification

Provide the following note after both Figures 16-1 and 16-2:

NOTE – The vertices on the state diagram graph can be qualified as either "tense" or "relaxed" forming the yellow and grey subgraphs, respectively. As a rule, an output PLOAM message is generated only on a state transition that crosses the subgraph boundary.

4.8) Modified clause 16.2 – Power management parameter description

In Table 16-1 of clause 16.2, modify the parameter descriptions as follows:

(1) *Tsleep*:

Local timer at ONU. Upon entry to Asleep or Listen state, the ONU initializes Tsleep to a value equal to or less than Isleep.

(2) *Iaware*:

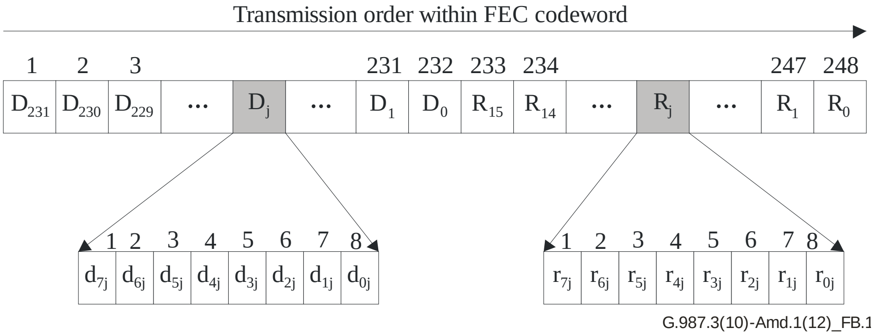
Iaware is the minimum time the ONU spends in its SleepAware or DozeAware state before transitioning to a low power state (Asleep or Listen, respectively), as a count of 125 microsecond frames

(3) *Taware*:

Local timer at ONU. Upon entry to Asleep or Listen state, the ONU initializes Tsleep to a value equal to or less than Isleep.

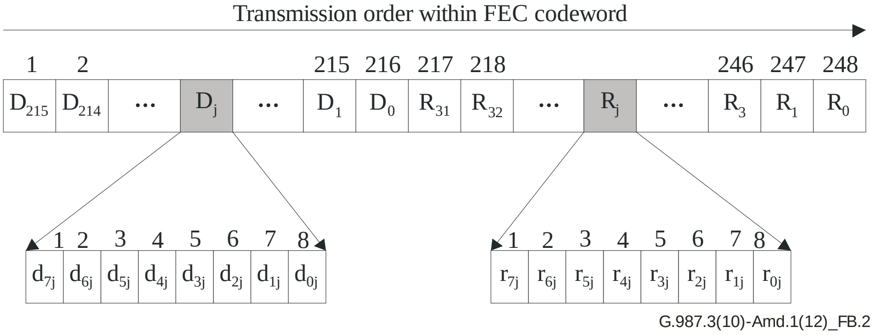
4.9) Modified Annex B – Octet expansion in Figures B.1 and B.2.

In Annex B, to avoid confusing octet expansion, replace Figures B.1 and B.2 with the following enclosed Figures:



Transmission order within FEC codeword
1 2 3 231 232 233 234 247 248
D231 D230 D229 ··· Dj ··· D1 D0 R15 R14 ··· Rj ··· R1 R0
1 2 3 4 5 6 7 8
d7j d6j d5j d4j d3j d2j d1j d0j
1 2 3 4 5 6 7 8
r7j r6j r5j r4j r3j r2j r1j r0j
G.987.3(10)-Amd.1(12)_FB.1

Figure B.1 – Transmission order of the RS(248, 232) codeword



Transmission order within FEC codeword
1 2 215 216 217 218 246 247 248
D215 D214 ··· Dj ··· D1 D0 R31 R32 ··· Rj ··· R3 R1 R0
1 2 3 4 5 6 7 8
d7j d6j d5j d4j d3j d2j d1j d0j
1 2 3 4 5 6 7 8
r7j r6j r5j r4j r3j r2j r1j r0j
G.987.3(10)-Amd.1(12)_FB.2

Figure B.2 – Transmission order of the RS(248, 216) codeword

5) New Annex E

Amend ITU-T G.987.3 (10/2010) with Annex E below (appropriately numbered) specifying the PON-ID maintenance functionality.

Annex E

PON-ID maintenance

(This annex forms an integral part of this Recommendation.)

The implementation of this annex is optional. The ITU-T G.987 XG-PON systems, OLTs, or ONUs that are required to support the provision of the present annex are herein referred to as compliant. An ONU's compliance with this annex can be discovered via OMCI (see clause 9.1.1 of [ITU-T G.988]).

E.1 Introduction

This annex contains provisions enabling field personnel to retrieve a PON port identifier and an indication of the launched power on the network, adapted from the optical layer supervision concept defined in [b-ITU-T G.984.2A2], and applied to the optical module capabilities of XG-PON. The specified method defines the format of the PON-ID structure. Comparison of the locally measured optical power and the image of the source launched power coded in the PON-ID field should give operators a means to differentiate fibre plant loss from variations in launched power. Coding commonality with existing power measurements in [ITU-T G.988] is intended, as well as alignment with [b-SFF SFF8472] which defines the information available at the RSSI interface of opto-electrical converters of interest in OLT implementations.

E.2 PON-ID structure

A system compliant with this annex shall support a PON-ID structure according to the following definition, which supersedes clause 10.1.1.3.

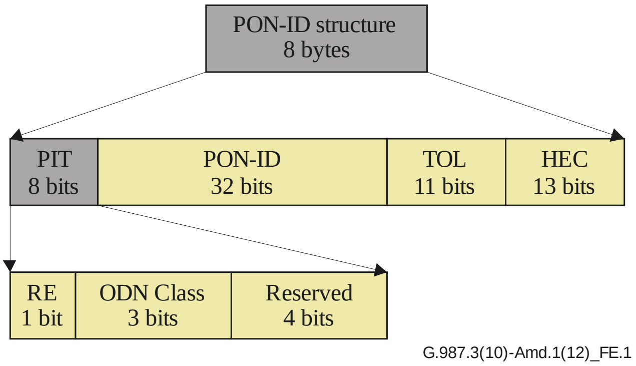


Figure E.1 – PON-ID structure

The PON-ID structure (see Figure E.1) contains the following fields:

PIT, or **PON-ID Type** (8 bits, static, provisioned by the operator): an indication of the ODN architecture, the source of the reported launch power and the ODN class. The PON-ID type (PIT) field is further partitioned as follows:

RE flag (1 bit): indicates whether the transmit optical level (TOL) field contains the launch power of the OLT or of a reach extender;

ODN Class (3 bits): Identifies the nominal optical parameters of the transceiver according to ODN class as defined in [ITU-T G.987.2] with the following coding

Code value	ODN Budget class
000	N1
001	N2a
010	N2b
011	E1
100	E2a
101	E2b
110	Reserved
111	Reserved

Four bits reserved for future use; set to 0000 unless otherwise specified.

PON-ID (32 bits, static, provisioned by the operator): any value of interest to the operator, which may, for example, reflect the established logical address plan;

TOL (11 bits, dynamic, maintained by the system): transmit optical level, an indication of the current transceiver launch power of the appropriate network element. Its value is an integer referred to 1 µW (i.e., the value zero represents –30 dBm), with 0.1 dB granularity. The 0x7FF default value indicates that TOL is not supported on the given PON interface. The coding is adapted to support the entire suite of specified XG-PON ODN classes (N1, N2a, N2b, E1, E2a, E2b) and reach extender options, covering the transceiver launch power range from +2dBm to +16.5dBm.

HEC (13 bits, dynamic inserted by the transmitter): a combination of a BCH(63,12,2) code operating on the 63 initial bits of the SFC structure and a single parity bit. The details of HEC construction and verification are specified in Annex A of this Recommendation.

6) New Annex F

Amend ITU-T G.987.3 (10/2010) with Annex F below (appropriately numbered) specifying the extended rogue ONU mitigation capabilities of XG-PON systems.

Annex F

Extended rogue ONU mitigation capabilities

(This annex forms an integral part of this Recommendation.)

The implementation of this annex is mandatory for all new implementations. The ITU-T G.987 XG-PON systems, OLTs, or ONUs that support the provision of the present annex are herein referred to as compliant.

F.1 Introduction

The present annex contains provisions that allow an XG-PON system to mitigate the condition when an ONU exhibits rogue behaviour at the discovery stage of the activation process, before its serial number is discovered and before it is assigned an ONU-ID. The provisions of this annex allow the OLT, upon detecting rogue interference on the PON, to selectively disable the ONUs at the discovery stage of the activation process.

F.2 Extra codepoint of Disable PLOAM message type

A compliant OLT and a compliant ONU support a Disable_Serial_Number PLOAM message, whose definition is modified with respect to the summary of clause 11.3.1 and format specification of clause 11.3.3.5 as follows.

Message Type ID	Message name	Function	Trigger	Effect of receipt
0x06	Disable_Serial _Number	Broadcast message to disable/enable a specified ONU set.	At the OLT's discretion.	Disable options: Moves the specified ONU, the ONU in the discovery stage, or all ONUs to the Emergency Stop state. The disabled ONU is prohibited from transmitting. Enable options: Moves the specified ONU or all ONUs in the Emergency Stop state to the Initial state. The enabled ONU discards the TC layer configuration and restarts the activation process, as specified in clause 12. No Acknowledgement.

The modified Disable_Serial_Number message has the following format.

Octet	Content	Description
1-2	0x03FF	Broadcast ONU-ID.
3	0x06	Message type ID "Disable_Serial_Number".
4	SeqNo	Broadcast PLOAM sequence number.
5	Disable/enable	0xFF – The ONU with this serial number is denied upstream access. 0x00 – The ONU with this serial number is allowed upstream access. 0x0F – All ONUs are denied upstream access. The content of bytes 6-13 is ignored. 0x3F – Disable_Discovery: the ONUs in O2-3 state are denied upstream access. The content of bytes 6-13 is ignored. 0xF0 – All ONUs are allowed upstream access.
6-9	Vendor-ID	ONU Vendor-ID code, a four-character combination discovered at SN acquisition.

Octet	Content	Description
10-13	VSSN	Vendor-specific serial number, a four-byte unsigned integer discovered at SN acquisition.
14-40	Padding	Set to 0x00 by the transmitter; treated as "don't care" by the receiver.
41-48	MIC	Message integrity check.

F.3 Extra transition of the ONU activation cycle state transition diagram

F.3.1 State transition diagram

A compliant system supports the standard ONU activation state transition diagram as reproduced in Figure F.1, where the Disable SN request event has state-specific definition.

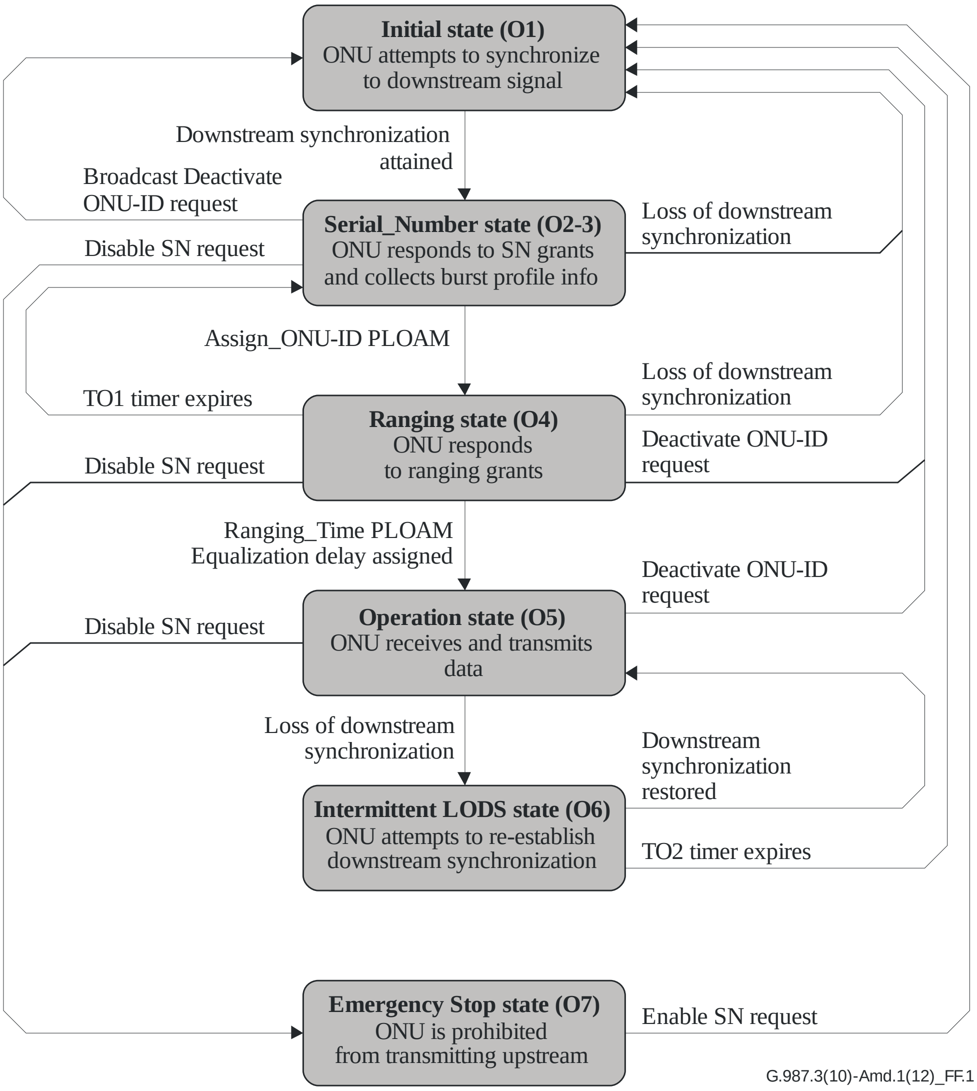

Initial state (O1)
ONU attempts to synchronize to downstream signal
Downstream synchronization attained
Broadcast Deactivate ONU-ID request
Serial_Number state (O2-3)
ONU responds to SN grants and collects burst profile info
Loss of downstream synchronization
Disable SN request
Assign_ONU-ID PLOAM
Loss of downstream synchronization
TO1 timer expires
Ranging state (O4)
ONU responds to ranging grants
Deactivate ONU-ID request
Disable SN request
Ranging_Time PLOAM Equalization delay assigned
Deactivate ONU-ID request
Operation state (O5)
ONU receives and transmits data
Disable SN request
Loss of downstream synchronization
Downstream synchronization restored
Intermittent LODS state (O6)
ONU attempts to re-establish downstream synchronization
TO2 timer expires
Emergency Stop state (O7)
ONU is prohibited from transmitting upstream
Enable SN request
G.987.3(10)-Amd.1(12)_FF.1

Figure F.1 – The modified ONU activation state diagram

In state O2-3, Disable SN requests is generated upon receipt of Disable_Serial_Number PLOAM message with Disable specific SN, Disable All, or Disable_Discovery options. In states O4 and O5, the Disable SN requests is generated upon receipt of Disable_Serial_Number PLOAM message with Disable specific SN or Disable All options, but is not generated upon receipt of Disable_Serial_Number PLOAM message with Disable_Discovery option.

F.3.2 ONU state transition table

In addition to the events and transitions of Table 12-1 in clause 12.2.4, a compliant system supports a transition from the Serial Number (O2-3) state to the Emergency Stop (O7) state upon receipt of the Disable_Serial_Number PLOAM message with Disable_Discovery option.

Event	**ONU activation state**						
	Initial **O1**	**Serial Number** **O2-3**	**Ranging** **O4**	**Operation** **O5**	**Intermittent LODS** **O6**	**Emergency Stop** **O7**	**Suspension** **O8**
Receive Disable PLOAM – Disable_Discovery option	–	==> O7;	–	–	–	–	–

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013