International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series G
Supplement 76
(12/2021)

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

Optical transport network security

ITU-T G-series Recommendations – Supplement 76

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
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.

Supplement 76 to ITU-T G-series Recommendations

Optical transport network security

Summary

Supplement 76 to ITU-T G-series Recommendations provides an overview of applications and use cases for secure optical transport in various optical transport network (OTN) layers.

The Supplement relates to Recommendations ITU-T G.709/Y.1331 and ITU-T G.709.1/Y.1331.1.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T G Suppl. 76	2021-12-17	15	11.1002/1000/14979

Keywords

Authentication, encryption, FlexOsec, ODUsec, OTN security, OTNsec, transport security.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 76 to ITU-T G-series Recommendations

Optical transport network security

1 Scope

This Supplement describes optical transport security applications, requirements and the use of multiple optical transport network (OTN) signals and structures to assist in implementing security solutions.

2 References

[ITU-T G.709] Recommendation ITU-T G.709/Y.1331 (2020), *Interfaces for the optical transport network*.

[ITU-T G.709.1] Recommendation ITU-T G.709.1/Y.1331.1 (2018), *Flexible OTN short-reach interfaces*.

[ITU-T G.798] Recommendation ITU-T G.798 (2017), *Characteristics of optical transport network hierarchy equipment functional blocks*.

[ITU-T G.806] Recommendation ITU-T G.806 (2012), *Characteristics of transport equipment – Description methodology and generic functionality*.

[ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[IEEE 802.1AE] IEEE Std 802.1AE (2018), *IEEE standard for local and metropolitan area networks-Media access control (MAC) security.*

[NIST SP 800-38D] *Recommendation for block cipher modes of operation: Galois/Counter mode (GCM) and GMAC.*

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the terms defined in [ITU-T G.709], [ITU-T G.709.1] and the following terms defined in [ITU-T X.800]:

3.1.1 confidentiality [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.2 encryption [ITU-T X.800]: The cryptographic transformation of data (see cryptography) to produce ciphertext.

3.1.3 integrity [ITU-T X.800]: Property that data has not been altered or destroyed in an unauthorized manner.

3.1.4 key [ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

CPE	Customer Premise Equipment
CST	Cipher Suite Type
DC	Data Centre
E-NNI	External Network to Network Interface
FlexOsec	Flexible Optical transport network security
GFP	Generic Framing Procedure
GMP	Generic Mapping Procedure
IMP	Idle Mapping Procedure
MAC	Media Access Control
MACsec	Media Access Control security
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
ODUCn	Optical Data Unit C
ODUk	Optical Data Unit k
OPUCn	Optical Payload Unit Cn
OTN	Optical Transport Network
OTNsec	Optical Transport Networking security
OTUCn	Optical Transport Unit Cn
OTUk	Optical Transport Unit k
OTUsec	Optical Transport Unit security
PHY	PHYsical layer
UNI	User to Network Interface

5 Conventions

None.

6 OTN Secure Transport

Security is an important aspect of today's modern networks and operators are continuously faced with various threats. There are many functions in a network that address security risks such as control management, denial of service, unauthorized access and so on. This Supplement will focus on protecting the confidentiality and integrity of the network data plane. More specifically, this Supplement will focus on optical transport networking security (OTNsec), e.g., encryption, authentication, based on OTN systems and structures defined in [ITU G.709] and [ITU G.709.1]. This is often referred to as "Layer 1 encryption" in the market.

The goal of this Supplement is to provide market guidance on the use of OTN for security applications. Other organizations such as the National Institute of Standards and Technology (NIST) and the National Information Assurance Partnership (NIAP) provide recommendations for security algorithms that are commonly used with IPSec, MACsec [IEEE 802.1AE] and, similarly, can be utilized with OTN.

6.1 Secure transport conceptual architecture

There are two conceptual approaches that could be considered for security transport applications. The first approach, which is depicted in the lefthand scenario of Figure 6-1, represents a service requestor deploying endpoints in its ports facing an untrusted domain. This is the preferred approach covered in this Supplement.

The second approach, which is depicted in the righthand scenario of Figure 6-1, represents a service provider providing security endpoints in its ports facing the service requestor equipment and gives a service requestor control over security parameters (key management and agreement).

The security endpoints, which are the OTNsec source and sink functions, are identified by lock icons in the scenario figures.

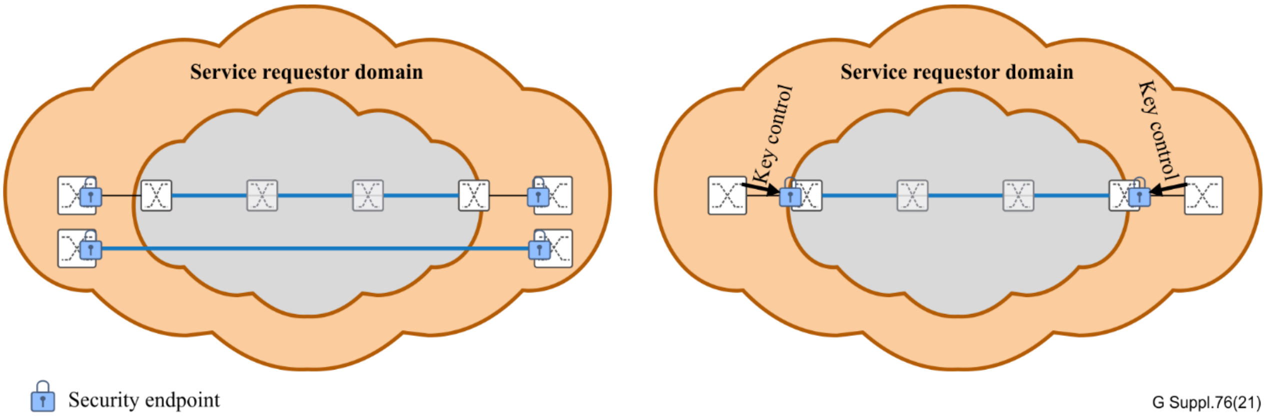

Figure 6-1 – Security conceptual architecture

6.2 Secure transport applications overview

Network operators and service providers have various applications that require confidentiality and authenticity of the data transported on their networks. We generically call these functions security in this Supplement. This section will go through a non-exhaustive list of the most commonly expected security applications for optical transport networks.

6.2.1 Client end-to-end security

The first set of applications explored in this Supplement apply security at the client layer, and the operator OTN network is agnostic to the client level security. The encryption and authentication, including associated key management and agreement, is entirely in the customer's domain. An example of client level encryption is media access control security (MACsec) [802.1AE] for Ethernet clients. OTN provides various mapping procedures (e.g., GMP, BMP, IMP and GFP-F) that can provide bit, code and timing or medica access control (MAC) frame transparency for the secured Ethernet clients. Other multiservice client scenarios are equally applicable to Figures 6-2 to 7-2.

In Figure 6-2, the customer equipment is connected directly to a tributary port of the operator's OTN (customer premise equipment) CPE with a user to network interface (UNI). In this scenario, the customer is the service requestor. The client security protects the UNI access link inside in the trusted customer premises as well as the operator outer domain which can be considered untrusted. The operator's OTN equipment will map the client onto the unsecured OTN network.

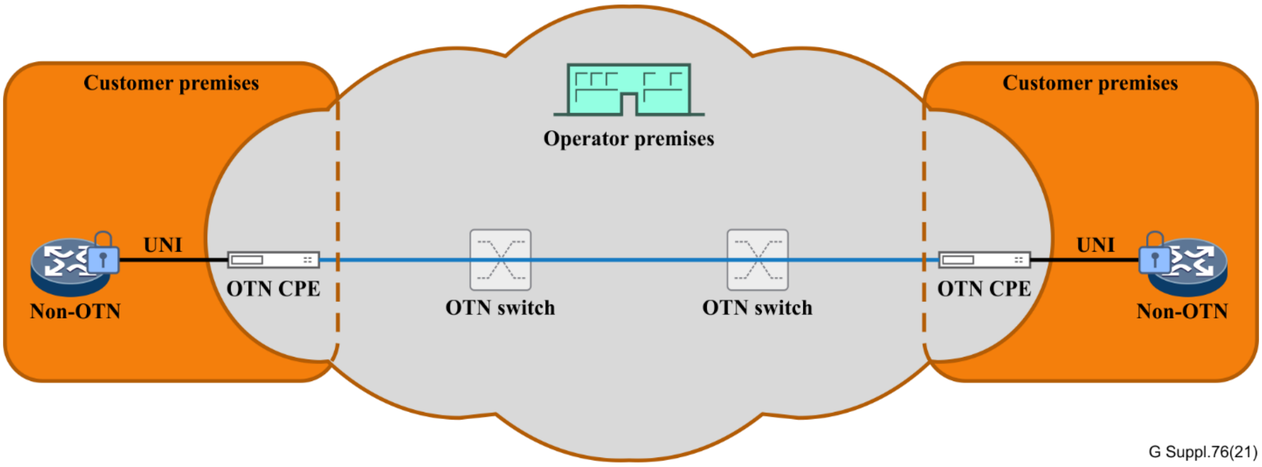

Figure 6-2 – Client end-to-end security (with CPE)

In Figure 6-3, the customer equipment is connected directly to a tributary port of the operator's OTN switch or transponder with a UNI. The client encryption protects the UNI access link, which in this case is exposed outside the customer premise as well as the operator outer domain. The operator's OTN equipment will map the client onto the unsecured OTN network.

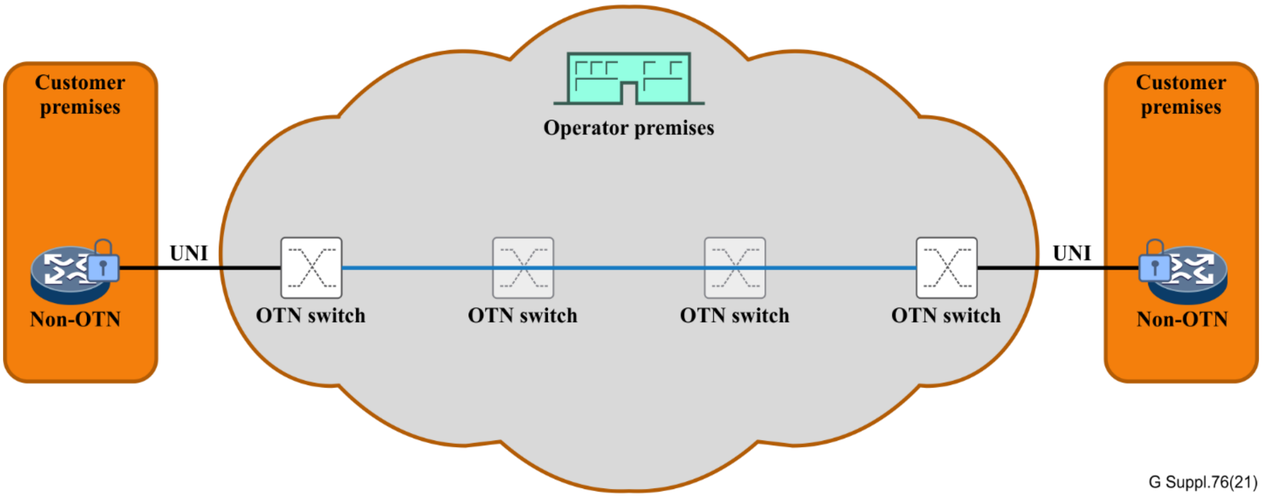

Figure 6-3 – Client end-to-end security (without CPE)

In Figure 6-4, an example data centre, content or mobile provider are the service requestors to another operator. The service requestor secures its end-to-end client using client encryption and authentication. The provider is connected directly to a tributary port of the operator's OTN switch or transponder with a UNI. The client encryption protects the UNI access link, which in this case is outside the provider's premise as well as the operator outer domain. The operator's OTN equipment will map the client onto the unsecured OTN network.

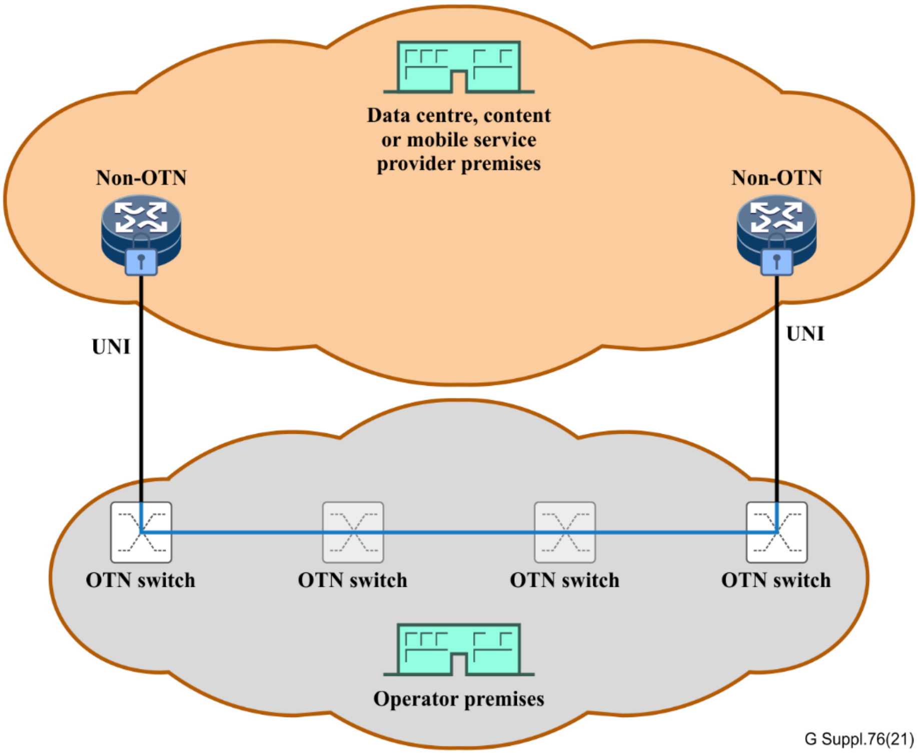

Figure 6-4 – DC, content or mobile service provider client end-to-end security

6.2.2 Service provider CPE end-to-end security

The scenario in Figure 6-5 is similar to that shown in Figure 6-2, where the customer equipment is connected directly to a tributary port of the operator's OTN CPE. However, in this scenario the service provider (which could also be the network operator) is providing the security on the OTN service within the operator's network. The key management and agreement are managed within the service provider's domain. The UNI access link is unprotected, but still within the trusted customer premises. In this scenario, ODUsec security can provide end-to-end optical data unit k (ODUk) security through the operator's network.

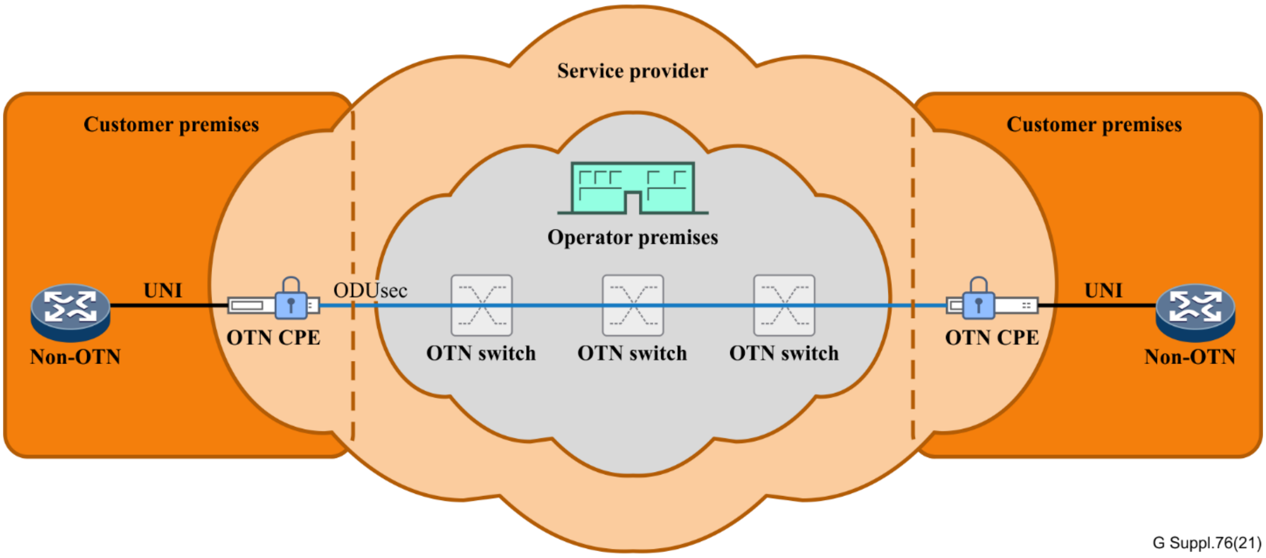

Figure 6-5 – Service provider CPE end-to-end security

6.2.3 OTN link/span security

Operators looking to secure their infrastructure in the network can use encryption and authentication on a per span (link) basis. The links/spans interconnect the OTN network elements (e.g., OTN switches, OTN regenerators, …) within the same administrative domain. The key management and agreement are owned by the network operator. All client and ODUk services transported by the links are agnostic to the security application. In Figure 6-6, security is applied at optical link/span. Flexible optical transport network security (FlexOsec) or optical transport unit security (OTUsec) at the physical layer (PHY) can be applied for this scheme.

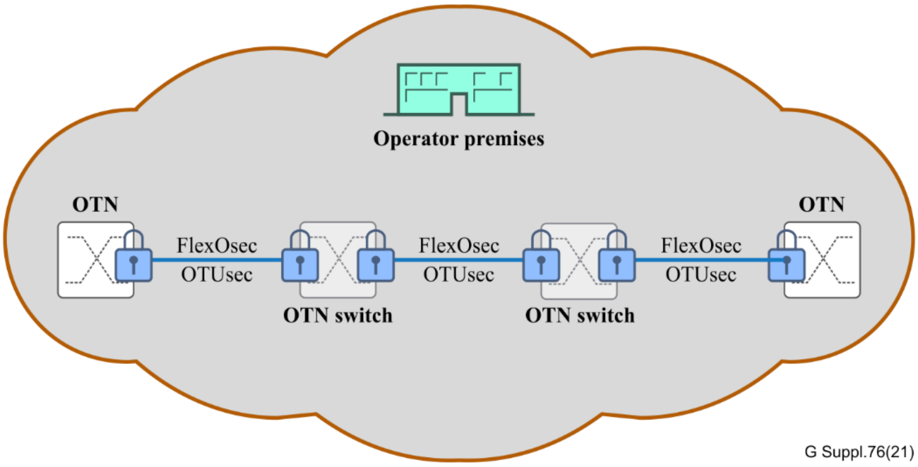

Figure 6-6 – OTN link/span security

In other scenarios, the optical links/spans are using leased fibre from another operator or can traverse other untrusted domains as shown in Figure 6-7. The secured spans are still managed and owned by the originating operator. The two operators have their separate administrative domains.

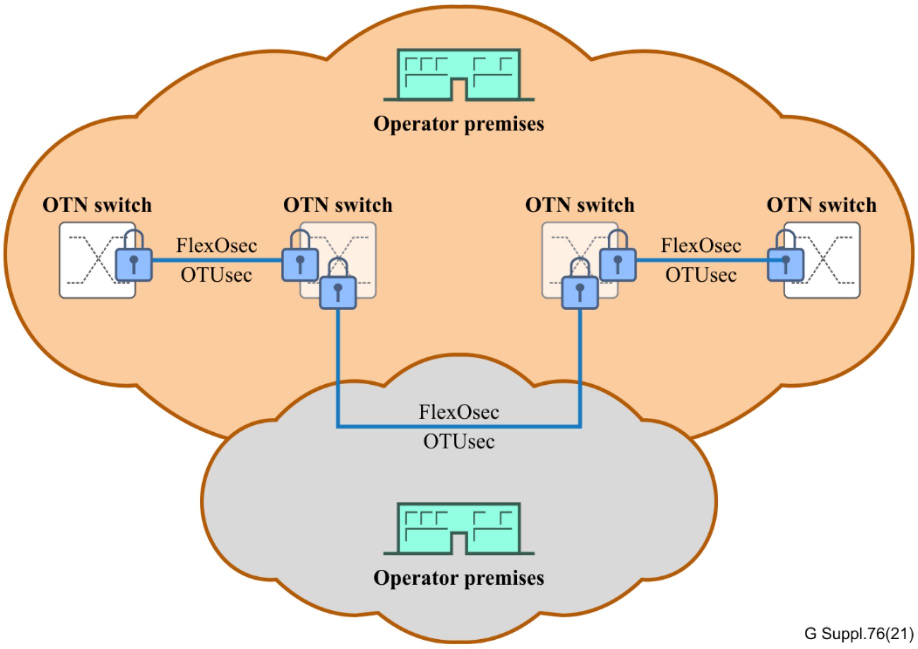

Figure 6-7 – OTN link/span leased fibre security

6.2.4 OTN second operator security

In Figure 6-8, a first operator leases an OTN service from a second operator. This scenario is often referred to as a carrier's carrier network. The OTN service would typically be secured from the service requestor (first operator) and traverse the unsecured second operator's network. The two operators have their separate administrative domains. ODUsec security would be applicable to such a scenario when the second operator operates OTN switches and regenerators.

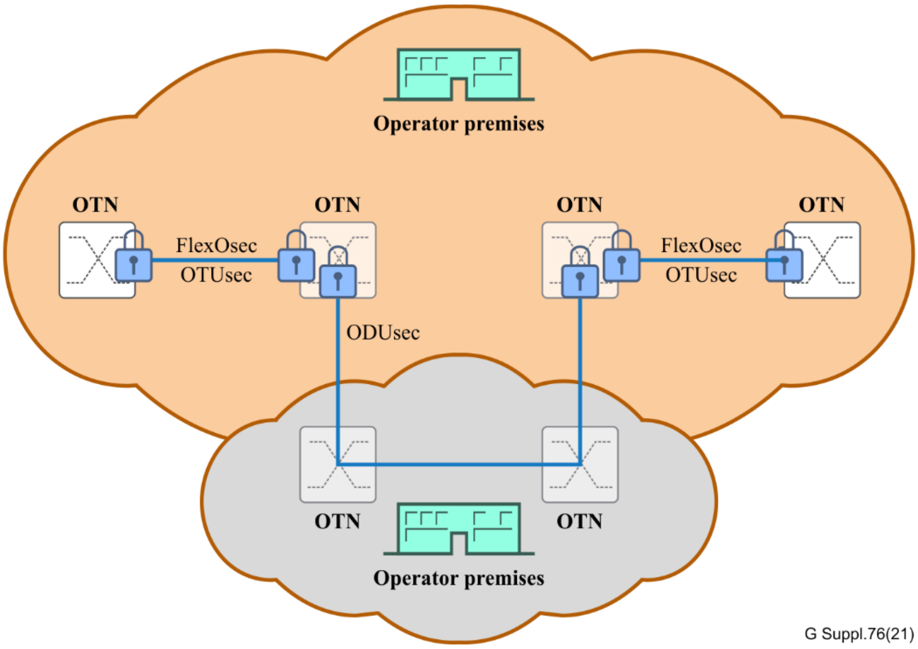

Figure 6-8 – OTN leased service security

6.2.5 Access link/span security

The access link part of the network refers to the handoff between customer premises to an operator. Security can be applied to this exposed fibre link. The access link can be a UNI, which connects to the operator's OTN equipment tributary ports as shown in Figure 6-9. For example, this could be a client Ethernet interface, which applies client MACsec, terminating the security on both ends of the link in the customer premise and the operator network. The key management and agreement are shared functions of both the customer and the operator.

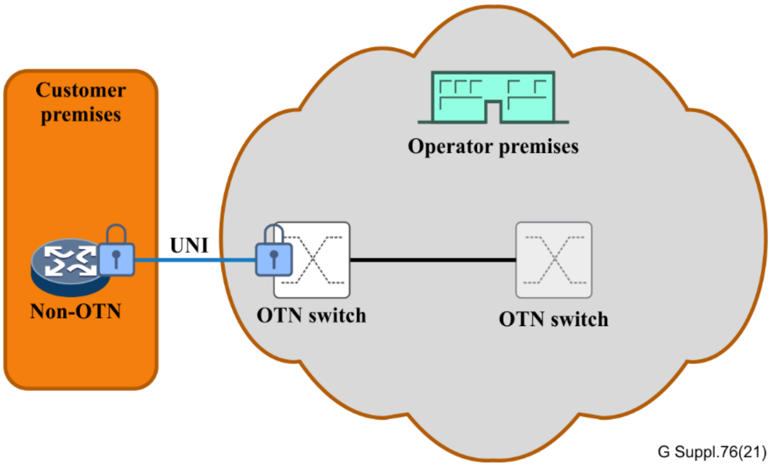

Figure 6-9 – Client access link/span security

In Figure 6-10, the access link can be an OTN E-NNI. The OTN security would originate from OTN CPE (on customer premises) and secure the link to the operator's equipment. The encryption and authentication can be applied to FlexOsec and OTUsec since it covers a single link/span. The key management and agreement are shared functions of both the service provider and the operator.

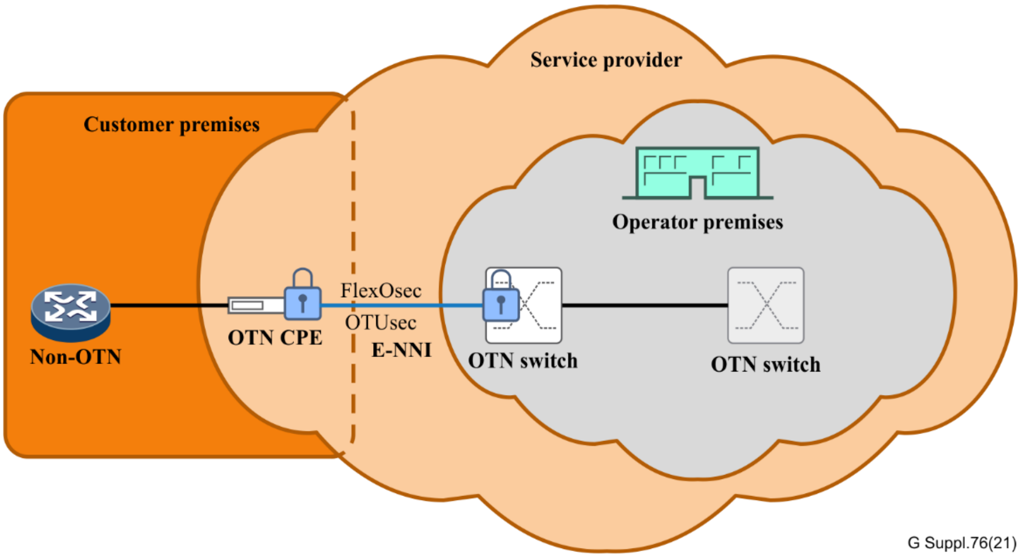

Figure 6-10 – OTN service provider access link/span security

6.2.6 OTN end-to-end security

In Figure 6-11, the customer equipment is connected directly to a tributary port of the operator's OTN CPE with a UNI. In this scenario, the customer is the service requestor, and may have control over the security parameters (key management and agreement). The security is provided by the operator on the client OTN service and protects the end-to-end OTN path within the operator's network, but the UNI is unprotected.

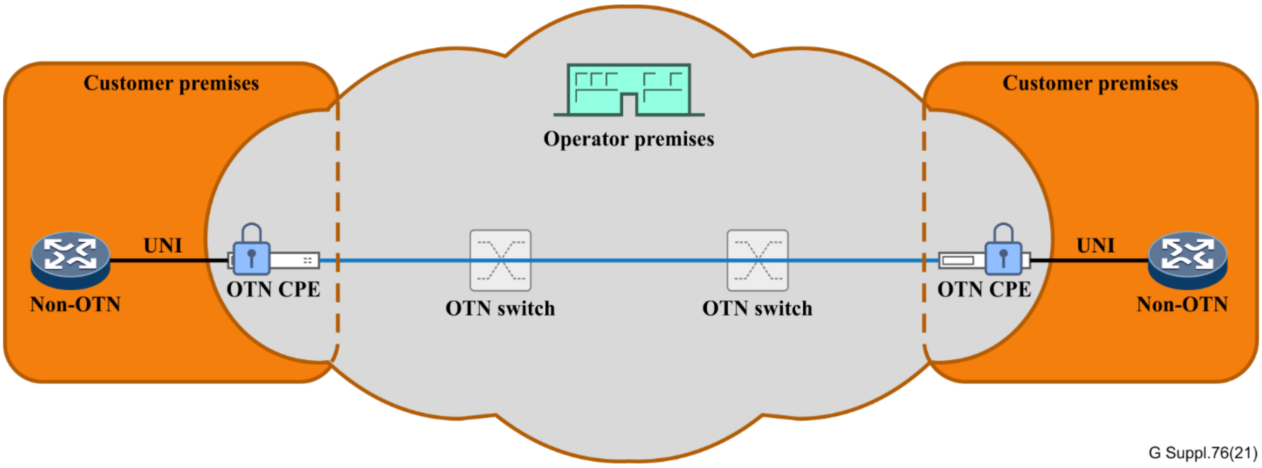

Figure 6-11 – OTN end-to-end security (with CPE)

In Figure 6-12, the customer equipment is connected directly to a tributary port of the operator's OTN switch or transponder with a UNI. The security is provided by the operator on the client OTN service and protects the end-to-end OTN path within the operator's network, but the UNI is unprotected.

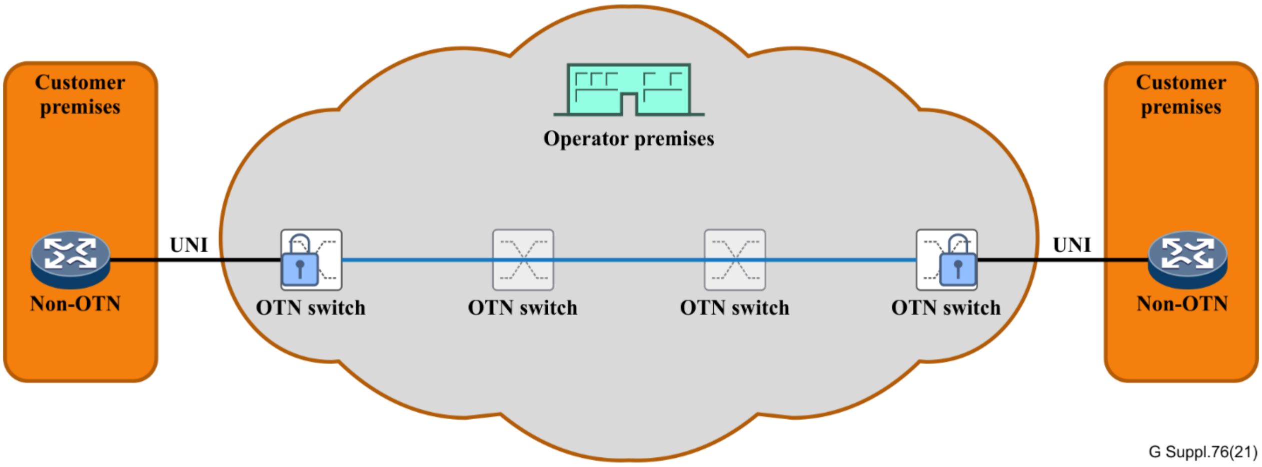

Figure 6-12 – OTN end-to-end security (without CPE)

In Figure 6-13, an example data centre, content or mobile provider is the service requestor to another operator. The security is provided by the operator on the client OTN service as in examples shown in other figures in this section.

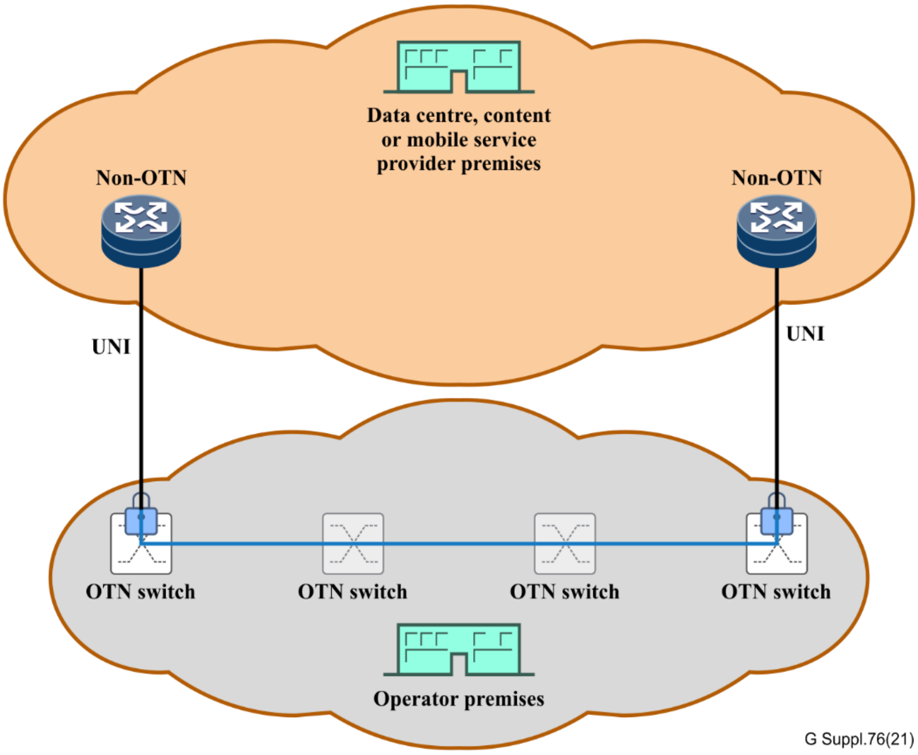

Figure 6-13 – DC, content or mobile service provider OTN end-to-end security

6.2.7 Service provider path end-to-end security

The scenario in Figure 6-14 is similar to Figure 6-11, where the customer equipment is connected directly to a tributary port of the operator's OTN CPE. However, in this scenario the operator is providing the security on the OTN client service within its network. The key management and agreement can be managed by the customer or the service provider. The UNI access link is unprotected. In this scenario, ODUsec security can provide end-to-end ODUk security through the operator's network.

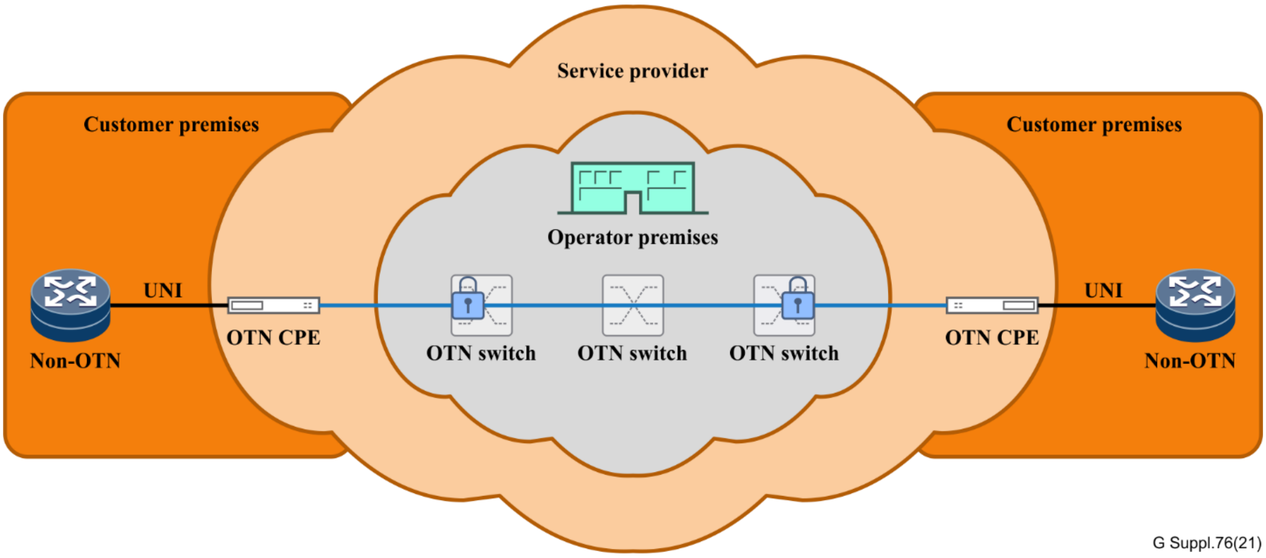

Figure 6-14 – Service provider path end-to-end security

7 Secure transport across layers

Security can be applied to a layered network, combining two or more of the applications described. While multiple layers of security may overlap in some respects, different security protocols provide different characteristics and can be complementary.

In Figure 7-1 the customer has end-to-end encryption at the client layer, which provides sufficient security within and between the customer premises. For any traffic leaving the customer premises at the OTN CPE, an additional layer of end-to-end encryption can be applied at the ODU layer (ODUsec 1st instance). ODU layer encryption provides the additional benefit of mitigating traffic analysis. FlexOsec/OTUsec provides link security to secure operator infrastructure as well as other traffic in the case of multiple ODU flows from the CPE. ODUsec security provides a similar function across a second operator's OTN switching network using OTN multiplexing to encapsulate the ODUsec 1st instance flow into an ODU prior to creating the ODUsec 2nd instance. The ODUsec 2nd instance may contain multiple ODU flows, some of which may be ODUsec 1st instances and others unsecured ODU. In this way the path an ODU takes does not push requirements across layers.

The layered approach can allow the customer to control security parameters for the client security and ODUsec, while the operator determines the appropriate parameters for link and OTN security. As an example of the flexibility possible, one could combine MACsec authentication-only, a first instance of ODUsec authenticated encryption, FlexOsec authentication-only and a second instance of ODUsec authenticated encryption.

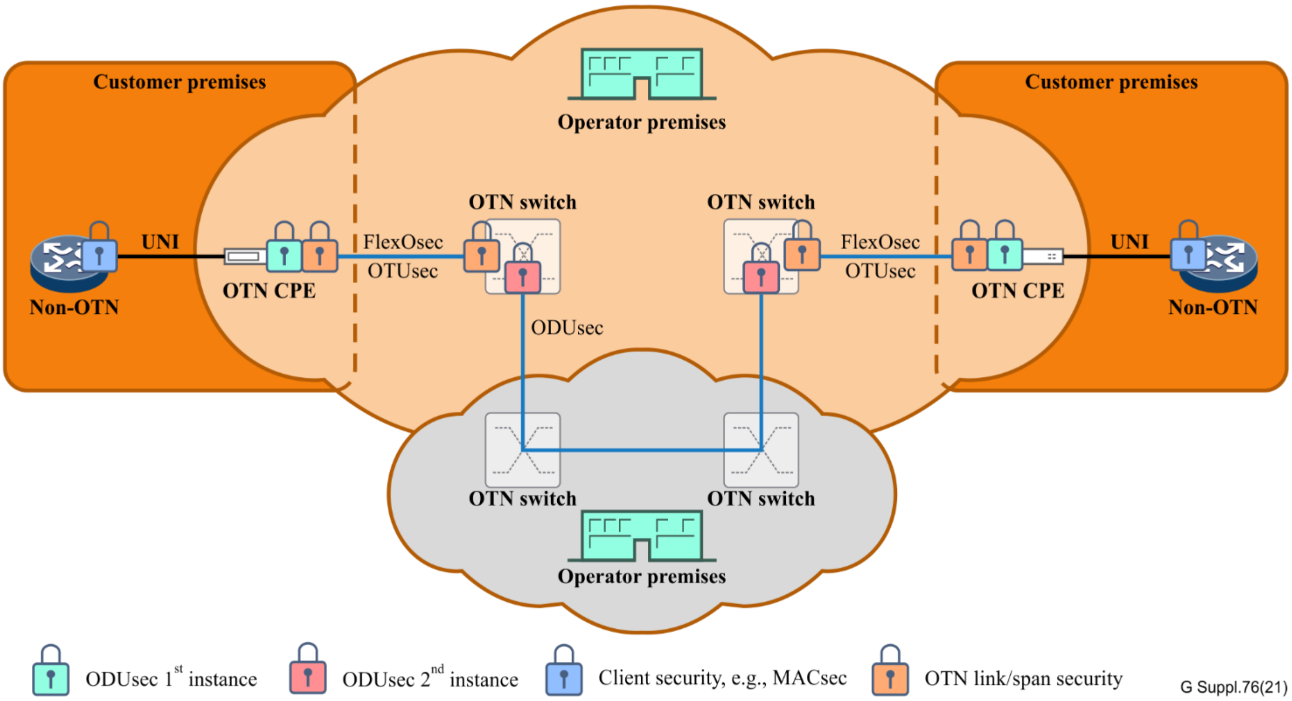

Figure 7-1 – Layered security example

Figure 7-2 illustrates possible containment relationships with ODUsec and FlexOsec (OTUsec is not illustrated). The details of some layers are not shown for clarity and full details can be found in [ITU-T G.709.1], [ITU-T G.709], and [ITU-T G.798]. The orange-shaded functions show the points at which security may optionally be applicable at different points in the path. The diverging branches show the layering options which are possible at different points in the path, for example:

– The secured ODUj could be multiplexed into ODUCn, ODUk or be sent on the line directly as an OTUk.

– The OPUk payload can carry a mixture of secured/non-secured ODUj clients and then the ODUk can be secured with ODUsec for transmission as an OTUk or further multiplexed into ODUCn.

– The OPUCn payload can carry a mixture of secured/non-secured ODUj and ODUk clients, and then can be secured with FlexOsec for transmission.

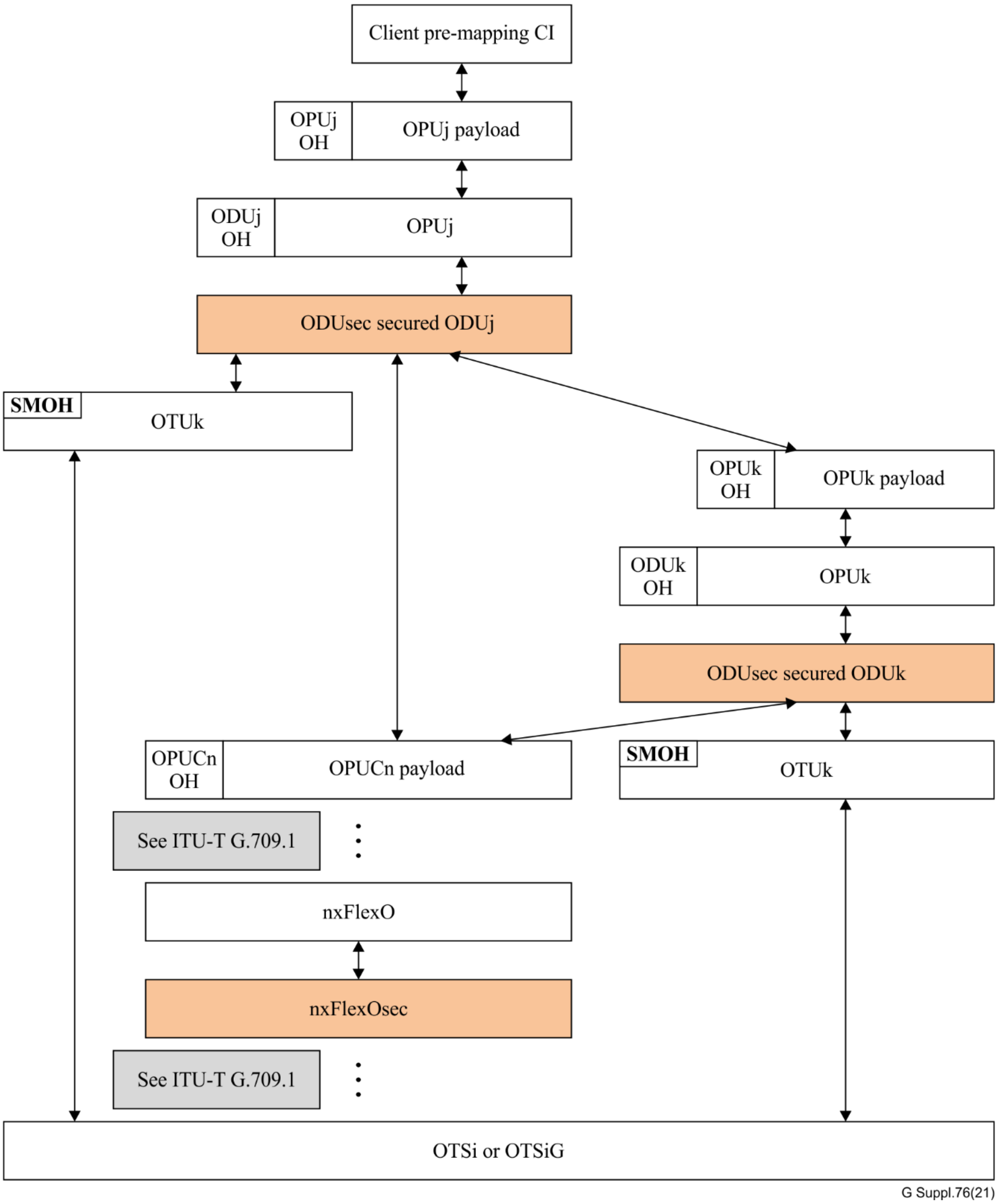

Figure 7-2 – ODUsec and FlexOsec containment relationships

8 Secure transport application observations

In the OTN security applications described in clauses 6 and 7, the following requirements can be derived:

- ODUsec security must be transparent to OTN network elements that do not participate as a security endpoint.
- OTN network equipment can provide client security (e.g. MACsec) transparent mappings.
- Multilevels of ODUj to ODUk schemes can be supported, up to two instances.
- Multilevels of ODUk to FlexO schemes can be supported, up to two instances.
- Subnetworks and TCMs are not required for security applications.

- Some PHY level security schemes (e.g., FlexOsec) need interoperable cipher suite type (CST) since the endpoints can be in different domains.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022