International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2705

(03/2013)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Security

Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS)

Recommendation ITU-T Y.2705

ITU-T

International
Telecommunication
Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	**Y.2700–Y.2799**
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

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

Recommendation ITU-T Y.2705

Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS)

Summary

Emergency telecommunications service (ETS) is a national service, providing priority communications services to ETS authorized users in times of disaster and emergencies. Recommendation ITU-T Y.2705 provides minimum security requirements for the inter-network interconnection of ETS. This will allow ETS to be supported with the necessary security protection between different national networks with bilateral and/or multilateral agreements in times of disaster and emergencies.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2705	2013-03-01	13

Keywords

Emergency telecommunications service (ETS), NGN security, priority services and capabilities.

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 not 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

Introduction

Emergency telecommunications service (ETS) is a national service, providing priority communications services to ETS authorized users in times of disaster and emergencies. ETS implementation is a national matter. However, disasters/emergencies can transcend international geographic boundaries, and thus there is a potential that countries/administrations may enter into bilateral and/or multilateral agreements to link their respective ETS systems. This would allow priority communications services (e.g., voice, messaging, video and data) under the umbrella of ETS to be supported between different national networks with bilateral and/or multilateral agreements in times of disaster and emergencies.

The integrity, confidentiality and availability of ETS between interconnected national networks will depend on the security of each national network involved in an end-to-end communication. To allow network-provided security of end-to-end ETS between different national networks (i.e., countries/administrations), security requirements for the interconnection of ETS are needed.

Recommendation ITU-T Y.2705

Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS)

1 Scope

This Recommendation provides the minimum security requirements for the inter-network interconnection of ETS. The scope of the security requirements includes the integrity, confidentiality and availability protection for ETS communications across network boundaries (i.e., between different national networks).

The purpose of this Recommendation is to provide a minimum set of security requirements that can be used to facilitate the support of ETS across directly or indirectly interconnected networks.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T E.106] Recommendation ITU-T E.106 (2003), *International Emergency Preference Scheme (IEPS) for disaster relief operations.*

[ITU-T E.107] Recommendation ITU-T E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS.*

[ITU-T M.3342] Recommendation ITU-T M.3342 (2006), *Guidelines for the definition of SLA representation templates.*

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks.*

[ITU-T Y.2205] Recommendation ITU-T Y.2205 (2011), N*ext Generation Networks – Emergency telecommunications – Technical considerations*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authorization [b-ITU-T X800]: The granting of rights, which includes the granting of access based on access rights.

3.1.2 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

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

3.1.4 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.5 emergency telecommunications service (ETS) [ITU-T E.107]: A national service, providing priority telecommunications to ETS authorized users in times of disaster and emergencies.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 Service Provider: Service Provider (initial capital letters) is a public telecommunications service provider authorized to provide emergency telecommunications service (ETS).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ANI	Application Network Interface
CVE	Common Vulnerabilities and Exposures
CVE	Common Vulnerability and Exposure
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CYBEX	Cybersecurity information Exchange
DDoS	Distributed Denial of Service
DNS	Domain Name Server
DoS	Denial of Service
DSCP	Diffserv Code Point
ETS	Emergency Telecommunications Service
IDS	Intrusion Detection System
IEPS	International Emergency Preference Scheme
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	IP Security
LAN	Local Area Network
NE	Network Element
NGN	Next Generation Network
NNI	Network-Network Interface
PII	Personally Identifiable Information
PSTN	Public Switch Telephone Network
QoS	Quality of Service
SLA	Service Level Agreement
SNI	Service Network Interface
UNI	User Network Interface

5 Conventions

In this Recommendation:

The initial letters of the term "Service Provider" are capitalized in this Recommendation where "Service Provider" refers to a public telecommunications service provider which is authorized to provide ETS (see clause 3.2.1).

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this Recommendation and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Security threats and risks

ETS communications may be targeted for cybersecurity attacks because of the critical nature of the communications. Refer to [ITU-T E.107], [ITU-T Y.2205] and [b-ITU-T Q-Sup.57] for the definition of and information on ETS. The source of threats or malevolent actions intent on disrupting, misusing, manipulating or otherwise harming ETS could originate from a variety of sources including interconnected networks. For example, ETS may be targeted for cybersecurity attacks for reason such as to:

- disrupt the ability of disaster recovery personnel to communicate
- obtain sensitive information by eavesdropping on ETS calls/sessions.

A threat is viewed as a security weakness or potential vulnerability that if exploited may negatively affect the availability, integrity or confidentiality of ETS communications.

This Recommendation focuses mainly on threats pertaining to network interconnection for ETS. Example threats relating to network interconnection include, but are not limited to:

- General interconnection threat: security weaknesses or potential vulnerabilities associated with connecting the network (e.g., NGN) to other managed and unmanaged networks, such as the public Internet.
- Design and implementation threat: security weaknesses or potential vulnerabilities in the network interconnection architecture and implementation designs.
- Management, operational and insider threat: security weaknesses or potential vulnerabilities in the command and control functions for ETS and their underlying infrastructure.

- Transport and facilities threat: security weaknesses or potential vulnerabilities associated with the underlying transport network (e.g., routing, network duplication, diversity, resiliency), support systems (e.g., power, environmental) and the physical protection of network assets.

7 Reference architecture for ETS interconnection security

This Recommendation relies on the functional architecture and network connectivity model defined in [ITU-T Y.2012].

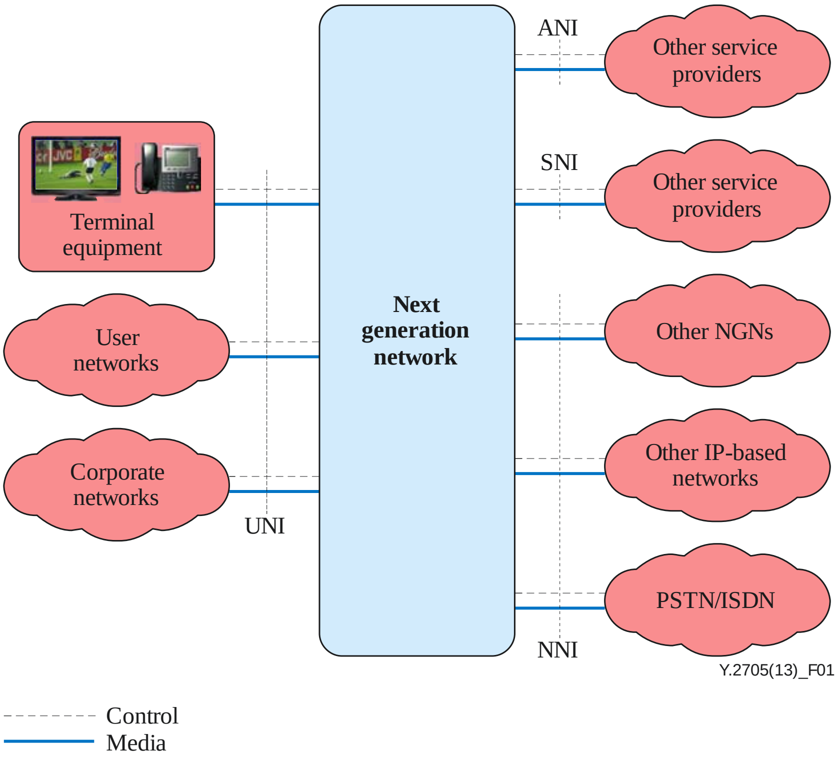

Figure 1 – Connectivity to the NGN [ITU-T Y.2012]

The interfaces pertaining to network interconnections are:

- application network interface (ANI)
- service network interface (SNI)
- network-network interface (NNI).

Refer to [ITU-T Y.2012] for descriptions of ANI, SNI and NNI.

To allow different networks to support ETS communications across network boundaries, specific security measures are needed for the integrity, confidentiality and availability of protection of the ETS communication within each national network and across the interconnection between national networks.

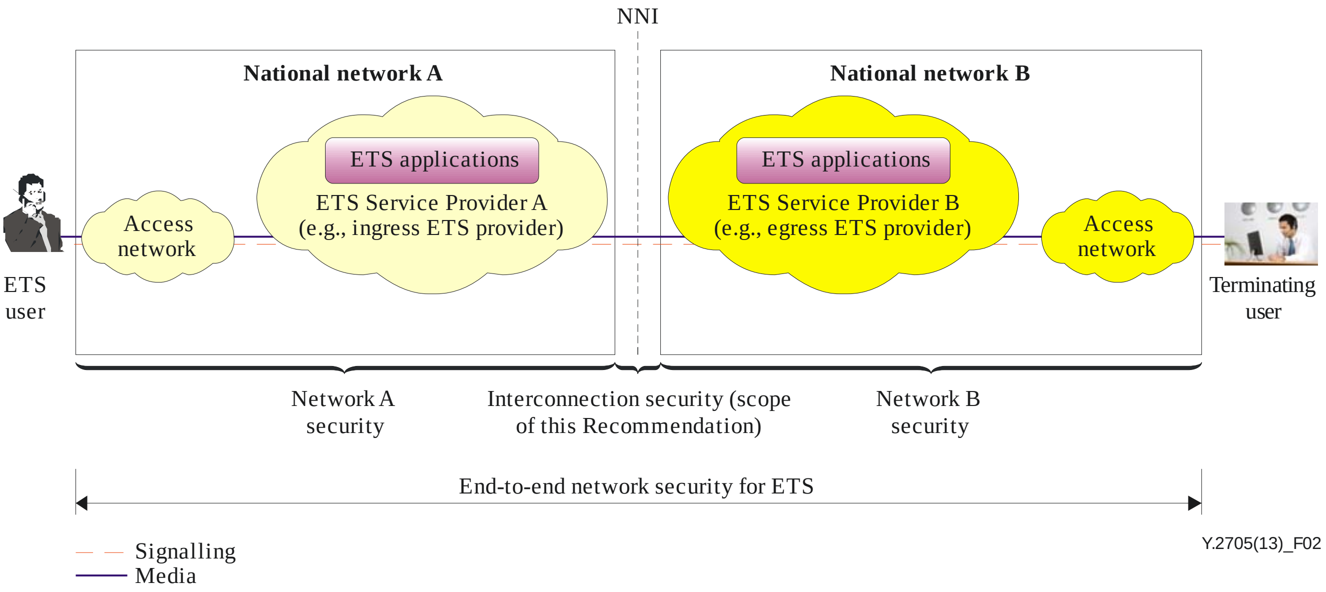

Figure 2 – End-to-end network security for ETS applications

Figure 2 shows that end-to-end security of an ETS communication traversing multiple networks (national networks A and B) will depend on the security measures enforced in the individual networks and security protection of the interconnection between the two networks.

Figure 2 shows that the focus of this Recommendation is for secure interconnection of ETS.

8 Security objectives and guidelines for interconnection of ETS

8.1 General objectives

The general objective is to provide network security protection of end-to-end ETS communications that may traverse different network provider domains of national and international networks (i.e., countries/administrations) where each network is responsible for security within its domain on a hop-by-hop basis.

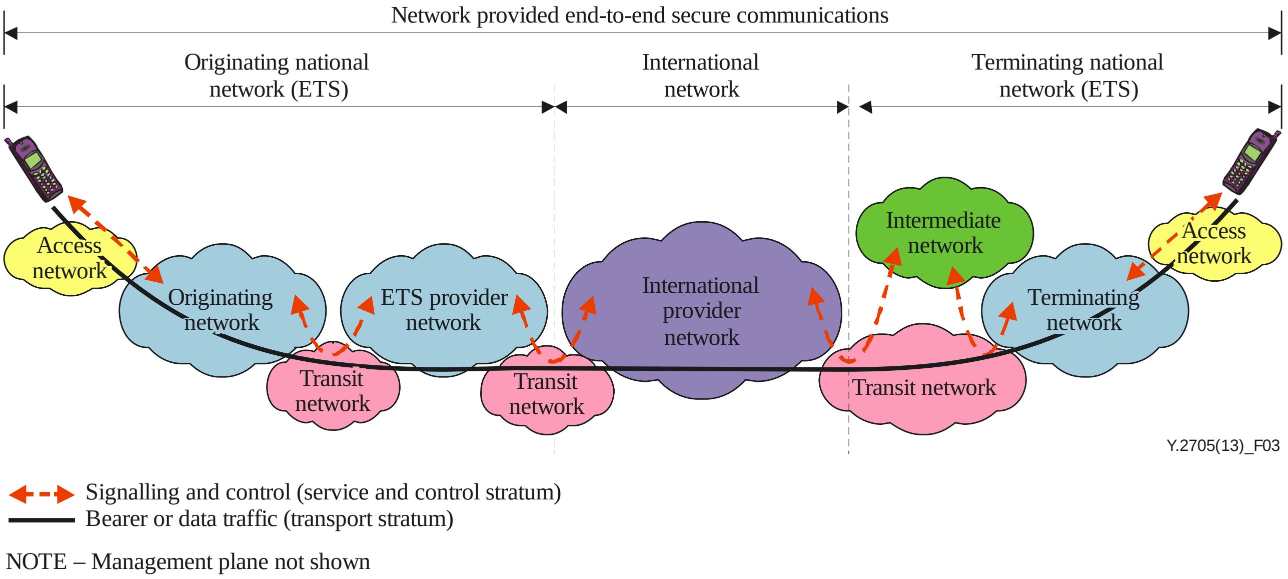
Network provided end-to-end secure communications
Originating national network (ETS)
International network
Terminating national network (ETS)
Access network
Originating network
Transit network
ETS provider network
Transit network
International provider network
Intermediate network
Transit network
Terminating network
Access network
Y.2705(13)_F03
Signalling and control (service and control stratum)
Bearer or data traffic (transport stratum)
NOTE – Management plane not shown

Figure 3 – Example of end-to-end communications across different national ETS implementations

Figure 3 illustrates end-to-end ETS communications (e.g., priority voice, video, data or messaging communications) originating and terminating in two different national networks. The example illustrates that the end-to-end priority communication for ETS may traverse multiple network segments and administrative domains (e.g., access network, originating network, ETS provider network, international provider network, intermediate network and terminating network). The general objective is for each of the interconnected networks along the path of the end-to-end ETS communication to provide the necessary security protection within its domain including the interconnection to the adjacent network so that the integrity, confidentiality and availability of the end-to-end ETS communication are not compromised.

8.2 General guidelines

A structured approach and methodology should be established and implemented between interconnecting networks for ETS through the use of service level agreements (SLAs). This should include:

1. Security risk assessment: Risk assessment of an ETS asset, threat and vulnerability analysis related to the interconnection of ETS. It is critical that a security risk assessment be performed periodically and when changes, new technology, services or applications are introduced.
2. Security architecture and solution: establishing a security policy, security architecture design and specification of solutions to mitigate identified threats to ETS. This includes establishing the necessary bilateral or multilateral SLAs for ETS security ([ITU-T M.3342] and [b-TMF GB917] for information on SLAs). Areas addressed include security policies, requirements, architecture design, situational awareness and forensics tools, and infrastructure security to be included in SLAs for interconnection.
3. Security implementation: implementation and deployment of the security architecture and solutions based on the bilateral or multilateral SLAs as appropriate for ETS interconnection security.
4. Security operations: operational measures for the management of the security solutions for ETS interconnection should be specified and implemented. For example, management of insider threats, management of configurable parameters and default values, resiliency and failure recovery operations, ETS security testing, logging and auditing of ETS security-related events.

8.3 Common objectives and requirements

This clause provides common requirements and objectives.

R-1 The Service Provider shall protect ETS communications from intrusions (e.g., interception, hijacking and replay) that would compromise the authenticity, integrity, confidentiality and availability of ETS in accordance with commercially-available security best practices while the ETS traffic is traversing the Service Provider's domain.

In the above requirement, a domain is a physical or logical "network segment" over which the Service Provider exercises full administrative and operational control, management, maintenance and security.

It is expected that Service Providers would be supporting and using a wide range of security tools and capabilities to protect both ETS and the entire network and all supported applications. It is important that appropriate measures be taken to ensure that the use of these security capabilities do not negatively impact the performance of ETS or introduce any unintended security compromises to ETS.

R-2 Service Provider use of security mechanisms (e.g., intrusion detection system and intrusion prevention system [IDS/IPS] and encryption) shall not interfere with the priority treatment mechanisms used to support ETS (refer to [ITU-T Y.2205] for the definition and description of priority treatment mechanisms).

O-1 It is desirable that the Service Provider's use of security tools and capabilities include appropriate measures to minimize negative impacts on ETS quality of service (QoS) (e.g., by introducing unnecessary delays).

8.4 ETS authentication, authorization and access control

This clause covers:

- authentication and authorization of ETS users
- ETS user authentication and authorization of ETS providers
- authentication of data sources for ETS
- mutual authentication and authorization of ETS providers.

8.4.1 Mutual authentication

Authentication is the process of verifying the claimed identity of a party that is participating in some form of communication. Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication.

End-to-end communication for ETS may involve multiple network segments and administrative domains (e.g., originating access network, ETS Service Provider network, intermediate network, terminating access network). When receiving ETS traffic, the Service Provider is required to verify the validity and authorization of the source (e.g., network) of the received traffic. When handing off ETS traffic, the Service Provider is required to verify the validity and authorization of the entity to which it is handing off the NGN traffic (e.g., network). Presently, security trust relationships for interconnection are verifiable only through direct physical interconnection between two interconnected networks.

R-3 Service Providers shall mutually authenticate each other for exchanging (i.e., handing off or receiving) ETS traffic. This includes any ETS signalling or media traffic exchanges between two Service Providers across NNIs, ANIs or SNIs.

This may be accomplished through verification of direct physical interconnections and service level agreements (SLAs).

NOTE – The intention here is not authentication on a per call/session basis. The intention is to introduce the notion of mechanisms to do authentication on an as-needed basis or periodically.

8.4.2 Access control

Access control measures are necessary to protect against unauthorized use of network resources, including use of resources in an unauthorized manner. Access control ensures that only authorized users or devices are allowed access to network elements, stored information, information flows, services and applications.

Access control at the NNI refers to the capability of the receiving network to accept or reject specific traffic inbound from a neighbouring network and to restrict access to resources within the network by entities outside the network.

R-4 The Service Provider shall establish rules and enforce access control measures to protect against unauthorized ETS communications across the NNIs. Specifically, the SPs should only allow communications to traverse the NNI between NEs that have been identified and pre-authorized (e.g., through SLAs).

R-5 When receiving ETS signalling traffic from another service provider, the Service Provider shall verify the trust relationships between itself and the service provider from which it receives the traffic.

R-6 When receiving ETS media traffic from another service provider, the Service Provider shall verify the trust relationships of the service provider from which it receives ETS traffic.

R-7 When handing off ETS signalling traffic to another service provider, the Service Provider shall verify the trust relationships of the service provider to which it hands off ETS traffic.

R-8 When handing off ETS media traffic to another service provider, the Service Provider shall verify the trust relationships of the service provider to which it hands ETS traffic.

NOTE – The above are not intended to imply verification on a per call/session basis.

Authorization is the granting of privileges, which includes the granting of access based on access privileges. Authorization is given to an entity after validation by an authentication and access control process.

R-9 The Service Provider is required to provide security protection to prevent unauthorized access to ETS.

The means by which R-9 may be accomplished include, but are not limited to the following (as appropriate):

- authentication and authorization of ETS end-users and devices
- authentication and authorization of data sources for ETS communications (e.g., message source or data source)
- security capabilities to protect against unauthorized access to ETS information and resources (e.g., user information in authentication servers and management systems).

System access control involves security measures to prevent unauthorized access to network elements and systems and their associated access points. There are threats associated with unauthorized access to network elements and systems supporting ETS. Therefore, appropriate access control measures to prevent unauthorized access must be established and enforced.

R-10 Service Providers shall establish rules and enforce system access control measures to prevent unauthorized access to network elements and systems supporting ETS. This includes security protection for both logical and physical access.

R-11 The Service Provider shall protect against unauthorized access to ETS data and resources (i.e., the Service Provider shall permit only authorized administrators to access ETS data and resources [e.g., files, command sets, software] on network elements and systems supporting ETS).

8.5 ETS integrity

This clause covers:

- integrity protection of ETS signalling
- integrity protection of ETS media.

8.5.1 Signalling integrity

Inter-network ETS signalling has to be protected against interception, corruption and manipulation (e.g., deletion, creation or replay).

R-12 Service Providers shall protect the integrity of all inter-network ETS signalling traffic crossing NNIs, ANIs or SNIs.

Actions that could be taken to protect the integrity of ETS signalling traffic include, but are not limited to:

a) physical security measures (e.g., physical protection of network elements, transmission medium and facilities, and enforcement of appropriate access control measures)

b) cryptographic protection

c) establishment and enforcement of appropriate integrity requirements and objectives defined in service level agreements

d) monitoring integrity of NNIs configurations.

8.5.2 Media integrity

The media associated with inter-network ETS communications has to be protected against interception, corruption and manipulation (e.g., deletion, creation or replay).

R-13 The Service Provider shall protect the integrity of all inter-network ETS media traffic crossing NNIs or SNIs.

Actions that could be taken to protect the integrity of media traffic include, but are not limited to:

a) physical security measures (e.g., physical protection of network elements, transmission medium and facilities, and enforcement of appropriate access control measures)

b) cryptographic protection

c) establishment and enforcement of appropriate integrity requirements and objectives defined in service level agreements

d) monitoring integrity of NNIs configurations.

8.6 ETS communications confidentiality and PII protection

ETS communications across NNI, ANI and SNI have to provide confidentiality protection to prevent unauthorized entities from obtaining sensitive information. This includes confidentiality protection of:

- ETS signalling and control
- ETS bearer traffic (e.g., voice, video or data)
- personally identifiable information (PII).

8.6.1 Signalling confidentiality

Service Providers have to protect inter-network ETS signalling supported over NNI, ANI or SNI against unauthorized access. The signalling information has to be protected from eavesdropping to reduce the chance of signalling traffic analysis revealing sensitive information which has a potential for misuse (e.g., calling patterns, location information and identity of users).

R-14 The Service Provider shall protect the confidentiality of all inter-network ETS signalling crossing NNIs, ANIs or SNIs.

Actions that could be taken to protect the confidentiality of signalling and media traffic include, but are not limited to:

a) physical security measures (e.g., physical protection of network elements, transmission medium and facilities, and enforcement of appropriate access control measures)

b) cryptographic protection

c) establishment and enforcement of appropriate confidentiality requirements and objectives in service level agreements.

While confidentiality protection is often associated with cryptographic mechanisms, the requirement in this clause to provide confidentiality protection of inter-network signalling is not intended to imply that cryptographic methods must be used in all scenarios or for all end-to-end signalling flows. The intent of this requirement is that the Service Providers must provide and implement the necessary measures to ensure that the signalling communications across NNIs, ANIs and SNIs are protected from eavesdropping. This means that each interconnection must be examined to determine the appropriate mechanisms to be used to provide confidentiality protection, as mandated by a security policy. For example, it might be possible to provide confidentiality protection through the use of physical and the associated operation depending on the architectural and physical configurations of the IP interconnection (e.g., dedicated physical link scenario).

8.6.2 Media confidentiality

Media streams (e.g., voice, video and data) have to be protected against unauthorized access because eavesdropping on ETS media streams could reveal sensitive security information (i.e., conveyed in the media communication).

R-15 The Service Provider shall protect the confidentiality of all inter-network ETS media traffic crossing NNIs or SNIs.

Actions that could be taken to protect the confidentiality of signalling and media traffic include, but are not limited to:

(a) physical security measures (e.g., physical protection of network elements, transmission medium and facilities, and enforcement of appropriate access control measures)

(b) cryptographic protection

(c) establishment and enforcement of appropriate confidentiality requirements and objectives in service level agreements.

8.6.3 PII protection

Personally identifiable information (PII) associated with ETS has to be protected against unauthorized observation or disclosure (e.g., ETS end-user identities, communicating entities identities, ETS subscription information and ETS end-user location).

R-16 The Service Provider shall allow selected ETS users to use ETS anonymously.

R-17 The Service Provider shall protect the confidentiality of selected ETS user identities.

R-18 The Service Provider shall protect the confidentiality of the location of selected ETS users.

Protection against unauthorized observation of ETS usage information (e.g., usage patterns such as ETS traffic volume, locations, time, frequency, etc.) is needed. This includes the support and use of security capabilities to protect sensitive information derived from the observation of network activities such as websites that an end-user has visited, an end-user's geographic location, and the IP addresses and domain name server (DNS) names of devices in a service provider network.

O-2 It is desirable that the Service Provider protect against unauthorized observation or disclosure of ETS usage information (e.g., observation of network activities such as websites that an ETS user has visited, ETS user IP addresses, or usage patterns such as ETS traffic volume, locations, time, frequency).

8.7 Inter-network IP transport

8.7.1 General

The IP-to-IP interconnection between two Service Providers will have architectural and physical connectivity variations with different security implications.

The integrity and availability of the IP-to-IP interconnection between two Service Providers will depend on factors such as architecture, physical connectivity and service level agreements.

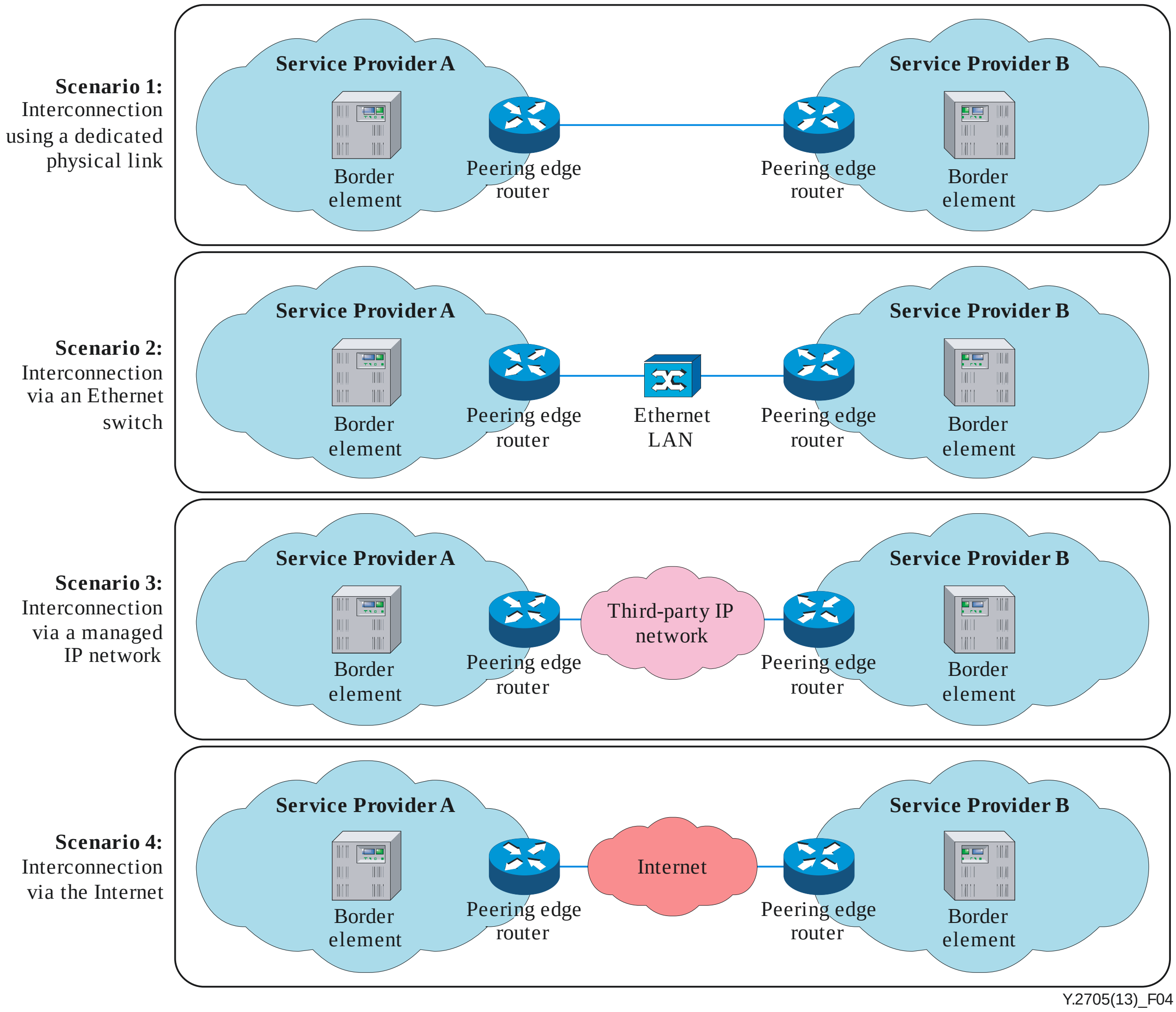

Figure 4 – IP-to-IP interconnection configurations

Figure 4 shows a set of possible IP-to-IP interconnection configurations:

1. Interconnection using a dedicated physical link: In this configuration, a dedicated physical link is used to connect the peering edge router of Service Provider A to the peering edge router of Service Provider B.
2. Interconnection via an Ethernet switch: In this configuration, the peering edge router of Service Provider A and the peering edge router of Service Provider B is physically connected via an Ethernet switch of a local area network (LAN).
3. Interconnection via a managed IP network: In this configuration, the IP interconnection between Service Provider A and Service Provider B occurs via a managed IP network. This could be the managed IP network of a 3rd party provider.

4. Interconnection via the Internet: In this configuration, the IP interconnection between Service Provider A and Service Provider B occurs via the open Internet.

There are different ETS security implications for each of the scenarios depicted in Figure 4.

There are no stipulations or restrictions being made in this document as to the IP interconnection being used for Service Provider interconnection. The general objective is that it is incumbent on the Service Providers to support and implement based on the specific IP-to-IP configuration, the appropriate security measures to protect the interconnection and prevent impacts to services from occurring through compromises of the IP interconnection.

R-19 The Service Provider shall protect the IP transport network between two interconnected Service Provider networks from intrusions (e.g., interception, hijacking and replay) that would compromise the authenticity, integrity, confidentiality and availability of ETS in accordance with commercially-available security best practices.

To meet this requirement, the Service Provider should establish and enforce rules to protect the IP transport network between the interconnected Service Provider networks, and document the rules in SLAs.

R-20 The Service Provider shall protect the integrity of the IP traffic priority mechanisms, functional capabilities and the accompanying protocol data (e.g., Diffserv code points) employed to support ETS over IP network interconnection between Service Providers.

NOTE – This includes integrity protection of any ETS-related configured data or parameters related to the IP interconnection as well as any mapping that is involved (e.g., mapping of Diffserv code points based on the scheme being used in the individual interconnection Service Provider).

CR-1 If ETS signalling is traversing an untrusted IP transport network segment (e.g., third-party IP transport), the Service Provider shall use encryption (e.g., IPsec) for integrity and confidentiality protection.

CR-2 If ETS media is traversing an untrusted IP transport network segment (e.g., third-Party IP transport), the Service Provider shall use encryption (e.g., IPsec) for integrity and confidentiality protection.

8.7.2 Use of encryption

The use of security mechanisms (e.g., encryption) shall not interfere or obscure information for priority treatment mechanisms.

The following requirement is applicable when IPsec tunnels are used for inter-network ETS traffic (i.e., crossing NNIs, ANIs and SNIs):

R-21 The Service Provider shall establish and enforce rules to populate and protect the integrity of priority information (e.g., DSCP values) when IPsec tunnels are used for inter-network ETS traffic. Specifically, rules on how the Diffserv code point (DSCP) values from the inner header is populated in the IPsec tunnel header at the IPsec ingress point, shall be established in SLAs and enforced to allow priority treatment between the ingress and egress IPsec points.

8.8 ETS availability

8.8.1 General objective

To ensure a greater availability of ETS, failures of each service system (supporting ETS) must be kept small, and service recovery must be expeditious (once there is an outage or failure). Failures as a result of security compromises should be taken into account in the overall availability planning and design for ETS. The following is a general objective for ETS availability in the context of security:

O-3 It is desirable that the Service Providers take into account potential failures or service disruptions due to security events affecting inter-network interconnections in the overall planning and design for end-to-end service availability of ETS (i.e., ETS calls/sessions traversing multiple Service Provider networks). This includes measures for expeditious recovery from failures due to security events.

8.8.2 Availability protection

ETS has to be protected against denial of service (DoS), distributed denial of service (DDoS), and other types of attacks that could affect ETS availability. This includes protection against attacks affecting ETS availability for individual ETS users, a group of ETS users, ETS users in a specific location or site (e.g., a government agency enterprise network site), ETS user in a targeted geographic or regional area or ETS as a whole.

R-22 Service Provider shall protect the availability of ETS (e.g., protection against DoS, DDoS, and other types of attacks impacting ETS availability) in accordance with commercially-available security best practices. This shall include protection against DoS, DDoS and other types of attacks affecting ETS availability for individual ETS users, a group of ETS users, ETS users in a specific location or site (e.g., a government agency enterprise network site), ETS user in a targeted geographic or regional area or ETS as a whole.

Actions that may be taken to protect the availability of ETS include but are limited to:

a) use of admission control and throttling mechanisms

b) use of DoS and DDoS mitigation tools and functions

c) use of intrusion detection systems and intrusion prevention systems (IDS/IPS)

d) use of security monitoring tools

e) use of situational awareness tools.

R-23 Service Providers use of security tools and capabilities for availability protection (e.g., DoS and DDoS mechanisms) shall include appropriate measures to prevent unintended denial of legitimate ETS calls/sessions (e.g., blocking or preventing a legitimate ETS call/session from completing or the discard of legitimate ETS packets).

8.9 Management and operations security

This clause covers some topics related to:

- security of management operations (e.g., configurable and default parameters related to the provisioning of ETS interconnection),
- logging of ETS security-related events,
- alerts and alarms when security breaches have or may have occurred.

8.9.1 ETS data integrity

The stored ETS data must be provided with integrity protection to prevent any corruption or manipulation of the data impacting the integrity or availability of ETS.

R-24 The Service Provider shall protect the integrity of ETS-provisioned data. This includes any ETS specific data, such as subscription data, that is provisioned.

8.9.2 Configurable parameters and default values

There are many security threats related to the management of configurable parameters and default values set by vendors and equipment suppliers. For example, the default values of various configurable parameters, as delivered by the vendor, have to be adjusted to meet Service Provider requirements. The configurable parameters must be properly assigned and kept up to date so they can function satisfactorily. This human administrator must be appropriately authorized to perform the security administration.

R-25 The Service Provider is required to establish and enforce rules for the administration of configurable parameters and default values in the context of supporting ETS. Access control measures shall be implemented and enforced so that the execution of these functions is reserved only for the authorized administrator (i.e., all other users shall be denied this permission).

8.9.3 Management of insider threats

An individual (e.g., an employee, contractor or other worker) may be able to gain unauthorized management access or misuse their management access to network elements and systems supporting ETS. Therefore, there is a need to minimize insider threats.

R-26 The Service Provider shall establish and implement security processes to minimize insider threats to ETS.

Example mitigation methods that could be considered include:

- authentication controls, role-based privileging, separation of functions and secure access methods for remote, console, craft and automated system access;
- logging of security events related to management actions;
- compartmenting of ETS information, applications, and access to shared systems and applications;
- auditing of configured data in network elements and databases (e.g., subscriptions profiles) for recording and exposure of unauthorized changes.

8.9.4 Collaboration for cybersecurity information exchange

Service Providers should establish collaborative relationships with partners for sharing information about cybersecurity events (including real-time exchange of information during cybersecurity attacks). An exchange of information about cybersecurity incidents can provide mutual benefits and can be used to anticipate threats to ETS placing the Service Provider in a situation to provide effective countermeasures.

O-4 It is desirable that Service Providers establish and implement management and operational processes sufficient to provide collaborative relationships for sharing and exchanging information about cybersecurity events. The processes should take into consideration analysis functions to make the information useful as input into security actions and counter-measures to protect ETS.

Refer to the following ITU-T Recommendations for information about cybersecurity information exchange:

- [b-ITU-T X.1500]
- [b-ITU-T X.1500.1]
- [b-ITU-T X.1520]
- [b-ITU-T X.1521]
- [b-ITU-T X.1524]
- [b-ITU-T X.1570]

8.9.5 Management of incident response and recovery from security events

Availability of ETS depends on the operational procedures in place for recovery and service restoration from security events. It is critical that these procedures be clearly defined, documented and implemented. This includes the necessary policies and practices for service recovery and restoration within a Service Provider domain and across domains for interconnection and inter-network services. Protection of the operational procedure documentation and implementation from intruders and insider threats is necessary.

R-27 The Service Provider is required to have a documented "Incident Response and Recovery" plan describing the policies, management, operational steps, processes and procedures for service recovery and restoration from security events. This includes the necessary policies and practices for service recovery and restoration within the Service Provider domain and across domains for interconnection and inter-network services.

Bibliography

[b-ITU-T Q-Sup.57] ITU-T Q-series Recommendations – Supplement 57 (2008), *Signalling requirements to support the emergency telecommunications service (ETS) in IP networks*.

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

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*.

[b-ITU-T X.1500.1] Recommendation ITU-T X.1500.1 (2012), *Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange*.

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (2011), *Common vulnerabilities and exposures.*

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system.*

[b-ITU-T X.1524] Recommendation ITU-T (2012), *Common weakness enumeration*.

[b-ITU-T X.1570] Recommendation ITU-T X.1570 (2011), *Discovery mechanisms in the exchange of cybersecurity information*.

[b-TMF GB917] GB 917 (2012), *SLA Management Handbook, Release 3.1*, TM Forum.

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