

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2701

(04/2007)

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

Next Generation Networks – Security

Security requirements for NGN release 1

ITU-T Recommendation Y.2701

ITU-T



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

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
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

ITU-T Recommendation Y.2701

Security requirements for NGN release 1

Summary

ITU-T Recommendation Y.2701 provides security requirements for next generation networks (NGNs) and its interfaces (e.g., UNIs, NNIs and ANIs) by applying ITU-T Rec. X.805, *Security architecture for systems providing end-to-end communications* to ITU-T Recs Y.2201, *NGN release 1 requirements* and Y.2012, *Functional requirements and architecture of the NGN release 1*.

The requirements are to provide network-based security of end user communications across multiple-network administrative domains. Security of customer assets and information in the customer domain (e.g., user network), and the use of peer-to-peer application capabilities on customer equipment are not within the scope of this Recommendation.

This Recommendation uses trust model based on network elements (physical boxes). NGN providers will be deploying network elements that support the functional entities defined in ITU-T Rec. Y.2012. The bundling of these functional entities to a given network element will vary, depending on the vendor. Therefore, this Recommendation will not attempt to show a strict and fixed bundling between logical functional entities and physical network elements.

The requirements in this Recommendation should be treated as a minimum set of security requirements, and NGN providers are encouraged to take additional measures beyond those specified in Recommendations for NGN security.

Source

ITU-T Recommendation Y.2701 was approved on 27 April 2007 by ITU-T Study Group 13 (2005-2008) under the WTSA Resolution 1 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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/>.

© ITU 2008

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
1.1	X.805 principles	1
1.2	Assumptions	2
1.3	Overview	3
2	References.....	3
3	Definitions and abbreviations	4
3.1	Terms defined elsewhere	4
3.2	Terms defined in this Recommendation.....	4
3.3	Abbreviations and acronyms	5
4	Security threats and risks	6
5	Security trust model.....	8
5.1	Single network trust model.....	8
5.2	Peering network trust model.....	10
6	Security architecture	10
6.1	Functional NGN architecture reference.....	10
6.2	Mapping to NGN functional architecture.....	12
6.3	Identification of NGN resources for security protection.....	14
7	Objectives and requirements.....	18
7.1	General security objectives.....	18
7.2	Objectives for security across multiple network provider domains	19
7.3	Requirements specific for security dimensions	19
8	Specific security requirements.....	21
8.1	Common security requirements for NGN elements	21
8.2	Requirements for NGN elements in the trusted zone	24
8.3	Requirements for NGN border elements in the "trusted-but-vulnerable" domain	24
8.4	Requirements for TE border elements in the "un-trusted" domain	26
8.5	Security recommendations for terminal equipment in the "un-trusted" domain	26
Appendix I – Security objectives and guidelines for interconnection of emergency telecommunications services		27
I.1	Background.....	27
I.2	Scope/purpose.....	27
I.3	General objectives	27
I.4	General security capabilities.....	29
I.5	Authentication, authorization and access control	29
I.6	Confidentiality and privacy	29

	Page
I.7 Data integrity	30
I.8 Communication	30
I.9 Availability	30
Bibliography.....	31

Copyright © 2007 ITU-T. All rights reserved.

ITU-T Recommendation Y.2701

Security requirements for NGN release 1

1 Scope

This Recommendation provides security requirements for next generation networks (NGNs) against security threats. It is achieved by applying the principles of [ITU-T X.805], *Security architecture for systems providing end-to-end communications* to [ITU-T Y.2201], *NGN release 1 requirements* and [ITU-T Y.2012], *Functional requirements and architecture of the NGN release 1*.

The requirements are to protect the following in a multi-network environment:

- network and service provider infrastructure and its assets (e.g., NGN assets and resources such as network elements, systems, components, interfaces, and data and information), its resources, its communications (i.e., signalling, management and data/bearer traffic) and its services;
- NGN services and capabilities (e.g., voice, video and data services);
- end user communication and information (e.g., private information).

The requirements are to provide network-based security of end user communications across multiple-network administrative domains. Security of customer assets and information in the customer domain (e.g., user network), and the use of peer-to-peer application capabilities on customer equipment are not within the scope of this Recommendation.

The requirements specified in this Recommendation are applicable to an NGN, including user-to-network interfaces (UNIs), network-to-network interfaces (NNIs) and application-to-network interfaces (ANIs) in a multi-network environment.

NGN service providers will be deploying "network elements" that support the functional entities defined in [ITU-T Y.2012]. The bundling of these functional entities to a given network element will vary, depending on the vendor. Therefore, this Recommendation will not attempt to show a strict and fixed bundling between logical functional entities and physical network elements.

The requirements in this Recommendation should be treated as a minimum set of requirements for NGN security and should not be considered to be exhaustive. Therefore, an NGN provider may need to take additional measures beyond those specified in Recommendations for NGN security.

In addition, the requirements in this Recommendation cover some of the technical aspects of what is generally known as IdM ("identity management"). A working definition of IdM is "management by NGN providers of trusted attributes of an entity such as: a subscriber, a device or a provider". This is not intended to indicate positive validation of a person.

Administrations may require NGN providers to take into account national regulatory and national policy requirements in implementing this Recommendation.

1.1 X.805 principles

[ITU-T X.805] defines the following security dimensions:

access control;
authentication;
non-repudiation;
data confidentiality;
communication security;
data integrity;

Copyright International Telecommunication Union

availability;

privacy.

It also identifies the following security threats.

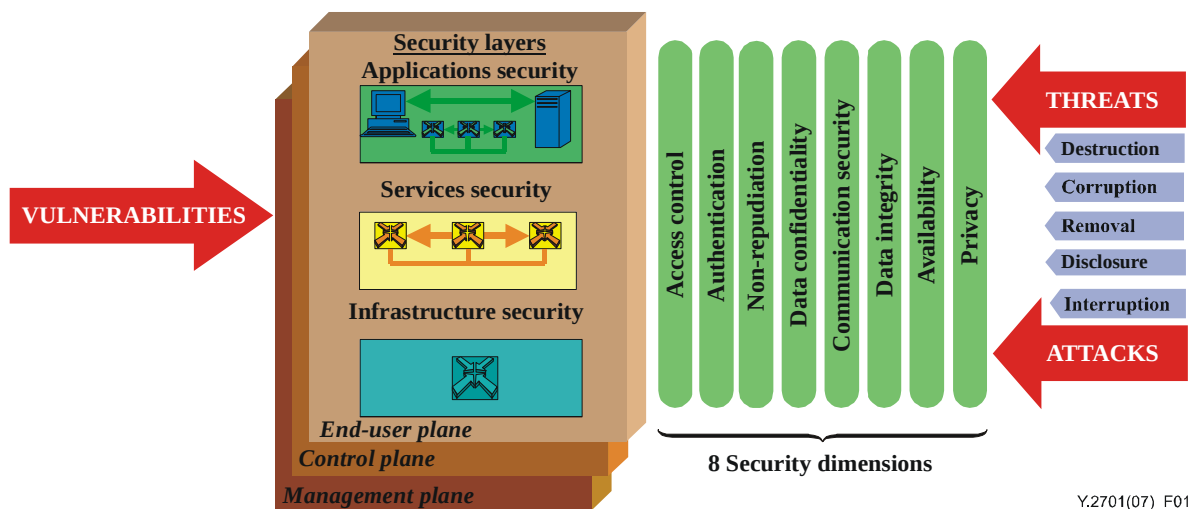


Figure 1 – Security architecture of X.805 (Figure 3/X.805)

These security dimensions and security threats stated above are considered as the base of this Recommendation.

This Recommendation does not further define or distinguish the use of the X.805 security layers (applications, services, or infrastructure) and compliance with this standard does not require such a distinction. This Recommendation does make reference to a distinction between management, control, and user plane traffic, but cautions the reader that the utilization of that classification varies depending on the layer in a protocol stack that is under consideration. Therefore, additional standards will need to be referenced to determine compliance with such distinctions. This standard provides recommendations concerning application of the security dimensions, but does not infer completeness for use as a security assessment for NGN networks.

1.2 Assumptions

This Recommendation is based on the following assumptions:

- 1) The bundling of functional entities, as defined in [ITU-T Y.2012], to a given network element will vary, depending on the vendor.
- 2) Each NGN provider has specific responsibilities within its domain for security. For example, implementing applicable security services and practices to:
 - a) protect itself;
 - b) assure end-to-end security is not compromised within its network; and
 - c) assure high availability of NGN communications.
- 3) Each network domain will establish and enforce policies for service level agreements (SLAs) to assure the security of its domain and the security of the network interconnections. It is assumed that the SLAs would specify security services, mechanisms and practices to be implemented to protect the interconnected networks and the communications (signalling/control traffic, bearer traffic and management traffic) across UNIs, ANIs and NNIs.

- 4) This Recommendation addresses network-based security, which is a layered architecture, consisting of perimeter security to trusted domains, physical security of provider equipment, and potentially the use of encryption.

1.3 Overview

This Recommendation is organized as follows:

- Clause 2 (References) – This clause provides normative references.
- Clause 3 (Definitions and abbreviations) – This clause provides definitions and abbreviations used in this Recommendation.
- Clause 4 (Security threats and risks) – This clause highlights security threats and risks assumed for the NGN environment. Assumed security threats and risks are used as guidance to develop requirements for security and to identify security capabilities and procedures to be supported.
- Clause 5 (Security trust model) – This clause describes a trust model for NGN security. The trust model can be used to develop trust relations for UNI, ANI and NNI connectivity and design of security architecture.
- Clause 6 (Security architecture) – This clause describes the relationship between the functional NGN architecture defined in [ITU-T Y.2012] and composite security architectures.
- Clause 7 (Objectives and requirements) – This clause describes security objectives and general requirements for NGNs to be used as the basis to define security requirements for NGNs.
- Clause 8 (Specific security requirements) – This clause provides specific security requirements as defined in clause 7.
- Appendix I – Security objectives and requirements for emergency telecommunications services (ETS).
- Bibliography.

This Recommendation is defined to provide a base for NGN security. Various companion Recommendations for specific security areas, e.g., authentication and authorization, certificate management, identity management, among others, are to be provided in the future.

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 M.3016.0] ITU-T Recommendation M.3016.0 (2005), *Security for the management plane: Overview*.
- [ITU-T M.3016.1] ITU-T Recommendation M.3016.1 (2005), *Security for the management plane: Security requirements*.
- [ITU-T X.800] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

- [ITU-T X.805] ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.
- [ITU-T Y.2012] ITU-T Recommendation Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.
- [ITU-T Y.2201] ITU-T Recommendation Y.2201 (2007), *NGN release 1 requirements*.

3 Definitions and abbreviations

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 emergency telecommunications service (ETS): National service, providing authorized priority communications to facilitate the work of emergency personnel in times of disaster. (See ITU-T Rec. E.107.)

3.1.2 user: A user includes end user (ITU-T Rec. Y.2091), person, subscriber, system, equipment, terminal (e.g., FAX, PC), (functional) entity, process, application, provider, or corporate network.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 asset: Anything that has value to the organization, its business, its operations and its continuity.

3.2.2 border element: Network element providing functions connecting different security and administrative domains.

3.2.3 corporate network: A private network that supports multiple users and may be in multiple locations (e.g., an enterprise, a campus).

3.2.4 domain border element: Border element under sole control of the provider, providing security functions with other network domains.

3.2.5 network border element: Border element under sole control of the provider, providing security functions with terminal equipment.

3.2.6 security domain: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the elements are managed in accordance with the security policy. The policy will be administered by the security authority. A given security domain may span multiple security zones.

3.2.7 security zone: This Recommendation defines 3 security zones:

- 1) trusted;
- 2) trusted but vulnerable; and
- 3) un-trusted.

A security zone is defined by operational control, location, and connectivity to other device/network elements.

3.2.8 terminal equipment border element: Border element providing security functions between customer premises equipment and service provider network.

3.2.9 trust: Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities.

3.2.10 trusted but vulnerable zone: From the viewpoint of a NGN provider, a security zone where the network elements/devices are operated (provisioned and maintained) by the NGN provider. The equipment may be under the control by either the customer/subscriber or the NGN provider. In addition, the equipment may be located within or outside the NGN provider's domain. They communicate with elements both in the trusted zone and with elements in the un-trusted zone, which is why they are "vulnerable". Their major security function is to protect the NEs in the trusted zone from the security attacks originated in the un-trusted zone in a fail-safe manner.

3.2.11 trusted zone: From the viewpoint of a NGN provider, a security domain where a NGN provider's network elements and systems reside and never communicate directly with customer equipment. The common characteristics of NGN network elements in this domain are that they are under the full control of the related NGN provider, are located in the NGN provider premises (which provides physical security), and they communicate only with elements in the "trusted" domain and with elements in the "trusted-but-vulnerable" domain.

3.2.12 un-trusted zone: From the viewpoint of a NGN provider, a zone that includes all network elements of customer networks or possibly peer networks or other NGN provider zones outside of the original domain, which are connected to the NGN provider's border elements.

3.2.13 user network: A private network consisting of terminal equipment that may have multiple users.

3.3 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms.

3G	3rd Generation
AGW	Access Gateway
ANI	Application-to-Network Interface
B2BUA	Back-to-Back User Agent
BE	Border Element
CSC-FE	Call Session Control Functional Entity
DBE	Domain Border Element
DNS	Domain Name System
ETS	Emergency Telecommunications Service
FE	Functional Entity
GW	Gateway
I-CSC-FE	Interrogating Call Session Control Functional Entity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
MPLS	Multi Protocol Label Switching
MRP-FE	Media Resource Processing Functional Entity
NAC-FE	Network Access Control Functional Entity
NAPT	Network Address and Port Translation
NAT	Network Address Translation

NBE	Network Border Element
NE	Network Element
NGN	Next Generation Network
NNI	Network-to-Network Interface
OAMP	Operations, Administration, Maintenance and Provisioning
P-CSC-FE	Proxy Call Session Control Functional Entity
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAC-FE	Resource and Admission Control Functional Entity
RAN	Radio Access Network
RTSP	Real Time Streaming Protocol
SAA-FE	Service Authentication and Authorization Functional Entity
S-CSC-FE	Serving Call Session Control Functional Entity
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SL-FE	Subscription Locator Functional Entity
TAA-FE	Transport Authentication and Authorization Functional Entity
TE	Terminal Equipment
TE-BE	Terminal Equipment Border Element
TMN	Telecommunication Management Network
UA	User Agent
UICC	Universal Integrated Circuit Card
UNI	User-to-Network Interface
VLAN	Virtual LAN
W-CDMA	Wideband Code Division Multiple Access
WLAN	Wireless LAN
xDSL	x Digital Subscriber Line

4 Security threats and risks

This Recommendation assumes that the systems, components, interfaces, information, resources, communications (i.e., signalling, management and data/bearer traffic) and services that make up an NGN will be exposed to a variety of security threats and risks. Those threats and risks will depend on a variety of factors. In addition, end users will also be exposed to certain threats (e.g., unauthorized access to private information).

Threats to the NGN:

- unauthorized reconnaissance, such as the remote analysis of the system to determine points of weakness (these may include scans, sweeps, port interrogation, route tables, etc.);
- break-in/device takeover resulting in loss of control of the device, anomalies and errors in the configuration audits;
- destruction of information and/or other resources;
- corruption or modification of information;
- theft, removal or loss of information and/or other resources;
- disclosure of information; and
- interruption of services and denial of services.

Further, it is clear that NGNs will be operating in an environment different from the PSTN environment and may therefore be exposed to different types of threats and attacks from within or externally. NGNs will have direct or indirect connectivity to un-trusted and trusted networks and terminal equipment, and therefore will be exposed to security risks and threats associated with connectivity to un-secure networks and customer premises equipment. For example, a provider's NGN may have direct or indirect (i.e., through another network) connectivity to the following as shown in Figure 2:

- other service providers, and their applications;
- other NGNs;
- other IP-based networks;
- public switched telephone network (PSTN);
- corporate networks;
- user networks;
- terminal equipment;
- other NGN transport domains.

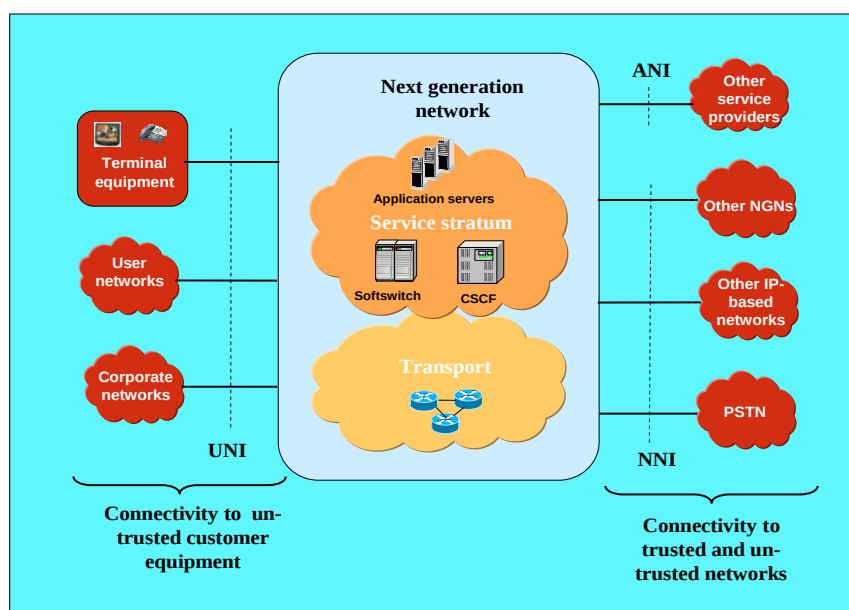


Figure 2 – Connectivity to networks and users

In the evolving environment, security across multiple network provider domains relies on the aggregation of what all providers elect to do for securing their networks. Unauthorized network access into one provider's network can easily lead to exploitation of an interconnected network and its associated services. This is an example of the exploitation of the weakest link that can threaten a provider network's integrity and service continuity along with a host of various types of attacks.

Each NGN provider is responsible for security within its domain. Each NGN provider is responsible for designing and implementing security solutions using network specific policy for trust relations (clause 5), to meet its own network-specific needs and to support global end-to-end security objectives across multiple network provider domains.

5 Security trust model

This clause defines the NGN security trust model.

The NGN functional reference architecture defines functional entities (FEs). However, since network security aspects depend heavily on the way that FEs are bundled together, the NGN security architecture is based on physical network elements (NEs), i.e., tangible boxes that contain one or more FEs. The way these FEs are bundled into NEs will vary, depending on the vendor.

5.1 Single network trust model

This subclause defines three security zones:

- 1) trusted;
- 2) trusted but vulnerable;
- 3) un-trusted,

that are dependent on operational control, location, and connectivity to other device/network elements. These three zones are illustrated in the security trust model shown in Figure 3.

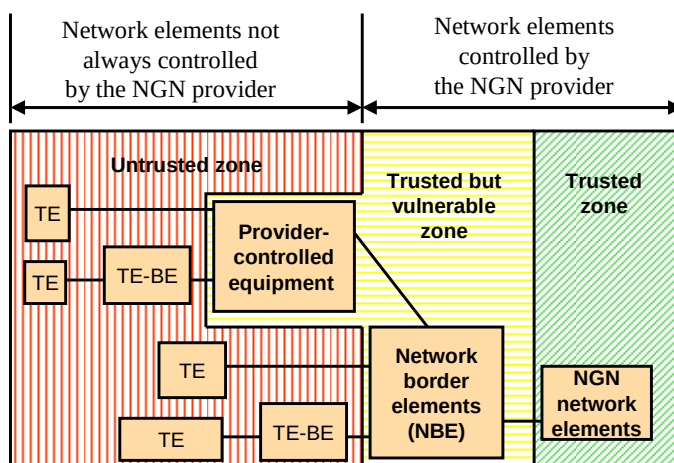


Figure 3 – Security trust model

A "trusted network security zone" or "trusted zone" in short is a zone where a NGN provider's network elements and systems reside and never communicate directly with customer equipment or other domains. The common characteristics of NGN network elements in this zone are that they are under the full control of the NGN provider, are located in the NGN provider domain, and they communicate only with elements in the "trusted" zone and with elements in the