International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3053

Amendment 1

(12/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Future networks

Framework of trustworthy networking with trust-centric network domains

Amendment 1

Recommendation ITU-T Y.3053 (2018) – Amendment 1

ITU-T

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

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
Enhancements to NGN	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
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3053

Framework of trustworthy networking with trust-centric network domains

Amendment 1

Summary

Recommendation ITU-T Y.3053 introduces a framework of trustworthy networking with trust-centric network domains. It describes a trustworthy networking conceptual model that includes features of identification, trust evaluation and trustworthy communication. For a solution of trustworthy networking, the extension of the conceptual model into a concept of trust-centric network domains should be done. With the described concept, this Recommendation specifies high-level and functional requirements, a functional architecture and scalability of trustworthy networking with trust-centric network domains.

Amendment 1 to Recommendation ITU-T Y.3053 (2018) contains modifications to add trustworthy networking deployment architecture and procedures for IP networks in the Internet.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.3053	2018-01-13	13	11.1002/1000/13465
1.1	ITU-T Y.3053 (2018) Amd. 1	2018-12-14	13	11.1002/1000/13807

Keywords

Trust, trust-centric network domain, trustworthy networking.

[*] 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

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

Page

Recommendation ITU-T Y.3053

Framework of trustworthy networking with trust-centric network domains

Amendment 1

Editorial note: This is a complete-text publication. Modifications introduced by this amendment are shown in revision marks relative to Recommendation ITU-T Y.3053 (2018).

1 Scope

This Recommendation addresses a framework for trustworthy networking with trust-centric network domains. The scope of this Recommendation includes:

– A conceptual model of trustworthy networking and trust-centric network domains;

– High-level and functional requirements;

– A functional architecture;

– Scalability of trust-centric network domains.

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 Y.3052] Recommendation ITU-T Y.3052 (2017), *Overview of trust provisioning for information and communication technology infrastructures and services*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 trust [ITU-T Y.3052]: The measurable belief and/or confidence which represents accumulated value from history and the expecting value for the future.

NOTE – Trust is quantitatively and/or qualitatively calculated and measured. Trust is used to evaluate values of entities, value-chains among multiple stakeholders and human behaviours, including decision making.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 trustworthy networking: A set of methods to provide reliable and secure communications among any pair of network elements that have trust relationships.

3.2.2 trust-centric network domain: An abstraction of a network which is characterized by administrative features with a certain trust level and all its members have a mutual trust relationship.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ADC	Access and Delivery Control
APCS-FE	Accessing/Peering Control Support Functional Entity
DMM-FE	Domain Membership Management Functional Entity
DNS	Domain Name Server
DPM-FE	Domain Policy Management Functional Entity
DTP-FE	Data Transport and Processing Functional Entity
ICT	Information and Communication Technology
ID	Identifier
ILMS-FE	ID-locator Mapping Support Functional Entity
IRS-FE	ID-based Routing Support Functional Entity
NAT	Network Address Translator
TILM-FE	Trust Information Lifecycle Management Functional Entity
TLV-FE	Trust Level Validation Functional Entity
TVS-FE	Trust Verification Support Functional Entity
VPN	Virtual Private Network

5 Conventions

In this Recommendation:

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

6 Overview

With the development of the Internet, many security techniques have been developed to keep communications safe against a variety of threats. The concept of trust provisioning is introduced to cope with potential risks in the information and communication technology (ICT) infrastructures and services [ITU-T Y.3052]. In the current state-of-the-art, a virtual private network (VPN) [b-ITU-T Y.1311] solution is widely used to provide secure communication between private domains in an open network. However, to achieve trust provisioning, various aspects of technological advancement beyond security are required. This Recommendation describes a conceptual model of trustworthy networking and trust-centric network domains.

6.1 A conceptual model of trustworthy networking

In order to make networks trustable in heterogeneous communication environments, fundamental features beyond the secure communications are needed. First, an identity of a network element should be well defined (identification). Then it is necessary to check whether the identified element is trustworthy (trust evaluation). Finally, trustworthy communication between the peer network elements should be provided (trustworthy communication).

– Identification

In the context of trustworthy networking, all the network elements should be identified to build a trust relationship. An identifier (ID) can be used to indicate a network element.

– Trust evaluation

To make a trust relationship, a trustor evaluates the trustworthiness of a trustee based on an expectation that the trustee will perform a particular action. Then, the trustor decides to believe the trustee for the corresponding communication procedures. To perform the trust evaluation, trust-related information of the network element is provided.

– Trustworthy communication

After the trust evaluation, the communication link between two network elements can be established. The networking environment then supports reliable, invulnerable and secured communications in order to maintain the trust relationship.

Based on the above three essential features, this Recommendation defines a conceptual model to realize trustworthy networking as shown in Figure 1. A network element in a network is classified as either a trustor or a trustee depending on its role. A trust relationship exists between the trustor and the trustee. The trustor evaluates a trust level of the trustee before initiating a communication procedure.

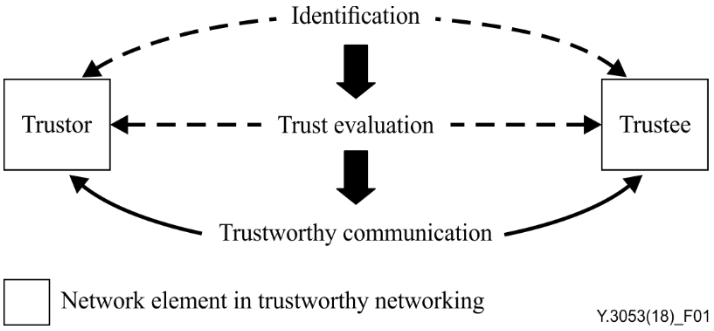
Identification
Trustor
Trust evaluation
Trustee
Trustworthy communication
Network element in trustworthy networking
Y.3053(18)_F01

Figure 1 – A conceptual model of trustworthy networking

6.2 Trust-centric network domains

To be protected from external attacks and threats, the network should be insulated from other external networks. This means that the insulated network enforces appropriate trust policy and procedures that will keep the network safe and protected. In this Recommendation, such a network is referred to as a trust-centric network domain. A trust-centric network domain is separated from other networks by a well-defined interface. This is similar to building a VPN through multiple domains of individual networks [b-ITU-T Y.1311].

Figure 2 illustrates a trust-centric network domain with its components and their relationships. The conceptual model of trustworthy networking assumes that any pair of network elements within the trust-centric network domain has a proper trust relationship. This means that intra communications inside the trust-centric network domain can be done without any security protection. Such a trust relationship is called a "mutual" trust relationship. Inter-domain communication between the trust-centric network domain and the external networks, however, is managed by a well-defined trustworthy interface and its relationship is called an "asymmetric" trust relationship. The trust-centric network domain according to the trustworthy networking conceptual model interacts with other networks. Briefly, a trust-centric network domain is the abstraction of a network in which all members have mutual trust relationships and it is characterized by specific properties such as functionalities and administrative features. The trust-centric network domain ensures trustworthy networking by performing domain administration, membership management and access and delivery control (ADC) functionalities. The detailed functional architecture is described in the clause 8.

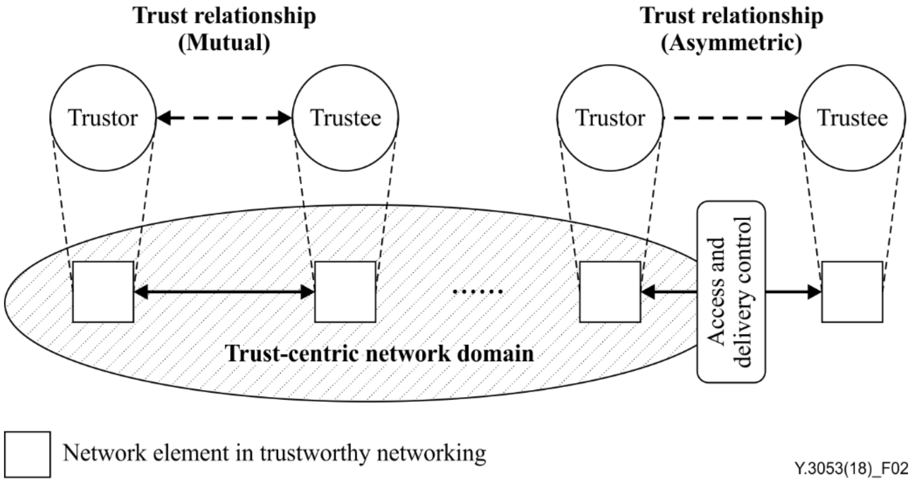

Figure 2 – Trust-centric network domain

7 Requirements

The high-level requirements and functional requirements for trustworthy networking with trust-centric network domains are identified in clauses 7.1 and 7.2 respectively.

7.1 High-level requirements

- The network elements are required to be managed by identifiers and locators;
- Trustworthy networking is required to evaluate trust of all the network elements within the trust-centric network domains;
- Trustworthy networking is required to provide an interface for communicating outside of the trust-centric network domain;
- Trustworthy networking is required to support the trust management for maintaining the trust-centric network domain;
- Trustworthy networking is required to provide a trustworthy communication link which satisfies the proper trust levels.

7.2 Functional requirements

7.2.1 Functional requirements for trust management

Trust management is required to:

- Evaluate trust levels of network elements or domains by aggregating their trust-related information;
- Validate trust levels of network elements or domains after trust evaluation process;
- Support lifecycle management of the trust information that includes planning, creation, allocation, modification and deletion.

7.2.2 Functional requirements for trust-centric network domain administration

A trust-centric network domain is required to:

- Provide mapping between IDs and locators for the access and delivery control;
- Manage the membership of the network elements during registration, identification and policy enforcement;
- Settle domain policies (e.g., the trust level of domain membership and security configuration of the domain).

7.2.3 Functional requirements for access and delivery control

A trust-centric network domain is required to:

- Check and control the communication link toward outside of the trust-centric network domain according to trust levels;
- Provide data delivery control for enabling data forwarding and routing according to trust levels;
- Control incoming/outgoing data packets to be forwarded to inside/outside of the trust-centric network domain;
- Make a decision on routing paths of incoming/outgoing packets according to the trust-centric network domain management policy.

8 Functional architecture

A functional architecture of trustworthy networking is shown in Figure 3.

In the trust-centric network domain, the network elements can communicate with each other without additional security concerns. The network elements inside the trust-centric network domain can communicate with the network elements outside of the trust-centric network domain through the access and delivery control functions.

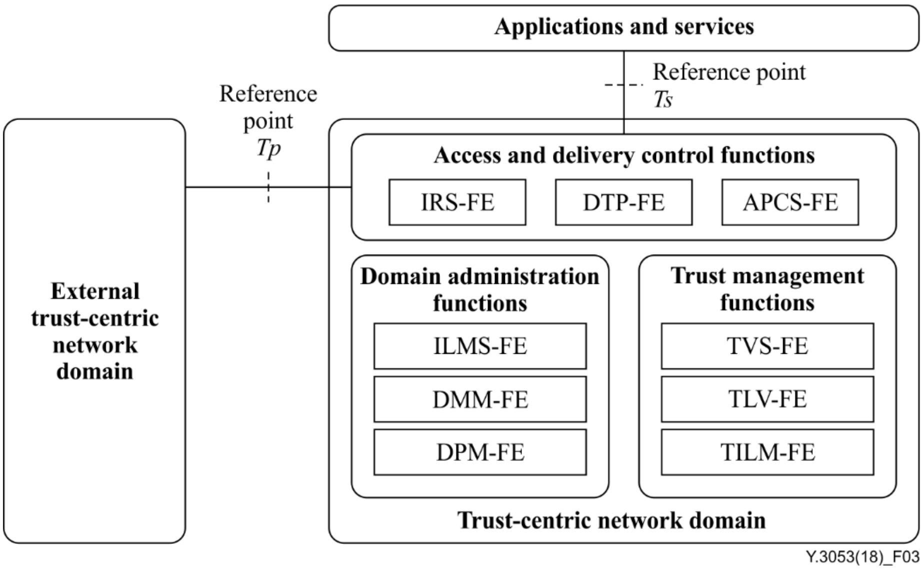
Applications and services
Reference point Ts
Reference point Tp
Access and delivery control functions
IRS-FE
DTP-FE
APCS-FE
External trust-centric network domain
Domain administration functions
ILMS-FE
DMM-FE
DPM-FE
Trust management functions
TVS-FE
TLV-FE
TILM-FE
Trust-centric network domain
Y.3053(18)_F03

Figure 3 – A functional architecture of trustworthy networking

8.1 Trust management functions

The trust management functions consist of trust verification support functional entity (TVS-FE), trust level validation functional entity (TLV-FE) and trust information lifecycle management functional entity (TILM-FE).

- The TVS-FE aggregates information for evaluating trust levels of network elements in a trust-centric network domain;
- The TLV-FE evaluates their trust levels. After completion of the trust evaluation, it provides trust values of the network elements inside and/or outside of the trust-centric network domain;
- The TILM-FE manages the lifecycle of the trust information: planning, creation, allocation, modification and deletion of trust values.

8.2 Domain administration functions

Trust-centric network domain administration functions include ID-Locator mapping support functional entity (ILMS-FE), domain membership management functional entity (DMM-FE) and domain policy management functional entity (DPM-FE).

– The ILMS-FE provides mapping between IDs and locators for the access and delivery control functions;

– The DMM-FE manages the membership by analysing IDs and their trust levels to maintain trust-centric network domain secured;

– The DPM-FE settles the domain policies such as the trust level of domain membership and security configuration of the domain via domain policy management.

8.3 Access and delivery control functions

Access and delivery control functions consists of accessing/peering control support functional entity (APCS-FE), data transport and processing functional entity (DTP-FE) and ID-based routing support functional entity (IRS-FE).

– The APCS-FE provides trustful and reliable links to communicate with the outside of the trust-centric network domain. It also checks and controls communication links toward outside of the trust-centric network domain to maintain the trustworthy network;

– The DTP-FE controls incoming/outgoing data packets to be forwarded to inside/outside of a trust-centric network domain;

– The IRS-FE decides the routing path of incoming/outgoing packets according to the trust-centric network domain management policy, which can be decided by the trust-centric network domain administration functions.

8.4 Reference point *Tp*

The reference point *Tp* enables reliable and secure request/response information for trustworthy networking to be exchanged between trust-centric network domains. It may operate as an intra-domain and/or an inter-domain reference point.

8.5 Reference point *Ts*

The reference point *Ts* enables reliable and secure request/response information for trustworthy networking to be exchanged between a trust-centric network domain and its applications and services. It may operate as an intra-domain reference point.

9 Scalability of the trust-centric network domain

This clause describes the scalability issues of the trust-centric network domain. To provide scalability of the trust-centric network domain, there are three key issues; building and managing trust-centric network domains, ensuring trustworthy communication between more than two trust-centric network domains and expanding the trust-centric network domain.

9.1 Building and managing trust-centric network domains

The trust-centric network domain builds autonomous network space which can replace the role of security. A new member can join the trust-centric network domain after passing a certain trust evaluation procedure. Trust-centric network domains should have access and delivery control functions to protect the domain from external networks and domain administration functions including identification, authentication and trust evaluation. To keep the trust-centric network domain, only the qualified network elements are admitted as member and the misbehaving network elements have to be quickly removed from the trust-centric network domain. For maintaining a trust-centric network domain safe, all the behaviour of network elements should be monitored. If suspicious activities are found, the corresponding network elements should be removed.

9.2 Trustworthy communication between more than two trust-centric network domains

The trust-centric network domain may initiate the trustful interactions from and to the external networks. There are access and delivery control functions which allow trustworthy communication across multiple trust-centric network domains. The trust-centric network domain identifies external network elements, evaluates trust levels and accepts or rejects their communications according to the trust levels of external elements. The access and delivery control functions will forward only authorized and sterilized packets to peer domains for keeping the trust-centric network domain safe. These kind of functions can replace or help the security functions of the traditional gateway.

Figure 4 shows a networking scenario among trust-centric network domains. In this figure, the trust-centric network domain A can communicate to a network element in trust-centric network domain B, in which the trust level of trust-centric network domain B is equal to or higher than trust-centric network domain A. However, the trust-centric network domain A could not communicate to a network element with the trust-centric network domain C if the trust level of the domain C is lower than that of the domain A.

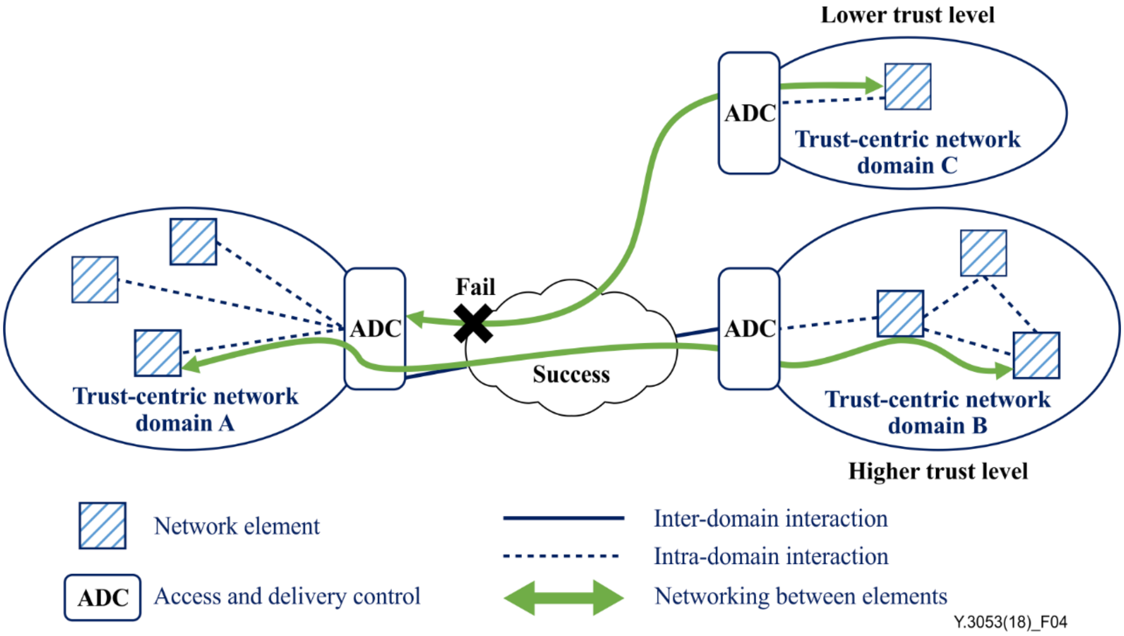
Lower trust level
ADC
Trust-centric network domain C
Fail
ADC
Success
ADC
Trust-centric network domain A
Trust-centric network domain B
Higher trust level
Network element
ADC
Access and delivery control
Inter-domain interaction
Intra-domain interaction
Networking between elements
Y.3053(18)_F04

Figure 4 – Networking scenario between the trust-centric network domains

9.3 Expanding trust-centric network domains

If the range of communication is bounded within a single trust-centric network domain, a scalability problem will arise with respect to wider connectivity. For supporting scalability, the trust-centric network domain starting from a small domain can be extended to connect multiple trust-centric network domains.

First, Figure 5(a) shows the situation to accept a new member in the trust-centric network domain, in which a network element outside of the domain tries to be a member when its trust level is equivalent to that of the target trust-centric network domain. The domain administration functions perform well-defined procedures for checking identity and evaluating the trust level of the external network element. Then only the qualified network elements are allowed to be registered as a new member in the trust-centric network domain. In addition, the access and delivery control functions are accordingly extended to communicate with external network elements.

Second, Figure 5(b) shows the collaboration scenario between two trust-centric network domains. If two domains trust each other and the reliable links are connected, then the network elements within one domain can trust network elements within another domain. The other trust-centric network domain may similarly connect to these two domains.

Third, Figure 5(c) shows the hierarchical configuration of the trust-centric network domains. Expanding a domain by accepting new network elements may have some limitations while the large number of network elements are managed by a single domain administrator. Also, there are some limitations when a lot of trust-centric network domains are interconnected among them. In the view of domain scalability, a lot of trust-centric network domains can configure the hierarchical relationships. By aggregating multiple trust-centric network domains, a larger trust-centric network domain can be formed as shown in this figure.

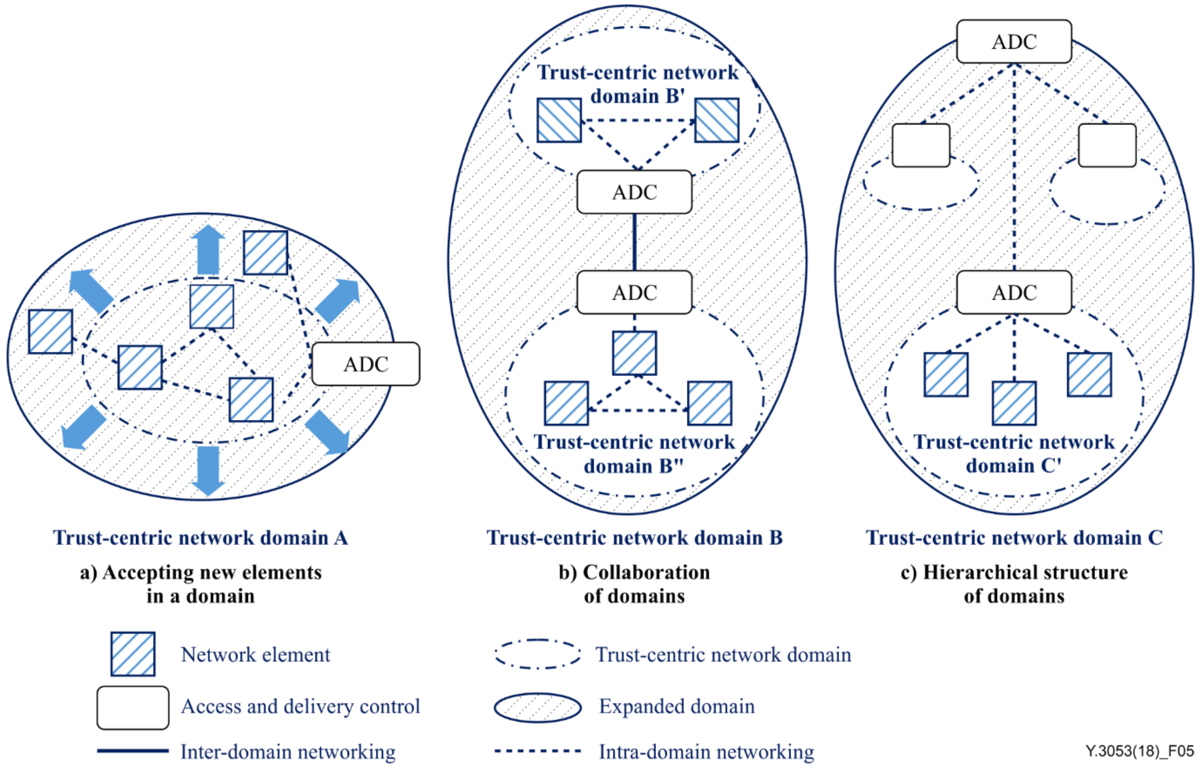
ADC
Trust-centric network domain A
a) Accepting new elements in a domain
Trust-centric network domain B'
ADC
ADC
Trust-centric network domain B''
Trust-centric network domain B
b) Collaboration of domains
ADC
ADC
Trust-centric network domain C'
Trust-centric network domain C
c) Hierarchical structure of domains
Network element
Access and delivery control
Inter-domain networking
Trust-centric network domain
Expanded domain
Intra-domain networking
Y.3053(18)_F05

Figure 5 – Expanding the trust-centric network domains

10 Deployment architecture and procedures for trustworthy networking with trust-centric network domains in IP networks

10.1 Introduction

This Recommendation specifies a generic functional architecture for trustworthy networking and thus does not illustrate how it can be deployed in IP networks of the current Internet. Amendment 1 describes how trustworthy networking based on the functional architecture defined in the Recommendation can be realized in IP networks.

With the trust-centric network domain, network entities can be securely protected from outside, and they have secure and trustworthy communications without additional security procedures. This clause specifies a deployment architecture and procedures for trustworthy networking with trust-centric network domains in IP networks.

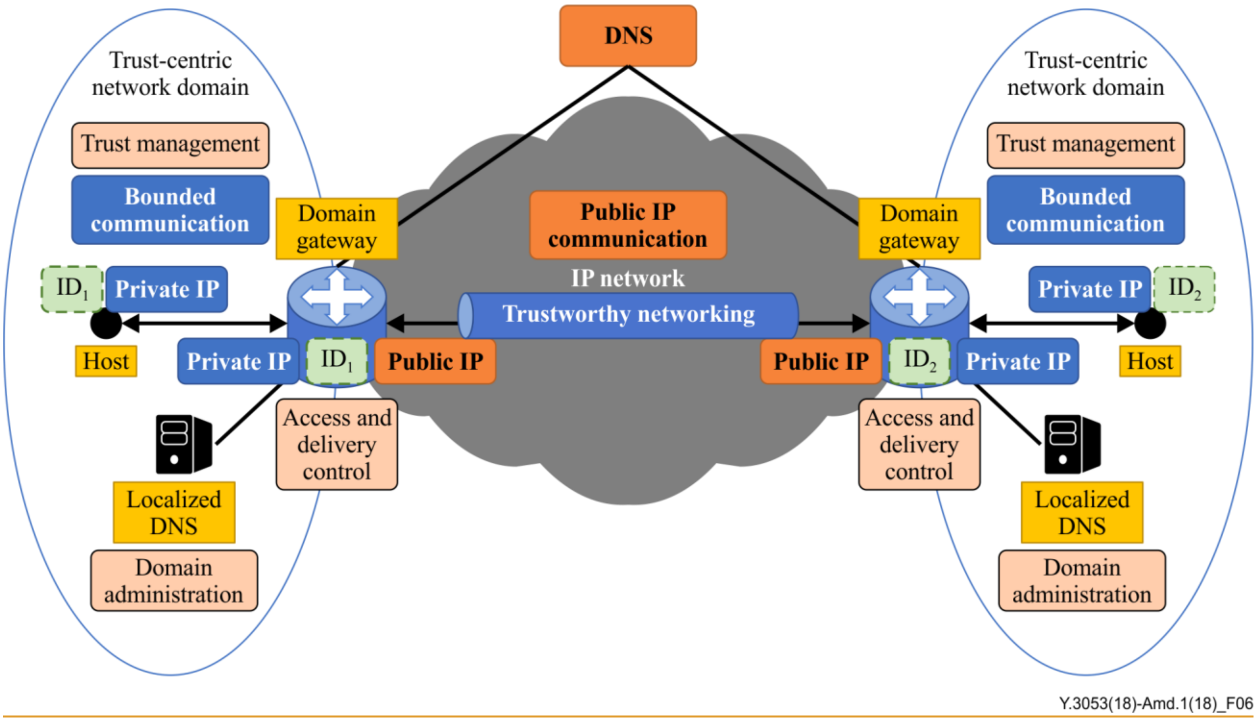

Figure 6 – Conceptual architecture of trustworthy networking in IP networks

Figure 6 describes a conceptual architecture of trustworthy networking with trust-centric network domains in IP networks. The bounded communication (i.e., secure and trustworthy communication without additional security procedures) in the trust-centric network domain is determined by a domain gateway. Private IP address is utilized for the bounded communication within the trust-centric network domain. Communications among network domains are performed with determined procedures through access and delivery control functions. A trust level of inbound traffic from the trust centric networking domain viewpoint is verified by the ADC to communicate with a network entity (i.e., host) outside of the trust-centric network domain while maintaining the trust level of the domain. Every host has its own identifier that can be recognized globally. The ADC performs address translation from a private IP address to a public IP address using an ID from a localized DNS and vice versa, which is similar to the function of the conventional network address translator (NAT).

Hosts can communicate to other hosts in the trust-centric network domain via the private IP addresses. Each trust-centric network domain has a localized DNS for domain administration functions that has an IP-ID mapping functionality. To communicate over the network domains, hosts need to delegate inbound/outbound communication functionality to the ADC that can allocate the appropriate public IP addresses. By IP address-space management and delegation of domain authentication, the concept of trustworthy networking with trust-centric network domains can be adopted to current IP networks, and it is possible to use existing hosts and applications without modification.

10.2 Deployment architecture of trustworthy networking in IP networks

Figure 7 illustrates a deployment architecture to describe how the trustworthy networking can be mapped into IP networks. A certain area of the IP network can be divided into a sub-network, that is, the trust-centric network domain with a domain gateway that understands trustworthy networking semantics at the ingress edge of the domain with ADC. This means that certain area of the IP network can only be accessed through the domain gateway so that the domain is securely protected from outside.

A domain administrator manages trust-centric network domain policies with domain administration functions and trust management functions. The domain setup criteria are based on various aspects (e.g., the services provided, security level, management authorities, logical grouping, etc.). IP/ID mapping among trust-centric network domains are handled through domain administrators.

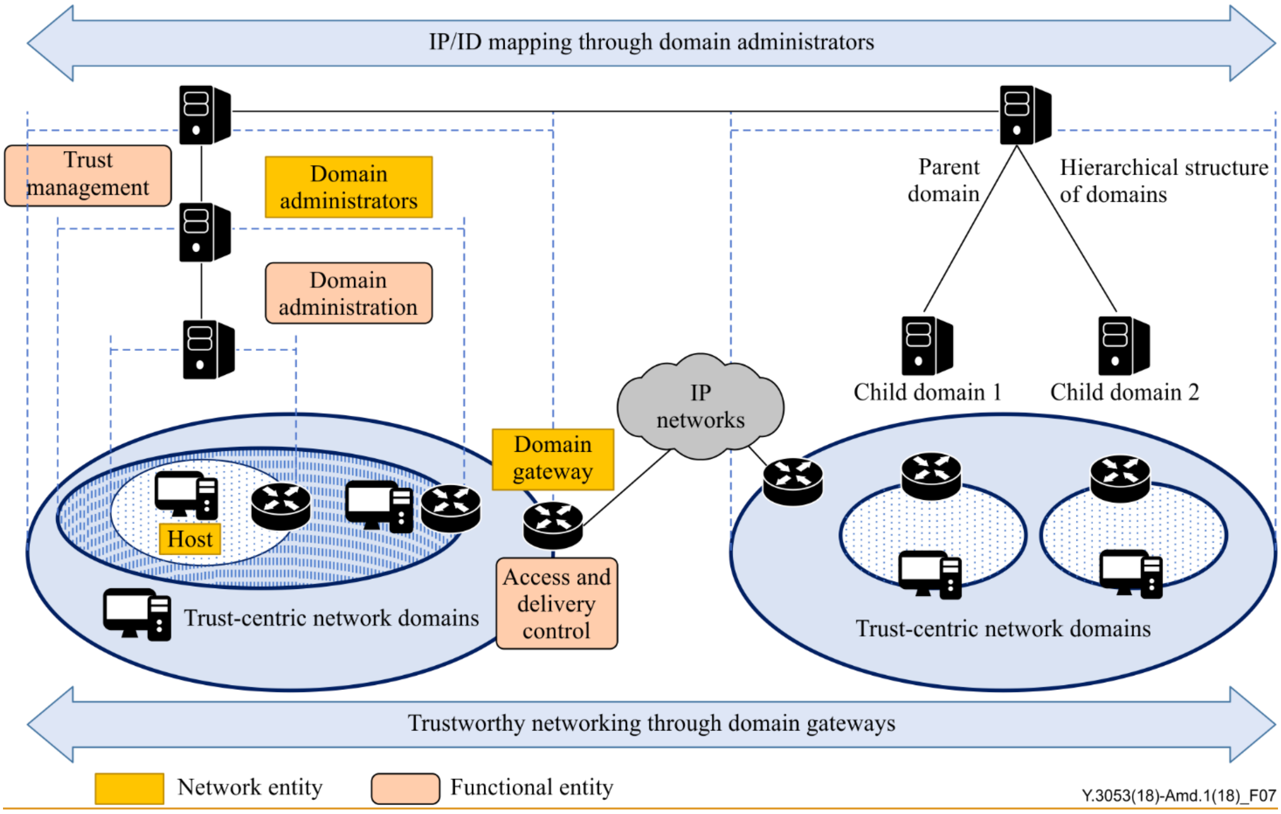
IP/ID mapping through domain administrators
Trust management
Domain administrators
Domain administration
Parent domain
Hierarchical structure of domains
Child domain 1
Child domain 2
IP networks
Domain gateway
Host
Access and delivery control
Trust-centric network domains
Trust-centric network domains
Trustworthy networking through domain gateways
Network entity
Functional entity
Y.3053(18)-Amd.1(18)_F07

Figure 7 – Deployment architecture for trustworthy networking in IP networks

10.3 Address mapping mechanism

In order to deploy the trustworthy networking concept to existing IP networks, the trust-centric network domains have to accommodate applications and devices that use IP addresses. The current IP address has the characteristics of both an identifier and a locator. However, in the trustworthy networking architecture, identifier and locator are considered separately. To accommodate the existing IP network entities that do not understand the identifier, it is assumed that the trust-centric network domain gateway can manage the mapping between them.

Since an IP address is used as a locator and it is within the domain it belongs to, a private IP address instead of a public IP address can also be used as a locator. Inside the trust-centric network domain, private IP addresses are locators, while public IP addresses are locators for inbound/outbound communication. Figure 8 illustrates the relationship between the two different IP addresses and how they are mapped with IDs in the trustworthy networking environment.

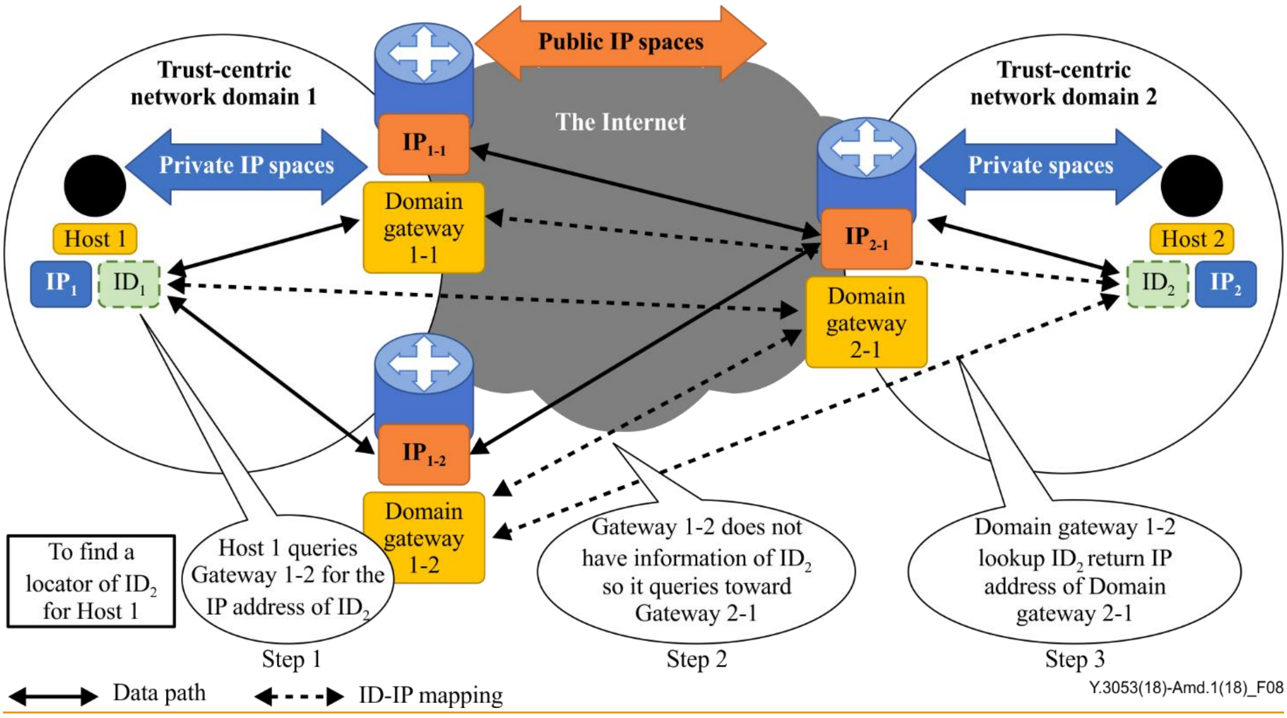
Public IP spaces
The Internet
Trust-centric network domain 1
Trust-centric network domain 2
Private IP spaces
Private spaces
Host 1
Host 2
IP1
ID1
ID2
IP2
IP1-1
IP1-2
IP2-1
Domain gateway 1-1
Domain gateway 1-2
Domain gateway 2-1
To find a locator of ID2 for Host 1
Host 1 queries Gateway 1-2 for the IP address of ID2
Gateway 1-2 does not have information of ID2 so it queries toward Gateway 2-1
Domain gateway 1-2 lookup ID2 return IP address of Domain gateway 2-1
Step 1
Step 2
Step 3
Data path
ID-IP mapping
Y.3053(18)-Amd.1(18)_F08

Figure 8 – Address mapping mechanism of trustworthy networking in IP networks

A host uses a private IP address in the domain, an ID that is assigned by the domain gateway when it leaves the domain, and a public IP address when it enters another domain. The mapping between the ID and the public IP address is done by the ILMS-FE of the domain gateway in another domain. The address mapping mechanism is similar to the existing NAT. To communicate among hosts, whose global IDs are given, it is required to look up the location of the hosts. Figure 8 illustrates one such example. If Host 1 tries to communicate with Host 2, where the global ID is given as ID_2, it queries the IP address of ID_2 to Domain Gateway 1-2. If the locator information of ID_2 is not registered in Domain Gateway 1-2, the gateway sends queries to the domain of other gateways, in this case, Domain Gateway 2-1. Since Domain Gateway 2-1 has the information of ID_2, it returns its own public IP address to Domain Gateway 1-2. Finally, Domain Gateway 1-2 registers the public IP address of ID_2 through the ILMS-FE, and Host 1 can communicate with Host 2 with ID_2.

10.4 Deployment procedures for trustworthy networking

This clause specifies procedures for trustworthy networking based on the deployment architecture and the address mapping mechanism described in the clauses 10.2 and 10.3. Note that terms representing functional entities are defined in the functional architecture of this Recommendation.

10.4.1 Building trust-centric networking domain

10.4.1.1 Domain initialization

To build a new trust-centric networking domain, a domain administrator needs to initiate the functionalities of the trust-centric networking domain as follows:

– Domain administration

To initialize a domain with respect to a trust-level, the domain administrator needs to configure trust and membership policies. To manage the trust level, the domain administrator sets the required trust level of membership with DPM-FE. The domain administrator can explicitly dedicate a host for trust management functions and domain administration functions.

– Access and delivery control

The hosts that need to connect outside of the domain should have ADC functions. For the IP network case, each domain host should assign its gateway to the hosts with ADC functions.

10.4.1.2 Host registration

After the trust-centric network domain has been initialized, the domain can adopt new network hosts. The procedure of a host registration is shown in Figure 9.

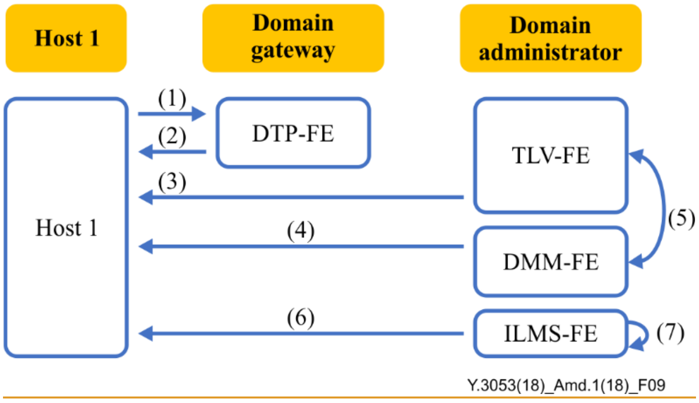

Figure 9 – Procedure of a host registration

1) Host 1 connects to the network of the trust-centric network domain;

2) The domain assigns a private IP address to Host 1. The domain gateway is assigned as the default gateway for IP network;

3) TLV-FE analyses the trust information of Host 1;

4) Host 1 requests to join the domain;

5) The DMM-FE of the domain administrator receives the requests and decides to accept Host A, based on the domain policy and the trust level of Host 1;

6) The ILMS-FE of the domain administrator issues a new identifier of Host 1;

7) ILMS-FE archives Host 1's ID and the private IP address.

10.4.2 Evicting an existing host from the trust-centric networking domain

A domain administrator can monitor the trust level of each host associated with the trust-centric networking domain. The domain administrator periodically aggregates necessary information to evaluate the trust levels of all hosts in the domain. When an associated host violates domain management policies and cannot maintain a certain level of trust, the host may be evicted from the trust-centric networking domain based on the decision of the domain administrator as shown in Figure 10.

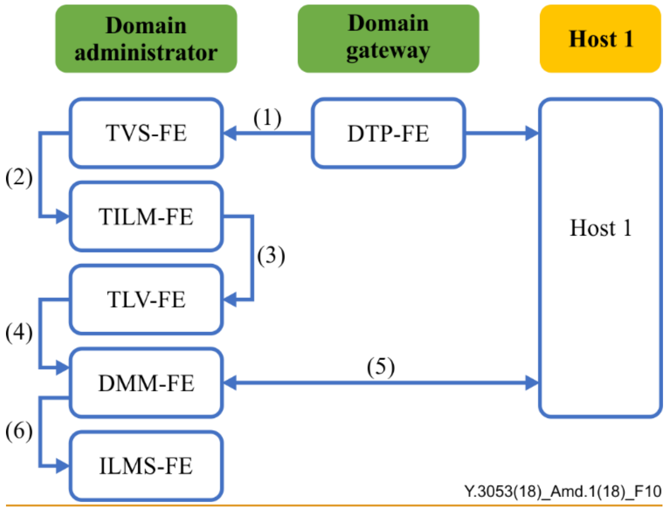

Figure 10 – Procedure of evicting a host from the trust-centric networking domain

Figure 10 shows the detailed procedure for evicting the existing host from the trust-centric networking domain as follows:

1) A domain administrator monitors a host's behavior through DTP-FE and TVS-FE gathers data to evaluate the trust level;

2) TILM-FE updates the trust information of each host associated with the trust-centric networking domain;

3) TLV-FE re-evaluates the trust level of each host;

4) Based on the evaluation of TLV-FE, DMM-FE checks a host which violates domain management policies;

5) DMM-FE sends a message to the designated host to cut off trust relationship and domain association;

6) The domain administrator deletes the ID-Locator mapping information of the host.

10.4.3 Terminating trust-centric networking domain

A domain administrator can determine to terminate its own trust-centric networking domain. To terminate the domain, the domain administrator needs to send messages informing of the termination of networking to its peer hosts and domains. If the domain is a member of a bigger domain, then the domain administrator sends the message of termination to its parent domain. The domain administrator then cuts off the relationship with all member hosts and child domains; it clears related information such as ID-location mapping and the trust level of member hosts and child domains.

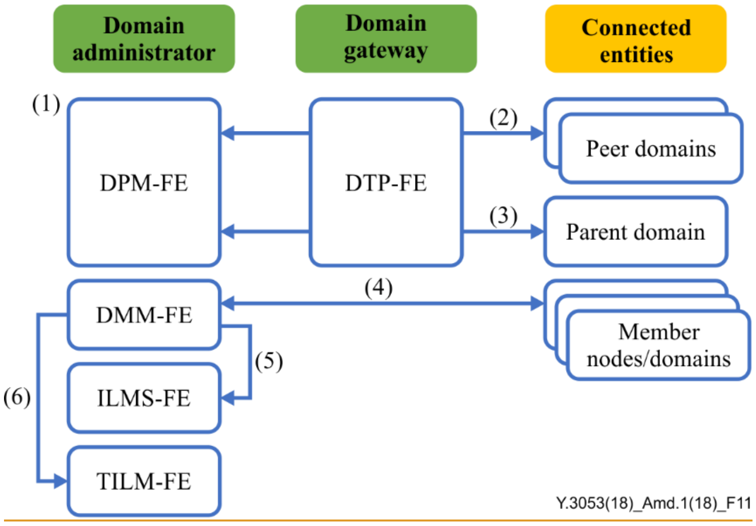

Figure 11 – Procedure of terminating a trust-centric networking domain

Figure 11 shows the detailed procedure for terminating the trust-centric networking domain as follows:

1) A domain administrator decides to terminate the domain;

2) DPM-FE sends messages informing of the networking termination to peer domains and hosts through DTP-FE;

3) DPM-FE sends a message of terminating the domain to the parent domain;

4) DMM-FE sends messages to all member hosts and child domains to cut off trust relationship and domain association;

5) The domain administrator deletes ID-Locator mapping information of member hosts and child domains;

6) The domain administrator deletes trust information of member hosts and child domains.

10.4.4 Trustworthy networking among trust-centric networking domains

10.4.4.1 Communication within a single trust-centric network domain

In order for the two hosts to send and receive messages to each other, a communication path must first be established. If the two hosts are located in the same domain, they already have the trust relationship with each other, which means no additional security procedures are needed.

10.4.4.2 Communication between trust-centric network domains

If two hosts are in different domains, it means that they do not know each other's IP address directly. The domain administrator provides an IP address of each host for trustworthy networking between two hosts in different domains. If Host 2 wants to perform trustworthy networking with Host 1 in another domain, it is necessary to establish a communication path between the two hosts through interactions between domain administration functions and access and delivery control functions. Figure 12 describes the detailed procedure for trustworthy networking between trust-centric network domains as follows:

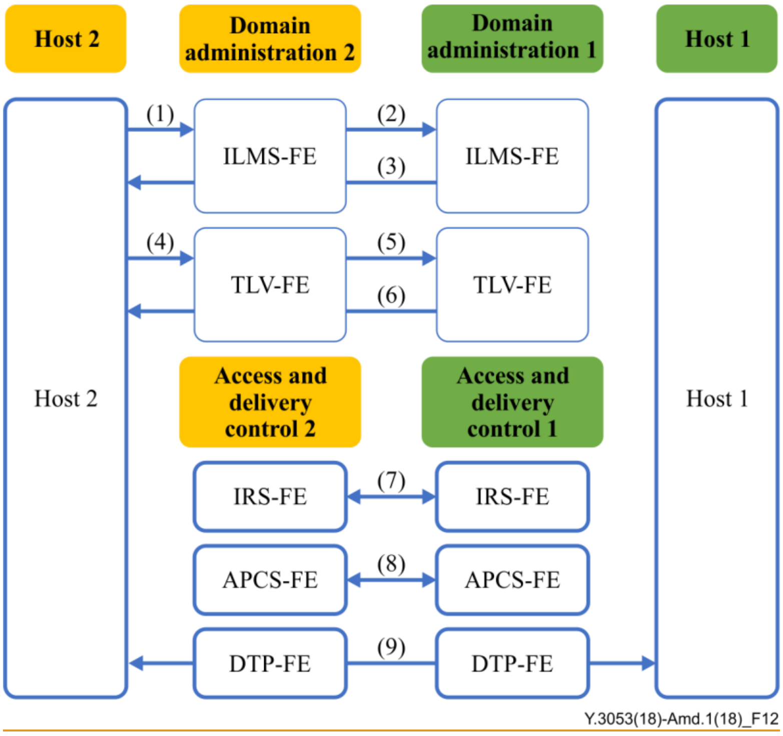

Figure 12 – Procedure of trustworthy networking between trust-centric network domains

1) Host 2 requests the IP address of Host 1 from domain administration 2 with the known ID of Host 1;

2) Domain administration 2 requests the IP address of Host 1 from domain administration 1 through ILMS-FE;

3) Domain administration 1 obtains the IP address of Host 1 through ILMS-FE and replies with the ID and IP address of Host 1 to domain administration 2, and then it replies to Host 2;

4) Host 2 requests the trust level of Host 1 through domain administration 2;

5) Domain administration 2 checks the trust level of Host 2 through TLV-FE and requests the trust level of Host 1 from domain administration 1;

6) Domain administration 1 obtains the trust level of Host 1 through the TLV-FE and forwards it to domain administration 2, and the result is sent to Host 2;

7) The access and delivery control 2 forms a communication path with the access and delivery control 1 through the IRS-FE;

8) Host 2 and Host 1 establish a reliable path through the APCS-FE of access and delivery control of each trust-centric network domain;

9) Communication path is established between Host 1 and Host 2.

~~10~~11 Security considerations

Trustworthy networking is a concept of networking to ensure a confident communication with among mutually known and trusting network elements. A trust-centric network domain can realize this concept. To meet a predefined trust level of trust-centric network domains, the trust-centric network domain administrator needs to provide security features for building, managing and operating the trust-centric network domain, such as checking identification, authorization and encrypted communication link. To be registered as new member of a new trust-centric network domain, network elements need to support some security functions that the trust-centric network domain requires. The detailed security requirements and mechanisms are based on [b-ITU-T Y.2701] and [b-ITU-T Y.2704].

Appendix I

Extending the trust model for trustworthy networking

(This appendix does not form an integral part of this Recommendation.)

The term "trust" is defined in many different ways in various areas. As pointed out in [b-Mayer], the lack of clear differentiation among the trust-related factors hinders trust related researches. Thus, this Recommendation follows the trust model proposed in [b-Mayer] and modifies some of the factors with respect to communication context. Figure I.1 shows extending of the trust model proposed in [b-Mayer] for trustworthy networking.

Trust is a directed relationship between two network elements. When a network element trusts the other network element, let us call the trusting network element as 'trustor' and the trusted network element as 'trustee'. The factors that contribute to build trust are classified into two categories: characteristics of the trustor and characteristics of the trustee. The characteristics of the trustor are called 'trust propensity' that affects the likelihood of trusting others. Trust propensity affects the likelihood that a trustor will trust other network elements. The trust propensity has more importance in situations involving different communication contexts. The characteristics of the trustee are called 'trustworthiness' that explains why the trustee can be trusted. Trustworthiness may stem from several perceptions of the trustor about the trustee. In the context of networking, the perceptions are affected by diverse factors such as past history of the trustee's behaviour, capabilities of the trustee, reputation of the trustee, etc. The trustworthiness of the trustee can be expressed in a single value or an array of values, called 'trust index' [ITU-T Y.3052]. Similarly, the trust propensity can also be expressed in a single value or an array of values, called 'trust measure'. When the trust index and the trust measure are arrays, each element is representing a specific factor contributing trust such as interaction history, reputation and accountability. In this case, the trust index is defined objectively so that any network element can utilize the index from the third party and the trust measure is defined subjectively to reflect the network element's own requirements. Note that one network element may have multiple trust measures for the separated context. Trust level is the value assigned to a trust relationship that indicates how much the trustor trusts the trustee.

Trust is not actual action taking but willingness to take risk. In the communication context action taking is trustors engaging communication with the trustee. Practically, communications often involve risks such as residual error in communication link or attacker intrusions. The risk incurred from the communication environment can be represented as 'risk level' and the actual communication takes place when a trust level surpasses the risk level. The outcome of the communication might affect the trustworthiness of the trustee.

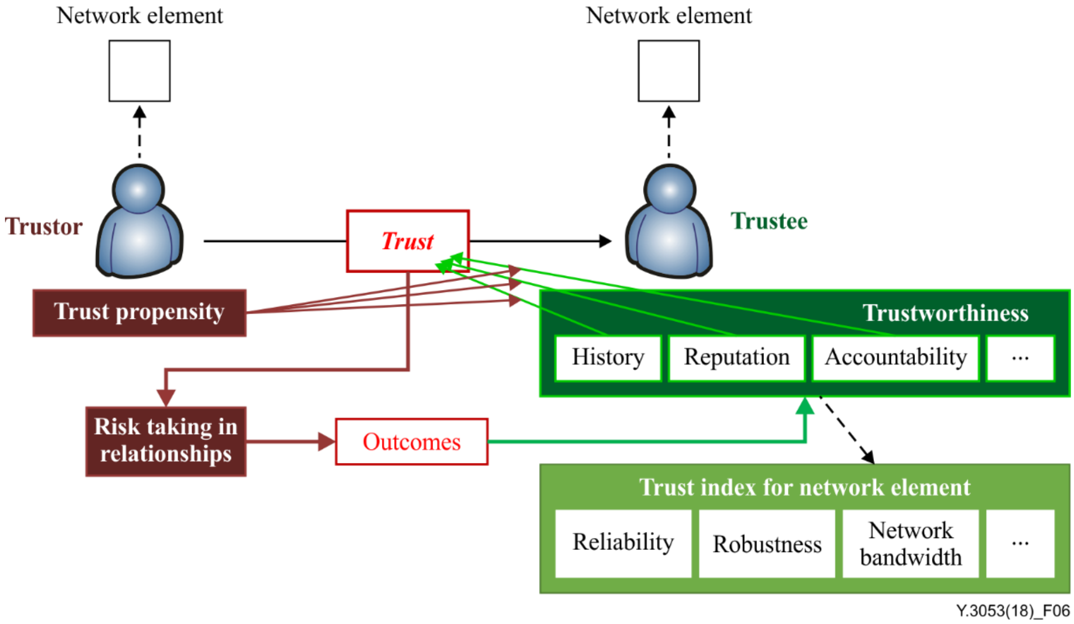

Figure I.1 – Extending the trust model of [b-Mayer] for trustworthy networking

Bibliography

[b-ITU-T Y.1311] Recommendation ITU-T Y.1311 (2002), *Network-based VPNs – Generic architecture and service requirements*.

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ITU-T Y.2704] Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN*.

[b-Mayer] R. Mayer, J. Davis, and F. Schoorman (1995), *An Integrated Model of Organizational Trust*, Academy of Management Review, vol. 20, No. 3, pp. 709-734. http://people.wku.edu/richard.miller/Mayer%20Trust%20article.pdf

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, 2019