International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 15

(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.800-X.849 series – Supplement on guidance for creating a national IP-based public network security centre for developing countries

ITU-T X-series Recommendations – Supplement 15

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Supplement 15 to ITU-T X-series Recommendations

ITU-T X.800-X.849 series – Supplement on guidance for creating a national IP-based public network security centre for developing countries

Summary

Supplement 15 to ITU-T X-series Recommendations provides guidance for the creation of a secure, stable and resilient national Internet protocol-based network infrastructure. The need for technical coordination (in creating secured, stable and resilient networks) arises in cases of failure (severe impairment of the quality of service) of any significant segment of the network which is part of the public network. The national ICT infrastructure includes fixed and mobile networks as well as the national segment of the Internet.

Security incidents may occur due to security problems: attacks like denial of service/distributed denial of service (DoS/DDoS); attacks aimed at network infrastructure; natural and anthropogenic disasters and other problems related to deterioration stability (quality of services and features) and security. Under such circumstances, technical coordination means gathering, analysis and managing information about incidents (including control information). This feature allows identifying threats and preparing the work of reconstruction.

This Supplement describes the architectural principles which ensure security, stability and recovery of the national ICT infrastructure in developing countries based on the IP-based protocol. Consistent application of the principle of "cooperation for safety and security" leads to the modern formation of the federated trust framework (FTF) or the so-called federated space of trust (FST). This new formation is usually distributed and then hosting services are available to all participants of the collective security system at the national level. Any national telecom operators have the opportunity to join to FTF. The members of FTF have access to all security services which were deployed in the FTF by other operators and the administration of a national centre for network security (NCNS).

FTF is organized as a stack of control planes: security control plane, information exchange plane and service exchange plane.

This Supplement opens a new dimension in security standardization – collaboration in security (alongside such works as security management, exchange of security incident and event information, application security, identification management, etc.).

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 15	2012-09-07	17

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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

Supplement 15 to ITU-T X-series Recommendations

ITU-T X.800-X.849 series – Supplement on guidance for creating a national IP-based public network security centre for developing countries

1 Scope

This Supplement describes models which can be used for creating a secure, stable and resilient IP-based network infrastructure, particularly for developing countries. The models of national centres may be federated, virtual and can be implemented separately or combined. In the framework of one country a number of similar equivalent centres may operate. The conceptual principle is "cooperation for safety and security".

2 References

None.

3 Definitions

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

BPM	Business process management
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
DB	Database
DoS	Denial of Service
DDoS	Distributed Denial of Service (attack)
DNS	Domain Name System
DWH	Data Warehouse
DDW	Distributed Data Warehouse
FTF	Federated Trust Framework
GIA	Group for Incident Analysis
IdM	Identity Management
IdP	Identity Provider
IP	Internet Protocol
MoU	Memorandum of Understanding
NCNS	National Centre for Network Security
NMS	Network Management System
NOC	Network Operations Centre
OSS/BSS	Operation Support System/Business Support System

SLA/NDA	Service Level Agreement/Non-Disclosure Agreement
SOC	Security Operations Centre
SSO	Single Sign-On
TNSS	Telecommunication Network Security System

5 Conventions

None.

6 General

This clause describes the architecture of inter-operator interaction which can help to build collective security and safety in the public service infrastructure, based on a national ICT infrastructure.

The national IP-based public network security centre for developing countries was created to promote the secure and sustainable operation of a national ICT infrastructure. This Supplement describes mainly the structure of a national centre for network security (NCNS) and its external interconnections.

The constituent elements of the NCNS are (architectural solutions):

- integration of functional and security components;
- organization of the functioning of the inter-operator group for incident analysis;
- monitoring the status of the ICT infrastructure based on its formal description (formal language);
- formation of the coordinating actions to provide continuity of service of the national ICT infrastructure to citizens, businesses and public authorities, both in daily operation and in emergency situations.

The development of a service infrastructure on the national level allows for national telco operators to move from personal protection of the network perimeter to other forms of security – using service platforms which are located in the inter-operator space – for building the collective national security.

In terms of integration, the NCNS is a multifunctional element in the infrastructure, which allows for the interaction of the functional elements placed there by national network operators – participants of the collective national security system. Primarily, this relates to service management platforms that are part of the OSS/BSS subsystems. Support for cross-interaction processes with the participants of the national collective security system is a prerequisite to participation.

The NCNS usually has no access (including the automatic mode) to the network management systems (NMSs) or other systems of national telco operators to collect any information.

At the same time, national telco operators may ask NCNS to turn on its automatic mode for formal exchange of the previously described objects (in special languages) for the definition of security incidents. The structured format will raise the level of automation in the processing of data on incidents through the exchange of structured information on incidents from the telco operator in the NCNS.

For solving the whole spectrum of problems in collective security, as described in this Supplement, ITU-T may need to develop new protocols/standards.

In accordance with the service-oriented architecture, the line between functional components and security service components fades. The security features should be incorporated into the architecture of each functional element. For the interaction of integrated security elements, an integrated environment is used for distribution of signals and information that can qualify as incidents or security threats from far outside the network in which the event has been registered/recorded. With this integrated environment, the pyramid of events (as described in Figure 1 of [b-ITU-T E.409]) refers to the entire space of inter-operator interactions for security.

An integrated environment is organized as the stack of three control planes: security control plane, information exchange plane and service exchange plane.

1) The environment for information distribution about security events is described as an additional structural element in the architecture: a specialized security control plane (see Figure 1) permeates the entire space of collective security. This plane serves as a mediator for distributing security events registered by networks that are connected to the NCNS. The described incidents are the result of signals processed from many network elements. Initial information about incidents is stored in an NCNS distributed data warehouse (DDW). DDW is under high protection. The security control plane is used for monitoring the status of networks and performing signal interaction of the network through an 'interaction broker'. In the event of an emergency situation, the plane is used to implement the NCNS provisions in the form of direct control (may be automatic mode) actions with respect to the networks that lost stability as a result of the emergency.

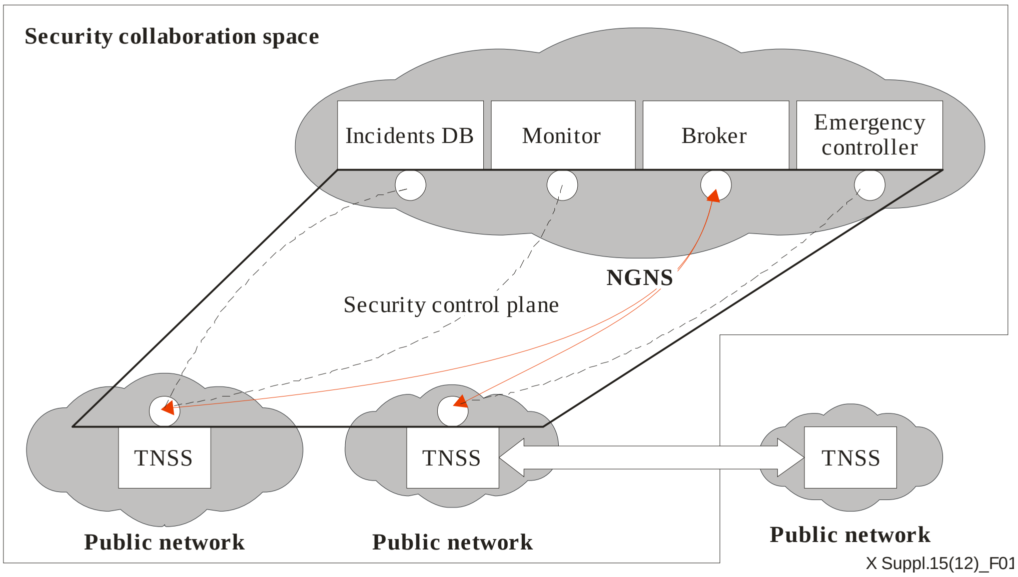

Figure 1 – Security control plane

2) To ensure normal functioning of each network, as well as to reflect threats, all necessary information interaction (in the form of statistical data requests) accumulate in the OSS/BSS. Information interaction should be organized in each network. Such requests may also come from NCNS on the basis of processing the incident database to analyse the state of resources and service levels. This interaction takes place via the information exchange plane (see Figure 2).

3) Transparent interaction processes between telecom operators (during provision of joint security) is realized by sending messages to/about security services. These services may be provided to each other and to the NCNS security services. All services available to participants in the system, as well as means of controlling them, form the service exchange plane (see Figure 3).

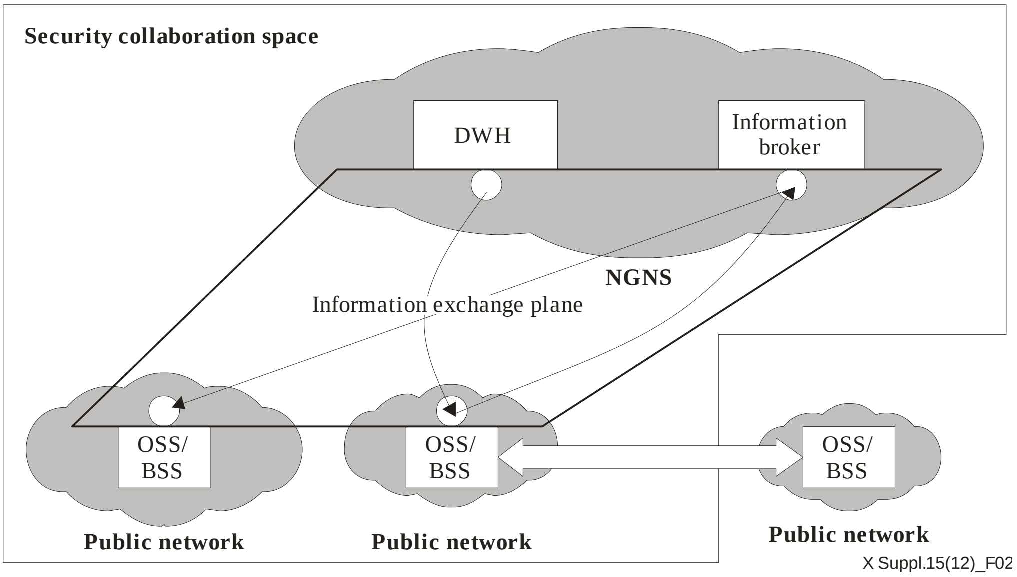

Figure 2 – Information exchange plane

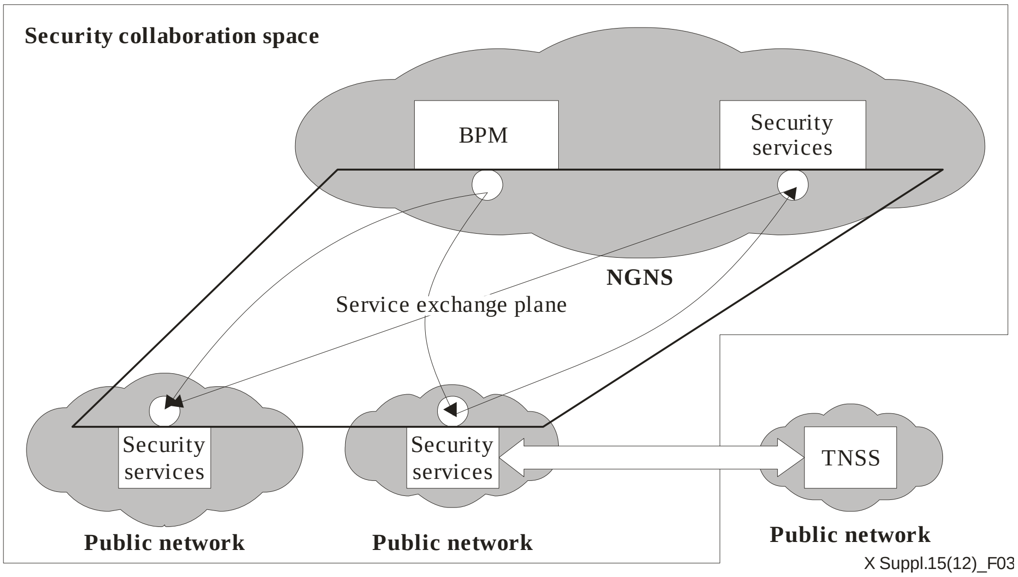

Figure 3 – Service exchange plane

7 Functioning architecture of the inter-operator group for incident analysis

The group for incident analysis (GIA) is an architectural component of the NCNS, which is dedicated to collecting and sharing information about incidents and security events among telecom operators, communication services consumers, equipment manufacturers and government agencies.

The main aim of creating the GIA is to consolidate all efforts to identify threats of information and network security of the national ICT infrastructure. GIA should detect and localize incidents that relate to information and network security. After that, GIA takes necessary measures to eliminate the negative impact of incidents and to prevent them in the future.

GIA fulfils the following functions:

1) forms and distributes instructions for telecom operators which have been certified in concordance with national security specifications (in accordance with [b-ITU-T X-Sup.2]);

2) examines and monitors information from communication systems of telecom operators for security vulnerabilities and provides instructions to eliminate them;

3) may provide support for users of telecom operators on improving stability and information security (consults with users on the fight against malware, installation of security settings, cases of unavailability of nodes and segments of the communication networks, and infringements of copyright when using the Internet, etc.);

4) handles messages from telecom operators about events and security incidents, including complaints about the actions of users and telecom operators, as well as incidents from telecom operators (e.g., technical fraud);

5) carries out analysis (investigation) of recorded incidents and security events in cooperation with telecom operators, equipment manufacturers, government agencies, and provides timely sending of information about threats, incidents and security events to eliminate their harmful effects;

6) organizes cooperation in the use of technical means of information security support, and an increase in stability for shared use;

7) provides advice to equipment manufacturers about requirements for increasing the stability and security of communication networks;

8) conducts information and analytical work on collecting data about past attacks, current methods of attack, resource violators and attack signatures, etc.

The list of incidents that GIA reacts to includes (but is not limited to):

- DoS/DDoS attack;
- unauthorized access to network resources;
- the presence of a known critical vulnerability on a significant resource in possession;
- an epidemic of computer viruses;
- operation of malware in the network;
- disruption of routing, resulting in the unavailability of subnetworks, segments and autonomous systems;
- false or malicious reconfiguration of network equipment resulting in the disruption of connected telecommunication networks;
- phishing;
- distribution of various types of spam;
- "DNS-poisoning" type attacks;
- unauthorized traffic admission ("grey" traffic).

The organizational structure of GIA is shown in Figure 4, and the technical scheme of interaction between GIA participants is shown in Figure 5.

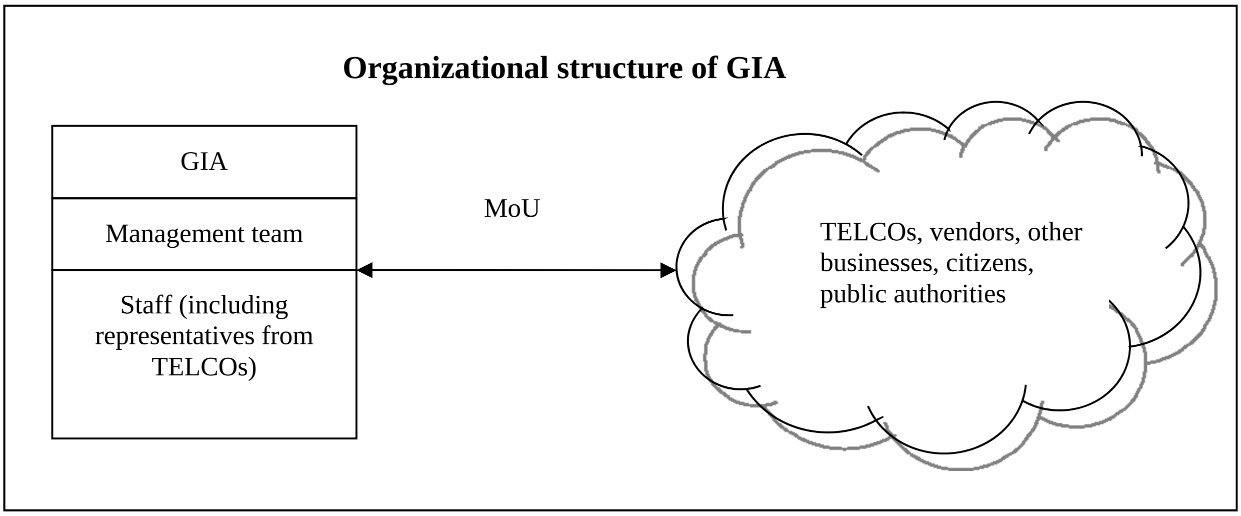
Organizational structure of GIA
GIA
Management team
Staff (including representatives from TELCOs)
MoU
TELCOs, vendors, other businesses, citizens, public authorities

Figure 4 – Organizational structure of GIA

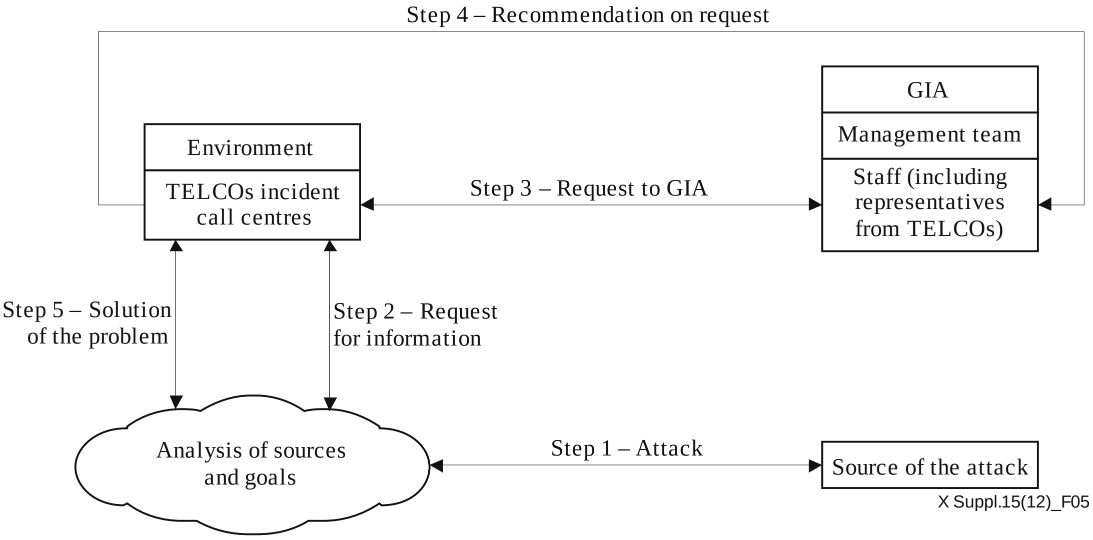
Step 4 – Recommendation on request
GIA
Management team
Staff (including representatives from TELCOs)
Environment
TELCOs incident call centres
Step 3 – Request to GIA
Step 5 – Solution of the problem
Step 2 – Request for information
Analysis of sources and goals
Step 1 – Attack
Source of the attack
X Suppl.15(12)_F05

Figure 5 – Technical scheme of interaction between GIA participants

8 Formation of control activities for telecom operators to ensure continuity of services in daily operation and in emergency situations

Control activities for telecom operators to ensure continuity of services are:

1) requests for non-automatic monitoring status and forecast of emergency security situations on the operator's networks (information about the results of monitoring might also be transferred from the telecom operators to NCNS automatically, if they have signed SLA/NDA);

2) organizing and conducting training of telecom operator staff to test the readiness of providing additional resources in case of security breaches, as well as emergency situations of a natural and man-made character;

3) coordination and consolidation of telco operators' efforts to detect security threats,

4) analysis of real-time information (if available) about the current status of telecom operator networks to assess the possibility of providing them with the necessary resources (services) in time of attack and emergency situations of a natural and man-made character;

5) coordination of telecom operator activity that bolsters their security services for events related to the prevention and elimination of security incidents;

6) monitoring the restoration of functionality of networks and telecommunications after emergency situations;

7) preparing and making available to the telecom operator operational solutions to provide for any additional security requirements;

8) development of proposals to eliminate emergency situations on telecom operator networks and counter attacks on critical infrastructures.

9 Architectural principles for NCNS creation

NCNS is designed and formed as the system of organization and technical control of the national ICT infrastructure in the process of inter-operator cooperation, and includes both existing control centres of communication networks and the newly-created telecom operator security control centres. NCNS provides coordination both in everyday activities as well as under emergency situations.

The formation of NCNS involves the creation of a special pool of telecom operators which have been selected and certified to work with the centre. Application of procedures and selection criteria helps telecom operators increase the number of cooperating participants.

The foundation of creating any NCNS is the creation of the architecture and a methodology of organizing and maintaining the exchange system with security operation centres (SOC) of national telecom operators. This approach involves the creation of NCNS as a multipoint system of inter-operator cooperation.

NCNS may include an administration centre and the GIA. The latter includes the following:

1. a monitoring and management subdivision for information security, the functions of which include:
   - creating and maintaining a database of security incidents on communication networks. Keeping databases up to date. Information support of protocol exchange for security events and good practices with other network security centres and the security centres for cooperating operators;
   - control, by using hardware and software, of the status of information security of networks and systems of essential operators;
   - cooperation with operational subdivisions of operators to localize and eliminate accidents on communication networks caused by destructive influences on the network and system resources controlling the communication network;
   - organizing cooperation among security centres of cooperating operators when deflecting massive attacks on communication network control systems;
   - organizing cooperation between the centres of competence and manufacturer support services of telecommunication and network equipment.
2. subdivision of analysis and development, the functions of which include:
   - development of regulatory and systematic methods to support the security of the national ICT infrastructure;
   - analysis of security threats and development of measures and recommendations to counter them;

- creation of a set of best practices and recommendations for providing security and response to security incidents;
- development of technical solutions and support of projects and work related to information security on communication networks and information resources;
- organization and certification of operators that join the GIA.

The objects of NCNS information cooperation are:

- security control centres (SOC) of telecom operators;
- other NCNS;
- organizations of federal regulators in the field of security and communications;
- security incident response centres (CERT, CSIRT, CIRT, etc.);
- organizations interested in increasing the stability of communication networks (vendors, community organizations, etc.).

The volume and nature of interaction is determined by the NCNS proceeding from the requirements of national legislation and building the national ICT infrastructure.

It is recommended that the NCNS maintain its own electronic database ("knowledge base") about threats and protection methods (in accordance with national regulations regarding the protection of confidential information).

Automation of NCNS activity is performed via a combination of hardware and software.

The choice of NCNS automation is determined on the basis of national legislation, the control infrastructure of national public communication networks and by taking into consideration the following sets of objectives:

- completeness (provision) of services. This prescribes NCNS to fulfil its stipulated functions as necessary.
- security of services. This prescribes NCNS to provide confidentiality, integrity, availability of circulating information, its protection from unauthorized access, malicious and improper use or damage, modification, alteration and prevention of the entrance of false information.
- stability. This prescribes NCNS to perform a full range of stipulated functions at the required times and for the necessary duration in all circumstances.

Proceeding from the common objectives, NCNS as a "tool for exchanging" must be able to implement these organizational and technical issues:

- inventory and monitoring of resource availability;
- collection and correlation of security events and security control incidents, and their analysis;
- countermeasures to massive attacks on critical elements of networks and control systems.

9.1 The principle of a federated trust framework (FTF)

The purpose of the federated space trust is to provide a mechanism for establishing trust between telecom operators (partners of cooperation for the sake of security) to each operator (the representative NOC/SOC).

The FTF will help to authenticate operator identities in the access to any secure services belonging to another authorized agent. This allows the use of many variants, such as single sign-on (SSO), which eliminates the need to support and manage peer-to-peer identification.

In the FTF model, NCNS authenticates and acts as the identification service provider.

The model simplifies administration and enables companies to extend identity and access management to users and services to NCNS for different approved network operators in any country.

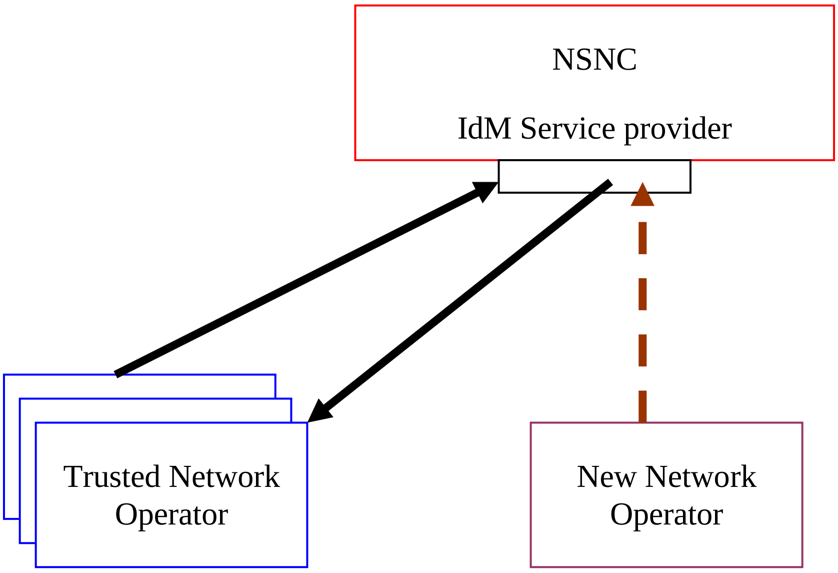

Figure 6 – Example of identification in the FTF

Bibliography

[b-ITU-T E.115] Recommendation ITU-T E.115 (2010), *Computerized directory assistance*.

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

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

[b-ITU-T X.816] Recommendation ITU-T X.816 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework.*

[b-ITU-T X.842] Recommendation ITU-T X.842 (2000) | ISO/IEC TR 14516:2002, *Information technology – Security techniques – Guidelines for the use and management of trusted third party services*.

[b-ITU-T X.843] Recommendation X.843 (2000) | ISO/IEC 15945:2002, *Information technology – Security techniques – Specification of TTP services to support the application of digital signatures*.

[b-ITU-T X.1032] Recommendation ITU-T X.1032 (2010), *Architecture of external interrelationships for a telecommunication IP-based network security system*.

[b-ITU-T X.1036] Recommendation ITU-T X.1036 (2007), *Framework for creation, storage, distribution and enforcement of policies for network security*.

[b-ITU-T X.1051] Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

[b-ITU-T X.1055] Recommendation ITU-T X.1055 (2008), *Risk management and risk profile guidelines for telecommunication organizations*.

[b-ITU-T X.1056] Recommendation ITU-T X.1056 (2009), *Security incident management guidelines for telecommunications organizations*.

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

[b-ITU-T X-Sup.2] ITU-T X-series Recommendations – Supplement 2 (2007), *ITU-T X.800-X.849 series – Supplement on security baseline for network operators*.

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