

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

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/>.

© ITU 2013

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
4	Abbreviations and acronyms	1
5	Conventions	2
6	General.....	2
7	Functioning architecture of the inter-operator group for incident analysis	4
8	Formation of control activities for telecom operators to ensure continuity of services in daily operation and in emergency situations	6
9	Architectural principles for NCNS creation	7
	9.1 The principle of a federated trust framework (FTF)	8
	Bibliography.....	10

