

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

M.3016.3

(04/2005)

SERIES M: TELECOMMUNICATION MANAGEMENT,
INCLUDING TMN AND NETWORK MAINTENANCE

Telecommunications management network

Security for the management plane: Security mechanism

ITU-T Recommendation M.3016.3

ITU-T M-SERIES RECOMMENDATIONS
TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Introduction and general principles of maintenance and maintenance organization	M.10–M.299
International transmission systems	M.300–M.559
International telephone circuits	M.560–M.759
Common channel signalling systems	M.760–M.799
International telegraph systems and phototelegraph transmission	M.800–M.899
International leased group and supergroup links	M.900–M.999
International leased circuits	M.1000–M.1099
Mobile telecommunication systems and services	M.1100–M.1199
International public telephone network	M.1200–M.1299
International data transmission systems	M.1300–M.1399
Designations and information exchange	M.1400–M.1999
International transport network	M.2000–M.2999
Telecommunications management network	M.3000–M.3599
Integrated services digital networks	M.3600–M.3999
Common channel signalling systems	M.4000–M.4999

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

ITU-T Recommendation M.3016.3

Security for the management plane: Security mechanism

Summary

This Recommendation identifies the security mechanisms for the management plane in the Telecommunications management network. This Recommendation focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the Telecommunication infrastructure.

Source

ITU-T Recommendation M.3016.3 was approved on 13 April 2005 by ITU-T Study Group 4 (2005-2008) under the ITU-T Recommendation A.8 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, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2005

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
2	References.....	1
3	Definitions	2
4	Abbreviations.....	2
5	Conventions	3
6	Security mechanisms	3
6.1	User authentication.....	4
6.2	Peer entity and data origin authentication	5
6.3	Access control	6
6.4	Data confidentiality	7
6.5	Data integrity	10
6.6	Audit trail.....	11
6.7	Key exchange	12
6.8	Alarm reporting	12
6.9	Packet filtering.....	13
Appendix I – IPsec, SSL/TLS and SSH security mechanisms		13
I.1	IPsec	13
I.2	SSL/TLS	14
I.3	SSH.....	15
Appendix II		16
II.1	Objectives	16
II.2	Network design considerations affecting packet filtering	16
II.3	Basic packet filtering	19
II.4	Enhanced packet filtering	19
BIBLIOGRAPHY		20

Copyright © 2005 ITU-T. All rights reserved.

Introduction

Telecommunications is a critical infrastructure for global communication and economy. Appropriate security for the management functions controlling this infrastructure is essential. Many standards for Telecommunications network management security exist. However, compliance is low and implementations are inconsistent across the various telecommunications equipment and software components. This Recommendation identifies the security mechanisms to allow vendors, agencies, and service providers to implement a secure Telecommunications management infrastructure. Although the present set of security mechanisms represents the current understanding of the state of the art, technologies will advance and conditions will change. To be successful, this Recommendation must evolve as conditions warrant. This Recommendation is intended as a foundation. Service providers may include additional security mechanisms to meet their specific needs over and above those in this Recommendation.

This Recommendation is part of the M.3016.x series of ITU-T Recommendations intended to provide guidance and recommendations for securing the management plane of evolving networks:

ITU-T Rec. M.3016.0 – *Security for the management plane: Overview.*

ITU-T Rec. M.3016.1 – *Security for the management plane: Security requirements.*

ITU-T Rec. M.3016.2 – *Security for the management plane: Security services.*

ITU-T Rec. M.3016.3 – *Security for the management plane: Security mechanism.*

ITU-T Rec. M.3016.4 – *Security for the management plane: Profile proforma.*

...

ITU-T Recommendation M.3016.3

Security for the management plane: Security mechanism

1 Scope

ITU-T Recs M.3016.1-M.3016.3 specify a set of requirements, services and mechanisms for the appropriate security of the management functions necessary to support the telecommunications infrastructure. Because different administrations and organizations require varying levels of security support, the ITU-T Recs M.3016.1-M.3016.3 do not specify whether a requirement/service/mechanism is mandatory or optional.

This Recommendation identifies the security mechanisms for the management plane in the Telecommunications management network. This Recommendation focuses specifically on the security aspect of the management plane for network elements (NE) and management systems (MS), which are part of the Telecommunication infrastructure.

This Recommendation is generic in nature and does not identify or address the security mechanisms for a specific Telecommunications Management Network (TMN) interface.

The proforma defined in ITU-T Rec. M.3016.4 is provided to assist the organizations, administrations and other national/international organizations, in specifying the mandatory and optional support of the requirements as well as value ranges, values etc., to help implement their security policies.

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 Recommendation G.8080/Y.1304 (2001), *Architecture for the Automatically Switched Optical Network (ASON)*, plus Amendment 2 (2005).
- ITU-T Recommendation M.3010 (2000), *Principles for a telecommunications management network*.
- ITU-T Recommendation M.3016.0 (2005), *Security for the management plane: Overview*.
- ITU-T Recommendation M.3016.2 (2005), *Security for the management plane: Security services*.
- ITU-T Recommendation M.3016.3 (2005), *Security for the management plane: Security mechanism*.
- ITU-T Recommendation M.3016.4 (2005), *Security for the management plane: Profile proforma*.
- ITU-T Recommendation X.509 (2000), *Information technology – Open Systems Interconnection: The Directory: Public-key and attribute certificate frameworks*, plus Corrigendum 1 (2001), Corrigendum 2 (2002), and Corrigendum 3 (2004).
- ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT Applications*, plus Amendment 1 (1996).

- ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

3 Definitions

This Recommendation does not define any new terms.

4 Abbreviations

This Recommendation uses the following abbreviations:

CORBA	Common Object Request Broker Architecture
DoS	Denial of Service
EMS	Element Management System
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
MS	Management System; any EMS, NMS, or OSS ¹
NE	Network Element
NE/MS	NE or MS
NMS	Network Management System
NTP	Network Time Protocol
NTPv3	NTP version 3
OAM&P	Operations, Administration, Maintenance and Provisioning
OS	Operating System
OSS	Operations Support System
RFC	Request for Comments
SAML	Security Assertion Markup Language
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol version 3
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Socket Layer

¹ OSSs generally can be used in the same context as MSs on any layer of the telecommunications management network hierarchy.

TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMN	Telecommunications Management Network
XML	Extensible Markup Language

5 Conventions

In ITU-T Recs M.3016.1, M.3016.2 and M.3016.3, a descriptor is used to identify the different requirements, services and mechanisms. The descriptor consists of one of the following three-letter label followed by a number:

- REQ for requirement;
- SER for service;
- MEC for mechanism.

6 Security mechanisms

This clause contains the specific security mechanisms for operations, administration, maintenance, and provisioning (OAM&P) and operations support system (OSS) security as they specifically apply to Management Plane security for infrastructure, services, and applications.

Table 1 below is reproduced from ITU-T Rec. M.3016.0 (Table 4 in ITU-T Rec. M.3016.0). This table gives an overview of the relationship between Requirements and Security services, and is used as the basis for organization of the other Recommendations in the series. For example, ITU-T Rec. M.3016.1 discusses the security Functional Requirements, ITU-T Rec. M.3016.2 discusses the Security Services, and this Recommendation (ITU-T Rec. M.3016.3) discusses specific security mechanisms corresponding to the Security Services.

This clause only defines the security services which are covered by standard solutions; other possible services (e.g., detection of denial of service) are left out.

Table 1/M.3016.3 – Mapping of security requirements and security services

Security functional requirement	Security service
Verification of identities	user authentication peer entity authentication data origin authentication
Controlled access and authorization	access control
Protection of confidentiality – stored data	access control confidentiality
Protection of confidentiality – transferred data	confidentiality
Protection of data integrity – stored data	access control
Protection of data integrity – transferred data	integrity
Accountability	non-repudiation
Activity logging	audit trail
Security alarm reporting	security alarm
Security audit	audit trail
Protection of the DCN	packet inspection