



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3016

(06/98)

SERIES M: TMN AND NETWORK MAINTENANCE:
INTERNATIONAL TRANSMISSION SYSTEMS,
TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE
AND LEASED CIRCUITS

Telecommunications management network

TMN security overview

ITU-T Recommendation M.3016

(Previously CCITT Recommendation)

ITU-T M-SERIES RECOMMENDATIONS

TMN AND NETWORK MAINTENANCE: INTERNATIONAL TRANSMISSION SYSTEMS, TELEPHONE CIRCUITS, TELEGRAPHY, FACSIMILE AND LEASED CIRCUITS

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 ITU-T List of Recommendations.

ITU-T RECOMMENDATION M.3016

TMN SECURITY OVERVIEW

Summary

This Recommendation provides an overview and framework that identifies security threats to a TMN and outlines how available security services can be applied within the context of the TMN functional architecture.

Source

ITU-T Recommendation M.3016 was prepared by ITU-T Study Group 4 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 26th of June 1998.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The 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 Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 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.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The 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, the 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 1998

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

CONTENTS

	<i>Page</i>
1 Introduction	1
1.1 Scope.....	1
1.2 References	1
1.3 Definitions.....	2
1.4 Rationale	2
2 System description.....	2
2.1 Actors and roles	3
2.2 Security domains.....	4
3 Generic security objectives for TMN	4
4 Legislation issues.....	5
5 Threats and risks.....	5
6 Security requirements and services	6
6.1 Security requirements and corresponding services	7
6.1.1 Mapping functional requirements, threats and security objectives	7
6.1.2 Description of functional requirements and the corresponding services.....	7
6.2 Requirements on the management of security	11
6.3 Architectural requirements.....	11
6.4 Security services and OSI layers.....	12
6.4.1 user authentication.....	12
6.4.2 authentication (peer entity and data origin).....	12
6.4.3 access control	12
6.4.4 security alarm, audit trail and recovery	12
6.4.5 integrity	12
6.4.6 confidentiality.....	13
6.4.7 non-repudiation	13
6.5 Security management	14
Appendix I – Legislation issues	14
I.1 Introduction.....	14
I.2 Applicable legislation areas	14
I.3 Sources of legislation	15
I.4 Possible consequences for TMN security standardization.....	15
Appendix II – Functional classes and security subprofiles.....	16
II.1 Grouping of security measures.....	16
II.1.1 The use of FCs in the inter-domain case	16
II.1.2 The use of FCs in the intra-domain case	16
II.2 Functional classes	16
II.3 Security profiles	18

Recommendation M.3016

TMN SECURITY OVERVIEW

(Geneva, 1998)

1 Introduction**1.1 Scope**

This Recommendation provides an overview and framework that identifies security threats to a TMN and outlines how available security services can be applied within the context of the TMN functional architecture, as described in Recommendation M.3010.

This Recommendation is generic in nature and does not identify or address the requirements for a specific TMN interface.

This Recommendation does not seek to define new security services but uses existing security services defined in other ITU-T Recommendations and ISO Standards.

It is envisaged that this Recommendation, along with Recommendation M.3400, will provide a basis for future standardization of TMN security services in the ITU-T.

1.2 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; all 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.

- ITU-T Recommendation M.3010 (1996), *Principles for a telecommunications management network*.
- ITU-T Recommendation M.3400 (1997), *TMN management functions*.
- ITU-T Recommendation X.509 (1997), *Information technology – Open Systems Interconnection – The Directory: Authentication framework*.
- ITU-T Recommendation X.741 (1995), *Information technology – Open Systems Interconnection – Systems management: Objects and attributes for access control*.
- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- ITU-T Recommendation X.802 (1995), *Information technology – Lower layers security model*.
- ITU-T Recommendation X.803 (1994), *Information technology – Open Systems Interconnection – Upper layers security model*.
- ITU-T Recommendation X.810 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- ITU-T Recommendation X.812 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.
- ITU-T Recommendation X.813 (1996), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.
- ITU-T Recommendation X.814 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework*.
- ITU-T Recommendation X.815 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework*.

- ITU-T Recommendation X.816 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework*.
- ISO/IEC 9979:1991, *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms*.

1.3 Definitions

1.4 Rationale

The requirement for security in TMN has originated from different sources:

- **Customers/subscribers** need confidence in the network and the services offered, including correct billing.
- **The Public Community/Authorities** demand security by Directives and Legislation, in order to ensure availability of services, fair competition and privacy protection.
- **Network Operators/Service Providers** themselves need security to safeguard their operation and business interests, and to meet their obligations to the customers and the public.

A TMN is intended to manage the underlying telecommunications network; therefore, the security of the TMN is essential to the proper functioning of the telecommunications network. Furthermore, the telecommunications network may incorporate security features that need to be managed by the TMN. Recommendation M.3400 enumerates those security management functions.

TMN Security Standards should preferably be based upon internationally agreed security standards as it is beneficial to reuse rather than create new ones. The provisioning and usage of security services and mechanisms can be quite expensive relative to the value of the transactions being protected. It is therefore important to have the ability to customize the security provided to the TMN transactions being protected. The security services and mechanisms that are used for securing TMN transactions should be provided in a way that allows such customization. Due to the large number of possible combinations of security features, it is desirable to have **security profiles** (see Appendix II) that cover a broad range of TMN security applications.

Standardization will facilitate **reuse of solutions and products** meaning that security can be introduced faster and at lower cost.

Important benefits of standardized solutions for vendors and users of the systems alike are the economy of scale in product development and component interoperation within a TMN system with regard to security.

It is necessary to provide security services and mechanisms to protect TMN transactions among TMN entities (as defined in M.3010) against malicious attacks such as eavesdropping, spoofing, tampering with messages (modification, delay, deletion, insertion, replay, re-routing, misrouting, or re-ordering of messages), repudiation or forgery. Protection includes prevention, detection and recovery from attacks, as well as management of security-related information. Standards should cover both intra-domain (Q3 and F) and inter-domain (X) interfaces.

2 System description

The objective of this Recommendation is an abstraction which makes it possible to avoid the many implementation details and to agree upon results that may be useful when later mapped on to specific implementations.

The TMN is described in terms of a functional architecture, an information architecture and a physical architecture (Recommendation M.3010).

It is recognized in Recommendation M.3010 that TMN building blocks may support other interfaces in addition to the Q, X and F. Similarly, the physical equipment may have other functionality in addition to that associated with information received via Q, X and F. These additional interfaces and related functionality are outside of the TMN and therefore outside the scope of TMN security standardization.

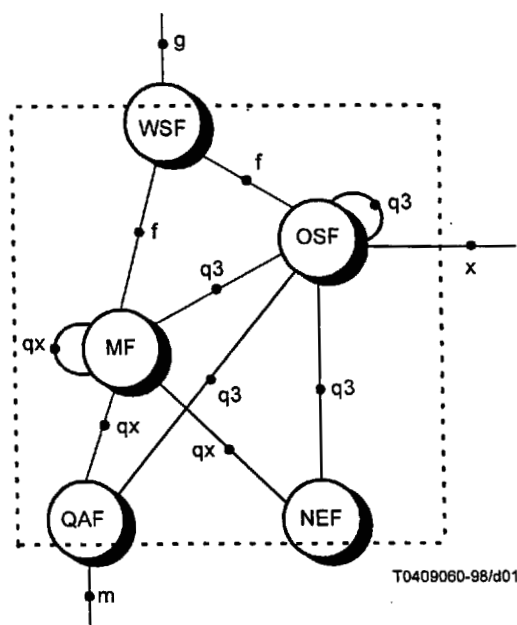


Figure 1/M.3016 – TMN functional architecture

2.1 Actors and roles

For the purpose of TMN security standardization, only technical security will be considered, which means that the relevant actors to consider are *TMN users*. A TMN user is a person or process applying TMN Management Services for the purpose of fulfilling management operations. TMN users can further be categorized dependent on whether they belong to the organization running the TMN (internal users) or whether they access the TMN as external users.

Each time a TMN user accesses a Management Service, the TMN user will take on a role. In some cases there will be a one-to-one relationship between a TMN user and a role, i.e. the TMN user will always stay in the same role. In other cases there will be a one-to-many relationship between a specific TMN user and the possible roles the TMN user can play.

The following gives a high-level classification of some common roles:

- Network Operators (*private or public*);
- Service Providers (*Bearer Service Providers or Value Added Service Providers*);
- Service Subscribers/Service Customers;
- Service End Users;
- Equipment/Software Vendors;
- Trusted Third Party.

When securing the TMN, it is not enough to control the behaviour of known TMN users. One must also consider the possibility of an intruder attempting illegal access to the TMN.

Some security measures require actors playing the role of a Trusted Third Party (TTP). An important security issue is how these actors should be allowed to interact with the TMN.