International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3016.1
Amendment 1
(07/2011)

SERIES M: TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Telecommunications management network

Security for the management plane: Security requirements

Amendment 1: Authentication extension

Recommendation ITU-T M.3016.1 (2005) – Amendment 1

ITU-T M-SERIES RECOMMENDATIONS

TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

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

Recommendation ITU-T M.3016.1

Security for the management plane: Security requirements

Amendment 1

Authentication extension

Summary

Amendment 1 to Recommendation ITU-T M.3016.1 adds requirements REQ 61 and REQ 62 to Rec. ITU-T M.3016.1 and updates Annex A accordingly.

History

Edition	Recommendation	Approval	Study Group	
1.0	ITU-T M.3016.1	2005-04-13	4	
1.1	ITU-T M.3016.1 (2005) Cor. 1	2005-11-13	4	
1.2	ITU-T M.3016.1 (2005) Amd. 1	2011-07-14	2	

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/.

Recommendation ITU-T M.3016.1

Security for the management plane: Security requirements

Amendment 1

Authentication extension

1   Scope

This amendment contains extensions to Rec. ITU-T M.3016.1 (2005).

2   Additions

Add new clauses 6.1.3 and 6.1.4

6.1.3   Authentication availability

At a fault event, the authentication system and all network services, including security services, become unavailable even though all other NE/MS are alive.

REQ 61: The NE/MS should support **Authentication** availability with proper redundancies.

This provides users with unceasing services even in the event of a fault, and can be achieved by applying dual (or multiple) authentication servers that can be operated in an active-active or active-standby mode. With an active-active configuration, load balancing between authentication servers is also possible, providing fault prevention. When a fault occurs in the primary authentication server, all pending authentication requests should be forwarded to the secondary authentication server. This is commonly referred to as fail-over. After the failed server has recovered, a switch-back procedure should also be supported, which can be performed automatically or manually by an operator. The servers can be located in separate networks in order to provide an unceasing authentication service in the event of a network fault, as well as of a fault of the server itself.

6.1.4   Authentication Identifier

In order to ease repeating authentication, an Authentication Identifier may be defined. An Authentication Identifier may be issued at successful authentication (e.g., by entering UserId and password). The Identifier grants rights to the user. Under certain circumstances (e.g., time period, in accordance with the security policy), the user can use the identifier to access specific resources without additional authentication. The Authentication Identifier can also be used for event logging or event retrieval for administrative purposes.

REQ 62: The NE/MS may provide an Authentication Identifier to grant rights to the user at successful authentication. The right assigned is according to the security policy. The Authentication Identifier can also be used in logging or retrievals for administrative purposes.

Add 2 new rows to the end of the table in Annex A

Annex A

ITU-T M.3016.1 security requirements	ITU-T M.3016.2 security services	ITU-T M.3016.3 security mechanisms
REQ 61: The NE/MS should support **Authentication** availability with proper redundancies.	**SER 1, SER 2, SER 3**	**MEC 43**
REQ 62: The NE/MS may provide an Authentication Identifier to grant rights to the user at successful authentication. The right assigned is according to the security policy. The Authentication Identifier can also be used in logging or retrievals for administrative purposes.	**SER 1, SER 2, SER 3**	**MEC 13**

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