International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3016.2

(04/2005)

SERIES M: TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Telecommunications management network

Security for the management plane: Security services

ITU-T Recommendation M.3016.2

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.3016.2

Security for the management plane: Security services

Summary

This Recommendation identifies the security services for the management plane in Telecommunication management. It 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.3016.2 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.

CONTENTS

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 services to allow vendors, agencies, and service providers to implement a secure Telecommunications management infrastructure. Although the present set of security services and mechanisms represent 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 services and 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-T Rec. M.3016.0 – *Security for the management plane: Overview*.

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

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

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

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

ITU-T Recommendation M.3016.2

Security for the management plane: Security services

1 Scope

ITU-T Recs M.3016.1, M.3016.2 and 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, 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 services requirements for the management plane in Telecommunication management. It 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 requirements for a specific Telecommunications Management Network (TMN) interface.

This Recommendation does not define the security requirements or the security mechanisms for supporting the security services requirements.

This Recommendation is part of the M.3016.x series of Recommendations. Security requirements, mechanisms, and profile proformas are specified in other parts of the M.3016.x series.

The Proforma defined in ITU-T Rec. M.3016.4 is provided to assist the organizations, administrations and other national/international organizations, specify 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 E.408 (2004), *Telecommunication networks security requirements*.

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

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

3 Definitions

This Recommendation uses the following terms from ITU-T Rec. X.800:

– access control;
– authentication;
– confidentiality;
– data integrity;
– non-repudiation.

4 Abbreviations

This Recommendation uses the following abbreviations:

MS Management System
NE Network Element
OAM&P Operations, Administration, Maintenance and Provisioning
OSI Open System Interconnection
TMN Telecommunications Management Network

5 Conventions

In the 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 a three-letter label followed by a number:

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

6 Security services

Figure 1 describes the relationships between Security objectives, Threats, Risks, Security requirements, and Services. It describes the process how to derive "Security requirements" from "Threats" and "Security objectives" which in turn will be realized by a set of security services. These "Services", which counteract threats, will make use of "Mechanisms" which themselves make use of "Security algorithms".

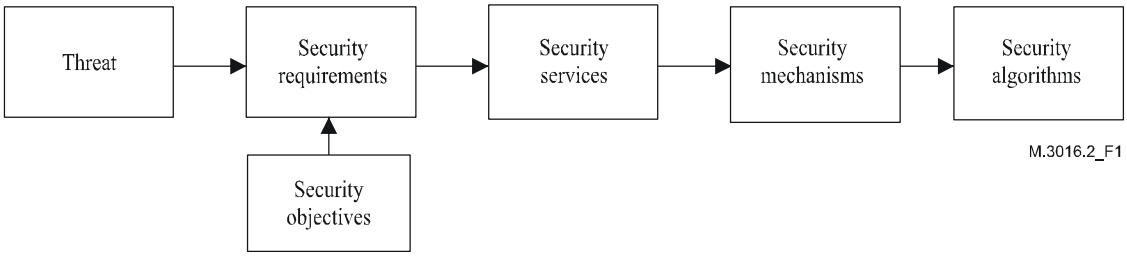

Figure 1/M.3016.2 – Security framework

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, this Recommendation (ITU-T Rec. M.3016.2) discusses the Security Services, and 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.3016.2 – Mapping of security requirements and security services

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

Table 2 outlines the organization of this clause:

Table 2/M.3016.2 – Organization of clause 6

Clause	Contents
6.1	Discusses authentication services including user authentication, peer entity authentication, and data origin authentication.
6.2	Discusses access control service.
6.3	Discusses data confidentiality service.
6.4	Discusses data integrity service.
6.5	Discusses non-repudiation service.
6.6	Discusses audit trail service.
6.7	Discusses security alarm service.

6.1 Authentication

A TMN should provide capabilities to establish and verify the claimed identity of any actor in the TMN.

Actors can be human users or entities within the TMN. Verified identities provide the basis of accountability and are fundamental in meeting most of the security requirements listed in this clause.

The security service to support the requirement is **authentication**. The authentication service delivers proof that the identity of an object or subject has indeed the identity it claims to have. Depending on the type of actor and on the purpose of identification, the following kinds of authentication may be required:

– user authentication, establishing proof of the identity of the human user or application process;
– peer entity authentication, establishing the proof of the identity of the peer entity during a communication relationship;
– data origin authentication, establishing the proof of identity responsible for a specific data unit.

Usage of an authentication service establishes the proof for a particular instance of time. To ensure continued proof, the authentication has to be repeated or linked to an integrity service.

Examples of mechanisms used to implement the authentication service are passwords and Personal Identification Numbers (PINs) (simple authentication) and cryptographic-based methods (strong authentication).

Authentication has two purposes in securing the **Management Plane**:

1) It ensures the identity of the communicating parties, providing a basis for setting up private communications with full data integrity and confidentiality between two systems; and
2) It provides a basic mechanism for logging events into a management system and/or auditing the management activities on any system.

The following layers can provide this service (according to ITU-T Rec. X.800):

– Network layer (corroboration of the identity of transport layer peers);
– Transport layer (corroboration of the identity of session layer peers);
– Application layer (corroboration of the identity of application processes);
– outside OSI: in the application process itself.

Considering that the requirement for the TMN will be to identify and authenticate managers and agents and the link of authentication with access control, recommended positions with respect to the OSI stack are the application layer and the application process.

6.1.1 User authentication

User Authentication concerns the **Authentication** of clients involved in the management of the network. In this case, **Authentication** proves the identity of the legitimate user and prevents masquerading attacks by illegitimate users. With proper **Authentication**, it is possible to track activities and restrict users to pre-authorized activities or roles.

SER 1: Each NE/MS providing user access should support a strong authentication service for proof of identity.

It should be noted that this Recommendation does not require a single sign-on service, but one may be provided in a future Recommendation. However, if one is established, the protocol must still challenge the entity(s) for credentials. A user may not have to enter the credentials if they are securely cached in some way (e.g., a Kerberos mechanism).

6.1.2 Peer entity authentication

Peer entity authentication concerns the **Authentication** of the peer entity during communication between entities, such as applications, systems or devices. The **Authentication** proves the identity of the peer and prevents masquerading attacks by illegitimate devices.

Peer entity **Authentication** provides **Authentication** during data communications between systems (e.g., system-to-system, application-to-application), and is the basis for setting up private communications with full data integrity. During data communications, **Authentication** of the sending entity allows the receiver of a message to ascertain the origin of the message. Within a secure communication channel, cryptographic **Authentication** should be associated with each message to bind the sending entity's identity to the message. The receiver will check the cryptographic information supplied with the message to verify the true identity of the sending entity.

SER 2: Each NE/MS providing data communications between systems should support peer entity **Authentication** for communications, and should use X.509 certificate-based systems for **Authentication** or **Protected Authentication**.

6.1.3 Data origin authentication

Data origin **Authentication** concerns establishing the proof of identity of a system entity that is claimed to be the original source of received data. This **Authentication** provides the substantiating of the source of data is as claimed. This service is usually bundled with a data integrity service. This service is independent of any association between the originator and the recipient, and the data in question may have originated at any time in the past.

SER 3: Each NE/MS providing the identity of a system entity with the substantiation of the source of data should support the data origin **Authentication** service.

6.2 Access control

A TMN should provide capabilities to ensure that actors are prevented from gaining access to information or resources that they are not authorized to access.

The security service to meet this requirement is **access control**. The access control service provides means to ensure that subjects access resources only in an authorized manner. There may be re-authentication required due to idle timeouts, or password change requirements. Resources concerned may be the physical system, the system software, applications and data. The access control service can be defined and implemented at different levels of granularity in the TMN: at agent level, object level or attribute level.

The limitations of access are laid out in access control information, which specify:

- the means to determine which entities are authorized to have access;
- what kind of access is allowed (reading, writing, modifying, creating, deleting);
- the means to associate the dimension of time with the authenticated entities and the tokens they use for authentication.

More specific TMN access control can be divided into three types:

- *Management association access control*

  This service enables access control at the management association level, meaning that the access rights are related to the association itself, i.e., the right to establish the association.

- *Management notification access control*

  This service enables access control with respect to notifications, i.e., to ensure that notifications are only disclosed to entities authorized to receive them.

- *Managed resource access control*

  This service provides access control with respect to the resources themselves.

The identity of the entity trying to gain access needs to be checked before access to the resource is granted. This means that usage of access control is always linked to the usage of an authentication service.

SER 4: Each NE/MS should support access control services for management association, management notification, and management resource access control.

6.3 Data confidentiality

A TMN should provide capabilities to ensure the confidentiality of stored and communicated data.

The security services to support the requirement are: **access control** for stored data and **data confidentiality** for communicated data.

The confidentiality service provides protection against unauthorized disclosure of exchanged data. The following kinds of confidentiality services are distinguished:

– *Selective field confidentiality*

  This service can be used in the Application layer or in the application process itself, since it is the application process, which can discriminate between fields.

– *Connection and connectionless confidentiality*

  Considering that end-to-end confidentiality is needed, which excludes the Physical layer and the Data link layer, confidentiality can be provided at the Network layer, the Transport layer, the Presentation layer, the Application layer or in the application process.

SER 5: Each NE/MS should support a data confidentiality service to protect against unauthorized disclosure of connection oriented or connectionless data exchanges and provide confidentiality on selected fields.

6.4 Data integrity

A TMN should be able to guarantee the integrity of stored and communicated data.

The security services to support the requirement are: **access control** for stored data and **data integrity** for communicated data.

The integrity service provides means to ensure the correctness of exchanged data, protecting against modification, deletion, creation (insertion) and replay of exchanged data. The following kinds of integrity services are distinguished:

– selective field integrity;

– connection integrity without recovery;

– connection integrity with recovery.

The data integrity service requires the use of a secret value known only to communicating parties. Several protocols use the secret value to create an HMAC-MD5 digest, and this digest is added to each message.

SER 6: Each NE/MS should support a data integrity service to protect against modification, deletion, insertion and replay of exchanged data.

6.5 Non-repudiation

A TMN should provide the capability that an entity cannot deny the responsibility for any of its performed actions as well as their effects.

The requirement is supported by the **non-repudiation** service binding the individual (or entity) to the operation performed. The non-repudiation services provide means to prove that exchange of data actually took place. It comes in two forms:

– non-repudiation: proof of origin;

– non-repudiation: proof of delivery.

The appropriate combinations of the authentication, access control and audit trail services may be used to achieve another more general realization of non-repudiation.

SER 7: Each NE/MS should support a non-repudiation service to ensure that no entity can deny responsibility for their actions and the effects of those actions.

6.6 Audit trail

A TMN should provide the capability of storing information about activities on the system with the possibility of tracing this information to individuals or entities. Also a TMN should provide the capability to analyze logged data on security relevant events in order to check them for violations of the security policy.

A log is a repository for records: it is the OSI abstraction of logging resources in real open systems. Records contain the information that is logged.

For the purpose of many management functions, it is necessary to be able to preserve information about events that have occurred, or operations that have been performed or attempted by, or on, various resources.

Furthermore, when such information is retrieved from a log, the manager must be able to determine whether any records were lost or whether the characteristics of the records stored in the log were modified at any time.

An audit should be seen as an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with the established security policy and operational procedures and to detect breaches in security. The result of the Audit would identify changes in control, policy and procedures.

It is important that each NE/MS provide adequate capabilities to allow investigation, audit, and real-time detection and analysis activities, so that proper remedial actions can be taken. This clause considers security audit logs; however, the specific details of the content and format of the security audit logs are beyond the scope of this Recommendation.

Note that investigation and forensic analysis activities may include investigation of non-security related OAM&P messages as well as the information stored in the security audit logs described in this clause. Logging of non-security related OAM&P messages, sometimes referred to as "recent change" messages, is required for any actions that are auditable.

SER 8: NE/MS should be able to log any action that changes the security attributes and services, access controls, configuration parameters of the devices, and each login attempt and its result that caused invocation of the system inactivity timer, and any action, which requires auditing. Each NE/MS should support the ability to audit these logs.

It is recommended that audit log entries be sent to an unalterable audit server after being sequence labelled and cryptographically authenticated (signed) by the NE/MS.

6.7 Alarm reporting

A TMN should provide the capability to generate alarm notifications on selected events. The user should be able to define the selection criteria.

The security audit control function is a systems management function describing the notification for collection of security events. The security alarm notification defined by this systems management function provides information regarding the operational condition pertaining to security.

SER 9: Each NE/MS should support an alarm notification service to alert security administrators about operational conditions pertaining to security.

6.8 Packet inspection

A TMN should provide the capability to inspect packets for packet-based traffic destined to the management plane of any TMN device. The user should be able to define the filtering based on the source and destination network addresses, the protocol and the source and destination ports of a packet.

Packet inspection is the process of examining the header values of each packet that passes through a network element based on specified match criteria. There could be an action taken based on the results of the packet inspection.

SER 10: Each NE/MS should support a packet inspection service to protect the management plane of the TMN from all traffic that does meet the security policy.

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	Telephone transmission quality, telephone installations, local line networks
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, 2005