Introduction of ITU-T SG2 related work on security management & User identity and access management for TMN

Fanqin Zhou
BUPT, China

ITU-T SG2 work on security management

◆ TMN in SG2 (SG4 before 2008)

■ TMN - Telecommunications Management Network

- ✓ **a protocol model** defined for managing open systems in a communications network. It is part of the ITU-T Recommendation series M.3000 and is based on the OSI management specifications in ITU-T Recommendation series X.700.
- ✓ TMN provides **a framework** for achieving interconnectivity and communication across heterogeneous operations system and telecommunication networks.
- ✓ TMN defines **a set of interface points** for elements which perform the actual communications processing to be accessed by elements, such as management workstations, to monitor and control them, allowing elements from different manufacturers to be incorporated into a network under a single management control.

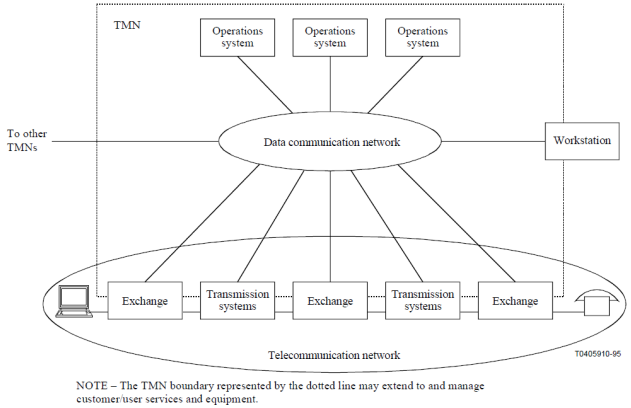


Fig.▲ General relationship of a TMN to a telcom Network [ITU-T M.3010].

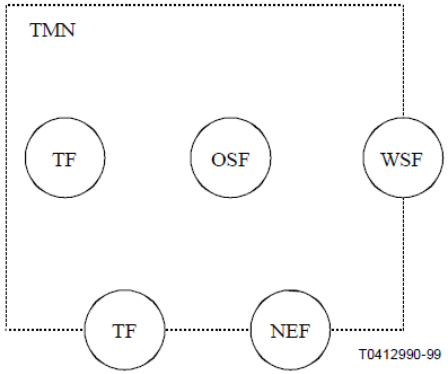


Fig.▲ TMN function blocks [ITU-T M.3010].

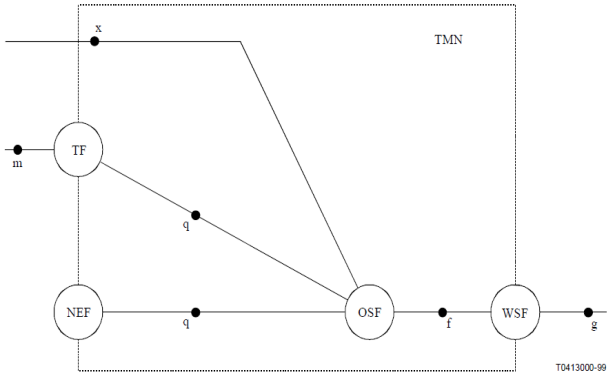


Fig.▲ Classes of reference points in the TMN [ITU-T M.3010].

[ITU-T M.3010] ITU-T M.3010 (2000), Principles for a telecommunications management network .

ITU-T SG2 work on security management

北京郵電大學 Beijing University of Posts and Telecommunications

◆ FCAPS in TMN

- **There are 5 function sets (FS) in TMN, shortened as FCAPS (M.3400)**
  - ✓ **Fault management**: a set of functions which enables the detection, isolation and correction of abnormal operation of the network and its environment.
  - ✓ **Configuration management**: functions to exercise control over, identify, collect data from and provide data to NEs.
  - ✓ **Accounting Management**: enables the measurement of the use of network services and the determination of costs to the service provider and charges to the customer for such use.
  - ✓ **Performance management**: provides functions to evaluate and report upon the behaviour of telecommunication equipment and the effectiveness of the network or network element.
  - ✓ **Security management**: provides for the management of security, including the following function sets (FS):
    - **Prevention**: FS to prevent intrusion.
    - **Detection**: FS to detect an intrusion.
    - **Containment** and **Recovery**: FS to deny access to an intruder, to repair damage done by an intruder, and to recover losses.
    - **Security Administration**: FS for planning and administering security policy and managing security related information.

[ITU-T M.3400] ITU-T M.340 (2000), TMN management functions.

ITU-T SG2 work on security management

北京郵電大學 Beijing University of Posts and Telecommunications

◆ In SG2, the following Recs. are related to security mgmt.

Aspects	Rec. number	Recommendation Title
Security for Management plan	M.3016.0	Security for the management plane: **Overview**
	M.3016.1	Security for the management plane: Security **requirements**
	M.3016.2	Security for the management plane: Security **services**
	M.3016.3	Security for the management plane: Security **mechanism**
	M.3016.4	Security for the management plane: **Profile proforma**
Security mgmt. services	M.3210.1	**TMN management services** for IMT-2000 **security** management
Security mgmt. systems	M.3410	Guidelines and requirements for **security management systems** to support telecommunications management

- SG2 does **not** create new security services or mechanisms, only reuses those that are defined by SG17 or the industry.
- But SG2 has its own requirements and systems on security mgmt.

- Currently, there is a new work item related to security mgmt:
  - ✓ **M.Uiamr**: "User Identity and Access Management Requirements for Telecommunications Management Network"

Work Item M.uiamr Introduction

北京郵電大學 Beijing University of Posts and Telecommunications

◆ Background and Motivation

- TMN needs enhancement in identity and access management
  - ✓ TMN is responsible for the management of telecom networks and consists of a large variety of management functional entities.
  - ✓ In the past, when the network management system was relatively centralized and management tasks and objects were limited; there are not specially designed IAM framework for TMN.
  - ✓ With the emergence of new network features, such as distributed core network, management capability exposure, smart agent-based intelligent network management, more strict but flexible identity and access management approaches are on demand.
- Identity and access management in general IT systems
  - ✓ IAM has been an important aspect of IT system management functions
  - ✓ ITU and ISO/IEC have carried out standardization research on IAM for general IT systems to varying degrees, such as concept, functional framework, use cases and key technologies [ITU-T X.1257, X509, ISO/IEC 24760 series, ISO/IEC 29164].
  - ✓ There are also some specifications on IAM system for specialized IT systems, such as massive IoT in industry [IEEE P2958]
  - ✓ However, there are not specific IAM framework for TMN discussed.

Work Item M.uiamr Introduction

北京郵電大學 Beijing University of Posts and Telecommunications

◆ Background and Motivation

■ Necessity of IAM for TMN

- ✓ IAM for TMN is to manage user access to entities in telecom management network to ensure that **only verified users can access the entities** with the correct level of accessibility based on the entities' identifications and other context information.
- ✓ Telecom management involves a variety of objects, e.g., massive managed network elements, and management systems from different suppliers in different network domains and geographic areas.
- ✓ TMN has to deal with the complex user and role management challenges brought about by distributed core network, management capabilities exposure, and support for REST-based management protocol, it has formed user and access management requirements that are different from general IT systems.
- ✓ In the process of user identity and access management system, it is necessary to have a clearer definition and uniform understanding of IAM requirements for TMN to guide the real-world management system.

This requires sorting out the IAM requirements for TMN through standardization research.

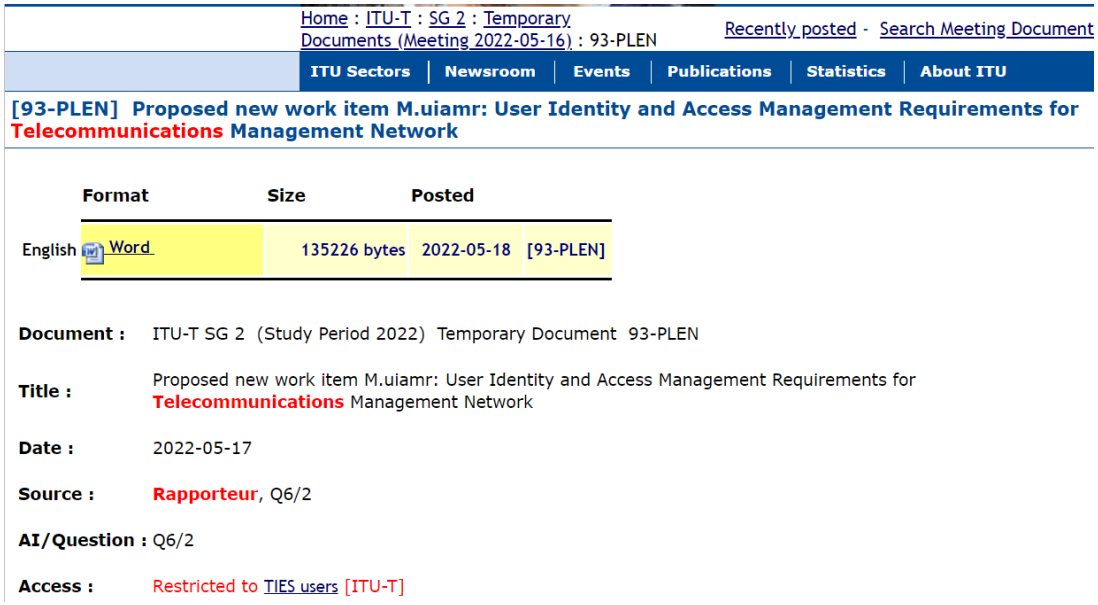
Work Item M.uiamr Introduction

北京郵電大學 Beijing University of Posts and Telecommunications

◆ M.uiamr overview

M.Uiamr - "User Identity and Access Management Requirements for Telecommunications Management Network"

- It describes user identity and access management requirements for telecommunications management network,
- specifies the general structural and functional requirements of the user identity and access management for TMN, as well as several use cases.



Home : ITU-T : SG 2 : Temporary Documents (Meeting 2022-05-16) : 93-PLEN

Recently posted - Search Meeting Document

ITU Sectors | Newsroom | Events | Publications | Statistics | About ITU

[93-PLEN] Proposed new work item M.uiamr: User Identity and Access Management Requirements for Telecommunications Management Network

	Format	Size	Posted	
English	Word	135226 bytes	2022-05-18	[93-PLEN]

Document : ITU-T SG 2 (Study Period 2022) Temporary Document 93-PLEN

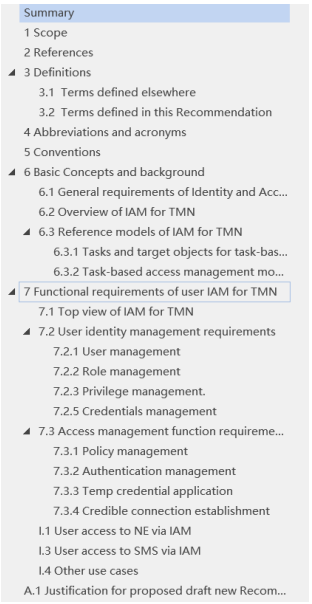
Title : Proposed new work item M.uiamr: User Identity and Access Management Requirements for Telecommunications Management Network

Date : 2022-05-17

Source : Rapporteur, Q6/2

AI/Question : Q6/2

Access : Restricted to TIES users [ITU-T]



Summary
1 Scope
2 References
3 Definitions
3.1 Terms defined elsewhere
3.2 Terms defined in this Recommendation
4 Abbreviations and acronyms
5 Conventions
6 Basic Concepts and background
6.1 General requirements of Identity and Acc...
6.2 Overview of IAM for TMN
6.3 Reference models of IAM for TMN
6.3.1 Tasks and target objects for task-bas...
6.3.2 Task-based access management mo...
7 Functional requirements of user IAM for TMN
7.1 Top view of IAM for TMN
7.2 User identity management requirements
7.2.1 User management
7.2.2 Role management
7.2.3 Privilege management.
7.2.5 Credentials management
7.3 Access management function requireme...
7.3.1 Policy management
7.3.2 Authentication management
7.3.3 Temp credential application
7.3.4 Credible connection establishment
I.1 User access to NE via IAM
I.3 User access to SMS via IAM
I.4 Other use cases
A.1 Justification for proposed draft new Recom...

Work Item - M. uiamr

北京郵電大學 Beijing University of Posts and Telecommunications

◆ Overview of IAM for TMN

■ General requirements of Identity and Access Management for TMN

To support telecom operation management for security assurance, **IAM for TMN** may satisfy the following requirements:

- ✓ compatible with TMN security management plane and security management system standards
- ✓ supports an integrated framework, which can be applied to current and future networks. It can also manage access to multiple different management domains.
- ✓ supports the exposure of authentication function to different entities
- ✓ supports exploiting context information of subject
- ✓ supports the authentication of automatic workflows derived from operations of authenticated a user.
- ✓ supports the identification of malicious access attempts.
- ✓ enables the integration of emerging IT, AI technologies for improved efficiency

Work Item - M. uiamr

北京郵電大學 Beijing University of Posts and Telecommunications

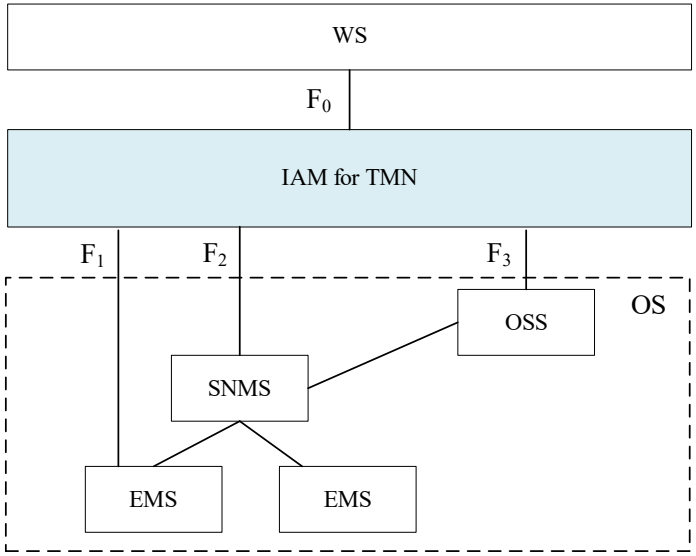
◆ Overview of IAM for TMN

■ Role of IAM for TMN

The IAM for TMN is to enable **a unified user authentication and access control gateway** for any access to the management entities (such as EMS, SNMS, OSS) in telecom management network. When IAM for TMN is enabled,

- ✓ user will interact with IAM for applying access to a target object
- ✓ only when verified, will IAM grant access permission (and approach) to the user
- ✓ IAM will **take over the complexity** in assuring credential to access a specific object with the proper authentication and access approaches the object requires
  - entities may support different authentication and access approaches. IAM' s interaction with one type of entities will be quite different from that with other types.
  - management operations usually demand different authority levels
  - When a very strict identify requirement is exerted on the access to an entity, IAM may initiate the establishment of a secure end-to-end link to implement the access.

=>new interfaces for interaction between IAM and a specific type of entity should be defined.



Work Item - M. uiamr

◆ Overview of IAM for TMN

■ Interfaces Definition

Defining interfaces for interaction between IAM and TMN entities. The considerations:

- ✓ According to Recommendation [ITU-T M.3010], the interfaces can be categorized into F interface, which represents the interaction between workstation function (WSF) to OSF in TMN.
  - ✓ refer to the interface between WS and IAM as F0
  - ✓ the interfaces to EMS, SNMS, OSS as F1, F2, and F3, respectively.

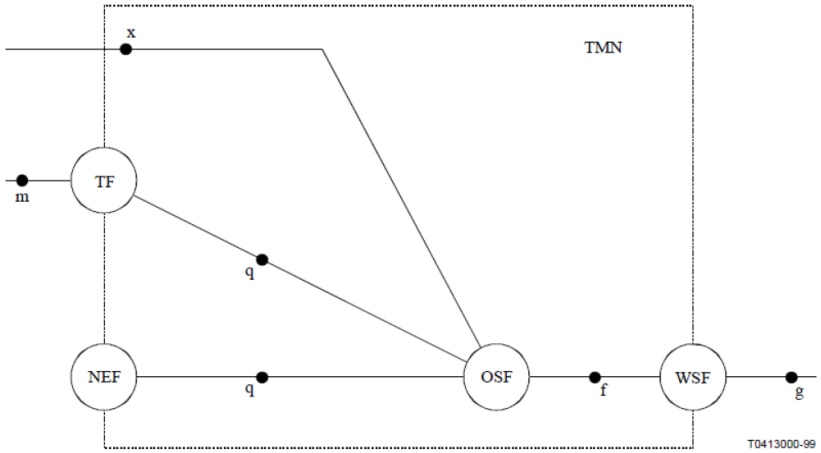
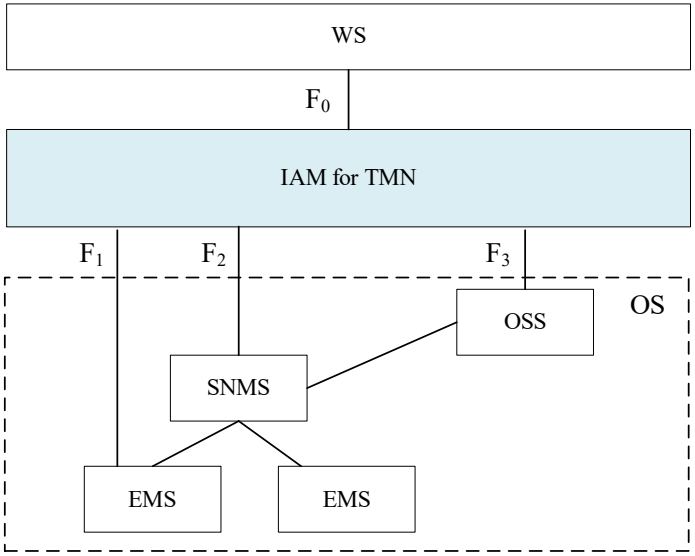


Fig.▲ Reference points in TMN [ITU-T M.3010].
The **f reference points** are located between WSF and other OSF blocks.



[ITU-T M.3010] ITU-T M.3010 (2000), Principles for a telecommunications management network .

Work Item - M. uiamr

北京郵電大學 Beijing University of Posts and Telecommunications

◆ Overview of IAM for TMN

■ Task-based access management in TMN

The tasks involved in IAM for TM mainly are the operations that will be performed by telecom network managers and maintainers (users of TMN)

- ✓ The operations, categorized in examination and adjustment, usually require different levels of privilege, and are implemented via different approaches for individual objects.
- ✓ In [ITU-T X.1257], task-based access control model is suggested to make IAM roles referenceable and traceable to the corresponding tasks throughout the IAM process lifecycle.

The task-based access control can **gain an IAM role and tasks business meanings**, so that IAM roles will not get lost or misinterpreted by applications. Following the principles in [ITU-T X.1257], tasks and target objects in TM are non-exhaustively listed below.

Business role	Task	Target object
IAM user of EMS	EMS usage operations	EMSs
IAM user of SNMS	SNMS usage operations	SNMS
IAM user of OSS	OSS usage operations	OSS
IAM manager	IAM management	Manageable user IAM functions

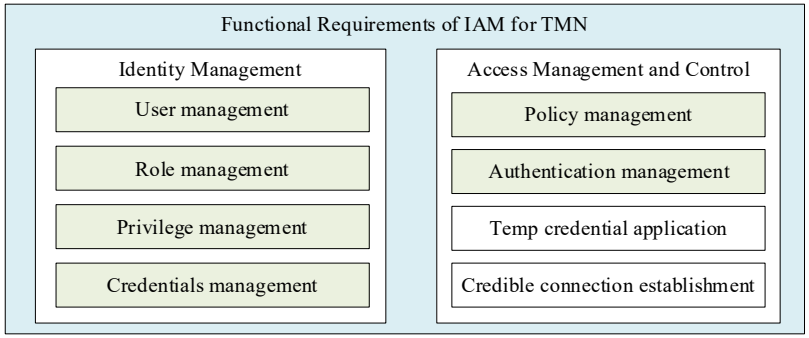
[ITU-T X.1257] ITU-T X.1257 (2016), Identity and access management taxonomy

Work Item - M. uiamr

北京郵電大學 Beijing University of Posts and Telecommunications

◆ Functional requirements of user IAM for TMN

■ Identity Management



- ✓ **User management:** addition, modification, and deletion of user accounts that are authorized to manage MEs or to use the management entities in TM
- ✓ **Role management:** a role is an identifier for a uniquely identifiable group of users. Role management can be implemented through grouping.
- ✓ **Privilege management:** management of the distribution, modification, and removal of authentication credentials, access rules, and privileges of users and roles.
- ✓ **Credentials management:** managing all authentication credentials related to subject identities for both human and non-human subjects, including the generation of new credentials.

■ Access Management and control

- ✓ **Policy management:** translation of access control policies to rules that can be communicated, interpreted, and implemented by entities and audited by the policy management function
- ✓ **Authentication management:** validation of systems or administrative users, ensuring that when a user claims to own a specific identity, the identity can be verified as truly belonging to the user.
- ✓ ***Temp credential application***: IAM will be responsible for getting correct access to the target entity. Although fixed credentials will work, temporary credentials or one-time credentials may be applied or appointed for certain access attempts
- ✓ ***Credible connection establishment***: When credible access is strictly required, IAM needs to support initiating an end-to-end secure connection to an entity for a user..

Work Item - M. uiamr

北京郵電大學 Beijing University of Posts and Telecommunications

◆ Document structure and future work

- **Scope/Reference/Definitions/Abbreviations and acronyms/Conventions.**
- **Basic Concept and Background**
  - General requirements of IAM for TMN
  - Overview of IAM for TMN
  - Reference models of IAM for TMN
- **Functional requirements of user IAM for TMN**
  - Top view of IAM for TMN
  - User identity management requirements [TBD]
  - Access management function requirements [TBD]
- **[Appendix I] Use cases of IAM for TMN** [TBD]
  - User access to NE via IAM
  - User access to SMS via IAM
  - Other use cases

北京郵電大學
Beijing University of Posts and Telecommunications

Thank you !