SLOVENSKI STANDARD
SIST EN 301 261-3 V1.2.1:2003

01-november-2003

Telekomunikacijsko upravljavno omrežje (TMN) - Varnost - 3. del: Varnostne storitve - Avtentikacija uporabnikov in osebkov v okolju TMN

Telecommunications Management Network (TMN); Security; Part 3: Security services; Authentication of users and entities in a TMN environment

Ta slovenski standard je istoveten z: EN 301 261-3 Version 1.2.1

ICS:

33.040.35 Telefonska omrežja Telephone networks

SIST EN 301 261-3 V1.2.1:2003 **en**

EN 301 261-3 V1.2.1 (1999-01)

European Standard (Telecommunications series)

Telecommunications Management Network (TMN); Security; Part 3: Security services; Authentication of users and entities in a TMN environment

Reference
DEN/TMN-00002-3 (bocr0ioo.PDF)

Keywords
TMN, security

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Telecommunications Management Network (TMN).

The present document is part 3 of a multi-part EN covering security, as identified below:

Part 1: "Framework";

Part 2: "Security support services and security management";

Part 3: "Security services; Authentication of users and entities in a TMN environment";

Part 4: "Security services; Access control".

National transposition dates	
Date of adoption of this EN:	18 December 1998
Date of latest announcement of this EN (doa):	31 March 1999
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 September 1999
Date of withdrawal of any conflicting National Standard (dow):	30 September 1999

Introduction

The authentication service ensures that the identities of the calling and called parties are indeed genuine, that is, they are who they claim they are. Authentication is a first step in establishing secure communications between the calling and called parties.

The verification of an identity can be ascertained only for the instant of the authentication exchange. To guarantee the identity of a communication party for subsequent communication data, the authentication exchange must be used combined with a secure means of communication (e.g. an integrity service).

Authentication is also a support service for many other security services such as e.g. secure exchange of secret keys between calling and called parties.

The authentication service is one of the TMN security services. A complete overview about all TMN security services and the relationships between security services will be given in a framework document.

Prerequisites for the use of the described authentication service (as well as for the use of other TMN security services) are:

- the availability of security support services (like key management etc.);
- the availability of management features for the authentication service; and
- the availability of management features for the security support services.

These prerequisites are described in separate documents.

The relationship between the present document and the GSS-API (*Generic Security Service Application Program Interface*, see IETF RFC 2078 [19]) is described in annex A.

The combined use of the present document and ITU-T Recommendation Q.813 [12] is given in annex D.

1 Scope

The present document specifies the authentication service for all kind of users involved in a TMN. Normally, one can distinguish between three types of authentication: (human) user authentication, peer-to-peer entity authentication and data origin authentication. The main scope of the present document is peer-to-peer entity authentication, even if human user authentication is also partly addressed. Data origin authentication will not be addressed as an explicit TMN authentication service for reasons described later in the present document.

The authentication service shall be realized by employing one of a set of various security mechanisms based on password and/or cryptographic means. The main focus of the present document is the description of security mechanisms for peer entity authentication even if these mechanisms may also be applicable for human user authentication. Authentication mechanisms, that may be applicable only for human user authentication, are outside the scope of the present document.

The content of the present document is applicable to communication between any two TMN system entities (e.g. Operations System (OS) and Network Element (NE)) that communicates via a TMN Q3-or an X-interface. The present document addresses peer-to-peer entity authentication at the OSI application layer (layer 7) through the use of ACSE. It does not attempt to cover authentication schemes that may be appropriate for lower OSI layers or other protocol stacks. This does not necessarily restrict the usability of the described authentication services (or part of them) at lower OSI layers or with other protocol stacks.

To the extent that human user authentication is covered, it will be related to the TMN F-interface.

The present document does **not** describe the relationships between authentication service and other security services, the features for managing the authentication service and the authentication support services.

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

[1] ITU-T Recommendation X.509 | ISO 9594-8: "Information technology - Open Systems Interconnection - The Directory: Authentication framework".

[2] ITU-T Recommendation X.511 | ISO 9594-3: "Information technology - Open Systems Interconnection -The Directory: Abstract service definition".

[3] ISO/IEC 9798-1: "Information technology - Security techniques -Entity authentication mechanisms - Part 1: General".

[4] ISO/IEC 9798-2: "Information technology - Security techniques -Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms".

[5] ISO/IEC 9798-3: "Information technology - Security techniques - Entity authentication mechanisms - Part 3: Entity authentication using a public key algorithm".

[6] ITU-T Recommendation X.227 | ISO/IEC 8650-1: "Information technology - Open Systems Interconnection – Connection-oriented protocol for the association control service element: Protocol specification".

[7] ITU-T Recommendation X.227 AM1 | ISO/IEC 8650 AM1:Series X: "Incorporation of extensibility markers".

[8] ITU-T Recommendation X.702 | ISO 11587: "Information technology - Open Systems Interconnection - Application context for systems management with transaction processing".

[9] ITU-T Recommendation X.501: "Information technology - Open Systems Interconnection - The Directory: Models".

[10] ISO/IEC 9797: "Information technology, Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm".

[11] ISO/IEC 10183-3: "Hash Functions - Part 3: Dedicated Hash Functions".

[12] ITU-T Recommendation Q.813: "Security Transformations Application Service Element for Remote Operations Service Element (STASE-ROSE)".

NOTE: ITU-T Recommendation Q.813 will be published shortly.

2.2 Informative references

[13] NMF Application Services - Security of Management, Issue 1, 9/92.

[14] IETF RFC 1321: "The MD5 Message Digest Algorithm".

[15] FIPSPUB 188: "Standard Security Label for Information Transfer".

[16] FIPS PUB 46-2: "Data Encryption Standard (DES)".

[17] FIPS PUB 186: "Digital Signature Standard (DSA)".

[18] ATM Forum: "ATM Security Specification Version 1.0, STR-SEC-01.01 (Straw Ballot)".

[19] IETF RFC 2078: "Generic Security Service Application Program Interface Version 2".

[20] IETF RFC 2025: "The Simple Public-key GSS-API Mechanism (SPKM)".

[21] IETF RFC 1964: "The Kerberos Version 5 GSS-API Mechanism".

[22] Lai On the design and security of block ciphers, ETH Series in Information Processing, J.L.Massey (editor), vol. 1, Hartung-Gorre Verlag Konstanz, ETH Zurich, 1992.

[23] Public Key Cryptography Standard #1 (PKCS #1): "RSA Encryption Standard, RSA Laboratories, Version 1.5".

[24] IETF RFC 2104 HMAC: "Keyed-Hashing for Message Authentication", 2/1997.

3 Definitions and abbreviations

3.1 Definitions

The following terms are defined in ITU-T Recommendation X.509 | ISO 9594-8 [1]:

authentication token, token: see [1].

certificate, user certificate: see [1].

certification authority: see [1].

cryptosystem, cryptographic system: see [1].

hash function: see [1].

one-way function: see [1].

public key: see [1].

private key, secret key: see [1].

simple authentication: see [1].

strong authentication: see [1].

trust: see [1].

The following terms are defined in ISO/IEC 9798-1 [3]:

authentication initiator: see [3].

authentication responder: see [3].

claimant: see [3].

exchange authentication information: see [3].

time variant parameter: see [3].

token: see [3].

trusted third party: see [3].

verification authentication information: see [3].

verifier: see [3].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACSE	Association Control Service Element
ATM	Asynchronous Transfer Mode
CMIP	Common Management Information Protocol
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
EN	European Standard (Telecommunications series)
FIPS	Federal Information Processing Standard
FTAM	File Transfer Access Method
GSS-API	Generic Security Service Application Programming Interface

HMAC	Hashed Message Authentication Code
IDEA	International Data Encryption Algorithm
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunication Union
MD5	Message Digest Algorithm No. 5
MF	Mediation Function
NE	Network Element
NMF	Network Management Forum
OS	Operations System
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PKCS	Public Key Cryptography Standard
PUB	Publication
RACE	Research and Development Program for Advanced Communications in Europe
RFC	Request for Comments
ROSE	Remote Operations Service Element
RSA	Rivest, Shamir, Aleman (Algorithm)
SHA	Secure Hash Algorithm
STASE	Security Transformation Application Service Element
TMN	Telecommunications Management Network
WSF	Workstation Function

4 Architectural aspects

The authentication service can be used for intradomain and interdomain TMN (for details see part 1 of " Security for TMN"). The authentication service has two facets:

- generate an authentication token and to transmit it to another communication partner (claimant facet);
- verify an authentication token forwarded by a communication partner (verifier facet).

4.1 General authentication model

As described in [3], the general authentication model involves a calling party, a called party and, if necessary, an authentication party.

If a calling party or a called party interact with an authentication party, then they shall trust the authentication party. The authentication party is a function that can be for example realized as a domain-internal unit (often called Certification Authority) or as part of a TTP (that could be used to settle legal disputes between different domains or legal parties).

The authentication party should only be used for the following tasks:

- generation of (some) authentication information; and/or
- verification of (some) authentication information.

The authentication party should not be used for the (direct) communication of the authentication token between calling and called party.

It is not essential that the authentication party and all the communication exchanges are present in every authentication mechanism. In figure 1, the lines indicate potential information flow. The calling respective called party may either directly or indirectly interact with the authentication party, or use some information issued by the authentication party.