

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study on Media Security in TISPAN NGN

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/7b018fb0-e33d-4f3c-baba-7e099ecc1a51/etsi-tr-187-007-v2.1.1-2008-08>



ReferenceDTR/TISPAN-07021-NGN-R2

Keywordsmultimedia, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - 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

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2008.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM, **TIPHON**TM, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intellectual Property Rights	4
Foreword.....	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	6
3 Definitions and abbreviations.....	7
3.1 Definitions.....	7
3.2 Abbreviations	7
4 General Overview.....	7
5 Media security regulatory considerations.....	9
5.1 Analysis.....	9
5.2 Lawful Interception and data retention.....	9
5.3 Requirements.....	10
6 Viability of media security provision	10
6.1 General requirements	10
6.2 Existing NGN capabilities.....	10
6.3 End to end encryption provision.....	11
6.4 End to middle encryption provision	11
6.4.1 Advantages	11
6.4.2 Disadvantages	11
6.5 Cryptographic media protection.....	11
6.6 Summary of requirements.....	12
6.6.1 NGN.....	12
6.6.2 NGCN.....	12
7 NGN media transfer architecture for security analysis	12
7.1 Functional model.....	12
7.2 Points of attack in NGN media architecture.....	13
7.2.1 Direct attack.....	13
7.2.2 Indirect attack	13
8 Media security solution	13
8.1 General	13
8.2 Cryptographic algorithm considerations	13
8.3 Cryptographic key management.....	14
Annex A: User to user media scenarios.....	15
A.1 SIP Session Establishment without Media Security.....	15
A.2 Media Security based on Secure Signalling Path.....	16
A.3 Media Security based on Key Management Protocol in Signalling Path.....	16
A.4 Media Security based on Media Path Keying Technique.....	17
A.5 Mixed Signalling and Media Path Keying Technique	18
Annex B: Bibliography	19
History	20

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 ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

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 ETSI 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 Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/7b018fb0-e33d-4f3c-baba-7e099ecc1a51/etsi-tr-187-007-v2.1.1-2008-08>

1 Scope

The present document reports on the feasibility of providing media security for TISPAN NGN Release 2 as defined by TR 180 002 [i.2]. Media security in the present document refers to the capability to securely transport interactive and non-interactive voice, video (including conferencing scenarios), and other multimedia data (including text based) in the user plane of a Next Generation Network (NGN).

The present document provides the results of an analysis of the stage 1 definition of media security requirements and service capabilities; and presents the analysis in support of these requirements for each of simplex and duplex communication in both point-to-point and point-to-multipoint architectures. The scenarios analysed are also considered with respect to the regulatory environment of NGN.

The present document presents, in clause 7, a series of stage 2 architectural models that may implement the stage 1 model for each of the NGN media deployment scenarios.

The present document provides in clause 8 some guidance for stage 3 design of security protocol(s) for media security.

NOTE 1: Media Security for IMS is not covered by the present document but is addressed by 3GPP TR 33.828 [i.17].

NOTE 2: Whilst the present document is a technical report it identifies requirements for future work. In all cases these requirements are considered indicative pending their ratification in formal ETSI Technical Specifications within the TISPAN Work Programme.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
 - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
 - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- [i.1] ITU-T Recommendation F.703: "Multimedia conversational services".
- [i.2] ETSI TR 180 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Release 2 definition".
- [i.3] ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".
- [i.4] Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
- [i.5] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".
- [i.6] ETSI ES 282 001 (Release 2): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".
- [i.7] ETSI EG 202 238: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Evaluation criteria for cryptographic algorithms".
- [i.8] ETSI SR 002 211 (V1.1.1): "List of standards and/or specifications for electronic communications networks, services and associated facilities and services; in accordance with Article 17 of Directive 2002/21/EC".
- [i.9] Wassenaar agreement: <http://www.wassenaar.org/>.
- [i.10] IETF RFC 3830 (2004): "MIKEY: Multimedia Internet KEYing".
- [i.11] IETF RFC 4566 (2006): "SDP: Session Description Protocol".
- [i.12] IETF RFC 4567 (2006): "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)".
- [i.13] IETF RFC 4568 (2006): "Session Description Protocol (SDP) Security Descriptions for Media Streams".
- [i.14] IETF draft-zimmermann-avt-zrtp-04 (2007): "ZRTP: Media Path Key Agreement for Secure RTP".
- [i.15] IETF draft-fischl-sipping-media-dtls-03.txt (2007): "Datagram Transport Layer Security (DTLS) Protocol for Protection of Media Traffic Established with the Session Initiation Protocol".
- [i.16] IETF draft-ietf-avt-dtls-srtp-00.txt (2007): "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP)".
- [i.17] 3GPP TR 33.828: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IMS media plane security".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 180 000 [i.3] and the following apply:

media security: collective term for provision of security aspects of confidentiality, integrity, authenticity to the transfer of media across a network

NOTE 1: In the NGN media security relates to the protection of interactive voice/video phone/conferencing on an IP transport plane.

NOTE 2: Multimedia services are those in the scope of ITU-T Recommendation F.703 [i.1]. In particular, such conversational services are between two communicating entities where the multimedia service provides real-time transmission of voice, including optionally conferencing with transmission of video and/or text and/or graphics and/or still pictures.

3.2 Abbreviations

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

3GPP	3rd Generation Partnership Project
AVP	Audio Video Profile
DES	Data Encryption Standard
DTLS	Datagram Transport Layer Security
IMS	IP Multimedia Subsystem
ISDN	Integrated Services Digital Network
MAC	Message Authentication Code
MKI	Master Key Identifier
NGCN	Next Generation Corporate Network
NGN	Next Generation Network
PSTN	Public Switched Telephone Network
RAN	Radio Access Network
RTP	Real-Time Transport Protocol
SA	Security Association
SAVP	Secure Audio Video Profile
SDES	Secure DEScription
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SIPS	Session Initiation Protocol Secure
SRTP	Secure Real-time Transport Protocol
TEK	Traffic Encryption Key
UA	User Agent

4 General Overview

In the PSTN security provisions were mostly physical as the access to the line in order to eavesdrop on traffic, or to inject and modify signalling, was presumed difficult, furthermore as the terminal devices were dumb (i.e. did not make any processing decisions) it was straightforward to partition trusted and untrusted areas of the network. Development of the PSTN has moved the boundary of the trusted domain to the network termination point and does not include the terminal itself.

In the NGN however the assumptions have changed. It is assumed in the NGN that eavesdropping of traffic is possible, and that as terminal devices have intelligence (i.e. processing power and state manipulation capability) that injection and modification of signalling is possible by manipulation at the end-points. The environment of the NGN as a PSTN (Public Services Telecommunications Network as opposed to Public Switched Telephone Network) requires that in most deployed regions that care is taken to ensure privacy of the end user. This implies giving some level of assurance that transmitted data remains confidential, and that data transmitted is faithfully reproduced.

The NGN, in common with ISDN, provides logical separation of signalling and traffic. The NGN, unlike ISDN, does not provide physical separation of signalling and traffic. For the purposes of the present document it is assumed that signalling is protected using mechanisms provided by SIP and/or the IMS. A review of the requirements and mechanisms for protection of traffic, where traffic may take the form of any digitized (user generated) content, are presented in the present document.

NOTE: Traffic is used to refer to the general case of media distinguished from signalling, however where specific media types are protected, by example using adaptive media encoding as happens in certain forms of vocoder, the specific media is referred.

In order to review the requirements for media security, and to determine the feasibility of providing mechanisms to implement the requirements it is essential to review how media may be compromised (attacked). Whilst it is suggested in TS 102 165-1 [i.5] that there is a small class of threats/attacks there are a very large number of threat agents/attack vectors to be addressed in analysis.

An attacker might be located along:

- the media path;
- the signalling path; or
- both the media and the signalling path.

It is also reasonable to consider the capabilities of the attacker (this is in order to evaluate that likelihood of an attack using the method defined in TS 102 165-1 [i.5]). The dynamics of attackers vary and these need to be taken into account as the form of attacker influences the form of attack:

- a) active attacker;
- b) passive attacker.

The following classifications for attack can be made.

- Class I:
 - Passive attack on the signalling and the data path sufficient to reveal the content of the media traffic.
- Class II:
 - Active attack on the signalling path and passive attack on the data path to reveal the content of the media traffic.
- Class III:
 - Active attack on the signalling and the data path to reveal the content of the media traffic.
 - Provisions for media security in the NGN should be designed to have minimum impact on already deployed network entities and should be offered as optional services. However to ensure interoperability where media security services are provided they should comply to a common standard.

5 Media security regulatory considerations

5.1 Analysis

The NGN is required to operate within a regulated environment. In Europe the privacy Directive 2002/58/EC [i.4] applies and article 5 states:

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.
2. Paragraph 1 shall not affect any legally authorized recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.
3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

5.2 Lawful Interception and data retention

SR 002 211 [i.8] identifies those aspects of standardization that are required to ensure compliance with the European Framework Directive. In some instances the right to privacy can be withheld as suggested in paragraph 2 of article 5 of the privacy directive [i.4] (see clause 5.1). Provisions for the lawful interception of traffic, and for retention of signalling data are allowed exceptions as defined in Article 15(1) of the privacy directive:

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

5.3 Requirements

The obligations from the directive are placed on member states but may be met by the provision of specific capabilities in the NGN. If the requirements are to be met by the NGN these may be stated as follows.

Id	Requirement text
R-MS-REG-1	An NGN SHALL provide mechanisms to prevent eavesdropping of traffic
R-MS-REG-2	An NGN SHALL provide mechanisms to prevent unauthorized recording and storage of traffic
R-MS-REG-3	An NGN SHALL provide mechanisms to prevent unauthorized interception of traffic
R-MS-REG-4 (note)	An NGN operator should provide mechanisms to ensure the interception and handover of signalling of specific NGN users if required to by a lawful authority
R-MS-REG-5	An NGN operator should provide mechanisms to ensure the interception and handover of the content of communication of specific NGN users if required to by a lawful authority
R-MS-REG-6 (note)	An NGN operator should provide mechanisms to ensure the retention and handover of signalling of specific NGN users if required to by a lawful authority
NOTE:	This requirement is not strictly related to media but may be correlated to media provision.

The requirements derived from the regulatory environment in Europe require that the NGN provides protection of media in the following areas: Confidentiality; Integrity.

Prevention of eavesdropping can be achieved in a number of ways:

NOTE 1: For the purposes of analysis it is assumed that the eavesdropping attacker has taken some care to be both anonymous and non-intrusive.

- Broadcast media paths (e.g. radio) should be protected by encryption of media content in such a manner that the encryption key can not be recovered from examination of the media stream or by injection of signals to the media stream (known text attacks). The key used for encryption should only be known to the parties directly involved in the transfer of the media over the broadcast path.

NOTE 2: Broadcast (radio) paths may be visible to an attacker at some considerable distance from the intended path.

- Non-broadcast media paths should be constructed such that eavesdropping cannot be achieved without intrusion to the media path (e.g. by direct access to a cable (fibre-optic or other)).

Id	Requirement text
R-MS-GEN-1	An NGN SHOULD ensure that non-broadcast media paths are constructed such that eavesdropping cannot be achieved without intrusion to the media path
R-MS-GEN-2	An NGN SHOULD ensure that broadcast media paths (e.g. radio) should be protected by encryption of media content
R-MS-GEN-3	An NGN SHOULD ensure that the key used for encryption is only known to the parties directly involved in the transfer of media over the broadcast path

6 Viability of media security provision

6.1 General requirements

Provision of security for media may be provided by cryptographic or non-cryptographic means. Where media is exposed in an untrusted domain the general assumption is that attack is more likely than when media is exposed in a trusted domain. For cryptographic media protection to work encryption keys will require to be distributed and managed.

6.2 Existing NGN capabilities

Where the access network is a native 3GPP RAN all media traffic may be encrypted across the Radio Interface with keys derived during registration and authentication.