ETSI TR 187 007 V2.1.1 (2008-08)

Technical Report

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

Reference

DTR/TISPAN-07021-NGN-R2

Keywords

multimedia, 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

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 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).

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.

6.3 End to end encryption provision

End to end encryption devices may be subject to restriction under the terms of the Wassenaar agreement either in the form of the encryption device or in the effective key length. End-to-end encryption may offer some advantage in minimizing delay (depending on the form of the algorithm and the transport) but may not be allowed by regulation on a national basis to be deployed by the core network. Where the provision of end-to-end encryption includes the selection of keys and algorithms by the end points it cannot be considered as an NGN service thus shall not be provided by the NGN.

NOTE: If users choose to provide their own end-to-end encryption solution it will be a decision of each NGN to support the resultant media service.

6.4 End to middle encryption provision

The protection of traffic and signalling in most instances is from the end point (terminal) to a fixed point within the trusted network.

6.4.1 Advantages

Key material used to give assurances of identity, integrity, and confidentiality is held within the trusted domain.

6.4.2 Disadvantages

Assumes a trusted end point within the network.

NOTE: Where an NGN service provider offers services it is assumed that the service provider is trusted by the service user.

6.5 Cryptographic media protection

The characteristics of media being transferred influence the specific cryptographic media protection that can be applied. The following classifications are applied:

- User generated delay intolerant (e.g. voice, video calling).
- User generated delay tolerant (e.g. video distribution).
- Block structured delay tolerant (e.g. file transfer).

The capabilities of the traffic network may also be considered:

- Synchronous vs. asynchronous.
- Datagram vs. virtual circuit.

Also to be considered is the topography of the media connection:

- Point to point.
- Point to multi-point.
- Broadcast (point to all points).

6.6 Summary of requirements

6.6.1 NGN

Table 1 lists a number of requirements for media security in NGNs from the preceding analysis.

Table 1: Requirements for media security in the NGN

(R-MS- 1):	The NGN shall not provide support for end-to-end media security
(R-MS- 2):	The NGN shall provide support for user-to-network media security (for the following security services Confidentiality, Integrity, Authenticity of source and destination end-points)
(R-MS- 3):	The NGN shall provide support for secure media transfer in point-to-point topologies
(R-MS- 4):	The NGN shall provide support for secure media transfer in point-to-multipoint topologies
(R-MS- 5):	The NGN shall provide support for secure media transfer in broadcast topologies
(R-MS- 6):	An NGN shall provide mechanisms to prevent eavesdropping of traffic
(R-MS- 7):	An NGN shall provide mechanisms to prevent unauthorized recording and storage of traffic
(R-MS- 8):	An NGN shall provide mechanisms to prevent unauthorized interception of traffic
(R-MS- 9):	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- 10):	An NGN should ensure that broadcast media paths (e.g. radio) should be protected by encryption of media content
(R-MS- 11):	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

6.6.2 NGCN

Table 2 lists a number of requirements for media security in NGCNs from the preceding analysis that are in addition to the NGN requirements found in table 1.

Table 2: Requirements for media security in the NGCN

(R-NGCN- 12):	The NGN shall provide support for secure media transfer between NGCNs and NGNs
(R-NGCN- 13):	An NGCN should permit media to be secured (encrypted, authenticated and integrity protected) transparently end-to-end or end to PSTN/ISDN gateway, except where requested or authorized intervention in media occurs
(R-NGCN- 14):	An NGCN should be transparent to key management for the purpose of media security to take place between the end devices (or end device to PSTN/ISDN gateway), with cryptographic evidence that the peer involved in key exchange or key agreement is the expected communication partner
(R-NGCN- 15):	An NGCN should be transparent to the end-to-end encryption of any key exchange required for the purpose of media security

7 NGN media transfer architecture for security analysis

7.1 Functional model

The functional architecture for transfer of media in the NGN is defined in ES 282 001 [i.6].

In the NGN architecture the transport plane resources are mediated by RACS on behalf of the service plane.

7.2 Points of attack in NGN media architecture

7.2.1 Direct attack

The NGN Media architecture has two phases which can be attacked:

- Path establishment
  - Redirection.
  - Manipulation of signalling.
- Path active
  - Eavesdropping.

7.2.2 Indirect attack

In order to support media transfer in the NGN a number of sub-systems are used. An attack against these subsystems may result in an attack to the media transfer capabilities.

8 Media security solution

8.1 General

A media security solution has to be able to provide confidentiality and integrity of media transfer for each of the classes of media identified in clause 6.5:

- User generated delay intolerant (e.g. voice, video calling).
- User generated delay tolerant (e.g. video distribution).
- Block structured delay tolerant (e.g. file transfer).

Traffic network capabilities:

- Synchronous vs. asynchronous.
- Datagram vs. virtual circuit.

Topography of the media connection:

- Point to point.
- Point to multi-point.
- Broadcast (point to all points).

Whilst it is possible to use a single algorithm for all of these media it is unlikely that a single mode can be applied to all. The advice of established algorithm designers should be sought as outlined in EG 202 238 [i.7].

8.2 Cryptographic algorithm considerations

Whilst there are essentially two forms of cryptographic algorithm the selection of algorithm type and algorithm implementation should be based on the traffic characteristics. In general the guidance for selection of cryptographic algorithms defined in EG 202 238 [i.7] should be applied with the additional considerations given in the remainder of this clause.

8.3 Cryptographic key management

When applying cryptographic solutions the provisions of the Wassenaar agreement [i.9] should be taken into account. These are summarized as follows: When using cryptographic algorithms for encryption there are restrictions in place on the distribution of key material if the intended application is for provision of end-to-end confidentiality. As of October 2007 there is no restriction for public cellular (telecommunications) networks where the encryption is provided between the terminal and the network, else there are likely to be export restrictions applied on the basis of key length as follows: for a "symmetric algorithm" employing a key length in excess of 56 bits; for an "asymmetric algorithm" where the security of the algorithm is based on any of factorization of integers in excess of 512 bits (e.g. RSA), computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g. Diffie-Hellman over Z/pZ), or discrete logarithms in excess of 112 bits (e.g. Diffie-Hellman over an elliptic curve).

Annex A: User to user media scenarios

NOTE: User-to-user scenarios where end-to-end encryption is deployed may be subject to export control restrictions as defined in the Wassenaar agreement [i.9].

A.1 SIP Session Establishment without Media Security

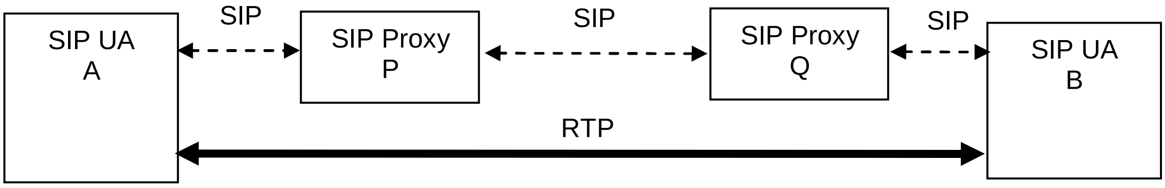

Figure A.1: SIP Session Establishment without Media Security

In figure A.1, RTP media exchange begins after establishing a call session between two SIP user agents A and B. SIP and RTP follow different paths, which SIP is along signalling path and RTP is along media path.

The media packet is not protected in this case. SRTP provides security services for RTP media. Figure A.2 shows the layout of an SRTP packet. MKI identifies the master key from which the session key(s) are derived. The session key(s) are used to authenticate and encrypt the packet. MKI is defined, signalled, and used by key management protocol. MAC is used to carry message authentication data.

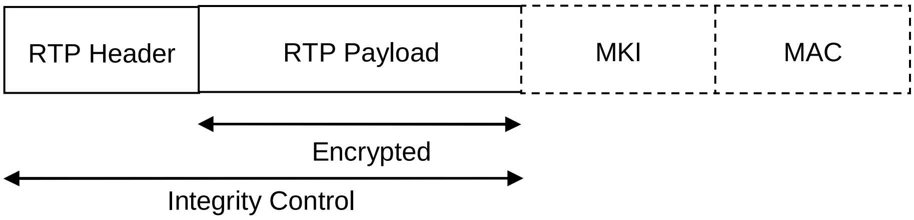

Figure A.2: SRTP Packet Layouts

Figure A.3 depicts that SRTP is signalled by use of secure RTP transport (e.g. "RTP/SAVP") in an SDP media (m=) line.

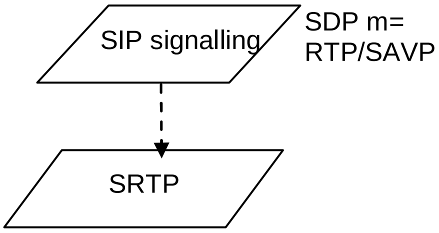

Figure A.3: Relationship between SIP Signalling and SRTP

Currently in SDP as defined in RFC 4566 [i.11], there exists one field (k=) to transport keys. However, this is not enough because there are more security parameters that need to be transported, and the "k=" field is not extensible. Furthermore, there are no means within SDP itself to configure SRTP except using the pre-defined cryptographic transform in [i.3].

A.2 Media Security based on Secure Signalling Path

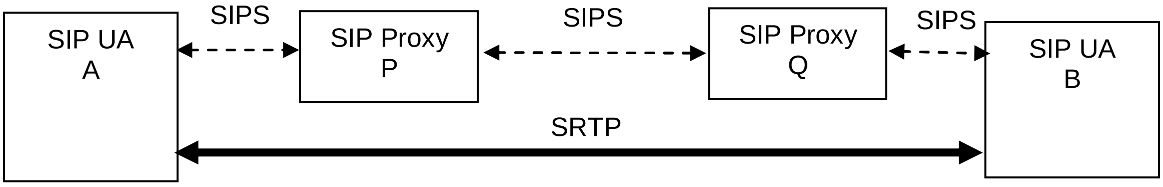

Figure A.4: Media Security using Signalling Protection

Figure A.4 shows that SDES as defined in RFC 4568 [i.13] needs each side to indicate the key material for SRTP media, and the keys are sent in the clear in SDP. SDES relies on secured signalling path (e.g. SIPS) to protect the keys exchanged in signalling.

SDES adds a new SDP attribute called "a=crypto" used to signal and negotiate cryptographic parameters for SRTP media, as shown in figure A.5.

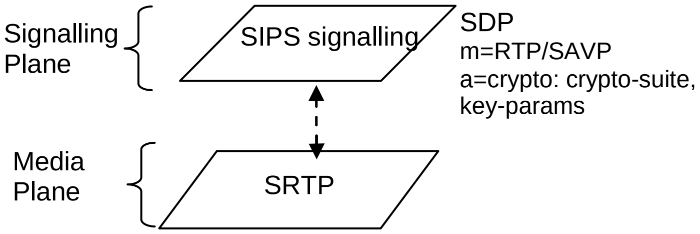

Figure A.5: Relationships between SIPS and SRTP

SDES can be regarded as a "key management protocol" embedded in a secure signalling protocol, which negotiates cryptographic parameters and passes them to SRTP.

A.3 Media Security based on Key Management Protocol in Signalling Path

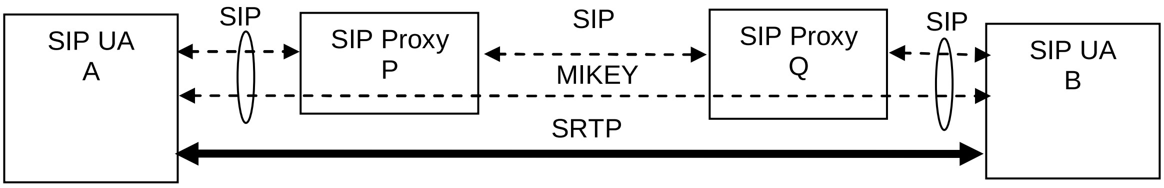

Figure A.6: Media Security using Keying Management Protocol

Figure A.6 shows that key management protocols such as MIKEY defined in RFC 3830 [i.10] used to establish a security association for the security protocol (e.g. SRTP). MIKEY message is transmitted along the SIP signalling path, and it can be piggybacked in the SDP.

RFC 4567 [i.12] defines an extension "a=key-mgmt" for SDP to carry messages specified by a key management protocol (e.g. MIKEY). The MIKEY message contains one or more cryptographic keys and the set of necessary parameters for the security protocol, e.g. cipher and authentication algorithms to be used.

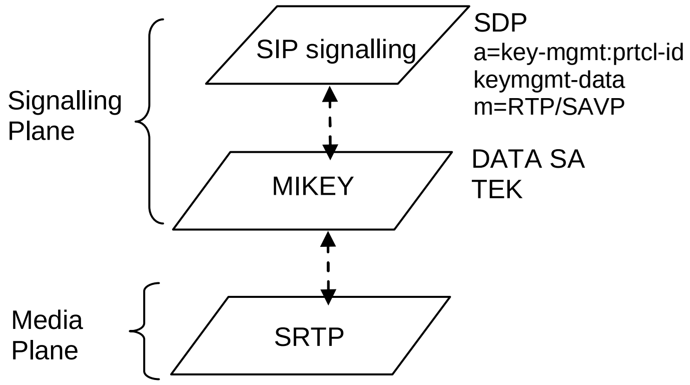

Figure A.7: Relationships between SIP, SDP, MIKEY and SRTP

RFC 4567 [i.12] can ensure end-to-end security establishment for the media and be independent of the signalling protection. It expects endpoints to have preconfigured keys or common security infrastructure.

A.4 Media Security based on Media Path Keying Technique

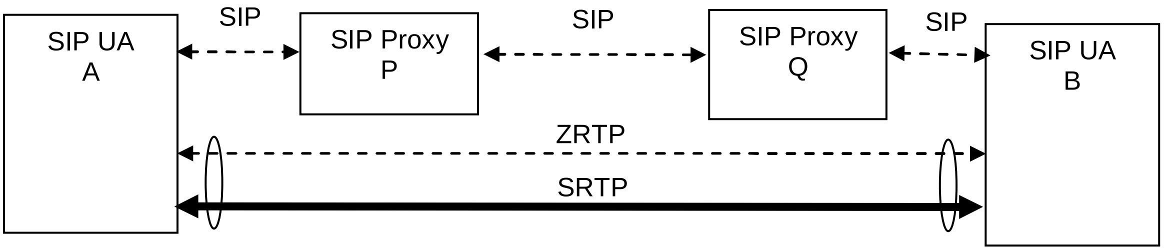

Figure A.8: Media Security using Media Path Key

Figure A.8 shows that in ZRTP [i.14] the keys are exchanged entirely in the media path. After ZRTP exchange has successfully done, SRTP session begins to establish. ZRTP uses several media path messages to establish the SRTP key.

ZRTP uses normal RTP/AVP profile (AVP) media lines in the initial offer/answer exchange. The ZRTP SDP attribute flag "a=zrtp-id" is used in all offers and answers to indicate support for the ZRTP protocol. Various keys, such as those used by SRTP, must be derived from the shared secret s0. The SRTP master key and master salt are derived from s0.

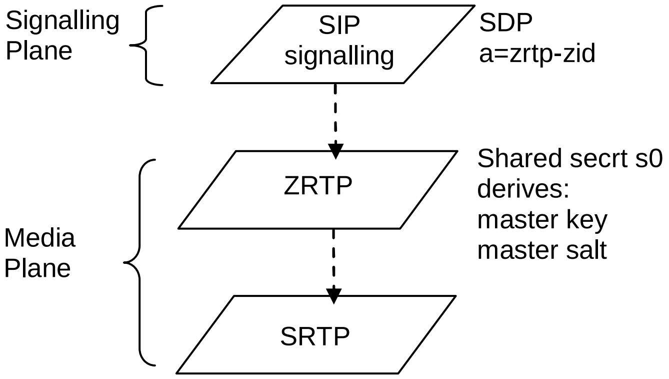

Figure A.9: Relationships between SIP, SDP, ZRTP and SRTP

ZRTP is a key agreement protocol which performs Diffie-Hellman key exchange in the media path. The advantage of ZRTP is that the signalling channel is used only for call setup and the media channel is used to establish an encrypted channel.

A.5 Mixed Signalling and Media Path Keying Technique

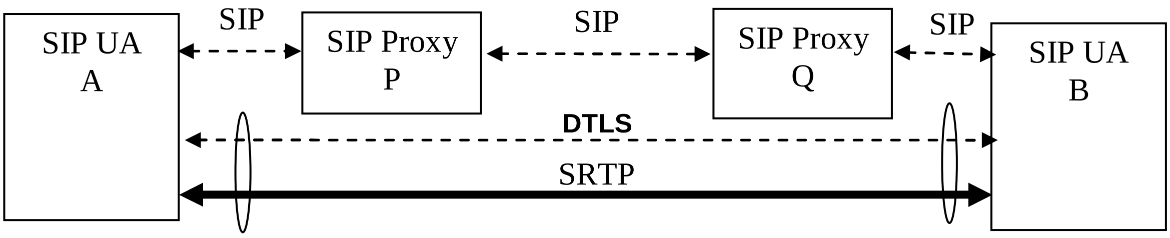

Figure A.10: Media Security using Mixed Signalling and Media Path Keying Technique

Figure A.10 shows that DTLS-SRTP [i.16] exchanges public key fingerprints in SDP and then establishes a DTLS session over the media channel. The endpoints use the DTLS handshake to agree on crypto suites and establish SRTP session keys. SRTP packets are then exchanged between the endpoints.

Figure A.11 shows that a DTLS-SRTP session can be indicated by an external signalling protocol like SIP and SDP and the endpoints are authenticated using fingerprints [i.15]. In order to negotiate the use of SRTP data protection, clients may include an extension of type "use_srtp" in the extended client hello. Once the "use_srtp" extension is negotiated, packets of type "application_data" in the newly negotiated association will be protected using SRTP.

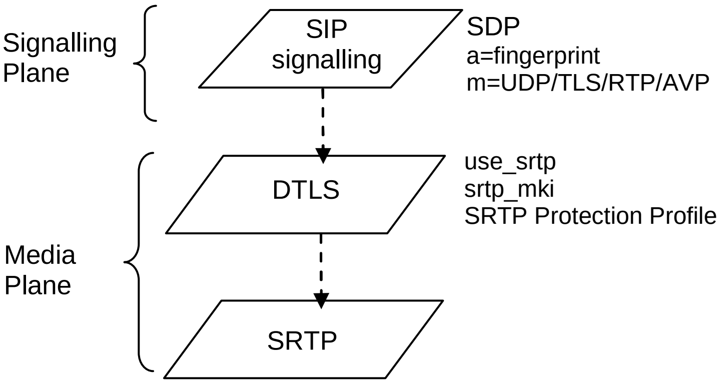

Figure A.11: Relationships between SIP, SDP, DTLS and SRTP

DTLS-SRTP is defined for point-to-point media sessions. For media over SRTP, DTLS-SRTP has been defined to provide for the negotiation of SRTP transport using a DTLS connection, thus allowing the performance benefits of SRTP with the easy key management of DTLS.

Annex B: Bibliography

ETSI TS 182 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem".

ETSI TS 182 028: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; Dedicated subsystem for IPTV functions".

IETF RFC 3261 (2002): "SIP: Session Initiation Protocol".

IETF RFC 3711 (2004): "The Secure Real-time Transport Protocol (SRTP)".

IETF draft-wing-srtp-keying-eval-00 (2006): "Evaluation of SRTP Keying with SIP".

IETF draft-fischl-mmusic-sdp-dtls-03.txt (2007): "Session Description Protocol (SDP) Indicators for Datagram Transport Layer Security (DTLS)".

History

Document history		
V2.1.1	August 2008	Publication