Technical Specification of the SIP (Gm) interface between the User Equipment (UE) and the NGN platform of Deutsche Telekom

1 TR 114

Version: 3.0.0 DRAFT

Amendment 2 (secure VoIP)

14. December 2016

Herausgeber / Publisher

Deutsche Telekom AG

Verantwortlich/ Responsible

Deutsche Telekom Technik GmbH

Fixed Mobile Engineering Deutschland

Abteilung FMED-93

64307 Darmstadt

Bestellangabe / Order Information

Kurztitel / Title: 1 TR 114

Ausgabe / Version: 3.0.0 Amendment 2 (December 2016)

Erweiterung für / Amendment for 1 TR 114, Ausgabe / Version 3.0.0 (June 2013)

Bezugsanschrift / Order address

Deutsche Telekom Technik GmbH

Fixed Mobile Engineering Deutschland

64307 Darmstadt

Internet Download

https://www.telekom.de/hilfe/geraete-zubehoer/telefone-und-anlagen/informationen-zu-telefonanlagen/schnittstellenbeschreibungen-fuer-hersteller?samChecked=true

Gültig ist immer die aktuelle Bildschirmausgabe des Deutschen Telekom-Servers /
Only the current release on the Deutsche Telekom server is valid

1 Scope

This Amendment is an addition to 1 TR 114 V3.0.0

2 References

[5] ETSI TS 102 144 V1.1.1 (2003-05): Services and Protocols for Advanced Networks (SPAN); MTP/SCCP/SSCOP and SIGTRAN (Transport of SS7 over IP); Stream Control Transmission Protocol (SCTP) [Endorsement of RFC 2960 and RFC 3309, modified]

[19C] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".

[34] IETF RFC 0768: User Datagram Protocol; 28 August 1980

[37] IETF RFC 0793: TRANSMISSION CONTROL PROTOCOL; DARPA INTERNET PROGRAM; PROTOCOL SPECIFICATION; September 1981

[44] IETF RFC 2411: IP Security Document Roadmap; November 1998

[53] IETF RFC 3550: RTP: A Transport Protocol for Real-Time Applications; July 2003

[62] IETF RFC 4040: RTP Payload Format for a 64 kbit/s Transparent Call; April 2005 [76] IETF RFC 3711 The Secure Real-time Transport Protocol (SRTP)

[77] RFC 4568 (July 2006): "Session Description Protocol (SDP) Security Descriptions for Media Streams".

[78] RFC 4347 (April 2006) "Datagram Transport Layer Security"

[79] IETF draft-dawes-dispatch-mediasec-parameter-07.txt "Security Mechanism Names for Media"

[80] BSI Technische Richtlinie TR-02102-2 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Teil 2 – Verwendung von Transport Layer Security (TLS)" Version 2014-01(12.02.2014)

[81] RFC 3713 – A Description of the Camellia Encryption Algorithm

[82] RFC 3657 – Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)

[83] RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation

[84] RFC7027 (October 2013) - Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)

[85] RFC6066 (Januar 2011) - Transport Layer Security (TLS) Extensions: Extension Definitions

[86] RFC5746 (February 2010) - Transport Layer Security (TLS) Renegotiation Indication Extension

[87] RFC5289 (August 2008) - TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)

[88] RFC5246 - The Transport Layer Security (TLS) Protocol Version 1.2

[89] RFC 5288 (August 2008) AES Galois Counter Mode (GCM) Cipher Suites for TLS

[90] RFC 5293 (June 2010) Connection Reuse in the Session Initiation Protocol (SIP)

[91] RFC 5260 (Oktober 2009) The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)

[92] RFC5280 (May 2008) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[93] RFC4961 (July 2007) - Symmetric RTP / RTP Control Protocol (RTCP)

[94] 3GPP TS 24.229: " Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3" Release 12. (Version 2015-12)

3 Additions to 1 TR 114 for TLS and SRTP support

Paragraphs beginning with § are endorsed paragraphs out of the main document 1 TR 114 V.3.0.0. These changes within these paragraphs take precedence.

Text modified due to new requirements that is added or deleted compared to 1 TR 114 V3.0.0 is shown as cursive and underlined (*example for added text*) or cursive and stricken (~~*example for stricken text*~~).

Options are marked in Orange text.

§7.4.1 Supported SIP Signalling Transport Protocols in UA

The following SIP Signalling Transport Protocols shall be supported:

Table 7-6: Supported SIP Signalling Transport Protocols in UA

Protocol (NOTE)	Specification	Ref.	Support
UDP	RFC 0768/STD006	[34]	m
TCP	RFC 0793/STD007	[37]	m
TLS	*RFC 5246* ~~*RFC 2246*~~	[88]	*m* ~~*o*~~
SCTP	ETSI TS 102 144	[5]	o
IPSec	RFC 2411	[44]	o
NOTE: The following combinations shall be possible to configure: ■ SIP over UDP ■ SIP over TCP without TLS ■ SIP over TCP with TLS			

SIP over TCP with TLS shall be supported.

§7.4.4 Real-time Transport Procedures

Table 7-11: Specifications Real-time Transport Procedures

Specification	Title	Ref.	Support
RFC 3550	RTP: A Transport Protocol for Real-Time Applications; July 2003	[53]	m
RFC 4040	RTP Payload Format for a 64 kbit/s Transparent Call; April 2005 (see Note)	[62]	c1
RFC 3711	*The Secure Real-time Transport Protocol (SRTP)*	*[76]*	*m NOTE3 NOTE 5*
RFC 4568	*Session Description Protocol (SDP) Security Descriptions for Media Streams*	*[77]*	*m NOTE3 NOTE4*
RFC4961	*Symmetric RTP / RTP Control Protocol (RTCP)*	*[93]*	*m*
RFC 4347	*Datagram Transport Layer Security*	*[78]*	*o*

Conditions *(Notes are mandatory)*:

c1: If ISDN interworking then m else o.

NOTE1: This protocol is applicable to carry 64 kbit/s channel data transparently in RTP packets, using a pseudo-codec called "Clearmode" and is used in case of ISDN accesses via IADs, only.

NOTE2: Fragmented IP packets are not supported by the NGN platform of Deutsche Telekom.
If the UA chooses to send RTCP/SDES packets it shall not send the UA's public IP address.

NOTE3: More detail is given in 1 TR 114 ANNEX B Section 4.2B.2 Media security. When media security is needed the Secure Real-time Transport Protocol (SRTP) according to RFC 3711 [76] shall be used

NOTE4: Encryption Algorithm AES (Advanced Encryption Standards), IP transport UDP and Authentication method SHA-1 cryptographic hash function shall be supported.

NOTE 5: The following requirements has to be fulfilled: Exchange of Master Keys over SDES (Security Descriptions for Media, SDES (Security Descriptions for Media Streams) in SIP/SDP, building of Session Keys from Master Key and Encryption Key (encryption of Payloads)

NOTE 6: "Security Mechanism Names for Media" draft-dawes-dispatch-mediasec-parameter-07.txt [79] shall be considered in addition.

3.1. Procedures

Key Negotiation Method SDES; 3DES(Session Description Protocol Security Descriptions for Media Streams) shall be supported.

IETF draft-dawes-dispatch-mediasec-parameter-07.txt "Security Mechanism Names for Media" [79] should be considered in addition.

Procedures described within 1 TR 114 ANNEX B are valid. The following text shows some parts of the valid text.

As shown in 1 TR 114 ANNEX B the UE behaviour is as follows:

To request end to access edge media security either on a session or media level, the UE shall send an SDP Offer for an SRTP stream containing one or more SDES crypto attributes, each with a key and other security context parameters required according to RFC 4568 [77], together with the attribute "a=3ge2ae:requested".

All references shown within the following endorsed paragraphs (starting with §) are the original references out of the origin specification i.e. TS 24.229 Release 12

This attribute is supported in the IMS of Deutsche Telekom. The definition if this element is shown below in Section §7.5

AND:

For the originating UE (Section 4.2B.2 TR 114 ANNEX B) shall be replaced with the following text out of 3GPP TS 24.229 Release 12:

General addition to 1TR114 in reflection to the added text of 3GPP Release 12 in this document:

General: end-to-end media security is NOT required, thus theirs procedures are not valid to be implemented.

MSRP using TLS, BFCP using TLS, UDPTL using DTLS are not part of this Amendment. These features are marked as brown ***and NOT underlined text may be implemented as an option. Such features if implemented must be configurable and are deactivated per default. Such features (MSRP using TLS, BFCP using TLS, UDPTL using DTLS) are NOT supported by the Deutsche Telekom network.***

Preconditions are NOT used within the Deutsche Telekom network. For further information please see 1TR114 Amendment 3. This text is also marked as blue text

§4.2B.2 Media security

3GPP TS 33.328 [19C] defines mechanisms for support of security on the media plane.

This document defines the required elements for signalling the support of media security.

The media security mechanisms are summarised as shown in table 4-2.

Table 4-2: Summary of media security mechanisms to the IM CN subsystem

Mechanism	Applicable to media	Support required by UE	Support required by IM CN subsystem entities	Network support outside IM CN subsystem entities
End-to-access-edge media security using SDES. ***Mandatory to be supported.***	RTP based media only.	Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/34, A.317/36 and A.317/37.	P-CSCF (IMS-ALG) is required. P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/34, A.317/36 and A.317/37. (NOTE)	Not applicable.
End-to-access-edge media security for MSRP using TLS and certificate fingerprints. ***not supported by the Deutsche Telekom network***	MSRP based media only.	Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/40, A.317/40A, A.317/51 and A.317/37A.	P-CSCF (IMS-ALG) is required. P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/40, A.317/40A, A.317/51 and A.317/37A. (NOTE)	Not applicable.
End-to-access-edge media security for BFCP using TLS and certificate fingerprints. ***not supported by the Deutsche Telekom network***	BFCP based media only.	Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/28, A.317/51 and A.317/37B.	P-CSCF (IMS-ALG) is required. P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/28, A.317/51 and A.317/37B. (NOTE)	Not applicable.
End-to-access-edge media security for UDPTL using DTLS and certificate fingerprints. ***not supported by the Deutsche Telekom network***	UDPTL based media only.	Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/52, A.317/51 and A.317/37C.	P-CSCF (IMS-ALG) is required. P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/52, A.317/51 and A.317/37C. (NOTE)	Not applicable.
End-to-end media security using SDES. ***not supported by the Deutsche Telekom network***	RTP based media only.	Support SDP extensions specified in table A.317, items A.317/34 and A.317/36.	Not applicable.	Not applicable.
End-to-end media security using KMS. ***not supported by the Deutsche Telekom network***	RTP based media only.	Support SDP extensions specified in table A.317, items A.317/34 and A.317/35.	Not applicable.	GBA and KMS support required.
End-to-end media security for MSRP	MSRP based media only.	Support SDP extensions specified	Not applicable.	GBA and KMS support required.

using TLS and KMS. ***not supported by the Deutsche Telekom network***		in table A.317, items A.317/40, A.317/40A and A.317/35, and support RFC 4279 [218].		
NOTE: Support of end-to-access-edge media security is determined entirely by the network operator of the P-CSCF, which need not be the same network operator as that of the S-CSCF.				

For RTP media security, the UE supports the SDES key management protocol and optionally the KMS key management protocol as defined in 3GPP TS 33.328 [19C] and SRTP as defined in RFC 3711 [169] for secure transport of media.

For end-to-access-edge media security for MSRP using TLS and certificate fingerprints, the UE supports MSRP over TLS as defined in RFC 4975 [178] and RFC 6714 [214] with certificate fingerprints as defined in 3GPP TS 33.328 [19C].

For end-to-access-edge media security for BFCP using TLS and certificate fingerprints, the UE supports BFCP over TLS as defined in RFC 4583 [108] with certificate fingerprints as defined in 3GPP TS 33.328 [19C].

For end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints, the UE supports UDPTL over DTLS as defined in RFC 7345 [217] with certificate fingerprints as defined in 3GPP TS 33.328 [19C].

For end-to-end media security for MSRP using TLS and KMS, the UE supports MSRP over TLS as defined in RFC 4975 [178] and RFC 6714 [214] with pre-shared key ciphersuites as defined in RFC 4279 [218] and the KMS key management protocol as defined in 3GPP TS 33.328 [19C]. The certificate fingerprints are not indicated.

There is no support for media security in the MGCF, because there would be no end-to-end media security support on calls interworked with the CS domain and the CS user. In this release of this document, there is no support for media security in the MRF. End-to-access-edge media security is not impacted by this absence of support.

For emergency calls, it is not expected that PSAPs would support end-to-end media security and therefore the procedures of this document do not allow the UE to establish such sessions with end-to-end media security. End-to-access-edge media security is not impacted and can be used on emergency calls.

When the UE performs the functions of an external attached network (e.g. an enterprise network):

- where end-to-access-edge media security is used, the UE functionality is expected to be in the gateway of the external attached network, and support for further media security is outside the scope of this document; and
- where end-to-end media security is used, the UE functionality is expected to be supported by the endpoints in the attached network.

AND:

For the originating UE (Section 6.1.2 TR 114 ANNEX B) shall be replaced with the following text out of 3GPP TS 24.229 Release 12:

General addition to 1TR114 in reflection to the added text of 3GPP Release 12 in this document:

General: end-to-end media security is NOT required, thus theirs procedures are not valid to be implemented.

MSRP using TLS, BFCP using TLS, UDPTL using DTLS are not part of this Amendment. These features are marked as brown ***and NOT underlined text may be implemented as an option. Such features if implemented must be configurable and are deactivated per default. Such features (MSRP using TLS, BFCP using TLS, UDPTL using DTLS) are NOT supported by the Deutsche Telekom network.***

Preconditions are not used within the Deutsche Telekom network. For further information please see 1TR114 Amendment 3.

§5.1.1.5.6 SIP digest with TLS – general

On receiving a 401 (Unauthorized) response to the REGISTER request, the procedures in subclause 5.1.1.5.4 ***(see 1TR114 Amendment 7)*** apply with the following differences:

- The UE shall check the existence of the Security-Server header field as described in RFC 3329 [48]. If the Security-Server header field is not present or the list of supported security mechanisms does not include "tls", the UE shall abandon the authentication procedure and send a new REGISTER request.

In the case that the 401 (Unauthorized) response to the REGISTER is deemed to be valid the UE shall:

- store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any; and

NOTE 1: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

- send another REGISTER request using the TLS session to protect the message.

When TLS is used, the UE (IAD) shall register all IMPUs (Contacts) via one shared TLS connection. Connection reuse for 'SIP over TLS over TCP' shall apply according RFC 5923 [90] and RFC 5630 [91]

Implementation of RFC 5923 as follows:

Benefits of TLS Connection Reuse:

Opening an extra connection where an existing one is sufficient can result in potential scaling and performance problems. Each new connection using TLS requires a TCP three-way handshake, a handful of round trips to establish TLS, typically expensive asymmetric authentication and key generation algorithms, and certificate verification.

Either the UE or the server may terminate a TLS session by sending a TLS closure alert. Before closing a TLS connection, the initiator of the closure MUST either wait for any outstanding SIP transactions to complete, or explicitly abandon them.

After the initiator of the close has sent a closure alert, it MUST discard any TLS messages until it has received a similar alert from its peer. The receiver of the closure alert MUST NOT start any new SIP transactions after the receipt of the closure alert.

Implementation of RFC5630 as follows:

Since SIP allows for requests in both directions (e.g., an incoming call), the UE is expected to keep the TLS connection alive, and that connection is expected to be reused for both incoming and outgoing requests.

This solution of having the UA always initiate and keep alive the connection also solves the Network Address Translation (NAT) and firewall problem as it ensures that responses and further requests will always be deliverable on the existing connection.

The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header field containing a challenge response, "cnonce", "qop", and "nonce-count" header field parameters as indicated in RFC 2617 [21]. The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

When SIP digest with TLS is used, and for the case where the 401 (Unauthorized) response to the REGISTER request is deemed to be valid, the UE shall establish the TLS session as described in 3GPP TS 33.203 [19]. The UE shall use this TLS session to send all further messages towards the P-CSCF towards the protected server port.

§6.1.2 Handling of SDP at the originating UE

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the SDP offer, the UE shall:

- indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1); and,

- set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in RFC 4566 [39], unless the UE knows that the precondition mechanism is supported by the remote UE.

NOTE 1: When setting the media streams to the inactive mode, the UE can include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

If the desired QoS resources for one or more media streams are available at the UE when the SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in the SDP message body.

~~*If t*~~The UE *shall* indicate~~*d*~~ support for end-to-access-edge media security using SDES during registration, and the P-CSCF indicated support for end-to-access-edge media security using SDES during registration, then upon generating an SDP offer with an RTP based media, for each RTP based media except those for which the UE requests an end-to-end media security mechanism, the UE shall:

- offer SRTP transport protocol according to RFC 3711 [169] and the profile defined in 3GPP TS 33.328 [19C] *(See ANNEX A of this document);*

- include the SDP crypto attribute according to RFC 4568 [168] and the profile defined in 3GPP TS 33.328 [19C] *(The used cipher Suits are shown in Section 3.2 within this document.)* ; and

- include an SDP "a=3ge2ae:requested" attribute.

If the UE indicated support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, then upon generating an SDP offer with an MSRP based media, for each MSRP based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP "a=3ge2ae:requested" attribute.

NOTE 3: TLS client role and TLS server role are determined according to RFC 6135 [215] (referenced by RFC 6714 [214]). If the SDP answer contains the SDP setup attribute with "active" attribute value, the answerer performs the TLS client role. If the SDP answer contains the SDP setup attribute with "passive" attribute value, the offerer performs the TLS client role.

If the UE indicated support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, then upon generating an SDP offer with an BFCP based media, for each BFCP based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer BFCP over TLS transport protocol according to RFC 4583 [108] and the profile defined in 3GPP TS 33.328 [19C];
- include the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C]; and
- include the SDP "a=3ge2ae:requested" attribute.

If the UE indicated support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, then upon generating an SDP offer with an UDPTL based media, for each UDPTL based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer UDPTL over DTLS transport protocol according to draft-ietf-mmusic-udptl-dtls [217] and the profile defined in 3GPP TS 33.328 [19C];
- include the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C]; and
- include the SDP "a=3ge2ae:requested" attribute.

If the P-CSCF did not indicate support for end-to-access-edge media security using SDES during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any RTP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any MSRP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any BFCP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any UDPTL based media in any SDP offer.

The UE shall not include an SDP "a=3ge2ae:requested" attribute in any media other than RTP based, MSRP based, BFCP based and UDPTL based in any SDP offer.

Deutsche Telekom Note: End-to-end media security for MSRP is currently not used in the Deutsche Telekom network.

Upon generating an SDP offer with an MSRP based media protected by the end-to-end media security for MSRP using TLS and KMS, the UE shall:

- offer MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C]; and
- include the SDP key-mgmt attribute according to RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C];

NOTE 3: SDP fingerprint attribute is not included.

Upon receiving an SDP answer to the SDP offer with the MSRP based media protected by the end-to-end media security for MSRP using TLS and KMS, and if the MSRP based media is accepted and associated with the SDP key-mgmt attribute as described in RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C] in the SDP

answer, then the UE indicate the pre-shared key ciphersuites according to RFC 4279 [218] and the profile defined in 3GPP TS 33.328 [19C] in TLS handshake of TLS connection transporting the MSRP based media.

When the UE detects that an emergency call is being made, the UE shall not include end-to-end media security on any media in the SDP offer.

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the SDP offer shall contain a subset of the allowed media types, codecs and other parameters from the SDP message bodies of all 488 (Not Acceptable Here) responses so far received for the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). For each media line, the UE shall order the codecs in the SDP offer according to the order of the codecs in the SDP message bodies of the 488 (Not Acceptable Here) responses.

NOTE 4: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP message bodies of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create an SDP offer in which:

- the related local preconditions are set to met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64]; and

- *if* the media streams *were* previously set to inactive mode *then they* are set to active (sendrecv, sendonly or recvonly) mode.

Upon receiving an SDP answer, which includes more than one codec per media stream, excluding the in-band DTMF codec, as described in subclause 6.1.1, the UE shall send an SDP offer at the first possible time, selecting only one codec per media stream.

If the UE sends an initial INVITE request that includes only an IPv6 address in the SDP offer, and receives an error response (e.g., 488 (Not Acceptable Here) with 301 Warning header field) indicating "incompatible network address format", the UE shall send an ACK as per standard SIP procedures. Subsequently, the UE may acquire an IPv4 address or use an existing IPv4 address, and send a new initial INVITE request to the same destination containing only the IPv4 address in the SDP offer.

For the terminating UE (Section 6.1.3 1 TR 114 ANNEX B) shall be replaced with the following text out of 3GPP TS 24.229 Release 12:

General: end-to-end media security is NOT required, thus the related procedures are not valid to be implemented.

MSRP using TLS, BFCP using TLS, UDPTL using DTLS are not part of this Amendment. These features are marked as brown ***and NOT underlined text may be implemented as an option. Such features if implemented must be configurable and are deactivated per default. Such features (MSRP using TLS, BFCP using TLS, UDPTL using DTLS) are NOT supported by the Deutsche Telekom network.***

Preconditions are not used within the Deutsche Telekom network. For further information please see 1TR114 Amendment 3. This text is also marked as blue text

§6.1.3 Handling of SDP at the terminating UE

Upon receipt of an initial SDP offer in which no precondition information is available, the terminating UE shall in the SDP answer:

- if, prior to sending the SDP answer the desired QoS resources have been reserved at the terminating UE, set the related media streams in the SDP answer to:

  - active mode, if the offered media streams were not listed as inactive; or

- inactive mode, if the offered media streams were listed as inactive.

If the terminating UE had previously set one or more media streams to inactive mode and the QoS resources for those media streams are now ready, the UE shall set the media streams to active mode by applying the procedures described in RFC 4566 [39] with respect to setting the direction of media streams.

Upon sending a SDP answer to an SDP offer (which included one or more media lines which was offered with several codecs) the terminating UE shall select exactly one codec per media line and indicate only the selected codec for the related media stream. In addition, the UE may indicate support of the in-band DTMF codec, as described in subclause 6.1.1.

Upon sending a SDP answer to an SDP offer, with the SDP answer including one or more media streams for which the originating side did indicate its local preconditions as not met, if the precondition mechanism is supported by the terminating UE, the terminating UE shall indicate its local preconditions and request the confirmation for the result of the resource reservation at the originating end point.

NOTE 1: If the terminating UE does not support the precondition mechanism it will ignore any precondition information received from the originating UE.

Upon receiving an initial INVITE request, that includes the SDP offer containing an IP address type (in the "c=" parameter) that is not supported by the UE, the UE shall respond with the 488 (Not Acceptable Here) response with 301 Warning header field indicating "incompatible network address format".

NOTE 2: Upon receiving an initial INVITE request that does not include an SDP offer, the UE can accept the request and include an SDP offer in the first reliable response. The SDP offer will reflect the called user's terminal capabilities and user preferences for the session.

If the UE receives an SDP offer that specifies different IP address type for media (i.e. specify it in the "c=" parameter of the SDP offer) that the UE is using for signalling, and if the UE supports both IPv4 and IPv6 addresses simultaneously, the UE shall accept the received SDP offer. Subsequently, the UE shall either acquire an IP address type or use an existing IP address type as specified in the SDP offer, and include it in the "c=" parameter in the SDP answer.

NOTE 3: Upon receiving an initial INVITE request, that includes an SDP offer containing connection addresses (in the "c=" parameter) equal to zero, the UE will select the media streams that is willing to accept for the session, reserve the QoS resources for accepted media streams, and include its valid connection address in the SDP answer.

~~*If t*~~***T***he UE ***shall*** support~~*s*~~ the end-to-access-edge media security using SDES, upon receiving an SDP offer containing an RTP based media:

- transported using the SRTP transport protocol as defined in RFC 3711 [169];
- with an SDP crypto attribute as defined in RFC 4568 [168]; and
- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the RTP based media, then the UE shall generate the SDP answer with the related RTP based media:

- transported using the SRTP transport protocol according to RFC 3711 [169] and the profile defined in 3GPP TS 33.328 [19C]; *(See ANNEX A of this document);* and
- including an SDP crypto attribute according to RFC 4568 [168] and the profile defined in 3GPP TS 33.328 [19C] *(See ANNEX C of this document)*.

If the UE supports the end-to-access-edge media security for MSRP using TLS and certificate fingerprints, upon receiving an SDP offer containing an MSRP based media:

- transported using the MSRP over TLS transport protocol as defined in RFC 4975 [178] and RFC 6714 [214];
- with the SDP fingerprint attribute as defined in RFC 4572 [216]; and
- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the MSRP based media, then the UE shall generate the SDP answer with the related MSRP based media:

- transported using the MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C]; and

- including the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C].

NOTE 4: TLS client role and TLS server role are determined according to RFC 6135 [215] (referenced by RFC 6714 [214]). If the SDP answer contains the SDP setup attribute with "active" attribute value, the answerer performs the TLS client role. If the SDP answer contains the SDP setup attribute with "passive" attribute value, the offerer performs the TLS client role.

If the UE supports the end-to-access-edge media security for BFCP using TLS and certificate fingerprints, upon receiving an SDP offer containing an BFCP based media:

- transported using the BFCP over TLS transport protocol as defined in RFC 4583 [108];

- with the SDP fingerprint attribute as defined in RFC 4572 [216]; and

- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the BFCP based media, then the UE shall generate the SDP answer with the related BFCP based media:

- transported using the BFCP over TLS transport protocol according to RFC 4583 [108] and the profile defined in 3GPP TS 33.328 [19C]; and

- including the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C].

If the UE supports the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints, upon receiving an SDP offer containing an UDPTL based media:

- transported using the UDPTL over DTLS transport protocol as defined in draft-ietf-mmusic-udptl-dtls [217];

- with the SDP fingerprint attribute as defined in RFC 4572 [216]; and

- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the UDPTL based media, then the UE shall generate the SDP answer with the related UDPTL based media:

- transported using the UDPTL over DTLS transport protocol according to draft-ietf-mmusic-udptl-dtls [217] and the profile defined in 3GPP TS 33.328 [19C]; and

- including the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C].

Upon receiving an SDP offer containing an MSRP based media:

- transported using the MSRP over TLS transport protocol as defined in RFC 4975 [178] and RFC 6714 [214]; and

- with the SDP key-mgmt attribute according to RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C];

and if the UE accepts the MSRP based media, the UE shall:

1) generate the SDP answer with the related MSRP based media:

   a) transported using the MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C]; and

b) include the SDP key-mgmt attribute according to RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C]; and

NOTE 5: SDP fingerprint attribute is not included.

2) indicate the pre-shared key ciphersuites according to RFC 4279 [218] and the profile defined in 3GPP TS 33.328 [19C] in TLS handshake of TLS connection transporting the MSRP based media.

If the terminating UE uses the precondition mechanism (see subclause 5.1.4.1), if the desired QoS resources for one or more media streams have not been reserved at the terminating UE when constructing the SDP offer, the terminating UE shall indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment.

NOTE 6: It is out of scope of this specification which media streams are to be included in the SDP offer.

If the terminating UE uses the precondition mechanism (see subclause 5.1.4.1) and if the desired QoS resources for one or more media streams are available at the terminating UE when the SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment.

If the terminating UE sends an UPDATE request to remove one or more media streams negotiated in the session for which a final response to the INVITE request has not been sent yet, the terminating UE sets the ports of the media streams to be removed from the session to zero in the new SDP offer.

For the current document (Section 7.5 1 TR 114 ANNEX B) shall be replaced with the following text out of 3GPP TS 24.229 Release 12:

§7.5 Session description types defined within the present document

§7.5.1 General

This subclause contains definitions for SDP parameters that are specific to SDP usage in the 3GPP IM CN Subsystem and therefore are not described in an RFC.

§7.5.2 End-to-access-edge media plane security

Editor's note: This subclause forms the basis for IANA registration of the new SDP attribute. The registration should be performed by MCC when the MEDIASEC_CORE work item is declared 100% complete.

§7.5.2.1 General

The end-to-access-edge media security-indicator is used to indicate that a UE requests a P-CSCF to apply media plane security or to indicate that a P-CSCF has applied end-to-access-edge media security as defined in 3GPP TS 33.328 [19C].

§7.5.2.2 Syntax

3GPP end-to-access-edge media security indicator is a value attribute which is encoded as a media-level SDP attribute with the ABNF syntax defined in table 7.5.1. ABNF is defined in RFC 2234 [20G].

Table 7.5.1: ABNF syntax of 3ge2ae attribute

```
3ge2ae-attribute = "a=3ge2ae:" indicator
indicator = "requested" / "applied" / token
```

"requested": the sender indicates its wish that end-to-access-edge media security is applied.

"applied": the sender indicates that it has applied end-to-access-edge media security.

This version of the specification only defines usage of the "requested" and "applied" attribute values. Other values shall be ignored.

The "3ge2ae" attribute is charset-independent.

§7.5.2.3 IANA registration

NOTE: This subclause contains information to be provided to IANA for the registration of the end-to-access-edge security indicator SDP attribute.

Contact name, email address, and telephone number:

3GPP Specifications Manager

3gppContact@etsi.org

+33 (0)492944200

Attribute Name (as it will appear in SDP)

3ge2ae

Long-form Attribute Name in English:

3GPP_e2ae-security-indicator

Type of Attribute

Media level

Is Attribute Value subject to the Charset Attribute?

This Attribute is not dependent on charset.

Purpose of the attribute:

This attribute specifies the end-to-access-edge security-indicator as used for IMS media plane security

Appropriate Attribute Values for this Attribute:

The attribute is a value attribute. The values "requested" and "applied" are defined.

3.2 Cipher Suites:

PFS (Perfect Forward Secrecy) Cipher Suites should be used only. Cipher suits define the "Key-negotiation" and "Key agreement" (and Authentication if needed), media encryption and a hash functionality for integrity protection (HAMAC-Algorithm) and use for the pseudorandom function starting with TLS 1.2.

A full list of all defined Cipher-Suites including references to the regarding specifications is given under http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml.

Table 3.2-1 shows the Cipher Suits required for Deutsche Telekom Client implementation. In brackets the OpenSSL equivalents are shown. The UE (IAD) shall support at minimum one of the following Cipher suits using TLSv1.2.

The cipher suit number 1, 2, 3 and 4 out of Table 3.2-1 SHALL be implemented, the chipher suit offer shall have the sequence as shown within Table 3.2-1.

Table 3.2-1: Supported Cipher Suits

Number	**Cipher Suit**	**TLS**	**Reference**	**Support in UA**
1	TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	RFC5288 [89]	m

	(AES256-GCM-SHA384)			
2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DHE-RSA-AES256-GCM-SHA384)	TLSv1.2	RFC5288 [89]	m
3	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (ECDH-RSA-AES256-GCM-SHA384)	TLSv1.2	RFC5289 [87]	m
4	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ECDHE-RSA-AES256-GCM-SHA384)	TLSv1.2	RFC5289 [87]	m
5	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (DHE-DSS-AES256-SHA256)	TLSv1.2	RFC5246 [88]	m (NOTE 1)
6	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (DHE-DSS-AES256-GCM-SHA384)	TLSv1.2	RFC5288 [89]	m (NOTE 1)
7	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DHE-RSA-AES256-SHA256)	TLSv1.2	RFC5246 [88]	m (NOTE 1)
8	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (DHE-DSS-AES256-SHA256)	TLSv1.2	RFC5246 [88]	m (NOTE 1)
9	TLS_RSA_WITH_AES_256_GCM_SHA384 (AES256-GCM-SHA384)	TLSv1.2	RFC5288 [89]	m (NOTE 1)
10	TLS_RSA_WITH_AES_256_CBC_SHA256 (AES256-SHA256)	TLSv1.2	RFC5288 [89]	m (NOTE 1)
11	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DHE-RSA-AES128-GCM-SHA256)	TLSv1.2	RFC5288 [89]	m (NOTE 1)
12	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ECDHE-RSA-AES128-GCM-SHA256)	TLSv1.2	RFC5289 [87]	m (NOTE 1, NOTE 3)
13	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (DHE-DSS-AES128-GCM-SHA256)	TLSv1.2	RFC5288 [89]	m (NOTE 1)
14	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DHE-RSA-AES128-SHA256)	TLSv1.2	RFC5246 [88]	m (NOTE 1)
15	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ECDHE-RSA-AES128-SHA256)	TLSv1.2	RFC5289 [87]	m (NOTE 2)
16	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (DHE-DSS-AES128-SHA256)	TLSv1.2	RFC5246 [88]	m (NOTE)
17	TLS_RSA_WITH_AES_128_GCM_SHA256 (AES128-GCM-SHA256)	TLSv1.2	RFC5246 [88]	m (NOTE 1, NOTE 4)
18	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ECDHE-RSA-AES128-GCM-SHA256)	TLSv1.2	RFC5289 [87]	m (NOTE 2)
19	TLS_RSA_WITH_AES_128_CBC_SHA256 (AES128-SHA256)	TLSv1.2	RFC5246 [88]	m (NOTE 1, NOTE 4)
20	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ECDHE-RSA-AES128-SHA256)	TLSv1.2	RFC5289 [87]	m (NOTE 2)
21	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (DHE-RSA-AES256-SHA)	TLSv1.1	RFC4346 [46]	m (NOTE 1)
22	TLS_DHE_DSS_WITH_AES_256_CBC_SHA (DHE-DSS-AES256-SHA)	TLSv1.1	RFC4346 [46]	m (NOTE 1)
23	TLS_RSA_WITH_AES_256_CBC_SHA (AES256-SHA)	TLSv1.1	RFC4346 [46]	m (NOTE 1)
24	SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA (EDH-RSA-DES-CBC3-SHA) (DHE-RSA-DES-CBC3-SHA)	TLSv1.1	RFC4346 [46]	m (NOTE 1)
25	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (EDH-DSS-DES-CBC3-SHA) (DHE-DSS-DES-CBC3-SHA)	TLSv1.1	RFC4346 [46]	m (NOTE 1)
26	TLS_RSA_WITH_3DES_EDE_CBC_SHA (DES-CBC3-SHA)	TLSv1.1	RFC4346 [46]	m (NOTE 1)
27	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (DHE-RSA-AES128-SHA)	TLSv1.1	RFC4346 [46]	m (NOTE 1)
28	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TLSv1.1	RFC4346 [46]	m (NOTE 1)

	(DHE-DSS-AES128-SHA)			
29	TLS_RSA_WITH_AES_128_CBC_SHA (AES128-SHA)	TLSv1.1	RFC4346 [46]	m (NOTE 1)
NOTE 1: At minimum one of the TLSv1.2 shown cipher suits shall be supported. Priority of implementation starts on top of the table. NOTE 2: Shall be implemented in addition if the non eliptical Cipher suit regarding RFC5246 [88] is implemented. NOTE 3: Mandatory for UE/IAD supporting SIP-Trunk (i.e SIP Connect 2.0) NOTE 4: Optional support for UE/IAD supporting SIP-Trunk (i.e SIP Connect 2.0) (for backward compatibility)				

3.4. Key Size / Key Lengh

It is recommended to use the following Key Length:

Table3.3-1: Supported Algorithms in UA

Algorithm	Minimal Key Length	Recommended use till year	Support in UA
Digital Signature Algorithm and key negotiation			
ECDSA	224 Bit	2015	m
ECDSA	250 Bit (NOTE 4)	2020+	m
DSS	2000 Bit (NOTE 5)	2020+	m
RSA	2000 Bit (NOTE 5)	2020+	m
Static Diffie-Hellman Key			
ECDH	224 Bit	2015	o
ECDH	250 Bit (NOTE 4)	2020+	o
DH	2000 Bit (NOTE 5)	2020+	o
Ephemerale Diffie-Hellman Key			
ECDH	224 Bit	2015	m
ECDH	250 Bit (NOTE 4)	2020+	m
DH	2000 Bit(NOTE 5)	2020+	m
NOTE 4: In this case 250 Bit (instead of 256 Bit) are used to allow small Co-Factors at elliptical curves. NOTE 5: For use beyond 2015 it is useful to use RSA/DSS/DH-Key of 3000 Bit length to ensure a consistent security level of all recommended asymmetric encryption methods.			

Session renegotiation based on RFC5746 [86] shall be implemented.

Client based Session Renegotiation must be rejected.

It is not needed to support the TLS 1.2 extension "truncated_hmac" as defined in RFC6066 [85].

A implementation TLS-Compression as defined in TLS 1.2 RFC 5246 [42] is not needed.

3.5 Algorithms for Elliptic Curve Cryptography

Elliptical curves recommended in Abschnitt 3.6 of BSI TR-02102-2 [80] shall be supported as follow.

Table3.4-1: Supported Elliptic Curve in UA

Curve	Specification and Reference	Support in UE
brainpoolP256r1	RFC5639 [83] and RFC7027 [84]):	m
brainpoolP384r1	RFC5639 [83] and RFC7027 [84]):	m
brainpoolP512r1	RFC5639 [83] and RFC7027 [84]):	m
secp224r1	SECG Standards; www.secg.org	o
secp256r1	SECG Standards; www.secg.org	o
secp384r1	SECG Standards; www.secg.org	o

3.6 Root Certificate

3.6.1 Initial

The UE MUST comply to X.509v3 acc. RFC 5280 [92].

The device MUST comply to industry standard guidelines related to security handling/administration as well as to the requirements of Deutsche Telekom like particularly " Security Requirement Home Gateway" (see chapter 'References').

The UE MUST store all Certificate Authority (CA) Information Chain according X.509v3 to ensure that a requestor (SIP client) is able to validate the Certificate.

The HG must be able to cope with a chain of trust depth of >2.

3.5.2 Update

The UE MUST provide the ability to update the root certificates by new Firmware update (regardless if locally or remotely initiated).
The secure connections described within this document are solely established to the trusted Telekom platform only, therefore as a matter of fact there seems to be no need for further manual update procedures for the moment.

3.5.3 Deutsche Telekom Certificate download

End-devices (UE) must install locally the certificate of Telesec Root-CA (manually) or it is pre-installed by the vendor of the corresponding operating system / SIP software.

https://www.telesec.de/de/public-key-infrastruktur/support/root-zertifikate

Note, depending on that certificate been used, only Telesec Root Certificate is required.

UE must check the validity of the certificate provided by P-CSCF/IBCF with help of root certificate.

4 Abbreviations

AES	Advanced Encryption Standard
3DES	Triple DES
DH	Diffie–Hellman
DHE	Diffie–Hellman Ephemeral
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDH	Elliptic curve Diffie–Hellman
ECDHE	Elliptic curve Diffie–Hellman ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
HMAC	Hash Message Authentication Code
RSA	Rivest, Shamir und Adleman
SHS	Secure Hash Standard
SHA	Secure Hash Algorithm
TLS	Transport Layer Security

ANNEX A SRTP Profile

§Annex C (Normative) out of 3GPP TS 33.328 [19C] Release 12: SRTP profiling for IMS media plane security

An IMS UE and IMS core network entity capable of supporting IMS media plane security (SDES and/or KMS based)

- Shall support all mandatory features defined in RFC 3711 [9] except that it does not have to support key derivation rates different from zero (KDR <> 0).
- May support RFC 4771, "Integrity Transform Carrying Roll-Over Counter for the Secure Real-time Transport Protocol (SRTP)" [RFC 4771] for SDES based media plane security. RFC 4771 shall be supported and used for KMS based media plane security RFC 4771 defines functionality that is essential to simplify late entry in group communications and broadcasting sessions.

ANNEX B Implementation example of DNS Procedures (Informative)

For DNS procedures the baseline 1TR114 Annex B is valid (Section ANNEX E)

B.1 VoSIP related DNS

Regarding VoIP communication the UE typically requests URI's like following (non-exhaustive):

- sip:tel.t-online.de (Register)
- sip:user@tel.t-online.de (Invite)

Thereafter VoSIP compliant UE's/IAD request NAPTR records for the requested (example) domain "tel.t-online.de"

Standard query

Queries

tel.t-online.de: type NAPTR, class IN

Standard query response

Answers

tel.t-online.de.	IN	NAPTR	50	50	"s"	"SIPS+D2T"	_sips._tcp.tel.t-online.de.
tel.t-online.de.	IN	NAPTR	90	50	"s"	"SIP+D2U"	_sip._udp.tel.t-online.de.
tel.t-online.de.	IN	NAPTR	100	50	"s"	"SIP+D2T"	_sip._tcp.tel.t-online.de.

After receipt of the DNS NAPTR response the UE must execute the entries according standards (RFC3263, 3401, 3402, 3403, 3404 etc.)

The IMS platform of Deutsche Telekom is responsible for the order of preference of the records within the DNS NAPTR response.

If the DNS server response contains multiple NAPTR records, the UE must discard any records which are not applicable.

In case the UE requested a SIP URI, if the DNS NAPTR response contains records with 'SIPS' as protocol this must be retained by the UE acc. to RFC 3263.

Which record finally is used depends therefore both on:

- UE: supported protocols by the UE (for VoSIP compliant UE's: 'TLS over TCP' or 'UDP') and
- VoIP core: the order of preference by the platform servers (according to the ranking in the NAPTR response)

B.2 Example VoSIP DNS message flow

Standard query

Queries

tel.t-online.de: type NAPTR, class IN

Standard query response

Answers

tel.t-online.de.	IN	NAPTR	50	50	"s"	"SIPS+D2T"	_sips._tcp.tel.t-online.de.
tel.t-online.de.	IN	NAPTR	90	50	"s"	"SIP+D2U"	_sip._udp.tel.t-online.de.
tel.t-online.de.	IN	NAPTR	100	50	"s"	"SIP+D2T"	_sip._tcp.tel.t-online.de.

Standard query

Queries

_sips._tcp.tel.t-online.de: type SRV, class IN

Standard query response

Answers

_sips._tcp.tel.t-online.de: type SRV, class IN, priority 0, weight 5, port 5061, target tas001.voip.t-ipnet.de

_sips._tcp.tel.t-online.de: type SRV, class IN, priority 1, weight 5, port 5061, target tas002.voip.t-ipnet.de

Additional records

tas001.voip.t-ipnet.de: type A, class IN, addr 217.1.1.1

tas002.voip.t-ipnet.de: type A, class IN, addr 217.1.1.2

Example DNS sequence diagrams

- Successful DNS query for secure _sips._tcp

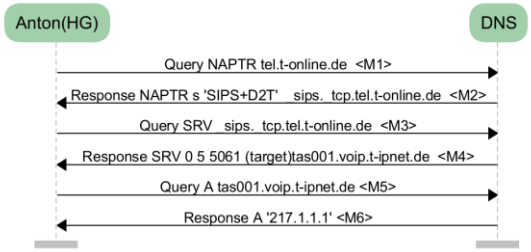

Figure B2.1 successful DNS (SIPS)

Annex C Profiling of SDES

§Annex E (normative):out of 3GPP TS 33.328 [19C] Release 12 Profiling of SDES

The present Annex contains a complete list of parameters that may be contained in an SDES crypto attribute, according to RFC 4568.

The following short-hand notation is used:

- "mandatory / optional to support / use" means: "This parameter shall / may be supported / used in implementations conforming to 3GPP specifications."

The default use is that the sender omits the parameters that are optional to use.

CRYPTOGRAPHIC ALGORITHMS

cryptosuite: mandatory to support and use

In addition to mandating the support and use of the parameter "cryptosuite" in an SDES crypto attribute, the cryptosuite "AES_CM_128_HMAC_SHA1_80", as defined in RFC 4568, is mandatory to support.

"KEY PARAMETERS" (ONE OR MORE TIMES):

key: mandatory to support and use

salt: mandatory to support and use

key lifetime: optional to support and use for e2e security, shall not be used for e2ae security (cf. clauses 7.2.1 and 7.3.1 of this specification).

Master Key Index (MKI): optional to support, mandatory to use if more than one set of key parameters is contained in the crypto attribute, otherwise optional to use. If only one master key is used, an MKI is not recommended to be used.

NOTE: It is not guaranteed that implementations support more than one master key per crypto attribute. If only one master key is used, an MKI has no function as it adds to the SRT(C)P packet overhead.

Length of MKI field: optional to support, mandatory to support if MKI is supported, mandatory to use if MKI is used.

"SESSION PARAMETERS"

key derivation rate: optional to support and use

UNENCRYPTED_SRTP: mandatory to support and optional to use

UNENCRYPTED_SRTCP: mandatory to support and optional to use

UNAUTHENTICATED_SRTP: mandatory to support and optional to use

NOTE: The flags “UNENCRYPTED_SRTP” and “UNENCRYPTED_SRTCP**”** may be useful when regulations do not permit encryption, but authentication is still desired. The flag “UNAUTHENTICATED_SRTP” may be useful to reduce the packet size for e.g. voice traffic where integrity protection may not be needed, cf. the situation on 3GPP radio interfaces over which user data are not integrity-protected.

forward error correction order: not applicable

key parameters for the FEC stream: optional to support and use

window size hint: optional to support and use

Deusche Telekom endorsment, the following prameter settings shall be used:

Parameter	***Default***
Key derivation rate	***0***
Master key length	***128 bits***
Master salt key length	***112 bits***
PRF	***AES_CM***
Session authentication key length	***128***
Session encryption key length	***128 bits***
Session salt key length	***112***
SRTP authentication	***HMAC-SHA1***
SRTCP authentication	***HMAC-SHA1***

Parameter	***Default***
SRTP HMAC tag length	***80***
SRTCP HMAC tag length	***80***
SRTP packets maximum lifetime	***2^48 packets***
SRTCP packets maximum lifetime	***2^31 packets***
SRTP replay-window size	***64***
SRTCP replay-window size	***64***

Version	Published	Remarks
3.0.0		-locating P-CSCF and correct prioritization of P-CSCF in case of registration including maintenance procedures. -Preconditions support "passive" better described -Early-Media Header and indication of early media described to avoid misinterpretation. And allow handling of calls initiated by mobile devices. - use of from-change. No default setting - deletion of Annex A - Update of Annex B - Deletion of TS 124.503 - UPDATE to 3GPP Release 11 documents -Correction of *# Procedures using PIN (ECT, OCB, Kick Out, Black List, White List, ACR, CB, ICB) - CLIR 3 included in D.2.0 - Documentation Update TIP/TIR and OIP/OIR -MWI voided - Documentation Update of " 8.6 Support of NAT traversal by the UE" -MIME Type UPDATE Table 7-5 -UPDATE Table 7-4 SIP Headers - add references TR-069, TR-104 and TR-181 - add reference 3GPP TS 23.003 - C.2.8 allow implementations acting on "application/vnd.3gpp.cw+xml" All changes are backward compatible with the procedures described within 1TR114 Version 2.4.0
Corrigendum 1	20.02.2014	Replacement of Page 30 in 1TR114 Version 3.0
Amendment 1		Additions to 1 TR 114 for the SIP REQUEST Retry Mechanism in Failure Cases
Amendment 2	14.12.2016	Addition of requirements for secure VoIP. TLS and SRTP added Replacement of text in Annex B of this document for sections 6.1.2 and 6.1.3. Cipher Suits, Algorithms, Keys and Hash procedures/requirements added. 3GPP procedures are shown but not yet decided to be supported by the IMS core. Eliptical Cipher Suits added New informative Annex for VoSIP DNS example New Annex for SDES profiling Annex for DNS examples

Version	Published	Remarks
		Download page for certificate included