FORUM NOKIA

Nokia Series 40 VoIP v72 Implementation Specifications

Version 1.1; November 27, 2008

VoIP

NOKIA

Contents

Change history

March 26, 2008	Version 1.0	Initial document release.
November 27, 2008	Version 1.1	Added descriptions about fallbacks for secure calls, boolean message waiting notifications, emergency calls, and device management.

1 Introduction

This document describes how the implementation of Nokia Series 40 Voice over IP (VoIP) v72 Release fulfills the IETF, 3GPP, ITU, OMA, and other specifications.

Note: Radio-related specifications, such as the IEEE specifications, fall outside the scope of this document.

2 Features

2.1 Basic call

Related specifications

- RFC 2617 HTTP Authentication: Basic and Digest Access Authentication [13]
- RFC 3261 SIP: Session Initiation Protocol [15]
- RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP) [19]
- RFC 3310 Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) [26]
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications [32]
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control [33]
- RFC 4855 Media Type Registration of RTP Payload Formats [35]
- RFC 4856 Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences [24]
- RFC 3665 Session Initiation Protocol (SIP) Basic Call Flow Examples [38]
- RFC 3824 Using E.164 numbers with the Session Initiation Protocol (SIP) [39]

Implementation notes

- Implementation supports Section 8.1.3.5 of RFC 3261 in creating a new request after 401 and 407 responses. Re-INVITE once after received 491 is supported. This is described in Section 14.2, RFC 3261.
- INVITE is supported in and outside dialog. CANCEL is supported outside dialog. ACK, BYE, NOTIFY, REFER, PRACK, UPDATE are supported inside existing dialog. Terminal responses to incoming unsupported messages with 501 Not Implemented or 405 Method Not Allowed.
- Implementation does not support Sections 3.2, 3.4 or 3.5 of RFC 3665.
- Implementation supports IPv4 and IPv6 in signaling.
- Implementation supports RFC 3824 by supporting E.164 numbers in SIP URI format sip:<telephone number>@<domain>, for example, sip:1234567@domain.com - that is, the parameter “user:phone” is not included.
- Both HTTP Digest and Digest AKA are supported as SIP authentication method.

2.1.1 Offer/answer

Related specifications

- RFC 4566 SDP: Session Description Protocol [11]
- RFC 3264 An Offer/Answer Model with the Session Description Protocol (SDP) [23]
- RFC 4855 Media Type Registration of RTP Payload Formats [35]
- RFC 4856 Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences [24]
- RFC 3960 Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP) [43]

Implementation notes

- Early Media is supported. Reference to RFC 3960 is made to point out a specification describing the generation of a local ringing tone, in case early media is not available.

- Implementation is done according to RFC 3264 with the following exceptions:
  - A port number of zero is used only for rejecting offered media for MT sessions, Section 5.1, RFC 3264.
  - Multicast streams are not supported.
  - Streams are marked as “sendonly” when generating offer for HOLD inside session and “recvonly” when generating answer to a HOLD offer. Streams are marked as “recvonly” in answer when “inactive” is received in offer. Attribute “sendrecv” is used only when resuming from HOLD (in offer and answer). Section 6.1, RFC 3264.
  - Every answer to any offer contains only the most preferred supported codec. Section 6.1, RFC 3264.
  - Packetisation interval is supported with "ptime" and "maxptime" attributes. Section 6.1, RFC 3264.
  - Only one media stream (audio) is supported, Chapter 8, RFC 3264.
  - Changing the port number during session is not supported in MO (Mobile Originated) direction, but it is supported in MT (Mobile Terminated) direction. In other words, a new offer with a different port number is not supported, but an arrived offer from another source with a changed port number is supported. Section 8.3.1, RFC 3264.
  - Changing the transport of a stream is not supported. Section 8.3.1, RFC 3264.
  - Changing the media type during the session is not supported. Section 8.3.3, RFC 3264.
  - Receiving audio with every codec presented in sent offer is supported.

2.1.2 Codec payloads

Related specifications

- AMR-NB
  - 3GPP TS 26.090 AMR Speech Codec; Transcoding Functions [1]
  - RFC 4867, RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs [25]
- G.711 (PCMA/PCMU)
  - ITU-T G.711 Appendix I [5]
  - ITU-T G.711 Appendix II [6]
  - RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control [33]
  - RFC 4855 Media Type Registration of RTP Payload Formats [35]
  - RFC 4856 Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences [24]
- G.729
  - ITU-T G.729 [8]
  - ITU-T G.729 Annex B [9]
  - RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control [33]
  - RFC 4855 Media Type Registration of RTP Payload Formats [35]
  - RFC 4856 Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences [24]
- G.726
  - ITU-T G.726 [7]
  - RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control [33]
  - ITU-T I.366.2 AAL type 2 service specific convergence sublayer for trunking [34]

- RFC 4855 Media Type Registration of RTP Payload Formats [35]
- RFC 4856 Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences [24]

Implementation notes

- AMR-NB:
  - Only AMR-NB is currently supported (RFC 4867 defines the same payload format for AMR-WB as well).
  - AMR-NB Payload format does not support UEP or UED, Section 3.6.1, RFC 4867. This also means that frame CRCs are not supported (Section 4.4.2, RFC 4867).
  - RTP Packets containing only NO_DATA frames are not sent. NO_DATA frame blocks that contain NO_DATA at the end of an RTP packet are sent Section 4.3.2, RFC 4867. Implementation can support receiving packets consisting of only NO_DATA frame blocks (for example between SID_UPDATEs).
  - AMR-NB payload format supports only single or double redundancy (AMR FEC), Section 3.7.1, RFC 4867. Redundancy is not supported on sender side.
  - Following MIME parameters are supported and can be negotiated: *octet-align*; *mode-set*; *mode-change-period*; *mode-change-neighbor*; *ptime*; *maxptime*.
  - Following MIME parameters are neither supported nor accepted in negotiation: *crc*; *robust-sorting*; *interleaving; mode-change-capability; max-red*.
  - Following MIME parameters have a restricted set of values which can be negotiated: *channels*, single channel payload is supported (channels=1) and used by default if omitted in negotiation.
- G.711:
  - DTX is supported with Generic Comfort Noise (CN) on sender side as specified in Section 4.1, RFC 3551.
  - G.711 payload format as specified in Section 4.5.14, RFC 3551.
  - Following MIME parameters are supported and can be negotiated: *ptime*, multiples of 10ms are supported; *maxptime*.
- G.729:
  - DTX is supported with G.729 Annex B on sender side as specified in Section 4.1, RFC 3551.
  - G.729 payload format as specified in Section 4.5.6, RFC 3551 (G.729 / G.729A only). G.729 Annex B is also supported. Other G.729 versions are not supported.
  - Following MIME parameters are supported and can be negotiated: *ptime*, multiples of 10ms are supported; *maxptime*; *annexb*, value “yes” is implied if this parameter is omitted in negotiation.
- G.726:
  - DTX is supported with Generic Comfort Noise (CN) on sender side as specified in Section 4.1, RFC 3551.
  - G.726 payload format as specified in Annex E of ITU-T I.366.2 or Section 4.5.4 of RFC 3551 depending on the VoIP settings as defined in the Nokia Series 40 VoIP v72 Configuration Tutorial.
  - All bitrates are supported, MIME subtypes: G726-16, G726-24, G726-32, G726-40
  - Following MIME parameters are supported and can be negotiated: *ptime*, multiples of 10ms are supported; *maxptime*.
- Payload types:

- Codecs having dynamic payload types will get numbers starting from 96 according to the order of codecs in the provisioned settings with the exception that the Telephone-event gets the last value.

2.1.3 Comfort noise

Related specifications

- RFC 3389 RTP Payload for Comfort Noise (CN) [29]
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control [33]
- RFC 4867 RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs [25]

Implementation notes

- Generic comfort noise support with G.711 (PCMA & PCMU) and G.726 codecs, as specified in RFC 3389.
- Update interval for generic CN depends on the used codec. The CN update happens when the encoder detects significant changes in the background noise, and the implementation will generate and send an update CN RTP packet.
- Generic comfort noise usage with AMR-NB is not supported as the AMR-NB codec itself contains a method for comfort noise/silence suppression that can be signaled inband if VAD is enabled.
- Generic CN usage with G.729 is not supported. Instead G.729 Annex B is used as specified in RFC 3551.

2.1.4 Media QoS marking

Related specifications

- None.

Implementation notes

- Implementation uses the code point 101110 (46 dec) as the default code point.

2.1.5 DTMF

Related specifications

- RFC 4733 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals [14]

Implementation notes

- Implementation supports:
  - Out-of-band (RFC 4733) DTMF sending.
  - Chapter 2 (RTP Payload Format for Named Telephone Events), RFC 4733. Supported event types are DTMF events, as specified in Section 3.2.
  - In-band DTMF playback.
- Implementation does not support:
  - Chapter 4 (RTP Payload Format for Telephony Tones), RFC 4733.
  - Out-of-band DTMF playback at the receiving end.
  - In-band DTMF sending.

2.2 Secure call

Related specifications

- RFC 3261 SIP: Session Initiation Protocol [15]
- draft-ietf-sip-sips-06.txt The use of the SIPS URI Scheme in the Session Initiation Protocol (SIP) [16]
- RFC 3711 The Secure Real-time Transport Protocol (SRTP) [17]
- RFC 4568 Session Description Protocol (SDP) Security Descriptions for Media Streams [18]
- RFC 3263 Session Initiation Protocol (SIP): Locating SIP Servers [20]
- RFC 2782 A DNS RR for specifying the location of services (DNS SRV) [21]
- RFC 2915 The Naming Authority Pointer (NAPTR) DNS Resource Record [22]

Implementation notes

- Supporting only SIPS scheme in all headers.
- TLS transport URI parameter is not supported (as defined in draft-ietf-sip-sips-06.txt).
- Re-direction from secure to unsecure is not allowed. No user query is made in that case.
- Implementation does not support security preconditions.
- Implementation supports the following fallback logic with MO calls:
  - If the destination address is a SIPS URI: A secure call is attempted without any fallback.
  - If secure call is mandated in VoIP settings: A secure call is attempted without any fallback.
  - If secure call is preferred in VoIP settings: A secure call is first attempted. If it fails, a fallback to non-secure call is attempted.
  - If non-secure call is preferred in VoIP settings: A non-secure call is first attempted. If the network or the remote endpoint rejects the call attempt with a 480 (Temporarily Unavailable) response with a Warning header with warn-code 381 "SIPS Required", a fallback to secure call is attempted.

2.3 Call forwarding

Related specifications

- draft-ietf-sipping-service-examples-12.txt Session Initiation Protocol Service Examples [2]
- RFC 3261 SIP: Session Initiation Protocol [15]
- ETSI TS 183 004 PSTN/ISDN simulation services: Communication Diversion (CDIV); Protocol specification V1.1.1 [44]

Implementation notes

- Implementation supports Section 21.1.3 of RFC 3261 by recognizing the 181 Call Is Being Forwarded answer.
- Implementation supports Section 21.3.2 of RFC 3261 by recognizing the response 301 Moved Permanently.
- Implementation supports Section 21.3.3 of RFC 3261 by recognizing the response 302 Moved Temporarily. 300 is handled as an error, 301 and 302 are redirected to the requested URI.
- 302 Moved Temporarily is used in the MT forwarding case.

2.4 Call transfer

Related specifications

- draft-ietf-sipping-service-examples-12.txt Session Initiation Protocol Service Examples [2]
- RFC 3515 The Session Initiation Protocol (SIP) Refer Method [31]
- RFC 3891 The Session Initiation Protocol (SIP) "Replaces" Header [41]
- RFC 3892 The Session Initiation Protocol (SIP) Referred-By Mechanism [42]
- ETSI TS 183 029 PSTN/ISDN simulation services: Explicit Communication Transfer (ECT); Protocol specification V1.1.1 [45]

Implementation notes

- Implementation supports:
  - Attended call transfer, Section 2.5 of the draft-ietf-sipping-service-examples-12.txt.
  - Rejected transfer with sending 503 Service Unavailable response to REFER.
  - Failed transfer with sending NOTIFY with 503 Service Unavailable content. No other failing NOTIFY responses are sent.
- Implementation does not support:
  - REFER coming in new dialog.
  - Unattended call transfer, Section 2.4 of the draft-ietf-sipping-service-examples-12.txt.
  - Section 2.4.6 of the RFC 3515.

2.5 CLIP

Related specifications

- RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP) [27]
- RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks [28]

Implementation notes

- In MO direction, when CLIP is on (that is, when CLIR is off), the "Privacy" header is omitted.
- Network might support/add:
  - P-Asserted-Identity header, Section 9.1, RFC 3325. If present, remote identity is read from this header, otherwise from the "From" header.

2.6 CLIR

Related specifications

- RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP) [27]
- RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks [28]

Implementation notes

- In MO direction, implementation supports:
  - Privacy header. Header value is “id” when CLIR is on. Section 9.3, RFC 3325 and Section 4.2, RFC 3323.

- From header as "Anonymous <sip:anonymous@anonymous.invalid>". Section 4.1.1.3, RFC 3323.

- In MT direction, the "From" header is checked for anonymous call.

2.7 Message waiting indicator (MWI)

Related specifications

- RFC 3842 A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP) [40]

Implementation notes

- Implementation supports:
  - MWI to user is done with audible and visible information. After user interaction, the MWI is discarded without storage in the message inbox. Chapter 2, RFC 3842.
  - Boolean message waiting notification (Message-Waiting: Yes) that does not contain a message summary, Sections 3.5, RFC 3842.
- Following parameters are parsed from the NOTIFY content and shown on UI (Sections 3.5 and 4.1, RFC 3842):
  - Message-Waiting
  - Voice-Messages
  - New messages
- Implementation does not support:
  - MWI indication NOTIFY without SUBSCRIBE
- Following parameters are not parsed from NOTIFY content, Sections 3.5 and 4.1, RFC 3842:
  - Fax-Messages
  - Message-Account
  - From
  - Old messages
  - Subject
  - Date
  - Priority
  - Message-ID
  - To

2.8 NAT/FW traversal

2.8.1 STUN

Related specifications

- RFC 3489 STUN: Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) [30]

Implementation notes

- Implementation does not support Section 10.3 (Binding Acquisition), RFC 3489 except STUN binding request/response and STUN binding refreshing (keep alive).
- Implementation does not support shared secret request/response Section 8.2 Shared Secret Requests, RFC 3489.

2.8.2 Symmetric signaling

Related specifications

- RFC 3581 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing [36]

Implementation notes

- Public IP address and port are discovered using STUN when SIP registration is done over UDP and STUN is enabled in settings. This is for checking if the public address seen by the SIP server differs from the address received in the network link setup.
- Implementation supports "rport" parameter for the "Via" header field, defined in RFC 3581, which allows a client to request that the server sends the response back to the source IP address and the port where the request came from.
- When SIP registration is done over TCP (or done over UDP and STUN is disabled in settings), the "Via" header (from the first response to REGISTER) is checked for “received” and “rport” parameters. Those parameters advertise the public IP address and port as seen by the SIP server. If they are different from the local addresses received in the network link setup, there are NATs on the route. In that case public IP address and port are learnt from the first response to REGISTER (when “rport” is used). This address is used in the next registration / re-registration in the Contact header.
- Default port number 5060 is used for SIP signaling if not otherwise discovered.
- For the symmetric SIP signaling, SIP requests and responses are received and sent from the same address and port.

2.8.3 Symmetric media

Related specifications

- RFC 4961 Symmetric RTP / RTP Control Protocol (RTCP) [3]

Implementation notes

- Implementation fully supports RFC 4961.
- Multiplexing RTP data and control packets on a single port is not supported. For more information, see draft-ietf-avt-rtp-and-rtcp-mux-07.txt [4].

2.8.4 Open ports for RTP/RTCP traffic

Related specifications

- RFC 3605 Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) [37]
- RFC 3960 Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP) [43]

Implementation notes

- Only separated RTP and RTCP ports are supported.
- Implementation does not support different IP addresses for RTCP and RTP.

2.8.5 NAT binding keep alive

Related specifications

- None.

Implementation notes

- Firewall keep alive for uplink stream is started in MO sessions every time a provisional answer with SDP content is received, and stopped when 200 OK is received. Keep alive is also used when session is on hold. In both situations, RTP dummy packets are sent with accepted audio codec's payload type.
- STUN protocol is used for getting the corresponding public IP address and the port for the private address and port.
- NAT and/or firewall bindings are kept alive by refreshing them while session is in hold state. If the own address of the terminal is different from the address returned by STUN, and the IP address and port of the outbound proxy (or registrar when there is no outbound proxy) and local STUN server are not identical, the following two types of packets are sent:
  - UDP packets containing CRLFCRLF to SIP proxy or registrar when there is no proxy (for keep-alive).
  - STUN binding requests to the separate STUN server (for detecting flow failure due to NAT reboot).
- When TCP is used, STUN is not used for public address query. TCP keep-alive (sending of a dummy octet and waiting for ack) is used to find out if TCP connection is disconnected.
- For keeping the media link alive in the MT call setup for possible early media, RTP packets are sent with silence information in the payload until 200 has been sent and encoding of the UL media has been started.

2.9 Hold

Related specifications

- RFC 3261 SIP: Session Initiation Protocol [12]
- RFC 3264 An Offer/Answer Model with the Session Description Protocol (SDP) [23]

Implementation notes

- Implementation supports:
  - Hold according to Section 8.4, RFC 3264.
  - Both unidirectional and bidirectional hold and resume.
  - Receiving of old-way hold (RFC 2543, Chapter B.5).
- Implementation does not support:
  - Multicast streams or holding them are not currently supported.

2.10 Call waiting

Related specifications

- RFC 3261 SIP: Session Initiation Protocol [15]

Implementation notes

- Incoming calls are responded with SIP message 182 (Queued) when the call is in the waiting state due to another call at the receiving end.

2.11 Emergency call

VoIP emergency call is not supported. An emergency call is always made through the cellular network.

2.12 Device management

Related specifications

- OMA Device Management version 1.1.2, http://www.openmobilealliance.com/ [46]
- OMA Client Provisioning version 1.1, http://www.openmobilealliance.com/ [47]

Implementation notes

- Implementation supports OMA Device Management version 1.1.2.
- Implementation supports OMA Client Provisioning version 1.1.

3 Terms and abbreviations

Term or abbreviation	Meaning
3GPP	The 3rd Generation Partnership Project
a-law	Name of G.711 PCMU algorithm
AKA	Authentication and Key Agreement
AMR-NB	Adaptive Multi-Rate Narrowband
AMR-WB	Adaptive Multi-Rate Wideband
AOR	Address-of-record
API	Application Programming Interface
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CN	Comfort Noise
CP	Client Provisioning
CRC	Cyclic Redundancy Check
CRLF	Formatting control codes Carriage Return (CR) and Line Feed (LF)
CS call	Circuit-switched call
DM	Device Management
DND	Do Not Disturb
DTMF	Dual-Tone Multifrequency
DTX	Discontinuous Transmission
FEC	Forward Error Correction
FW	Firewall
HTTP	Hyper Text Transport Protocol
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
IETF	The Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union
Maxptime	The maximum amount of media (in milliseconds) which can be encapsulated in a payload packet.
MIME	Multipurpose Internet Mail Extensions
MO	Mobile-originated
MT	Mobile-terminated
MWI	Message Waiting Indicator
NAT	Network Address Translation
OMA	Open Mobile Alliance

PCMA	Pulse Code Modulation a-law
PCMU	Pulse Code Modulation µ-law
Ptime	The preferred amount of media (in milliseconds) which is encapsulated in a payload packet. The actual packetisation interval is usually the same as ptime, but can vary depending on the usage of VAD and/or DTX.
PHB	Per-Hop Behaviour
PS call	Packet-switched call
QoS	Quality of Service
RFC	Request For Comments
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
SDP	Session Description Protocol
SID	Silence Insertion Descriptor
SIP	Session Initiation Protocol
STUN	Simple Traversal of UDP through NAT; a protocol that allows applications to detect that network address translation (NAT) is being used.
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UED	Unequal Error Detection
UEP	Unequal Error Protection
UI	User Interface
URI	Uniform Resource Identifier
VAD	Voice Activity Detection
VoIP	Voice over IP
µ-law	Name of G.711 PCMU algorithm

4 References

[1] 3GPP TS 26.090, AMR Speech Codec; Transcoding Functions, available at http://www.3gpp.org/

[2] draft-ietf-sipping-service-examples-12.txt, Session Initiation Protocol Service Examples, available at http://www.ietf.org/

[3] RFC 4961, Symmetric RTP / RTP Control Protocol (RTCP), available at http://www.ietf.org/

[4] draft-ietf-avt-rtp-and-rtcp-mux-07.txt, Multiplexing RTP Data and Control Packets on a Single Port, available at http://www.ietf.org/

[5] ITU-T G.711 Appendix I, available at http://www.itu.int

[6] ITU-T G.711 Appendix II, available at http://www.itu.int

[7] ITU-T G.726, available at http://www.itu.int

[8] ITU-T G.729, available at http://www.itu.int

[9] ITU-T G.729 Annex B, available at http://www.itu.int

[10] RFC 2198, RTP Payload for Redundant Audio Data, available at http://www.ietf.org/

[11] RFC 4566, SDP: Session Description Protocol, available at http://www.ietf.org/

[12] RFC 3261, SIP: Session Initiation Protocol, available at http://www.ietf.org/

[13] RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, available at http://www.ietf.org/

[14] RFC 4733, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, available at http://www.ietf.org/

[15] RFC 3261, SIP: Session Initiation Protocol, available at http://www.ietf.org/

[16] draft-ietf-sip-sips-06.txt, The use of the SIPS URI Scheme in the Session Initiation Protocol (SIP), available at http://www.ietf.org/

[17] RFC 3711, The Secure Real-time Transport Protocol (SRTP), available at http://www.ietf.org/

[18] RFC 4568, Session Description Protocol (SDP) Security Descriptions for Media Streams, available at http://www.ietf.org/

[19] RFC 3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP), available at http://www.ietf.org/

[20] RFC 3263, Session Initiation Protocol (SIP): Locating SIP Servers, available at http://www.ietf.org/

[21] RFC 2782, A DNS RR for specifying the location of services (DNS SRV), available at http://www.ietf.org/

[22] RFC 2915, The Naming Authority Pointer (NAPTR) DNS Resource Record, available at http://www.ietf.org/

[23] RFC 3264, An Offer/Answer Model with the Session Description Protocol (SDP), available at http://www.ietf.org/

[24] RFC 4856, Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences, available at http://www.ietf.org/

[25] RFC 4867, RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs, available at http://www.ietf.org/

[26] RFC 3310, Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA), available at http://www.ietf.org/

[27] RFC 3323, A Privacy Mechanism for the Session Initiation Protocol (SIP), available at http://www.ietf.org/

[28] RFC 3325, Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, available at http://www.ietf.org/

[29] RFC 3389, RTP Payload for Comfort Noise (CN), available at http://www.ietf.org/

[30] RFC 3489, STUN: Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), available at http://www.ietf.org/

[31] RFC 3515, The Session Initiation Protocol (SIP) Refer Method, available at http://www.ietf.org/

[32] RFC 3550, RTP: A Transport Protocol for Real-Time Applications, available at http://www.ietf.org/

[33] RFC 3551, RTP Profile for Audio and Video Conferences with Minimal Control, available at http://www.ietf.org/

[34] ITU-T I.366.2, AAL type 2 service specific convergence sublayer for trunking, available at http://www.itu.int

[35] RFC 4855, Media Type Registration of RTP Payload Formats, available at http://www.ietf.org/

[36] RFC 3581, An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing, available at http://www.ietf.org/

[37] RFC 3605, Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP), available at http://www.ietf.org/

[38] RFC 3665, Session Initiation Protocol (SIP) Basic Call Flow Examples, available at http://www.ietf.org/

[39] RFC 3824, Using E.164 numbers with the Session Initiation Protocol (S IP), available at http://www.ietf.org/

[40] RFC 3842, A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), available at http://www.ietf.org/

[41] RFC 3891, The Session Initiation Protocol (SIP) "Replaces" Header, available at http://www.ietf.org/

[42] RFC 3892, The Session Initiation Protocol (SIP) Referred-By Mechanism, http://www.ietf.org/

[43] RFC 3960, Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP), available at http://www.ietf.org/

[44] ETSI TS 183 004 PSTN/ISDN simulation services: Communication Diversion (CDIV); Protocol specification V1.1.1, available at http://www.etsi.org

[45] ETSI TS 183 029 PSTN/ISDN simulation services: Explicit Communication Transfer (ECT); Protocol specification V1.1.1, available at http://www.etsi.org

[46] OMA Device Management v1.1.2, available at http://www.openmobilealliance.com/

[47] OMA Client Provisioning v1.1, available at http://www.openmobilealliance.com/

5 Evaluate this resource

Please spare a moment to help us improve documentation quality and recognise the resources you find most valuable, by rating this resource.