

Implementation Specifications for Nokia S60 VoIP

Version 1.4; October 1, 2008

VoIP

Copyright © 2006-2008 Nokia Corporation. All rights reserved.

Nokia and Forum Nokia are trademarks or registered trademarks of Nokia Corporation. Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Disclaimer

The information in this document is provided “as is,” with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification, or sample. This document is provided for informational purposes only.

Nokia Corporation disclaims all liability, including liability for infringement of any proprietary rights, relating to implementation of information presented in this document. Nokia Corporation does not warrant or represent that such use will not infringe such rights.

Nokia Corporation retains the right to make changes to this document at any time, without notice.

License

A license is hereby granted to download and print a copy of this document for personal use only. No other license to any other intellectual property rights is granted herein.

Contents

1	Introduction	5
2	Features	6
2.1	Basic call	6
2.1.1	Offer/Answer	6
2.1.2	Codec Payloads	7
2.1.3	Comfort Noise.....	9
2.1.4	Media QoS Marking.....	10
2.1.5	Redundant Data.....	10
2.1.6	DTMF	10
2.2	Call Forwarding	10
2.3	Call Transfer	11
2.4	CLIP	11
2.5	CLIR.....	12
2.6	Message Waiting Indicator (MWI).....	12
2.7	Do Not Disturb (DND).....	13
2.8	Anonymous Call Blocking.....	13
2.9	NAT/FW traversal.....	13
2.9.1	STUN	13
2.9.2	Symmetric Signaling	13
2.9.3	Symmetric Media.....	13
2.9.4	Open Ports for RTP/RTCP traffic.....	14
2.9.5	NAT Binding Keep Alive.....	14
2.10	Hold.....	14
2.11	Call Waiting	15
2.12	Device Management SIP/VoIP/NATFW/GenVoIP Adapter	15
2.13	Client Provisioning SIP/VoIP/NATFW/GenVoIP Adapter	16
2.14	Emergency call.....	16
2.15	Secure VoIP call	16
2.16	VoIP Presence	18
2.17	Presence (SIMPLE/XDM) settings for VoIP	18
3	Terms and abbreviations	20
4	References	22
5	Evaluate this resource	25

Change history

December 21, 2006	Version 1.0	Initial document release
March 28, 2007	Version 1.1	Document title changed. Sections 2.14 and 2.15 added.
June 25, 2007	Version 1.2	Section 2.1.2 Codec payloads complemented with RFC 4867 information. Sections 2.12, 2.13 and 2.14 updated.
October 16, 2007	Version 1.3	Implementation notes on G.711 updated in Section 2.1.2 “Codec payloads”.
October 1, 2008	Version 1.4	Updated for Nokia S60 Voice over IP (VoIP) implementation Release 3.0. Sections 2.16, and 2.17 added. Sections 2.1.2, 2.1.5, 2.7, 2.9.1, 2.12, 2.13, 2.14, and 2.15 updated.

1 Introduction

This document describes how the Nokia S60 Voice over IP (VoIP) implementation (releases 2.0 – 2.3 and 3.0) 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 [18]
- RFC 3261 SIP: Session Initiation Protocol [22]
- RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP) [23]
- 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 [33]
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control [34]
- RFC 3555 MIME Type Registration of RTP Payload Formats [35]
- RFC 3665 Session Initiation Protocol (SIP) Basic Call Flow Examples [38]
- RFC 3824 Using E.164 numbers with the Session Initiation Protocol (SIP) [40]

Implementation notes:

- Implementation supports Section 8.1.3.4 of RFC 3261 in creating new INVITE to address given in contact header of the 3xx response by letting user decide about the new call.
- Implementation supports Section 8.1.3.5 of RFC 3261 in creating 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 method is supported in and outside dialog. ACK, BYE, CANCEL, NOTIFY, REFER, PRACK, OPTIONS are supported inside existing dialog. UPDATE is not supported. Terminal responses to incoming unsupported message with 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>;user=phone**, for example, sip:1234567@domain.com;user=phone.
- In insecure sessions, implementation does not support RFC 3262 in sending reliable response with require: 100rel if received request contains require: 100rel.
- Only HTTP digest authentication as SIP registration method supported (username + password needs to be configured in terminal).

2.1.1 Offer/Answer

Related specifications:

- RFC 2327 SDP: Session Description Protocol [15]
- RFC 3264 An Offer/Answer Model with the Session Description Protocol (SDP) [24]
- RFC 3555 MIME Type Registration of RTP Payload Formats [35]
- RFC 3960 Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP) [46]

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 HOLD offer. Streams are marked as “inactive” when generating both bidirectional hold (Double Hold) offer and answer. Streams are marked as “recvonly” when generating resuming offer from Double Hold and “sendonly” when generating answer to Double Hold resume offer. In session establishment phase, “inactive” is used in offer answer for MT sessions when two-phased session establishment is needed. 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.
 - Packetization interval is supported with `ptime` and `maxptime` attributes, Section 6.1, RFC 3264.
 - Current implementation neither supports adding new media streams during the session nor more than one media stream at session initialization phase although the implementation is designed to support them, Chapter 8, RFC 3264.
 - Adding new or removing existing media stream is not supported, Sections 8.1 and 8.2, RFC 3264.
 - Changing the port number during session is not supported in MO direction, but it is supported in MT direction, that is, new offer with different port number is not supported, but arrived offer from another source with 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 3267 RTP Payload Format for AMR and AMR-WB [25]
 - RFC 4867 RTP Payload Format and File Storage Format for AMR and AMR-WB [48] (restricted support)
- G.711 (PCMA/PCMU)
 - ITU-T G.711 Appendix I [6]
 - ITU-T G.711 Appendix II [7]
 - RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control [34]
 - RFC 3555 MIME Type Registration of RTP Payload Formats [35]
- 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 [34]
- RFC 3555 MIME Type Registration of RTP Payload Formats [35]
- iLBC
 - RFC 3951 Internet Low Bit Rate Codec (iLBC) [44]
 - RFC 3952 RTP Payload Format for iLBC Speech [45]

Implementation notes:

- AMR-NB:
 - Only AMR-NB is currently supported (RFC 3267 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 3267. This also means that frame CRCs are not supported, Section 4.4.2, RFC 3267.
 - RTP Packets containing only NO_DATA frames are not sent. Neither NO_DATA frame blocks that contain NO_DATA at the end of an RTP packet are sent, Section 4.3.2, RFC 3267. 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 3267.
 - The following MIME parameters are supported and can be negotiated: `octet-align`; `mode-set`; `mode-change-period`; `mode-change-neighbor`; `ptime`; `maxptime`.
 - The following MIME parameters are neither supported nor accepted in negotiation: `crc`; `robust-sorting`; `interleaving`.
 - The 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.
 - From Nokia VoIP release 2.2 onwards, parameter `mode-change-period` is supported as described in RFC 4867.
 - From Nokia VoIP release 2.2 onwards, parameter `max-red` described in RFC 4867 has a restricted set of values (allowed values are 0...100 and the value must be a multiple of the AMR frame time which is 20). If omitted from codec settings provisioning, the `max-red` parameter is not used in signaling.
 - From Nokia VoIP release 2.2 onwards, the `max-red` parameter enables Forward Error Correction (FEC) described in Section 3.7.1, RFC 4867.
 - The used redundancy level is determined by the `max-red` parameter. For example, if the `max-red` parameter is 20, redundancy level 1 is used, and if the `max-red` is 100, redundancy level 5 is used.
 - Note that the `max-red` parameter value 0 is valid, and it indicates that no redundancy is used.
 - The redundancy level determined from the `max-red` parameter is not changed during a call, thus the use of `max-red` parameter is discouraged because of added bandwidth usage.
 - By default the implementation can handle redundancy levels up to 5 without any signaling, as implied in Section 3.7.1, RFC 4867.
- G.711:
 - DTX supported as specified in Section 4.1, RFC 3551.
 - G.711 payload format as specified in Section 4.5.14, RFC 3551.

- The following MIME parameters are supported and can be negotiated: `ptime`, packet sizes ≥ 20 ms, and multiples of 10ms are supported in receiving, multiples of 20ms packet sizes are supported in sending; `maxptime`.
From Nokia VoIP release 2.3 onwards, multiples of 10 ms packet sizes are supported in sending and receiving.
- The following MIME parameters are neither supported nor accepted in negotiation: `channels`.
- G.729:
 - DTX supported 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.
 - The following MIME parameters are supported and can be negotiated: `ptime`, multiples of codec frame size (10ms) are supported; `maxptime`; `annexb`, value “yes” is implied if this parameter is omitted in negotiation.
- iLBC:
 - DTX supported as specified in Section 4.1, RFC 3551.
 - iLBC payload format, as specified in RFC 3952.
 - The following MIME parameters are supported and can be negotiated: `ptime`; `maxptime`; `mode`, 30ms mode (`mode=30`) is used by default if omitted in negotiation.
- Payload types:
 - The default dynamic payload types that are used are the following:
 - i. AMR-NB 96
 - ii. iLBC 97
 - iii. Telephone-events 98
 - By default, these dynamic payload types are used in the offer, but other dynamic payload types can be used if negotiated.

2.1.3 Comfort Noise

Related specifications:

- RFC 3389 RTP Payload for Comfort Noise (CN) [30]
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control [34]

Implementation notes

- DTX support as specified in Section 4.1, RFC 3551.
- Generic comfort noise support with G.711 (PCMA & PCMU) codec, as specified in RFC 3389.
- Generic comfort noise (RFC 3389) is supported with iLBC.
- G.729 uses DTX or Annex B, as specified in RFC 3551.
- Update interval for generic CN depends on the used codec. The CN update will happen 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.

2.1.4 Media QoS Marking

Related specifications:

- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behaviour) [20]

Implementation notes:

- Implementation uses the code point 101110 as the default code point, as specified in Section 2.7, RFC 3246.

2.1.5 Redundant Data

Related specifications:

- RFC 2198 RTP Payload for Redundant Audio Data [13]
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control [34]

Implementation notes:

- Implementation fully supports the IETF RFC 2198 specification with the following restrictions:
 - Supported when offered by remote party.
 - Supported redundancy levels are 0 and 1.
 - Mixing different kind of encoding is not supported; for example, redundant data cannot be encoded with G.711 codec when primary data is coded using AMR codec.

2.1.6 DTMF

Related specifications:

- RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals [19]

Implementation notes:

- Both inband and outband (RFC 2833) DTMF sending is supported.
- Implementation supports Chapter 3 (RTP Payload Format for Named Telephone Events), RFC 2833. Supported event types are DTMF events, as specified in Section 3.10, Table 1 with the exception of “Flash”, as specified in Section 3.3, RFC 2833.
- Implementation does not support Chapter 4 (RTP Payload Format for Telephony Tones) or Chapter 5 (Combining Tones and Named Events), RFC 2833.

2.2 Call Forwarding

Related specifications

- draft-ietf-sipping-service-examples-10.txt Session Initiation Protocol Service Examples [4]
- RFC 3261 SIP: Session Initiation Protocol [22]

Implementation notes:

- Implementation supports Section 21.1.3 of RFC 3261 by recognizing the 181 Call Is Being Forwarded answer.

- Implementation supports Sections 21.3.1, 21.3.2, and 21.3.3 of RFC 3261 by recognizing the answers 300 Multiple Choices, 301 Moved Permanently, and 302 Moved Temporarily.
- Implementation supports Sections 2.7, 2.8, and 2.9 of the draft-ietf-sipping-service-examples-10.txt by informing the user of the forwarded call in MO and MT sessions. In the MT case, this is done by comparing our registered AOR and To-Header of the INVITE.

2.3 Call Transfer

Related specifications:

- draft-ietf-sipping-cc-transfer-06.txt Session Initiation Protocol Call Control – Transfer [5]
- draft-ietf-sipping-service-examples-10.txt Session Initiation Protocol Service Examples [4]
- RFC 3515 The Session Initiation Protocol (SIP) Refer Method [32]
- RFC 3891 The Session Initiation Protocol (SIP) "Replaces" Header [42]
- RFC 3892 The Session Initiation Protocol (SIP) Referred-By Mechanism [43]

Implementation notes:

- Implementation supports:
 - Sections 2.4 and 2.5 of the draft-ietf-sipping-service-examples-10.txt.
 - Chapter 4 of the draft-ietf-sipping-cc-transfer-06.txt by using existing dialog to send REFER
 - Rejected transfer with sending 603 Decline 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
 - Sections 6.1, 6.2, 6.4, 6.5, 6.6, 6.7, 8.0, and 9.0 of the draft-ietf-sipping-cc-transfer-06.txt
 - Section 2.4.6 of the RFC 3515

2.4 CLIP

Related specifications:

- RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP) [28]
- RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks [29]

Implementation notes:

- In MO direction, implementation supports:
 - P-Preferred-Identity, Section 9.2, RFC 3325.
 - Privacy header. When CLIP is on (that is, when CLIR is off), the header value is "none", Section 9.3, RFC 3325 and Section 4.2, RFC 3323.
- In MT direction, CLIP is always on.
- Network might support/add:
 - P-Asserted-Identity header, Section 9.1, RFC 3325.

2.5 CLIR

Related specifications:

- RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP) [28]
- RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks [29]

Implementation notes:

- In MO direction, implementation supports:
 - P-Preferred-Identity, Section 9.2, RFC 3325.
 - 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.
- Network might support/add:
 - P-Asserted-Identity header, Section 9.1, RFC 3325.

2.6 Message Waiting Indicator (MWI)

Related specifications:

- RFC 3842 A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP) [41]

Implementation notes:

- Implementation supports:
 - MWI to user is done with adding a new SMS message to inbox including similar audible and visible information as in normal incoming SMS message, Chapter 2, RFC 3842.
- The following parameters are parsed from NOTIFY content, Sections 3.5 and 4.1, RFC 3842:
 - Message-Account
 - Message-Waiting
 - Voice-Messages
 - From
 - New messages
 - Old messages
 - Subject
 - Date
 - Priority
 - Message-ID
 - To
- Implementation does not support:
 - MWI indication NOTIFY without SUBSCRIBE
- The following parameters are not parsed from NOTIFY content, Sections 3.5 and 4.1, RFC 3842:
 - Fax-Messages

2.7 Do Not Disturb (DND)

Related specifications:

- RFC 4504 SIP Telephony Device Requirements and Configuration [54]
- RFC 3261 SIP: Session Initiation Protocol [22]

Implementation notes:

- Implementation supports:
 - "486 Busy Here" is responded to INVITE when Do Not Disturb is enabled, Section 2.5, RFC 4504.
 - Calls are logged to "Missed calls". No indication to user.
- Implementation does not support:
 - Retry-After header field not set, Section 21.4.24, RFC 3261.
 - "480 Temporarily Unavailable" not responded, Section 21.4.18, RFC 3261.

2.8 Anonymous Call Blocking

Related specifications:

- No related specifications.

Implementation notes:

- "488 Not Acceptable Here" responded to INVITE when Anonymous Call Blocking is enabled and From header is anonymous.

2.9 NAT/FW traversal

2.9.1 STUN

Related specifications:

- RFC 3489 STUN: Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) [31]
- draft-ietf-behave-rfc3489bis-10: Session Traversal Utilities for NAT (STUN) [2]

2.9.2 Symmetric Signaling

Related specifications:

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

Implementation notes:

- 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.

2.9.3 Symmetric Media

Related specifications:

- RFC 4961 Symmetric RTP / RTP Control Protocol (RTCP) [60]

Implementation notes:

- Implementation fully supports draft-wing-behave-symmetric-rtprtcp-01.txt.
- **Note:** Multiplexing RTP data and control packets on a single port is not supported. For more information, see draft-ietf-avt-rtp-and-rtcp-mux-03.txt.

2.9.4 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) [46]

Implementation notes:

- Implementation supports SDP rtcp attribute for IPv4 described in Section 2.1, RFC 3605.

2.9.5 NAT Binding Keep Alive

Related specifications:

- draft-ietf-sip-outbound-01.txt Managing Client Initiated Connections in the Session Initiation Protocol (SIP) [3]
- The following two methods are supported:
 - SIP over UDP using STUN
 - SIP over persistent TCP using CRLF burst

Implementation notes:

- From draft-ietf-sip-outbound-01 only the NAT binding keep alive has been implemented, but not any instance or flow ID processing. Implementation will create one single flow for a single registration (over UDP or TCP) and keep the flow alive, as specified in the above Internet-Draft, if the address and port for the STUN server is the same as for the SIP proxy.
- Firewall keep alive for uplink stream is started in MO sessions every time when 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 bindings are kept alive by refreshing them while session is in hold state. Refreshing is done by sending a request periodically to STUN server.

2.10 Hold

Related specifications:

- draft-ietf-sipping-service-examples-10.txt Session Initiation Protocol Service Examples [4]
- RFC 2543 SIP: Session Initiation Protocol [16]
- RFC 3264 An Offer/Answer Model with the Session Description Protocol (SDP) [24]

Implementation notes:

- Implementation supports hold according to Section 8.4, RFC 3264.
- Both unidirectional and bidirectional hold and resume are supported. Old-way hold (RFC 2543, Chapter B.5) is also supported for unicast streams for interoperability (MT direction), but it is considered in MO direction only if the remote participant does not support newer way. Old-way hold is supported only unidirectionally, that is, if a stream is already on hold by old-way hold either by MO or MT, it cannot be placed on hold by the other end. Multicast streams or holding them are not currently supported.
- Session Initiation Protocol Service Examples offers examples of holding a unicast stream (Section 2.1) and consultation hold (Section 2.2).

2.11 Call Waiting

Related specifications:

- RFC 3261 SIP: Session Initiation Protocol [22]

Implementation notes:

- There is an own setting for PS call waiting stored to the phone in contrary to CS call waiting which is a network setting.
- PS call waiting setting is accessible through the general settings application if VoIP feature is enabled. This setting is saved to the phone's memory.
- UI side functionality of PS call waiting is the same as in CS call waiting.
- In order to indicate to the caller that the callee has an active call and the caller's call is in waiting state, SIP message 182 Queued is used (RFC 3261).

2.12 Device Management SIP/VoIP/NATFW/GenVoIP Adapter

Related specifications:

- OMA Device Management version 1.1.2, <http://www.openmobilealliance.com/> [11]

Implementation notes:

- Implementation supports OMA Device Management version 1.1.2.
- The following functions are supported:
 - SIP, VoIP, NATFW, and generic VoIP settings handling. Settings include among others codec settings, voice mailbox settings, NATFW access point specific, and domain specific settings.
 - Adding new nodes (SIP, VoIP, NATFW).
 - Deleting existing nodes (SIP, VoIP, NATFW).
 - Listing leaf objects inside node.
 - Getting values from leaf objects inside node.
 - Updating leaf object values inside node.
- The following functions of DM Adapter API are not needed or supported by now:
 - Executing commands in client through DM Framework.
 - Streaming large object data.
 - Full Atomic commands support, rollback of atomic commands not supported.

2.13 Client Provisioning SIP/VoIP/NATFW/GenVoIP Adapter

Related specifications:

- OMA Client Provisioning version 1.1, <http://www.openmobilealliance.com/> [10]

Implementation notes:

- Implementation supports OMA Client Provisioning version 1.1.
- The following functions are supported:
 - Adding new SIP, VoIP, and NATFW settings. Settings include codec settings, voice mailbox settings, NATFW access point specific, and domain specific settings.
Some of these settings can be linked to network destinations or individual IAPs using OMA standardized linking capabilities. For further information, see document [Client Provisioning Registration](#) in Forum Nokia VoIP documentation.
 - NATFW Adapter supports updating existing domain specific settings.
 - General VoIP Settings Adapter supports updating generic VoIP settings.
 - Enhanced linking capability added to OMA Client Provisioning framework (APPREF / TO-APPREF parameter pairs and NAPID / TO-NAPID parameter pairs standardized by OMA).

2.14 Emergency call

This feature is supported from Nokia S60 VoIP Release 2.1 onwards.

Related specifications:

- RFC 3261 SIP: Session Initiation Protocol [22]

Implementation notes:

- An emergency call is first attempted as a CS call if CS coverage exists.
- Priority header 'emergency' is used.
- When 'always on' profile is selected, an emergency call is attempted even if registration fails.
- Registration is not done because of an emergency call; however, first priority for a VoIP emergency call is to use registered VoIP profile, if such exists.
- User is notified that the availability for VoIP emergency calls depends on the service provider.
- Recognizing commonly used emergency numbers.
- Anonymous user ID supported.
- A VoIP emergency call will be attempted in the following order: 1) using registered VoIP profiles, 2) using provisioned, but not registered VoIP profiles, and 3) using IAPs that can be found. In the last case, SIP proxy is requested by DHCP query.

In releases prior to 2.1, a CS emergency call is tried first and after every failed VoIP emergency call, if CS coverage exists. From release 2.1 onwards, only the first CS emergency call attempt is made.

2.15 Secure VoIP call

This feature is supported from Nokia S60 VoIP Release 2.1 onwards.

Related specifications:

- RFC 2246 The TLS Protocol Version 1.0 [14]

- RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP) [23]
- RFC 3312 Integration of Resource Management and Session Initiation Protocol (SIP) [26]
- RFC 3711 The Secure Real-Time Transport Protocol (SRTP) [39]
- RFC 4568 Session Description Protocol (SDP) Security Descriptions for Media Streams [55]
- RFC 5027 Security Preconditions for Session Description Protocol Media Streams [61]

Implementation notes:

- RFC 2246 The TLS Protocol Version 1.0:
 - SIP stack does not support incoming TLS connections. Thus proxies/registrars must support persistent TLS connections and be able to use existing connections to deliver SIP requests to the clients (connection reuse).
 - The following cipher suites may be used when setting up the TLS connection for SIP:
 - a. TLS_RSA_WITH_AES_256_CBC_SHA
 - b. TLS_RSA_WITH_AES_128_CBC_SHA
 - c. TLS_RSA_WITH_3DES_EDE_CBC_SHA
 - d. TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
 - e. TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
 - f. TLS_RSA_WITH_RC4_128_SHA
 - g. TLS_RSA_WITH_RC4_128_MD5
 - h. TLS_RSA_WITH_DES_CBC_SHA
 - i. TLS_DHE_DSS_WITH_DES_CBC_SHA
 - j. TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
 - k. TLS_RSA_EXPORT_WITH_RC4_40_MD5
 - l. TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
 - m. TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP):
 - Secure VoIP session establishment using security preconditions uses provisional responses sent by the UAS before the UAC has sent the SIP message "PRACK". Implementation follows RFC 3262 to achieve end-to-end reliability in transmitting such responses. Non-100 provisional responses are sent reliably if the initial INVITE request contained either a SUPPORTED or REQUIRE header field with the option tag "100rel".
- RFC 3711 The Secure Real-Time Transport Protocol (SRTP):
 - The SRTP use is signaled by either having defined secure RTP transport "RTP/SAVP" in an SDP media line or a=crypto as a media attribute in an SDP document. "RTP/SAVPF" is not supported.
 - Implementation supports RTP/RTCP stream authentication and encryption with replay protection according to RFC 3711:
 - a. Same master key is shared with RTP/RTCP streams.
 - b. Section 8.1.1 Use of the <From, To> for re-keying is not supported.
- RFC 4568 Session Description Protocol Security Descriptions for Media Streams:
 - SDP attribute "crypto" is used to signal and negotiate cryptographic parameters for media streams. This negotiation is secured by TLS.
 - Implementation supports security descriptions according to RFC 4568 with the following restrictions:

- a. The following crypto suites are supported: AES_CM_128_HMAC_SHA1_80 (offered as default), F8_128_HMAC_SHA1_80 (supported if offered in the initial INVITE), AES_CM_128_HMAC_SHA1_32 (supported if offered in the initial INVITE).
 - b. The following session parameters are supported: KDR.
 - c. The following session parameters are not supported: UNENCRYPTED_SRTCP, UNENCRYPTED_SRTP, UNAUTHENTICATED_SRTP, FEC_ORDER, FEC_KEY, WSH.
 - d. Re-keying is not recommended for IP telephony. Thus the optional lifetime field of the SRTP key parameter is not supported. Key rotation based on MKI is neither supported, though the MKI field in the SRTP key parameter is accepted if only one inline key parameter is provided with a=crypto attribute.
 - e. Section 6.4.2. Sharing cryptographic contexts among Sessions or SSRCS is not supported.
 - f. Section 7.1.4. Modifying the session: Only key parameters can be modified during the session. Initially negotiated crypto suite must remain the same through all session modifications. If new offer cannot be accepted, the old crypto parameters remain in place.
- RFC 5027 Security Preconditions for Session Description Protocol Media Streams:
 - The negotiation of cryptographic parameters when establishing a secure VoIP session may take use of security preconditions, as defined in RFC 5027. The only supported precondition type is "sec". All the precondition attributes ("curr", "des", "conf") are supported as are all the precondition tags (strength, status, and direction).

Strength is set as "optional" in the initial INVITE to increase interoperability with other vendors since security preconditions as a concept is published as a draft at this stage. When an offer with preconditions is received, the strength is increased to "mandatory" to prevent clipping effect and ghost calls from happening. Security descriptions may also be negotiated without using security preconditions if the other party does not support the concept.

2.16 VoIP Presence

This feature is supported from Nokia S60 VoIP Release 3.0 onwards.

Related specifications:

- RFC 3903 An Event State Publication Extension to the Session Initiation Protocol (SIP) [49]
- RFC 3863 Presence Information Data Format [50]
- RFC 3857 A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP) [51]
- RFC 3858 An Extensible Markup Language (XML) Based Format for Watcher Information [52]
- RFC 4479 A Data Model for Presence [53]
- RFC 4662 A Session Initiation Protocol (SIP) Event Notification for Resource Lists [56]
- RFC 4660 Functional Description of Event Notification Filtering [57]
- RFC 4661 An Extensible Markup Language (XML) -Based Format for Event Notification Filtering [58]
- RFC 4745 A Document Format for Expressing Privacy Preferences [59]
- Presence Authorization Rules [62]

2.17 Presence (SIMPLE/XDM) settings for VoIP

This feature is supported from Nokia S60 VoIP Release 3.0 onwards.

Related specifications:

- OMNA Device Management (DM) Application Characteristic (AC) Registry [12]

Implementation notes:

- The application identifiers of the implemented object formats are *ap00002* and *ap00003*.

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
DHCP	Dynamic Host Configuration Protocol
DM	Device Management
DND	Do Not Disturb
DSCP	Differentiated Services CodePoint
DTMF	Dual-Tone Multifrequency
DTX	Discontinuous Transmission
FEC	Forward Error Correction
FW	Firewall
HTTP	Hyper Text Transport Protocol
IAP	Internet Access Point
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
IETF	The Internet Engineering Task Force
iLBC	Internet Low Bitrate Codec
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

Term or abbreviation	Meaning
MKI	Master Key Identifier
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 packetization 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
SRTP	Secure Real-Time Transport Protocol
SSRC	Synchronization Source
STUN	Session Traversal Utilities for NAT (STUN)"; a protocol that allows applications to detect that network address translation (NAT) is being used.
TC	Traffic Class
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOS	Type of Service
UAC	User Agent Client
UAS	User Agent Server
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-behave-rfc3489bis-10.txt, Session Traversal Utilities for (NAT) (STUN)
- [3] draft-ietf-sip-outbound-01.txt, Managing Client Initiated Connections in the Session Initiation Protocol (SIP)
- [4] draft-ietf-sipping-service-examples-10.txt, Session Initiation Protocol Service Examples
- [5] draft-ietf-sipping-cc-transfer-06.txt, Session Initiation Protocol Call Control – Transfer
- [6] ITU-T G.711 Appendix I, available at <http://www.itu.int>
- [7] ITU-T G.711 Appendix II, 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] OMA Client Provisioning v1.1, available at <http://www.openmobilealliance.com/>
- [11] OMA Device Management v1.1.2, available at <http://www.openmobilealliance.com/>
- [12] OMNA Device Management (DM) Application Characteristic (AC) Registry, available at <http://www.openmobilealliance.com/>
- [13] RFC 2198, RTP Payload for Redundant Audio Data, available at <http://www.ietf.org/>
- [14] RFC 2246, The TLS Protocol Version 1.0, available at <http://www.ietf.org/>
- [15] RFC 2327, SDP: Session Description Protocol, available at <http://www.ietf.org/>
- [16] RFC 2543, SIP: Session Initiation Protocol, available at <http://www.ietf.org/>
- [17] RFC 2597, Assured Forwarding PHB Group, available at <http://www.ietf.org/>
- [18] RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, available at <http://www.ietf.org/>
- [19] RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, available at <http://www.ietf.org/>
- [20] RFC 3246, An Expedited Forwarding PHB (Per-Hop Behaviour), available at <http://www.ietf.org/>
- [21] RFC 3260, New Terminology and Clarifications for Diffserv, available at <http://www.ietf.org/>
- [22] RFC 3261, SIP: Session Initiation Protocol, available at <http://www.ietf.org/>
- [23] RFC 3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP), available at <http://www.ietf.org/>
- [24] RFC 3264, An Offer/Answer Model with the Session Description Protocol (SDP), available at <http://www.ietf.org/>
- [25] RFC 3267, RTP Payload Format for AMR and AMR-WB, 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 3312, Integration of Resource Management and Session Initiation Protocol (SIP), available at <http://www.ietf.org/>

- [28] RFC 3323, A Privacy Mechanism for the Session Initiation Protocol (SIP), available at <http://www.ietf.org/>
- [29] RFC 3325, Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, available at <http://www.ietf.org/>
- [30] RFC 3389, RTP Payload for Comfort Noise (CN), available at <http://www.ietf.org/>
- [31] RFC 3489, STUN: Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), available at <http://www.ietf.org/>
- [32] RFC 3515, The Session Initiation Protocol (SIP) Refer Method, available at <http://www.ietf.org/>
- [33] RFC 3550, RTP: A Transport Protocol for Real-Time Applications, available at <http://www.ietf.org/>
- [34] RFC 3551, RTP Profile for Audio and Video Conferences with Minimal Control, available at <http://www.ietf.org/>
- [35] RFC 3555, MIME 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 3711, The Secure Real-Time Transport Protocol (SRTP), available at <http://www.ietf.org/>
- [40] RFC 3824, Using E.164 numbers with the Session Initiation Protocol (SIP), available at <http://www.ietf.org/>
- [41] RFC 3842, A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP), available at <http://www.ietf.org/>
- [42] RFC 3891, The Session Initiation Protocol (SIP) "Replaces" Header, available at <http://www.ietf.org/>
- [43] RFC 3892, The Session Initiation Protocol (SIP) Referred-By Mechanism, available at <http://www.ietf.org/>
- [44] RFC 3951, Internet Low Bit Rate Codec (iLBC), available at <http://www.ietf.org/>
- [45] RFC 3952, RTP Payload Format for iLBC Speech, available at <http://www.ietf.org/>
- [46] RFC 3960, Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP), available at <http://www.ietf.org/>
- [47] RFC 4594, Configuration Guidelines for DiffServ Service Classes, available at <http://www.ietf.org/>
- [48] 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/>
- [49] RFC 3903, An Event State Publication Extension to the Session Initiation Protocol (SIP), available at <http://www.ietf.org/>
- [50] RFC 3863, Presencem Information Data Format, available at <http://www.ietf.org/>
- [51] RFC 3857, A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP), available at <http://www.ietf.org/>

- [52] RFC 3858, An Extensible Markup Language (XML) Based Format for Watcher Information, available at <http://www.ietf.org/>
- [53] RFC 4479, A Data Model for Presence, available at <http://www.ietf.org/>
- [54] RFC 4504, SIP Telephony Device Requirements and Configuration, available at <http://www.ietf.org/>
- [55] RFC 4568, Session Description Protocol (SDP) Security Descriptions for Media Streams, available at <http://www.ietf.org/>
- [56] RFC 4662, A Session Initiation Protocol (SIP) Event Notification for Resource Lists, available at <http://www.ietf.org/>
- [57] RFC 4660, Functional Description of Event Notification Filtering, available at <http://www.ietf.org/>
- [58] RFC 4661, An Extensible Markup Language (XML) -Based Format for Event Notification Filtering, available at <http://www.ietf.org/>
- [59] RFC 4745, A Document Format for Expressing Privacy Preferences, available at <http://www.ietf.org/>
- [60] RFC 4961, Symmetric RTP / RTP Control Protocol (RTCP), available at <http://www.ietf.org/>
- [61] RFC 5027, Security Preconditions for Session Description Protocol Media Streams, available at <http://www.ietf.org/>
- [62] Presence Authorization Rules, available at <http://www.ietf.org/internet-drafts/draft-ietf-simple-presence-rules-10.txt>

5 Evaluate this resource

Please spare a moment to help us improve documentation quality and recognize the resources you find most valuable, by [rating this resource](#).