Ziggo Residential Telephony

Interface specification

Versie 1.0 (20-01-2022)

Contents

1. Conventions

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST, SHALL”	This word means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there MAY exist valid reasons in particular circumstances to ignore this item, but the full implications SHOULD be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there MAY exist valid reasons in particular circumstances when the listed behaviour is acceptable or even useful, but the full implications SHOULD be understood and the case carefully weighed before implementing any behaviour described with this label.
"MAY"	This word means that this item is truly optional.

2. Contact

Queries regarding this specification can be addressed to:

CPE_supplier@vodafoneziggo.com

Please note that this is an address for hardware vendors only. Information for individual customers regarding the use of own devices on the Ziggo network is available here:

https://www.ziggo.nl/klantenservice/apparaten/wifi-modems/eigen-modem

3. Scope

This document contains the requirements for a residential telephony device or application to be used over the Ziggo cable network.

This interface specification may be changed at any time and may break backward compatibility with previous versions. Manufacturers are therefore asked to provide regular software updates. The user of this interface specification has to check for the newest version available from Ziggo. This interface specification may be superseded in total or in part by the terms of a contract between the individual network user and Ziggo.

4. References

In the case of a conflict between specific requirements in this document with requirements in any of the directly or indirectly referenced documents, the specific requirements of this document are applicable.

4.1. Normative References

[G.168]	ITU-T, G.168 : Digital network echo cancellers
[G.711]	ITU-T, G.711 : Pulse code modulation (PCMA) of voice frequencies
[RFC1034]	Domain Names – Concepts and Facilities
[RFC1035]	Domain Names – Implementation and Specification
[RFC2131]	Dynamic Host Configuration Protocol
[RFC2617]	HTTP Authentication: Basic and Digest Access Authentication
[RFC2782]	A DNS RR for specifying the location of services (DNS SRV)
[RFC2915]	The Naming Authority Pointer (NAPTR) DNS Resource Record
[RFC3261]	SIP: Session Initiation Protocol
[RFC3262]	Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
[RFC3263]	Session Initiation Protocol (SIP): Locating SIP Servers
[RFC3264]	An Offer/Answer Model with the Session Description Protocol (SDP)
[RFC3311]	The Session Initiation Protocol (SIP) UPDATE Method
[RFC3326]	The Reason Header Field for the Session Initiation Protocol (SIP)
[RFC3550]	RTP: A Transport Protocol for Real-Time Applications
[RFC3551]	RTP Profile for Audio and Video Conferences with Minimal Control
[RFC3611]	RTP Control Protocol Extended Reports (RTCP XR)
[RFC3960]	Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
[RFC4566]	SDP: Session Description Protocol
[RFC4733]	RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
[RFC6337]	Session Initiation Protocol (SIP) Usage of the Offer/Answer Model

4.2. Informative References

[RFC3312]	Integration of Resource Management and Session Initiation Protocol (SIP)
[RFC3323]	A Privacy Mechanism for the Session Initiation Protocol (SIP)
[RFC3325]	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
[RFC3329]	Security Mechanism Agreement for the Session Initiation Protocol (SIP)
[RFC4032]	Update to the Session Initiation Protocol (SIP) Preconditions Framework
[T.38]	ITU-T, T.38 : Procedures for real-time Group 3 facsimile communication over IP networks

4.3. Reference Acquisition

COIN: https://coin.nl/

Netherlands Numbering Plan: https://wetten.overheid.nl/

IETF RFCs: http://www.ietf.org

ITU recommendations: http://www.itu.int

5. Definitions and abbreviations

5.1. Definitions

This specification uses the following terms:

Public User Identity: A logical identity for purposes of communication with a User.

Server: A network element that receives requests in order to service them and sends back responses to those requests. Examples of servers are proxies, User Agent servers, redirect servers, and registrars as defined by [RFC3261].

User: A person who, in the context of this document, uses the telephony service.

User Agent (UA): A software entity contained in a device that acts on behalf of the user to send requests to and receive responses from the network for a particular application. In the context of this document, a UA refers to a SIP User Agent as defined by [RFC3261].

User Equipment (UE): The User device or application that is compliant to this specification, used by the User that wants to get telephony service.

Ziggo: the fixed network telecommunications brand of VodafoneZiggo Group B.V.

Ziggo Vast Bellen: the residential voice service product name of VodafoneZiggo Group B.V.

5.2. Abbreviations

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSx	Dynamic Service flow Add/Change/Delete
DTMF	Dual-tone multi-frequency
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
NA(P)T	Network Address (and Port) Translation
NAPTR	Name Authority Pointer
QoS	Quality of Service
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time To Live
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
URI	Uniform Resource Identifier
VSC	Vertical Service Code

6. IP Connectivity

The SIP UE MUST use a dedicated IP interface that is specifically provisioned as the Voice Service [Voice Interface].

It MUST be possible to enable the dedicated IP interface for SIP via the administrator web interface or other interface available for the user.

The SIP UE MUST obtain an IP address using standard DHCP [RFC2131].

The SIP UE MUST use IPv4.

The SIP UE MUST NOT be used behind a NAT.

The SIP UE MUST NOT use IPv6.

The SIP UE MUST NOT announce itself as a Packetcable device by containing string like “pktc1.0”, “pktc1.5” or “pktc2.0” in DHCP option 60.

The SIP UE MUST at least request following options (Parameter Request List) to the DHCP server: 1 = Subnet Mask, 3 = Router, 6 = Domain Name Server.

The SIP UE MUST NOT be configured with a static IP address.

The SIP UE MUST conform to the requirements in DNS standards: [RFC1034], [RFC1035], [RFC2782], [RFC2915].

The SIP UE MUST follow standard industry best practice behaviour with regards to usage of TTL.

7. SIP Profile

7.1. Configuration of SIP client

Ziggo will provide a set of SIP credentials to the end user, one set for each assigned phone number.

The following entries MUST be configurable in the SIP UE (separately for each assigned phone number):

a. Phone Number (below referred to as "PHONE_NUMBER")
b. SIP Domain (below referred to as "SIP_DOMAIN")
c. Outbound SIP Proxy
d. (Authentication) Username
e. (Authentication) Password

The SIP UE MUST support a Username in the format of this regular expression:

"[a-zA-Z0-9_]{9,20}"

The SIP UE MUST support a password in the format of this regular expression:

"[a-zA-Z0-9!$/()=?*+#-_.:,]{30,40}"

7.2. Standard SIP Support

The SIP UE MUST be compliant to the base SIP specification [RFC3261], implementing the "User Agent (UA) role" in particular.

The SIP UE MUST support DNS NAPTR [RFC2915], DNS SRV [RFC2782] and DNS A [RFC1035] record queries for locating the SIP server as defined in [RFC3263]. These are to be used to resolve the provided Outbound Proxy into an IP address, destination port and protocol to be used.

The SIP UE MUST use the transport protocol as provided in the DNS NAPTR [RFC2915] response as defined in [RFC3263].

The SIP UE MUST use the SIP port as provided in the DNS SRV [RFC2782] response as defined in [RFC3263] to contact its outbound proxy.

The Public User Identity MUST take the form of a SIP URI as specified in [RFC3261].

The Public User Identity MUST be built as follows (based on the phone-number and SIP domain as received from Ziggo): sip:PHONE_NUMBER@SIP_DOMAIN

Any other URI format (e.g., tel URI) MUST NOT be used by the SIP UE.

The SIP UE MUST never put "anonymous" in any outgoing message.

The SIP UE MUST be compliant to [RFC3262] (Provisional Acknowledgement - PRACK).

The SIP UE MUST be compliant to [RFC3311] (aka. SIP-UPDATE).

The SIP UE MUST be compliant to [RFC3960] (Early Media and Ringing Tone Generation in the Session

Initiation Protocol (SIP)).

The SIP UE MUST be compliant to [RFC6337] (Session Initiation Protocol (SIP) Usage of the Offer/Answer Model).

The SIP UE MUST NOT subscribe to any event packages (via SUBSCRIBE/NOTIFY).

The SIP UE MUST NOT use the Privacy mechanism for SIP specified in [RFC3323]

The SIP UE MUST NOT use the Private Extensions to SIP specified in [RFC3325].

The SIP UE MAY be compliant to [RFC3326] (Reason Header Field).

7.3. SIP Registration and Redundancy

The SIP UE MUST be compliant to [RFC3263] (Locating SIP Servers).

The SIP UE MUST support DNS NAPTR [RFC2915], DNS SRV [RFC2782] and DNS A [RFC1035] record queries for locating the SIP server as defined in [RFC3263]. These are to be used to resolve the provided Outbound Proxy into an IP address, destination port and protocol to be used.

If more than one SIP servers are resolved, the SIP UE MUST always try to register to the first priority SIP server coming from DNS SRV response. The second priority SIP server is only used in case of an outage of the first priority SIP server.

The SIP UE MUST NOT register against two SIP servers in parallel.

The SIP UE MUST always register all of its phone numbers with the same SIP server to avoid a situation where registrations are sent to different SIP server addresses.

In case of a SIP UE failover and registration to the second priority SIP server, the SIP UE MUST try with the next re-registration attempt to register all phone numbers back to the first priority SIP server again.

If the SIP UE re-registration attempt towards first priority SIP server fail, the SIP UE MUST stay registered on the second priority SIP server but the fallback to the first priority SIP server MUST be retried again with the next re-registration attempt.

If SIP UE fallback registration attempt to the first priority SIP server is successful for one phone number all other phone numbers MUST fallback too.

Unless either the user or the application within the SIP UE has determined that a continued registration is not required, the SIP UE MUST re-register an already registered Public User Identity either 600 seconds before the expiration time if the previous registration was for greater than 1200 seconds, or when half of the time has expired if the previous registration was for 1200 seconds or less.

If the IP address of the SIP UE changes (e.g., upon DHCP Renew), the SIP UE MUST start a new SIP registration.

7.4. SIP Security

The SIP Digest method as specified in [RFC3261] MUST be supported.

Any other mechanisms or protocols to protect the SIP signalling MUST NOT be used.

On receiving a “401 (Unauthorized)” response to the REGISTER request, and where the "algorithm" Authorization header field parameter is "MD5", the SIP UE MUST extract the digest-challenge parameters as indicated in [RFC2617] from the WWW-Authenticate header field, calculate digest-response parameters as indicated in [RFC2617], send another REGISTER request containing an Authorization header field containing challenge response as indicated in [RFC2617]. The SIP UE MUST set the Call-ID of the REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge. The SIP UE MUST NOT include [RFC3329] header fields with this REGISTER.

Similarly, upon receiving a “407 (Proxy Authentication Required)” response to an initial request, the originating SIP UE MUST extract the digest-challenge parameters as indicated in [RFC2617] from the Proxy-Authenticate header field, calculate the response as described in [RFC2617], and send a new request containing a Proxy-Authorization header in which the header fields are populated as defined in [RFC2617] using the calculated response.

The SIP UE MUST NOT authenticate the SIP server.

The SIP UE SHOULD only accept SIP requests from the SIP server IP addresses that are resolved via DNS SRV / A records (SIP server whitelist).

If an incoming SIP request is received by the SIP UE from a SIP server which is not on the SIP server whitelist, the SIP UE SHOULD respond with "403 Forbidden".

7.5. SIP Sessions – Originating

A SIP INVITE message MUST only be sent out by SIP UE during an active registration and only to the SIP server on which the SIP UE is currently registered.

The SIP UE as Caller (side A) MUST apply local ring back tone towards the connected telephone set when it receives “180 (Ringing)” without SDP.

The SIP UE as Caller (side A) MUST NOT apply local ring back tone towards the connected telephone set when it receives “180 (Ringing)” with SDP.

The SIP UE as Caller (side A) MUST NOT apply local ring back tone towards the connected telephone set when it receives “183 (session progress)” with SDP.

An outgoing INVITE MUST use the following format for the “Request-URI” field:

sip:CALLED_PHONE_NUMBER@SIP_DOMAIN

An outgoing INVITE MUST use the following format for the “To:” field:

<sip:CALLED_PHONE_NUMBER@SIP_DOMAIN>

The SIP UE MUST apply the following digit map when determining when to send out an INVITE message with a dialled digitstring:

112

12xx

18xx

1xxx.[#T]

[2-8]xxxxxx.[#T]

0[1-7]xxxxxxxx

067xxxx.[#T]

0[8-9]xxxxxxx.[#T]

00[1-9]xx.[#T]

21[0-9]xxxx.[#T]

#21#

31[0-9]xxx.[#T]

#31#[0-9]xxx.[#T]

*6[17]*x.[#T]

#6[17]#

43

#43#

141

#141#

0[1-9]x.[#T]

00x.[#T]

Notes

- "x." stands for a digit string consisting of zero or more digits 0-9.
- A digit range between square brackets (e.g., "[1-9]") corresponds with exactly one digit in the given range.
- T is digit input timer (inter digit timer).

The SIP UE SHOULD use a value of 4 seconds for T.

7.6. SIP Sessions – Terminating

When it receives an INVITE the SIP UE as Callee (side B) MUST respond with “180 (Ringing)” without SDP.

When it receives an INVITE the SIP UE as Callee (side B) MUST NOT send out any in-band ring back tone via RTP.

When it receives an INVITE the SIP UE as Callee (side B) MUST apply local ringing towards the connected telephone(s).

7.7. SDP Profile

The SIP UE MUST be compliant to [RFC3264] (Offer/Answer Model with SDP).

The SIP UE MUST be compliant to [RFC4566] (Session Description Protocol).

An INVITE request generated by a SIP UE MUST contain an SDP offer with at least one media description.

This SDP offer MUST reflect the calling user's terminal capabilities and user preferences for the session.

The SIP UE MUST NOT use the precondition mechanism specified in [RFC3312] and [RFC4032].

The SIP UE MUST NOT request/enable authentication/encryption for the media streams.

Upon sending an SDP answer to an SDP offer (which included one or more media lines which was offered with several codecs) the terminating SIP UE MUST select exactly one codec per media line and indicate only the selected codec for the related media stream.

The SIP UE MUST support configuration of dynamic RTP payload type number which is used for DTMF RTP Events as defined by [RFC4733].

The SIP UE MUST be configured to use DTMF RTP Events as defined by [RFC4733], then it MUST add the following in its outgoing SDP:

a=rtpmap:101 telephone-event/8000

a=fmtp:101 0-15

The SIP UE MUST include the "a=ptime" attribute for all "audio" media lines as described in [RFC4566], with value 20.

If a SIP UE receives an "audio" media line with "a=ptime" specified, the SIP UE MUST transmit at the specified packetization rate.

If the SIP UE supports RTCP Extended Reports per [RFC3611], then this MUST be indicated in its SDP offer per [RFC3611] with encoding “a=rtcp-xr:voip-metrics”.

The SIP UE MUST NOT try to set up any video sessions.

Other SDP parameters as “b=AS”, “b=TIAS”, “a=maxprate” SHOULD NOT be present.

For the forming of SDP the SIP UE MUST follow the examples as given in Annex B

8. Call features / Supplementary Services

The SIP UE MUST NOT interpret Vertical Service Codes (VSC) locally.

VSCs follow this regular expression: ^(*67){0,1}*[0-9]{1,25}$

Overview of VSCs:

Service VSC

Calling Line Identification Restriction *31*<target phone number>#

Calling Line Identification Presentation per call #31#<target phone number>#

Call Forwarding Unconditional – Activation *21*<target phone number>#

Call Forwarding Unconditional – Deactivation #21#

Call Forwarding Busy – Activation *67*<target phone number>#

Call Forwarding Busy – Deactivation #67#

Call Forwarding No Reply – Activation *61*<target phone number>#

Call Forwarding No Reply – Deactivation #61#

Call Waiting – Activation *43*

Call Waiting – Deactivation #43#

VSCs beginning with an asterisk (*) MUST be sent transparently and unchanged by the SIP UE to the SIP server (per the digit map as specified above in chapter 7.5).

VSCs beginning with a hash (#) MUST be sent transparently and unchanged by the SIP UE to the SIP server (per the digit map as specified above in chapter 7.5).

9. Quality of Service

Quality of Service for voice calls (signalling and media) set up per this specification will be taken care of by the network.

The SIP UE MUST NOT in any way try to request quality of service. E.g, the SIP UE must not initiate any DSx signaling by itself.

10. CODEC-MEDIA

10.1. Codecs

The SIP UE MUST support [G.711] a-Law voice codec (PCMA).

10.2. RTP and RTCP

The SIP UE MUST send and receive RTP and RTCP packets as defined in [RFC3550] and [RFC3551] for transport of audio flows.

The SIP UE MAY support RTCP Extended Reports per [RFC3611].

The SIP UE MUST use a packetization time of 20ms for RTP packets.

The SIP UE MUST NOT apply any authentication/encryption on RTP and RTCP.

10.3. DTMF Relay

The SIP UE MUST be compliant to [RFC4733] (RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals).

The SIP UE MUST send DTMF RTP Event packets strictly according to 20ms packetization time.

The SIP UE MUST stop the audio RTP stream temporarily for duration of DTMF RTP Event transmission.

10.4. Fax

[T.38] fax relay MUST NOT be used.

Faxes and other modem transmissions MUST be sent in-band over the voice codec.

11. Service Disconnections

The ACM recognizes that providers need to protect their network on different levels & in different scenarios. The following nuisance or damage scenarios MAY result in temporary suspension or disconnection from the voice network.

- Multiple failed attempts to adequately or appropriately authenticate SIP username or password.
- Attempting to register more than 2 accounts from the same locale.
- Using a device with outdated software & known security vulnerabilities.
- General misuse of network resources.

Initial instances of the above mentioned conditions will result in the customers voice service being suspended, whereas continued attempts to gain access may result in suspension of the service.

12. History

Document history		
V 1.0	20-01-2022	Version submitted for publication

13. Annex A Example SIP messages

This Annex provides some example supported SIP messages:

13.1. REGISTER

```
REGISTER sip:SIP_DOMAIN SIP/2.0
Via: SIP/2.0/UDP UE_ADDRESS:UE_PORT;rport;branch=aaaabbbbcccc
From: <sip:PHONE_NUMBER@SIP_DOMAIN>;tag=123456789
To: <sip:PHONE_NUMBER@SIP_DOMAIN>
Call-ID: xxxxyyyyzzzz
CSeq: 123 REGISTER
Contact: <sip:PHONE_NUMBER@UE_ADDRESS>
Authorization: Digest username="AUTH_USER", realm="SIP_REALM",
nonce="NONCE_VALUE",
uri="sip:SIP_DOMAIN", response="AUTH_RESPONSE", algorithm=MD5
Max-Forwards: 70
Expires: 3600
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,PRACK,UPDATE
Content-Length: 0
```

13.2. INVITE

```
INVITE sip:CALLED_PHONE_NUMBER@SIP_DOMAIN SIP/2.0
Via: SIP/2.0/UDP UE_ADDRESS:UE_PORT;rport;branch=aaaabbbbcccc
From: <sip:PHONE_NUMBER@SIP_DOMAIN>;tag=123456789
To: <sip:CALLED_PHONE_NUMBER@SIP_DOMAIN>
Call-ID: xxxxyyyyzzzz
CSeq: 123 INVITE
Contact: <sip:PHONE_NUMBER@UE_ADDRESS>
Proxy-Authorization: Digest username="AUTH_USER", realm="SIP_REALM",
nonce="NONCE_VALUE", uri="sip:CALLED_PHONE_NUMBER@SIP_DOMAIN",
response="AUTH_RESPONSE", algorithm=MD5
Max-Forwards: 70
Expires: 120
Supported: 100rel
Allow: ACK,BYE,CANCEL,INVITE,OPTIONS,PRACK,UPDATE
Content-Type: application/sdp
Content-Length: 321
v=0
o=<username> <sess-id> <sess-version> IN IP4 <unicast-address>
s=-
c=IN IP4 <connection-address>
t=0 0
m=audio <port> RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=rtcp-xr:voip-metrics
```

14. Annex B Example SDP Encodings

This Annex shows allowed options for SDP contents:

14.1. SDP Option 1

SIP UE Support	Answer
PCMA (ptime 20ms)	Yes
DTMF RTP Events (RFC4733)	Yes
RTCP-XR Reports (RFC3611)	No

```
v=0
o=<username> <sess-id> <sess-version> IN IP4 <unicast-address>
s=-
c=IN IP4 <connection-address>
t=0 0
m=audio <port> RTP/AVP  8 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

14.2. SDP Option 2

SIP UE Support	Answer
PCMA (ptime 20ms)	Yes
DTMF RTP Events (RFC4733)	Yes
RTCP-XR Reports (RFC3611)	Yes

```
v=0
o=<username> <sess-id> <sess-version> IN IP4 <unicast-address>
s=-
c=IN IP4 <connection-address>
t=0 0
m=audio <port> RTP/AVP 8 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=rtcp-xr:voip-metrics
```

This page is intentionally left blank.