Subject:	**Technical guidelines for IP-IP interconnection in the Netherlands**
Date:	**March 17, 2020**
Version:	**Final version 1.3**
Authors:	**Participants of the FIST IP Interconnect Taskforce**
Contact:	**www.stichting-fist.nl**
Classification:	**Public**

Summary
This document provides technical guidelines to network operators and service providers that want to interconnect their voice telephony service with that of other network operators and service providers in the Netherlands for IP-based interconnection enabling inter-operator voice and multimedia services.

This document has been prepared by the members of the Dutch forum of registered providers of telecommunication networks and services.

Disclaimer
The technical guidelines for IP-IP interconnection in the Netherlands are based upon international published standards and recommendations. Functions or parameters not mentioned in this document may not be supported on the IP-IP interconnection in the Netherlands. Offering of these functions or parameters is not prohibited nor actively blocked. FIST has been very careful in describing these guidelines below. FIST cannot be held responsible for any damages resulting from the use of this document. The reader is encouraged to contact FIST in case of any doubt concerning the correctness of the content in this document or possible misinterpretations. Contact details are given in the header above.

Table of contents

1 Introduction 3
1.1 Scope 3
1.2 Participants 3
1.3 Terminology 3
1.4 Process for managing and maintaining this document 3
2 Protocols 4
2.1 Messages, Methods and Response Codes 4
2.1.1 INVITE method 4
2.1.2 To header 5
2.1.3 From header 5
2.1.4 Privacy header 5
2.1.5 P-Asserted-Identity (PAI) header 5
2.1.6 Contact header 5
2.1.7 History-info header 5
3 SIP INVITE header example 7
3.1 VoLTE / SIP precondition 8
3.2 Supplementary Services 8
4 Handling of SIP response codes on IP IP interconnect 10
4.1 Codecs 12
4.1.1 Narrow Band Codecs 12
4.1.2 ISDN data calls (optional) 12
4.1.3 Fax handling (optional) 12
4.2 DTMF detection 13
4.3 Wideband Codecs 13
4.3.1 Recommended CoDecs Fixed Networks 13
4.3.2 Recommended CoDecs Mobile Networks 13
4.3.3 Session setup procedure for the negotiation of SDP AMR-NB or AMR-WB 13
4.3.4 AMR-WB optional parameters: 13
4.3.5 Video 14
4.4 Initial INVITE without SDP (late SDP offer) 14
4.5 Echo cancellation 14
5 Addressing, naming & numbering 15
5.1 Telephone number format 15
5.1.1 E.164 normalization number overlap 15
5.1.2 URI 15
5.2 ENUM 15
5.3 Number portability, COIN 15
6 Interconnect Access 16
6.1 Architecture 16
6.2 Transport Protocols 16
6.3 Security 16
6.4 Authentication 17
6.5 Authorization 17
6.6 QoS bits 17
6.7 Traffic type separation 17
6.8 112 Emergency traffic 17
6.9 Carrier (Pre)Select calls 17
6.10 Service availability 17
7 Processes 18
7.1 Testing 18
7.2 Billing / verification 18
7.3 Shielding of B-numbers 18
A. ENUM services and Infrastructure ENUM 19
B. Issues for future study – Longlist 20

1 Introduction

FIST is the Forum for Interconnection and Special Access, a discussion platform to which all providers of telecommunication networks or - services with an ACM registration can participate. Spring 2011, the FIST Taskforce “IP Interconnect” was brought to live.

1.1 Scope

This document describes the minimum set of requirements for VoIP interconnection between telecommunication operators in the Netherlands, this to ensure high quality, efficient, reliable and standardized method so that it can be supported by a sustainable commercial model. This document has the status of an advisory document.

Minimum business requirements are:

- End-to-End (focused service delivery, QoS requirements)
- Service interoperability – between networks (including mobile)
- Connectivity (Managed access/redundancy/availability and scalability)
- Security and customer protection
- Charging
- Relevant national regulatory compliancy.

Not in scope (should be on beforehand commercially arranged on a bilateral agreement between parties):

- Value based pricing
- Increased customer choice
- Support alternative business models

1.2 Participants

The following parties participate in this taskforce: BT, COIN, Colt, gnTel, KPN, OneCentral, SpeakUp, T-Mobile, VodafoneZiggo and Voiceworks.

1.3 Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 and indicate requirement levels for compliant SIP implementations.

1.4 Process for managing and maintaining this document

The taskforce IP Interconnect aims to keep this document up-to-date and actual. The following agreements have been made to achieve this:

- The Deliverable IP Interconnect is a product of the FIST taskforce IP Interconnect and its contributing participants.
- The FIST secretary will organize a FIST taskforce IP Interconnect (at least) two times per year
- Participants will be requested to submit agenda items and/or add topics to the longlist.
- The taskforce meeting agenda will at least consist of the following topics:
    - Open action items
    - Topics submitted by the participants
    - Discussion of (topics on) the longlist
    - Discussion on parallel initiatives (e.g. COIN ENUM).
- The taskforce will decide if (a series of) working sessions are required to address the topics raised by participants or on the longlist and to update this document.
- The taskforce will approve the changes to this document proposed in the working sessions, after which a new version will be released.

2 Protocols

2.1 Messages, Methods and Response Codes

SIP messages are used to establish a communication session between nodes. SIP messages are of two types − requests and responses:

- The opening line of a request contains a method that defines the request, and a Request-URI that defines where the request is to be sent.
- Similarly, the opening line of a response contains a response code.

SIP requests are answered by a corresponding SIP response that indicate whether a request succeeded, is being tried or failed. SIP requests are known as METHODS that request a specific action to be taken by another user agent or server. METHODS are distinguished into two types, only ACK, BYE, CANCEL, INVITE, OPTIONS, PRACK and UPDATE are used at IP Interconnect:

Core methods	**Reference**	**Extension methods**	**Reference**
ACK	[RFC3261]	INFO	[[RFC3428]
BYE]	[RFC3261]	MESSAGE	[RFC6086]
CANCEL	[RFC3261]	NOTIFY	[RFC6665]
INVITE	[RFC3261][RFC6026]	PRACK	[RFC3262]
OPTIONS*	[RFC3261]	PUBLISH	[RFC3903]
REGISTER	[RFC3261]	REFER	[RFC3515]
		SUBSCRIBE	[RFC6665]
		UPDATE**	[RFC3311] [RFC4028]

** used for keep alive at IP Interconnect*
********RFC 3311 (update media), RFC 4028 (timer refresh*)

2.1.1 INVITE method

- A session is considered established if an INVITE has received a success response(2xx) and an ACK has been sent
- A successful INVITE request establishes a dialog between the two user agents which continues until a BYE is sent to terminate the session
- An INVITE MUST contain the media information of the caller in the message body
- An INVITE sent within an established dialog is known as a re-INVITE
- Re-INVITE is used to change the session characteristics or refresh the state of a dialog.

2.1.1.1 SIP URI Format

SIP URI format is standardized (RFC3261) in the format: sip:user:password@host:port;uri-parameters?headers

User
- Contains a phone number in international number format as specified in “chapter 5. Addressing, naming & numbering”

Password
- Not used over the interconnect

Host
- MUST be agreed IP address or agreed domain name

Port
- MUST be agreed between partners

Uri-parameters
- The parameter "user=phone" MUST be included

Headers
- MUST NOT contain a phone-context.

Example: sip:+31702345678@example.com;user=phone.

2.1.2 To header

The To header does not contain crucial information for the interconnect and contains a phone number in international number format as specified in “chapter 5. Addressing, naming & numbering”

2.1.3 From header

The “From” header field contains the Originating Identification (OI) that the user wants to pass transparently through the network to the destination. This is comparable with a user-provided (i.e. a non-verified generic E.164 number) parameter in ISUP [ECC recommendation11(02) Calling Line Identification and Originating Identification] .

- The From header fields MUST contains a phone number in international number format as specified in “chapter 5. Addressing, naming & numbering”, or anonymous
- The parameter "user=phone" MUST be included when the user part of a URI is a telephone number
- The "From" header fields MUST be used for presentation of the Origination Identity (CLIP and CLIR.

2.1.4 Privacy header

The “Privacy” header field gives the possibility to control the withholding of the identity as standardized in RFC 3323 and RFC 3325. For the interconnect we restrict the usage to “Privacy: id” or “Privacy: none”.

When Privacy: id is set:

- the “From” header field MUST contain sip:anonymous@anonymous.invalid
- the “From” header field MUST NOT contain “user=phone”
- the “From” header field MUST NOT contain port number.

2.1.5 P-Asserted-Identity (PAI) header

The “P-Asserted-Identity” header field is designed to carry the network-provided identifier (in ISUP the corresponding parameter is the Calling-Party-Number parameter). This field SHOULD be set by the originating service provider. This header only has meaning within a trusted network by mutual agreement on the requirements for its use. The P-Asserted-Identity header field is defined in RFC 3325 and contains a phone number in international number format as specified in “chapter 5. Addressing, naming & numbering”

- The “P-Asserted-Identity” header MUST exist in SIP message between operators over the sip-interconnect in case the call is originated in the Netherlands
- The “P-Asserted-Identity” header MUST contain the original calling party number
- The “P-Asserted-Identity” header can be different to the FROM header in case another number should be displayed, e.g. main telephony number of the hospital should be displayed instead of the actual number of the doctor
- Interconnection between telecommunication operators in the Netherlands, SHOULD be trusted as the definition of trusted in RFC3325. (accepting the “P-Asserted-Identity” header field into the network)
- Interconnection between telecommunication operators in the Netherlands and another telecommunication operator, are to be classified as not-trusted* for Dutch phone numbers in the “P-Asserted-Identity” header field, other phone numbers in the “P-Asserted-Identity” header field MAY be accepted as trusted. *as the definition of trusted in RFC3325.

2.1.6 Contact header

The “Contact” header field MUST contain one of the following possibilities:

- Telephone number in ITU-T E.164 international format with leading “+” sign, or
- another routing identifier, or
- empty user part in the SIP URI.

2.1.7 History-info header

Although the use of the Diversion header is widespread and currently in use on most interconnects, the use history-info header is RECOMMENDED. To conform to the guidelines for national IP Interconnection as described in ETSI TISPAN document Technical Report on NGN Interconnection, paragraph 4.6.

- The History-info header field is the preferred header for conveying call diversion information on Dutch IP interconnects according ETSI TS 124.229 / 3GPP TS 24.229 / RFC 4244.
- Diversion header MAY be used on SIP interconnect. If interworking is needed, this MUST be in the local network.
- RFC 4244 and 7044 (An Extension to the SIP for Request History Information) (SIP header History-Info) are not supported on the IP-interconnect.
- The call-forwarding related History Info-entry MUST contain the number with the active forwarding.

Example call scenario: A calls B1 is forwarded to B2 is forwarded to B3 is forwarded to C (audio follows the path, A, B1, B2, B3, C):

A	**➔**	**B1**	**➔**	**B2**	**➔**	**B3**	**➔**	**C**
	From = A PAID = A Request-URI = B1 To = B1 (ITU-T)		From = A PAID = A **History-info: = B1** Request-URI = B2 To = B1 (ITU-T)		From = A PAID = A **History-info: = B2, B1** Request-URI =B3 To = B1 (ITU-T)		From = A PAID = A **History-info: = B3, B2, B1** Request-URI = C To = B1 (ITU-T)	

3 SIP INVITE header example

Header	Description/RFC	Example	Comment
Allow	Described in RFC 3261	ACK,BYE,CANCEL,INVITE,OPTIONS	Mandatory header field
Call-ID	Described in RFC 3261	66d1c66830016e5013c42ec3aab6ac53e420cc03cd150f07e8-0018-7823	Mandatory header field
Contact	Described in RFC 3261	sip:213.124.239.9:5060;transport=udp	Mandatory header field
Content-Length	Described in RFC 3261	188	Mandatory header field
Content-Type	Described in RFC 3261	application/sdp	Optional header field (Mandatory when SDP)
CSeq	Described in RFC 3261	CSeq: 1 INVITE	Mandatory header field
From	contains the A number	<sip:+31182690074@213.124.239.9:5060;user=phone>;tag=c4-45026-2ec3aa-1a074a43-2ec3aa	Mandatory header field
INVITE Request line*	sip-uri contains the B number or, call forwarding, the C number	sip:+31110238164@80.231.93.39:5060;user=phone SIP/2.0	Mandatory header field “user=phone” Must be present*
Max-Forwards	<<n>> is usually between 30 and 80	69	Mandatory header field
P-Asserted-ID	Described in RFC 3325	<sip:+31182690070@urn>	Mandatory header field
Privacy	Described in RFC 3325	Id	Optional header field
Record-Route	RFC 3261	Record-Route: <sip:172.30.48.77;lr=on;ftag=566BA9F1-535791D600067738-DC92E700;nat=yes>	Optional header field
RSeq	Described in RFC 3262	RSeq: 818172	Optional header field (mandatory when 100rel)
Server	Described in RFC 3261	VoIP-Server	Optional header field
Session-Expires	Described in RFC 4028	Session-Expires: 50;refresher=uac	Optional header field
Supported	RFC 3261& RFC 3262	replaces, timer	Mandatory header field
To	sip-uri contains the B number	<sip:+31110238164@80.231.93.39:5060;user=phone> (format may differ)	Mandatory header field (format may differ)
User-Agent	Described in RFC 3261	FPBX13.09/5.0	Optional header field
Via	Protocol/Version/Transport protocol Server_IP_address: port RFC 3261	Via: SIP/2.0/UDP 172.30.48.77;branch=z9hG4bKa82c.4d173716.0;received=172.30.48.77	Mandatory header field

Table 1: Examples of Invite header fields

** SIP parameter user=phone MUST be used in every SIP header that includes a telephone number in the user part of a SIP URI. SIP parameter user=phone MUST NOT be used in a SIP header if anonymous (see privacy).SIP parameter user=phone MUST NOT be used in a SIP header that does not include a telephone number in the user part of a SIP URI Presence of this parameter MUST NOT be used to make a choice on the contents of media (voice, fax, modem).*
Exception: “user=phone” is OPTIONAL in the Contact header.

3.1 VoLTE / SIP precondition

With current knowledge and application of SIP trunks and SIP based services in the Netherlands there are no benefits for inter operator E2E application of SIP Precondition (SIP resource allocation as described in IETF RFC3312 "Integration of Resource Management and Session Initiation Protocol " and RFC4032 "Update to the Session Initiation Protocol (SIP) Preconditions Framework"). Leaking explicit SIP precondition related signaling to older SIP stacks will only increase interoperability risk. Therefore, national IP interconnects in the Netherlands shall not support/convey SIP precondition signaling. Any originating or terminating networks in the Netherlands applying SIP precondition shall assure that explicit precondition related signaling information is removed from the SIP signaling (SIP and SDP) when exchanging SIP traffic over a national IP interconnect in the Netherlands. Operators may support E2E precondition over IP interconnects based on bilateral agreement for on net terminating traffic between each other but shall remove explicit precondition related signaling information from the signaling in transit use cases (e.g. forwarding).

3.2 Supplementary Services

The supplementary service Calling Line Presentation/Restriction (CLIP/CLIR) MUST be implemented in VoIP interconnection in order to guarantee privacy to the users. Other supplementary services are subject of bilateral agreement.

CLIP/CLIR
For a proper interworking of CLIP/CLIR between IP networks and between ISUP and IP networks RFC3323, RFC3325 and ITU Q.1912.5 MUST be supported. RFC3323 and RFC3325 talk about security and identity issues of voice services within IP networks. The interoperability between ISUP and IP networks is described in ITU Q.1912.5. Notice that all three ITU-T Q.1912.5 profiles support CLIP/CLIR.

Screening
The originating network is responsible for correctly filling the data for CLIP/CLIR presentation of the Originating Identification (A number) per end user so that the terminating network is able to provide the correct presentation. The terminating network is not responsible for the screening of invalid CLIP/CLIR values.

CLI mapping ISUP to SIP
The User part of a P-Asserted-Identity header in a SIP request will be created based on the ISUP calling party address when the Screening Indicator = "network provided" or "user provided, verified and passed ". No privacy header is added or Privacy header with value "none" (RFC3325) is created in the SIP message, if the Presentation Indicator (ISUP-calling party address) = "Allowed".
Privacy value "id" is used in the SIP message if the Presentation Indicator value is "Restricted".

Regarding privacy (RFC3325) operators must:

- Treat the SIP-interconnect as a trusted Network. (e.g. in case of Privacy=Id),
- Preserve the P-Asserted-Identity header when the call is sent to a trusted network.
- Delete the P-Asserted-Identity header when call is sent to an untrusted network.
- History-info header (RFC7044), Diversion header (RFC5806) are OPTIONAL headers, used only in case of call forward scenarios.

ISUP protocol			SIP protocol		
Calling Party number parameter		Generic Number parameter (ACgPN)	P-Asserted-Identity header field	From header field	Privacy header field
Screening indicator	Address presentation restricted indicator	Address presentation restricted indicator			
UPVP or NP	PA	PA	Derived from address included in the CPN	Derived from address included in the GN	Not included
UPVP or NP	PR	PA	Derived from address included in the CPN	Derived from address included in the GN	Priv-value="id"
UPVP or NP	PA	-	Derived from address included in the CPN	SIP URI derived from address included in the CPN	Not included
UPVP or NP	PR	-	Derived from address included in the CPN	SIP URI with "*Anonymous*" address	Priv-value="id"
UPVP or NP	PA	PR	Derived from address included in the CPN	SIP URI derived from address included in the CPN	Not included
UPVP or NP	PR	PR	Derived from address included in the CPN	SIP URI with "*Anonymous*" address	Priv-value="id"
UPVF or UPNV	PA or PR	-	Not included	SIP URI with address "*Unavailable User Identity*"	Not included

Legend:

NP – Network provided
UPNV – User provided not validated
UPVF- User provided verified and failed
UPVP – User provide verified and passed
PA – Presentation allowed
PR – Presentation restricted
GN – Generic Number
CPN – Calling Party Number

Table 2 mapping of ISUP parameters to SIP header fields

4 Handling of SIP response codes on IP IP interconnect

Following table presents shows what SIP response codes are expected at the Dutch IP IP Interconnect and if hunting is allowed.

	Response	Expected on Interconnect	*Hunting allowed
code	**3xx - redirection**		
300	Multiple Choices	NOT TRUE	NOT TRUE
301	Moved Permanently	NOT TRUE	ENOT TRUE
302	Moved Temporarily	NOT TRUE	NOT TRUE
305	Use Proxy	NOT TRUE	NOT TRUE
380	Alternative Service	NOT TRUE	NOT TRUE
code	**4xx - client error**		
400	Bad Request	TRUE	NOT TRUE
401	Unauthorized	NOT TRUE	NOT TRUE
402	Payment Required	NOT TRUE	NOT TRUE
403	Forbidden	TRUE	NOT TRUE
404	Not Found	TRUE	NOT TRUE
405	Method Not Allowed	TRUE	NOT TRUE
406	Not Acceptable	TRUE	NOT TRUE
407	Proxy Authentication Required	NOT TRUE	NOT TRUE
408	Request Timed Out	TRUE	NOT TRUE
410	Gone	NOT TRUE	NOT TRUE
413	Request Entity Too Large	TRUE	NOT TRUE
414	Request – URI Too Long	TRUE	NOT TRUE
415	Unsupported Media Type	TRUE	NOT TRUE
416	Unsupported URI Type	TRUE	NOT TRUE
420	Bad Extension	TRUE	NOT TRUE
421	Extension Required	TRUE	NOT TRUE
422	Session Timer Too Small	TRUE	NOT TRUE
423	Interval Too Brief	TRUE	NOT TRUE
480	Temporarily Unavailable	TRUE	NOT TRUE
481	Call/Transaction Does Not Exist	TRUE	NOT TRUE
482	Loop Detected	TRUE	NOT TRUE
483	Too Many Hops	TRUE	NOT TRUE
484	Address Incomplete	TRUE	NOT TRUE
485	Ambiguous	TRUE	NOT TRUE
486	Busy Here	TRUE	NOT TRUE
487	Request Terminated	TRUE	NOT TRUE
488	Not Acceptable Here	TRUE	NOT TRUE
491	Request Pending	TRUE	NOT TRUE
493	Undecipherable	TRUE	NOT TRUE
code	**5xx - server Failure**		
500	Server Internal Error	TRUE	TRUE
501	Not Implemented	TRUE	NOT TRUE

502	Bad Gateway	TRUE	TRUE
503	Service Unavailable	TRUE	TRUE
504	Server Time – out	TRUE	TRUE
505	Version Not Supported	TRUE	TRUE
513	Message Too Large	TRUE	NOT TRUE
580	Precondition failure	NOT TRUE	NOT TRUE
code	**6xx - global failure**		
600	Busy Everywhere	TRUE	NOT TRUE
603	Decline	TRUE	NOT TRUE
604	Does Not Exist Anywhere	TRUE	NOT TRUE
606	Not Acceptable	TRUE	NOT TRUE
607	Unwanted	NOT TRUE	NOT TRUE

Table 3: SIP responses on IP IP interconnect level

*Hunting: re-initiating the same session via an alternative route at the same party /domain.

4.1 Codecs

Codecs are divided in different types.

4.1.1 Narrow Band Codecs

In i3 Forum document "Technical Interconnection Model for International Voice Services (Release 5.0), May 2012" a split between MANDATORY and OPTIONAL Narrow Band Codecs is proposed.

As a deviation to the international standards, in The Netherlands it is RECOMMENDED that codec G.711 A-Law MUST be supported. All other codecs are optional and subject to bilateral agreements.

In the i3 Forum document guidelines are given for the Packetization Period and Payload Type Definition for each of the codecs. Apart from Codec G.723.1, the RECOMMENDED Packetization Period for all Codecs is 20 ms.

4.1.2 ISDN data calls (optional)

ISDN data calls (bearer capability 64 kb/s unrestricted) cannot be transferred through normal voice encoding/decoding media gateways. When 64 kb/s unrestricted traffic exchange is a requirement for an IP interconnect then this MUST be done according RFC4040 with following additional requirements.

- Payload type MUST be dynamically assigned
- Clock frequency(rate) SHOULD be 8000 Hz
- 64kb/s calls in combination with SIP-I (ISUP encapsulated signaling) the SDP SHALL contain only and exclusive CLEARMODE payload type
- Packetization time SHOULD be equal.
- Packetization times MUST NOT exceed 20ms.

RFC4040 will not guarantee that a 64kb/s unrestricted call will be answered at the far end. There are devices which will check also the ISUP message. E.g. whether or not the Forward call indicator "ISDN user part used all the way" is present. If "ISDN user part used all the way" is not present, the call might be rejected by the far end. To increase the success rate of connections from/to traditional ISDN, it is possible to make use of SIP-I* and encapsulate C7 into SIP-I* (ITU T-REC-Q.1912.5 profile C). Bilateral agreements between connecting parties increase the correct and successful usage of SIP-I.

*Encapsulating C7 into SIP-I should be considered as an extraordinary measure, only to be used in situations where parties necessarily want to make use of IP technology.

4.1.3 Fax handling (optional)

On IP interconnects where G3 facsimile and SG3 facsimile transmissions are a mandatory supported service this SHOULD be done according the methods described below.

Equipment MUST use the default values in ITU-T Recommendation T.38 (09/2010) Annex H table H.1 and H.2. Following attributes and values MUST be included in SDP offer and SDP answer with the T.38 image:

m=image <portnumber> udptl t38
a=T38FaxVersion:0
a=T38FaxRateManagement:transferredTCF
a=T38FaxUdpEC:t38UDPRedundancy
a=T38MaxBitRate:14400
a=T38FaxMaxBuffer:1800
a=T38FaxMaxDatagram:150.

Limitations in support for T.38: [IETF RFC 5939] "revised SDP Offer/Answer" MUST NOT be used.
[ITU-T V.34] "V.34G3" (Super Group 3 fax) (33 600 bit/s modem) MUST NOT be used.
Fallback Pseudo-VBD as defined in i3 forum "Technical specification for Fax Over IP service (Release 3.0), April 20103", Chapter 4, page 7.
In unfortunate scenarios where access services on originating and terminating must continue to support G3 and SG3 facsimile and interoperability fails due to endpoint incompatibility the involved service providers MAY solve this through T.38 – G.711 transcoding on IP interconnect border elements.

4.2 DTMF detection

DTMF tones on IP interconnects MUST be transmitted according RFC4733/RFC2833. To ensure mutual compatible implementation/configuration of RFC4733*/RFC2833 DTMF telephone events, implementation SHOULD be according following additional requirements:

- Payload type MUST be dynamically assigned
- Clock frequency(rate) MUST be 8000 Hz
- Telephone events 0-15 (0-9,*,#,A-D) MUST be supported

*RFC2198 redundancy not supported

4.3 Wideband Codecs

With the adoption of Wideband codec on the IP IP interconnect the Dutch telecommunication users will be provided with better quality voice. Wideband codecs SHOULD be used when an origination endpoint indicates support for one of the common codecs. When a Wideband codec is added the corresponding Telephone-events MUST be added and the total bandwidth for media SHOULD NOT exceed 64Kb/s per session (set at media-level). In the i3 Forum document guidelines are given for the Packetization Period and Payload Type Definition for each of the codecs. The RECOMMENDED Packetization Period for all Codecs is 20 ms.

4.3.1 Recommended CoDecs Fixed Networks

Narrowband	**Wideband***
G.711a	G.722
Telephone-event/8000	AMR-WB/16000 (for interworking with Mobile Networks)
	Telephone-event/16000

4.3.2 Recommended CoDecs Mobile Networks

Narrowband	**Wideband***
G.711a	AMR-WB/16000
AMR/8000	Telephone-event/16000
Telephone-event/8000	EVS

4.3.3 Session setup procedure for the negotiation of SDP AMR-NB or AMR-WB

The session setup procedure for the negotiation of SDP AMR-NB or AMR-WB should be conform the document 3GPP TS 126.114 version 15.7.0 2 paragraph 6.2. The 2-phase negation procedure as proposed by GSMA will NOT be used. (phase 1 bw efficient, phase 2 octet alignment), fallback is to G.711A.

4.3.4 AMR-WB optional parameters:

Following SDP parameter settings are RECOMMENDED for AMR-WB:

Parameter	Default value	RECOMMENDED Usage
octet-align	0 (bandwidth optimized)	Shall not be included [1]
mode-set	When absent, All mode set allowed	Shall not be included [1]
mode-change-period	1 (mode change may happen in any frame)	Shall not be included [1]
mode-change-capability	1 (client is not able to restrict mode changes to a specific period)	Shall be set to 2, indicating the client can restrict the mode change period to 2
mode-change-neighbor	0 client can change to any mode in the mode set.	Shall not be included [1]
maxptime	The client may put any amount of AMR media in RTP packet.	Shall be set to 240

crc	0 Not use CRC	Shall not be included [1]
robust-sorting	0 simple sorting is used	Shall not be included [1]
interleaving	Not used	Shall not be included [1]
ptime		20 ms
max-red	No limitation is present	Shall be included and shall be set to 220 or less
ecn-capable-rtp; leap ect=		Shall be included if offering to use ECN and if the session setup allows bitrate adaptation

Table 4: SDP parameters for AMR-NB or AMR-WB when the MTSI client in terminal offers the bandwidth-efficient payload format

[1] When parameters are not included, the default value is assumed.

Parameter	Usage
bw type	Maximum bw type is to be set <= 64 Kbits/sec (bw usage for AMR-WB can scale dynamically; max bw value is to be set at media level, not at session level)
pre-conditions	Not supported
conference total	Not set
comfort noise	Not supported

Table 5: other SDP parameters

4.3.5 Video

Because it is difficult to control and support Video on all possible endpoints, it is recommended that Video SHOULD NOT be offered at IP IP Interconnect. When (bilaterally agreed that) Video is supported, endpoints SHOULD comply to the following specification [rfc 3264]:

One additional Media Stream Description ("m=") line for video RTP/AVP MAY be used in the SDP offer if the originating end point wants to setup a call with both audio and video. Equipment that does not support video MUST be able to process the audio part of the SDP normally, and reject the video part of the SDP by assigning port 0 on the “m=” line for video in the SDP offer and SDP answer. The number of “m=” lines in the SDP answer MUST be identical to the number of “m=” lines in the SDP offer. Attributes and parameters related to a “m=” line with port 0 MUST be ignored.

4.4 Initial INVITE without SDP (late SDP offer)

Initial INVITEs without SDP (late SDP offer) SHOULD NOT be offered (and consequently SHOULD NOT be accepted) at service access and therefore in case of national traffic SHOULD NOT pass a NL IP interconnect. Networks receiving initial INVITEs without an SDP for national traffic on IP interconnects should reject these initial INVITEs. Initial INVITEs without SDP compromises the early media capability which is a mandatory requirement from legal perspective (i.e. premium rate early media tariff announcement must be played) and national network agnostic service consistency.

4.5 Echo cancellation

When using echo cancellers, it is RECOMMENDED to use G.168 compliant echo cancellers according the ITU-T. The tail length is RECOMMENDED to be 128 ms or longer. The echo return loss is RECOMMENDED to be 30 dB or more.

Because buffering is necessary for echo-cancelling, G.168 binary induces around 20ms delay (40ms for G.165) on the echo-cancelled path. However, depending on the DSP platform there can be different characteristics concerning the delay on the non-echo-cancelled path.
It is RECOMMENDED to use on the non-echo-cancelled path a delay as close as 250 microseconds with a maximum of 10 ms.

5 Addressing, naming & numbering

5.1 Telephone number format

Dutch Telephone number types and ranges are described in the "Nummerplan telefoon- en ISDN-diensten" by the ministry of Economic Affairs, Agriculture. All Dutch operators share information on their telephone number ranges via COIN procedures and the CRDB as the national reference database for telephone numbers. More details can be found at Vereniging COIN website https://coin.nl.

5.1.1 E.164 normalization number overlap

When normalizing Dutch telephone numbers in the 1xx.. number ranges to E.164 international format, number overlap may occur with numbers in 01xx.. geographical number ranges. To avoid this overlap the 1400 number prefix should be used during normalization (e.g. the number “18xx” will be normalized to “+31140018xx”). The 1400 prefix here prevents overlap with +3118xx… geographical numbers. The “144” animal rescue service number will be normalized to “+311400144”. The routing prefix 1400 MUST be used for interconnection. This mechanism is described in decision ET/TM/8118029, published in Staatscourant nr 117 dated June 29th, 2009.
Another example of normalization using the 14xx prefix is for “112” emergency services that will be normalized to “+311412PE112” where the “PE” digits are area dependent and established by "vts Politie Nederland".

5.1.2 URI

Uniform Resource Indicators (URIs) are used for identifying an abstract or physical resource and are described in IETF RFC2396 Uniform Resource Identifiers (URI): Generic Syntax. Telephone numbers in URIs MUST be presented as an international E.164 number, preceded by "+". For the Netherlands the first 2 digits will be 31 as this is the country code for the Netherlands. If it is a geographical number, e.g. subscriber number 0182690074 in Gouda (area code 182) it will be +31182690074. When interworking from SIP to ISUP, the nature of address type SHOULD be normalized to ‘international’ number format.

SIP URI’s are preferred for identifying a SIP service for a telephone number and SHOULD have the format as described in chapter 2.1.:

A URI MUST NOT include visual separators. It MUST be possible to add more tags.

5.2 ENUM

ENUM stands for E.164 Number mapping and describes how DNS (IETF RFC3401) MAY be used for identifying available services and gateway connected to one E.164 number as described in IETF RFC6116. More information on ENUM can be found in Annex A.

5.3 Number portability, COIN

The COIN procedures for activation, porting and deactivation of telephone numbers MUST be used in PSTN, PLMN and Next Generation Networks in the Netherlands. These processes are described in the End-to-End Number Portability Standard which is managed by Vereniging COIN.
COIN services are offered to the members of COIN based on the Central Reference DataBase (CRDB) that contains the reference data per operator for all Dutch numbers, number ranges, ported numbers and service numbers including rates for activated service number if applicable.
More details can be found on the Vereniging COIN website https://coin.nl .

6 Interconnect Access

6.1 Architecture

In i3 Forum document "Technical Interconnection Model for International Voice Services (Release 5.0), May 2012", the following interconnect transport functions are proposed:

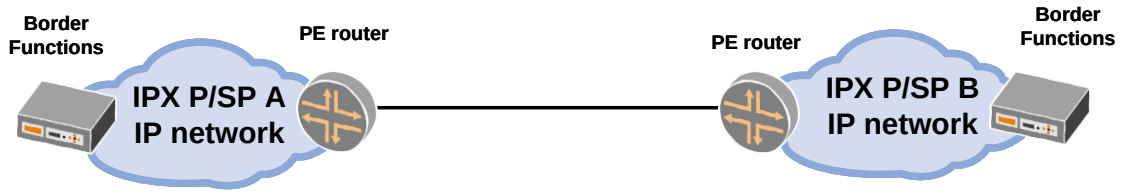

Figure 1: Layer 1 interconnection

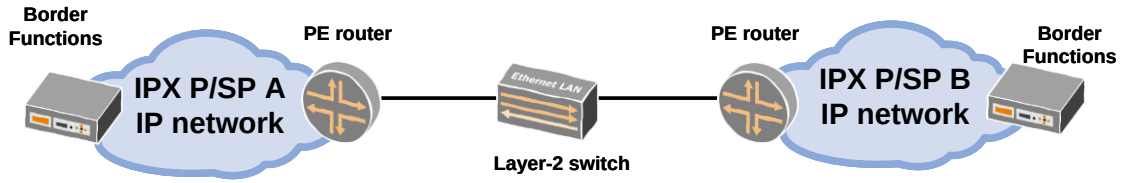

Figure 2: Layer 2 interconnection

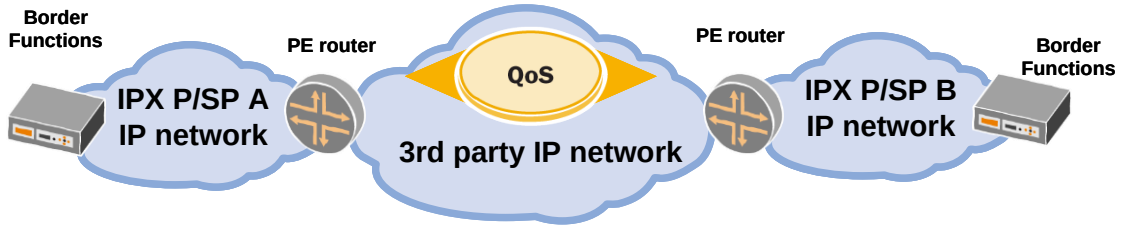

Figure 3: Layer 3 interconnection

RECOMMENDED is not to publish the IP-addresses of the PE-routers that are on the border of your network. Preferably the VoIP traffic SHOULD be separated from the Internet Traffic, either physically or logically.

For the physical connectivity, the i3 Forum document "Technical Interconnection Model for International Voice Services (Release 5.0), May 2012" proposes the following alternatives:

- PDH-based transport systems based on ITU-T Rec. G.703, G.704 and G.705
- SDH-based transport systems based on ITU-T Rec. G.707
- Ethernet-based transport systems bases on IEEE recommendation 802.3; here you need to consider using fast-Ethernet, gigabit-Ethernet or 10 gigabit-Ethernet
- DWDM-based transport systems

For redundancy, multiple PE-routers could be used that are connected to the other party via geographically separated physical connections.

6.2 Transport Protocols

The transport protocols used MUST follow the recommendations as described in the i3 Forum document: Technical Interconnection Model for International Voice Services (Release 5.0), May 2012, Chapter 7.1.1 Transport of SIP (IETF RFC3261) signaling information and Chapter 8.1 Voice calls – protocol profiles.

6.3 Security

It is the responsibility of each operator to maintain a secure environment and interconnect with other parties in an agreed and secure way. The ETSI TR 187 019 SHOULD be followed for the establishment of IP interconnect.

6.4 Authentication

Authentication of interconnecting parties is strongly RECOMMENDED. Multiple methods are available for authentication. The choice of the authentication method is currently not explicitly defined.

6.5 Authorization

Authorization of interconnecting parties is strongly RECOMMENDED.

6.6 QoS bits

Traffic Classification and DiffServ markings MUST follow the recommendations as described in the i3 Forum document: Interconnection Model for International Voice Services (Release 5.0), May 2012, Chapter 6.6 IP Packet marking.

6.7 Traffic type separation

Traffic type separation is MANDATORY for guaranteeing the termination of emergency traffic (see 6.8). Additionally, parties MAY agree on separating other traffic flows such as for example incoming outgoing, mobile and fixed traffic. Reasons for this MAY include but are not limited to capacity dimensioning and security. Different mechanisms MAY be used for this at different layers in the network. One possibility to manage this in layer 2 is the separation of traffic types in different Ethernet VLAN's (802.1Q).

6.8 112 Emergency traffic

Within the Netherlands, it is MANDATORY for providers of telecommunication networks to make provision to guarantee the access to emergency services in case of congestion in the related public network in line with the Telecom Wet (Tw).

By using the SIP Resource Priority Header Field (RFC4412) namespace 'esnet' for Local Emergency Communications (RFC7135), it is possible to assign a relative priority to emergency traffic. The possible classification for the 'esnet' namespace is as follows:

- esnet.0 (lowest)
- esnet.1
- esnet.2
- esnet.3
- esnet.4 (highest)

For 112 emergency traffic the classification 'esnet.2' will be used. This leaves room for assigning lower or higher priorities to other (emergency) traffic for future use. No other priorities than esnet.2 have been assigned and will therefore be ignored if used. The use of RFC4412 for classifying 112 emergency traffic should be bilaterally agreed.

6.9 Carrier (Pre)Select calls

Handling of Carrier (Pre)Select via SIP is RECOMMENDED to conform to the guidelines for national IP Interconnection as described in ETSI TISPAN document Technical Report on NGN Interconnection, paragraph 4.4..

6.10 Service availability

To prevent unnecessary delay due to timeouts and subsequent message re-transmissions, a method by which each entity may discover the operational status of its communicating peers is advised.
Implementation of such a discovery mechanism will enhance the robustness of the IP interconnect and will assist in identifying possible outages at an early stage.
The method of using an "OPTIONS ping" similar to the method described in "Using OPTIONS to Query for Operational Status in the Session Initiation Protocol (SIP)" SHOULD be implemented to enable the operational status discovery. Please note that the referenced document is work in progress.

7 Processes

7.1 Testing

Functional testing of the IP interconnect MUST be performed conform the i3 Forum document: Interoperability Test Plan for International Voice Services, Release 3.0, May 2014.
Optional functional tests MAY be performed according to chapter “5.1.4 ISDN Supplementary Services” test cases of the Plug Box test document "PlugBox - Detail Test Plan for the Model Compatibility Test".
Charging tests SHOULD be performed according to the Plug Box test document "Detail Test Plan for the First Office Application (Billing)".

7.2 Billing / verification

Wholesale billing and verification is REQUIRED if bilaterally agreed. The billing processes as already in place for ISUP interconnections are RECOMMENDED. For (specification of) Billing the "P-Asserted-Identity" MUST be used, by absence of "P-Asserted-Identity" the From MUST be used.

For VoIP interconnection usage SHALL be measured based on call duration. The unit of measurement for call duration SHALL be 0.1 seconds. The call duration is defined as the time in seconds between call start and call end. Call start is defined as the moment at which a 200 OK message is received from the interconnected IP Telco after the sending of an invite message. Call end is defined as the moment at which a BYE message is received from the interconnected IP Telco or a BYE message is sent towards the interconnected IP Telco. No maximum shall be set on long duration calls. Calls MUST be interrupted after a maximum of 3 minutes of receiving and sending no RTP or RTCP packets.

It is RECOMMENDED the call session state is periodically refreshed according to RFC4028. This will ensure closed CDRs in all cases, even when the media (RTP/RTCP) uses a different path than the SIP signaling.

The following recommendations are mentioned in RFC4028:

- The RECOMMENDED Session-Expires timer is 30 minutes
- The RECOMMENDED Min-SE value is 90 seconds
- The RECOMMENDED session refresh method is UPDATE

To compare billing data during a billing period for purposes such as bill disputes or validation of billing data the 'common base CDR' MUST be used for exchanging the basic charging records from the network elements.

The 'common base CDR' exchange format MUST at least contain:

- A-number
- B-number
- Start date/time
- Duration

The following items are RECOMMENDED for the ‘common base CDR’:

- Originating network (COIN operator code, if available)
- Terminating network (COIN operator code, if available)
- Originating (interconnecting) SIP server
- Terminating (interconnecting) SIP server
- Codec
- Recording network element ID (first hop in case of interconnection for incoming traffic)
- Long call indicator
- SIP CallID

7.3 Shielding of B-numbers

For the shielding of B-numbers on the bill of the caller who called that B-number a different mechanism is used independent of CLIP/CLIR. Every Dutch telephony subscriber is entitled to request his telecom provider to shield his number on itemized invoices. This obligation to shield telephone numbers applies to the provider from which the subscriber obtains his telephone or carrier services, as well as to the parties providing itemized invoices to their own subscribers. Vereniging COIN provides a solution for the exchange of information between telecom providers for this purpose.
More details can be found on the Vereniging COIN website https://coin.nl.

A. ENUM services and Infrastructure ENUM

ENUM services
ENUM services are used to indicate the services that are associated with a telephone number. ENUM services MUST be registered using IANA Registration of Enumservice: Guide, Template, and IANA Considerations as described in IETF RFC6117.

The ENUM services E2U+pstn:tel, E2U+pstn:sip and E2U+sip are proposed for use in ENUM NAPTR records as described in IETF RFC4796 IANA Registration for an Enumservice Containing Public Switched Telephone Network (PSTN) Signaling Information, IETF RFC3764 Enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record updated with IETF RFC6118 Update of Legacy IANA Registrations of Enumservices. For indicating that a number can be reached via SIP the service "E2U+sip" may be used with Enumservice subtype "sip" using the URI Scheme “sip”.

If an operator for number 0612345678 wants to use the sip service for the number and the domain string "operatorx.coin" the record may be:

$ORIGIN 8.7.6.5.4.3.2.1.6.1.3.ie164.arpa.
IN NAPTR 100 10 "u" "E2U+sip" "!^.$!sip:+31612345678@operatorx.i-enum.nl!"*

The detailed formatting of ENUM services and applicable values are standardized using Vereniging COIN Standardization and Change Management procedures.

Domain string format
The purpose of the domain string (part after the "@" sign) in a URI is to give information about a telephone number location. This can be in the form of a domain, or as a domain with additional information passed on as tags. The private Top Level Domain (TLD) ".ie164.arpa" is proposed for infrastructure ENUM in the Netherlands. The domain in the domain string must be unique per COIN operator code and must consist of only letters, numbers and/or the hyphen "-" character. It will be possible for an operator to have several domains including several levels of sub-domains. The detailed formatting of domain strings and applicable values are standardized using Vereniging COIN Standardization and Change Management procedures.

Infrastructure ENUM
Infrastructure ENUM information SHOULD be offered in a private ENUM tree for the Dutch operators based on IETF RFC6116 The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM) and IETF RFC3403 The Domain Name System (DNS) Database . An example of a private ENUM tree is shown in Figure 4.

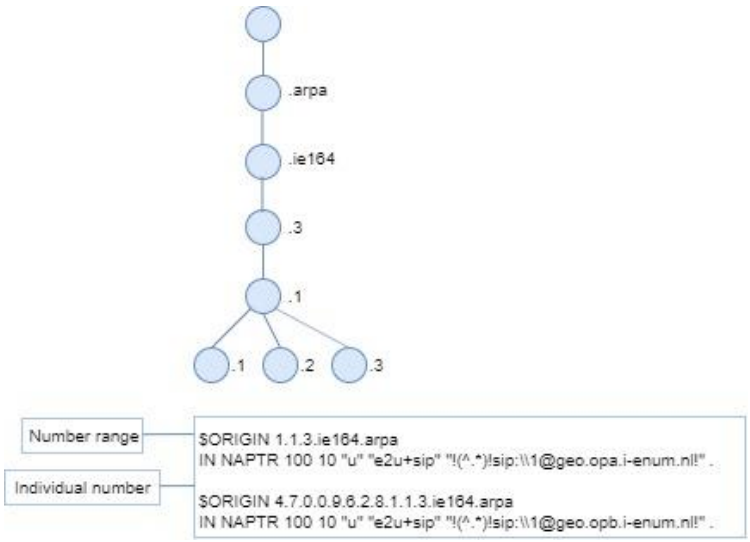

Figure 4: DNS tree for Infrastructure ENUM

Figure 4 illustrates a DNS tree including examples for NAPTR Resource Records for both individual numbers and ranges. The format chosen for this information is NAPTR records, the information may be distributed in DNS Zone File or another suitable format.

B. Issues for future study – Longlist

TOPIC
Rules for generating SIP response codes
Rewrite rules for SIP response codes at IP IP Interconnect
Rules for playing of tones/ announcements on reception of SIP response codes
Description of hunting mechanisms at IP IP Interconnect
Description of other fields in the SIP message
180/183 Progress Indicators
Quality Management (E2E)
End-to-end quality and troubleshooting (“level of insight in connected networks”)