Business Talk
Mitel MiVoice 5000 IPBX

Versions concerned by this guide: R8.3, R8.2, R8.1, R8.0

Information included in this document is dedicated to customer equipment (IPBX, TOIP ecosystems) connection to Business Talk service: it shall not be used for other goals or in another context.

Latest edition: 07/10/2026

Contents

1 Goal of this document 4
2 Certified architectures 5
2.1 Introduction to architecture components and features 5
2.2 Mivoice 5000 Direct SIP trunk architecture on Business VPN 5
2.3 SIP trunk «Enterprise SBC» architecture on Business VPN 7
2.4 SIP trunk « Mitel integrated SBC» architecture on Internet 9
2.4.1 Configuration models 10
2.4.2 Prerequisites 10
2.4.3 Publique IP address assignment 10
2.4.4 Public DNS record 11
2.4.5 Public DNS relay 11
2.4.6 NTP configuration 11
2.4.7 Firewall updates 11
2.4.8 Certificates 11
2.4.9 TLS Mutual Authentication Mechanism Support regarding public certificate Extended Key Usage (EKU) 12
2.4.10 TLS v1.2 and TLS v1.3 cypher suites compliance 14
2.4.11 SRTP encryption on BTalk over Internet 15
2.4.12 Supported codecs on BTalk over Internet 15
3 Parameters to provide by customer to Orange Business for the connection to the service 16
3.1 Mivoice 5000 direct SIP trunk architecture on Business VPN 16
3.2 SIP trunk « SBC Enterprise» architecture on Business VPN 18
3.3 SIP trunk Mitel « integrated SBC» architecture over Internet 18
4 BTalk/BTalk over Internet certified MiVoice 5000 versions 20
4.1 Mitel Mivoice 5000 IPBX versions supported with BTalk/BTalk over Internet 20
4.2 Mitel Mivoice 5000 endpoints and applications supported with BTalk/BTalk over Internet 20
5 Parameters to configure to connect Mivoice 5000 solution to BTalk on BVPN 22
5.1 SIP trunk creation 22
5.2 SIP trunk configuration 22
5.3 Additional configuration: DCF parameters 24
5.4 Coding laws configuration: network calls 25
5.5 Coding laws configuration: If G729 codec only used for network calls 25
6 Parameters to configure to connect Mivoice 5000 solution to BTalk over Internet 26
6.1 Public DNS relay configuration 26
6.2 NTP configuration 26
6.3 Certificates process 27
6.4 Integrated SBC configuration 29
6.5 SRTP support 29
6.6 SIP trunk creation 30
6.7 SIP trunk configuration 30
6.8 Additional configuration: DCF parameters 32
6.9 Coding laws configuration: network calls 33
7 Parameters to be configured common to sections 5 and 6 34
7.1 Routes configuration 34
7.2 Outgoing calls handling: IID configuration 34
7.3 Outgoing calls handling: Outgoing handling configuration 35
7.4 General settings configuration 35
7.5 Subscribers characteristics configuration 36
7.6 Coding laws configuration: local calls 36
7.7 Configuration marquage DSCP 36
7.8 CAC configuration 37
7.9 Fax configuration with Mitel MiVoice 5000 37

7.9.1 T.38 Fax 37
7.9.2 G.711 Inband Fax 38

1 Goal of this document

This document defines the technical requirements for ensuring interoperability between Mitel Mivoice 5000 IPBX and Orange Business's Business Talk (BTalk) international service, collectively referred to hereafter as the "Service."

2 Certified architectures

2.1 Introduction to architecture components and features

This document exclusively describes the architectures supported by Orange that are mainly used by its customers.

Concerning the Quality of Service, Business VPN and BTalk networks trust the DSCP (Differenciated Services Code Point) values sent by customer voice equipment. That's why Orange strongly recommends setting the IPBX, IP phones and other voice applications with a DiffServ/TOS value* = 46 (or PHB value = EF) at least for media.

Fax flows are allowed by BTalk.

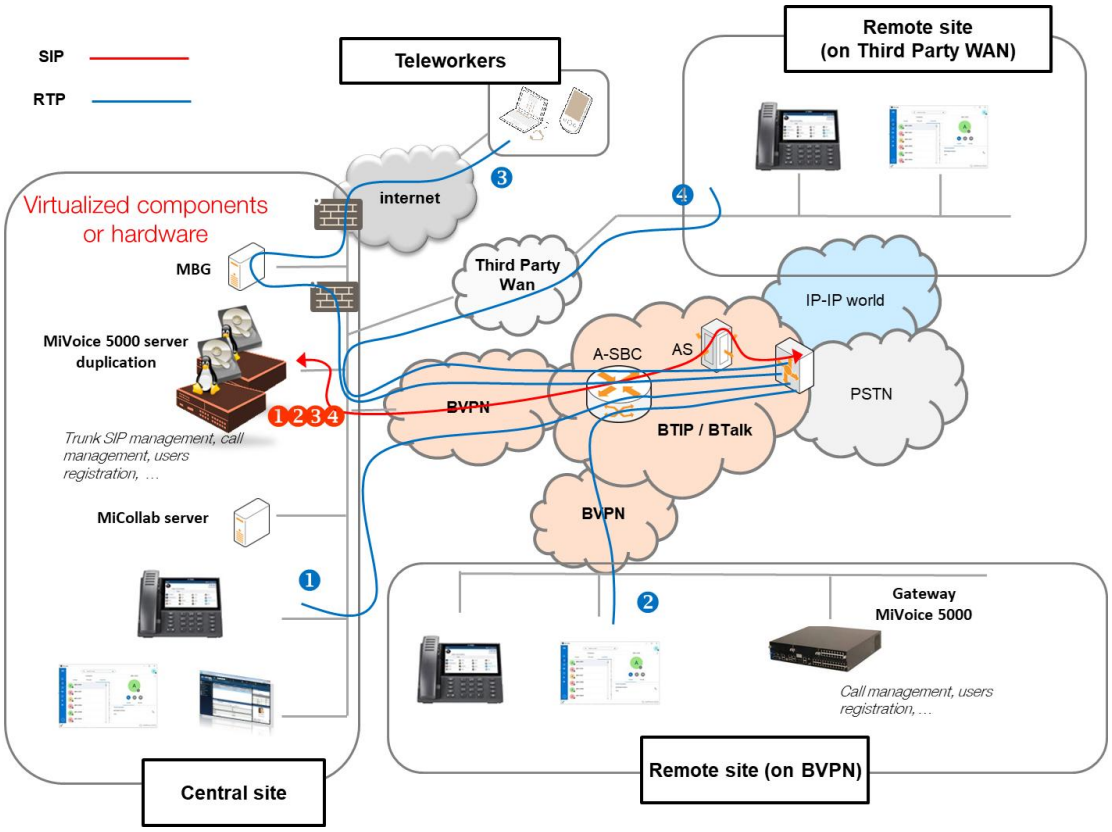
Both inband fax (G.711 passthrough) and T.38 are available by default.

T.38 and G.711 Fax are opened on BTalk network with no end-to-end guarantee. Orange cannot certify the reliability of the fax interoperability that may occur at interconnection points with terminating carriers.

*cf 7.7 section of this document.

2.2 Mivoice 5000 Direct SIP trunk architecture on Business VPN

Access to the Business Talk service is via 2 A-SBCs (nominal and backup).



In the diagram above, the SIP and proprietary internal flows are hidden.

❶ Call from/to central site
❷ Call from/to remote site (on Business VPN)
❸ Call from/to teleworker site (on Internet)
❹ Call from/to remote site (on Third Party WAN)

All SIP trunking signaling flows are carried by the MiVoice 5000 server and routed on the central site BVPN connection.

Media flows are direct between endpoints and BTalk but IP routing differs from one site to another:

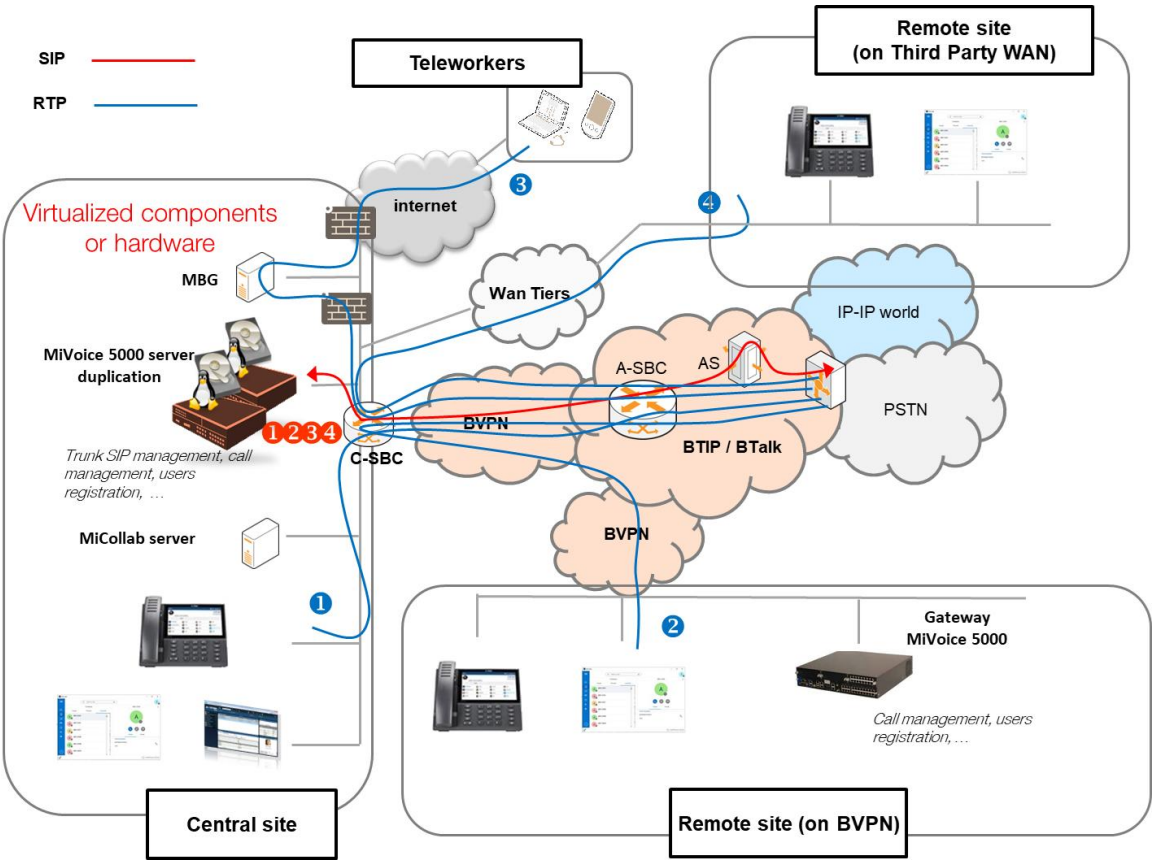
- For the central site, media flows are routed on the main BVPN connection
- For the remote sites on BVPN, media flows are routed on the local BVPN connection (= distributed architecture)
- For the remote sites on Third Party WAN or Internet, media flows are routed through the central site (but not through the IPBX) and use the main BVPN connection (= centralized architecture)

Below a table including information relative to sizing.

Call scenario	**nb of voice channels/media resources used**		
	IPBX	**WAN router***	**BTalk**
1 offnet call from/to the central site (=HeadQuarter=HQ)	**1** in HQ	**1** in HQ	**1** in HQ
1 offnet call from/to a remote site (RS) on BVPN	0 in HQ **1** in RS	0 in HQ **1** in RS	0 in HQ **1** in RS
1 offnet call from/to a remote site (RS) on TP Wan	0 in HQ **1** in RS	**1** in HQ BVPN **1** in HQ TP Wan **1** in RS TP Wan	0 in HQ **1** in RS
1 offnet call from/to a remote site (RS) **with put on hold**	**1** in HQ **1** in RS	**1** in HQ **1** in RS	0 in HQ **1** in RS
1 offnet call from/to a remote site (RS) **after transfer/forward to BTalk**	0 in HQ **0** in RS	0 in HQ **0** in RS	0 in HQ **2** in RS
1 **forced onnet** call from the central site (HQ) to a remote site (= through Business Talk infrastructure)	**2** in HQ **2** in RS	**1** in HQ **1** in RS	**0** in HQ **0** in RS

*On the WAN router, 1 voice channel= 80Kb/s

2.3 SIP trunk «Enterprise SBC» architecture on Business VPN



If the Mitel Mivoice 5000 customer solution is complemented by a SBC equipment, named commonly Enterprise SBC or Customer SBC ("C-SBC" on the picture above), Orange will offer one of the following approaches:

- A "Certified Border" approach (or "Certified SBC equipment"), if the SBC used is already certified by Orange*, regardless of the PBX solution used. Recommendations on this SBC are also available on the Orange Business website.
- A "Generic Offer" approach, if the SBC is not certified by Orange. Orange will not be able to give any recommendation on the choice of hardware, software or configuration, but offers a 'Validation Assistance Service' for the SBC+PBX architecture.

In the diagram above, the proprietary internal flows are hidden.

❶ Call from/to central site
❷ Call from/to remote site (on Business VPN)
❸ Call from/to teleworker site (on Internet)
❹ Call from/to remote site (on Third Party WAN)

Both 'SIP trunking' and RTP media flows between endpoints and the BTalk are anchored by the enterprise SBC:

- On the central site, media flows are routed through the enterprise SBC and the main BVPN connection
- On the remote sites either on BVPN or Third-Party WAN, media flows transit through the enterprise SBC and use the central BVPN connection (= centralized architecture)

*** The list of enterprise SBC equipment models supported by Orange is available in section 4.2 of the document.**

The fact that the flows are anchored via the C-SBC equipment requires particular attention to be paid to the capacity and sizing of the access network at the central site.

Below is a table with some information on sizing:

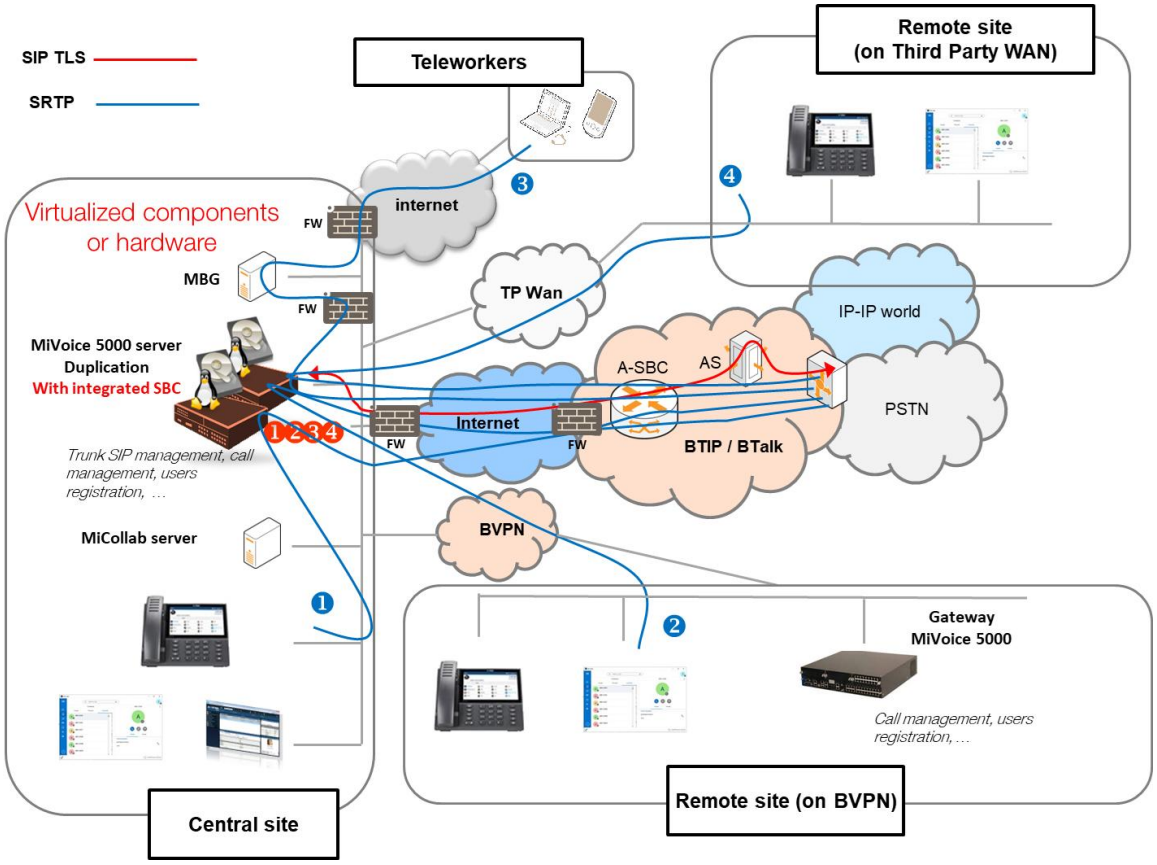
Call scenario	**nb of voice channels/media resources used**		
	IPBX	**WAN router***	**BTalk**
1 offnet call from/to the central site (=HeadQuarter=HQ)	**1** in HQ	**1** in HQ	**1** in HQ
1 offnet call from/to a remote site (RS) on BVPN	0 in HQ **1** in RS	**2** in HQ **1** in RS	0 in HQ **1** in RS
1 offnet call from/to a remote site (RS) on TP Wan	0 in HQ **1** in RS	**1** in HQ BVPN **1** in HQ TP Wan **1** in RS TP Wan	0 in HQ **1** in RS
1 offnet call from/to a remote site (RS) **with put on hold**	**1** in HQ **1** in RS	**3** in HQ **1** in RS	0 in HQ **1** in RS
1 offnet call from/to a remote site (RS) **after transfer/forward to BTalk**	0 in HQ **0** in RS	0 on HQ** / 3 on HQ*** **0** on RS	0 in HQ **2** in RS
1 **forced onnet** call from the central site (HQ) to a remote site (= through Business Talk infrastructure)	**2** in HQ **2** in RS	**3** in HQ **1** in RS	**0** in HQ **0** in RS

*On the WAN router, 1 voice channel= 80Kb/s

**if media release is activated on the enterprise SBC

***if media release is not activated on the enterprise SBC

2.4 SIP trunk « Mitel integrated SBC» architecture on Internet



In the diagram above, the proprietary internal flows are hidden.

❶ Call from/to central site
❷ Call from/to remote site (on Business VPN)
❸ Call from/to teleworker site (on Internet)
❹ Call from/to remote site (on Third Party WAN)

In this architecture, the SBC used is the one integrated in the Mitel MiVoice 5000 solution.

SIP TLS et Secured RTP

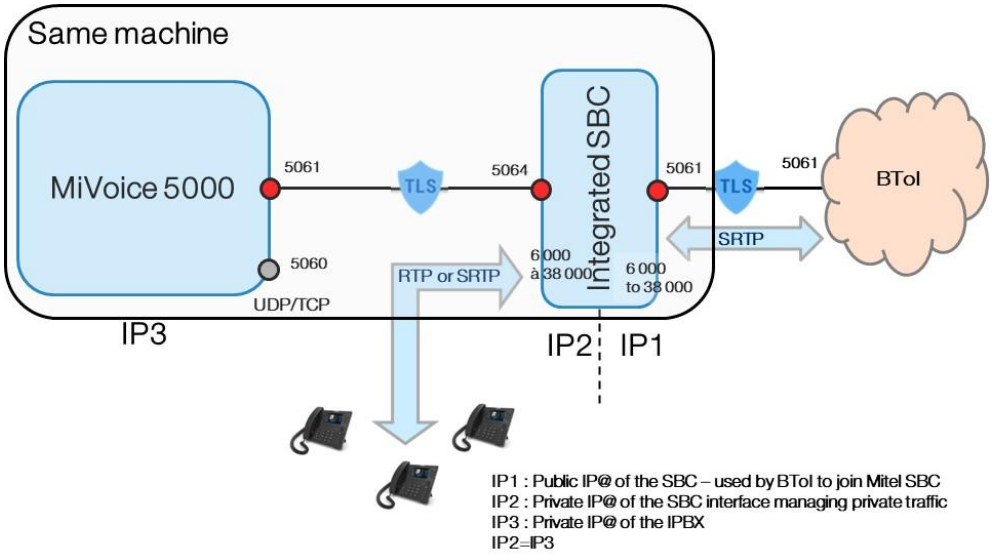
By default, Orange recommends that for security and privacy reasons all SIP messages and media packets are encrypted over the public Internet between the Orange infrastructure and the customer's SIP equipment on the Internet.

Both SIP trunking and RTP media flows between the terminals and BTalk are anchored on the Mitel integrated SBC:

- At the central site, media streams are routed via the Mitel SBC and the central site Internet connection
- At remote sites, over BVPN, Third Party WAN or Internet, media streams are routed via the integrated SBC and use the central site's BTalk over Internet connection (= centralized architecture).

2.4.1 Configuration models

The recommended configuration model for integration with the BTalk over Internet offer (see BTalk Internet Technical Requirements), as part of the Mitel 5000 solution with integrated SBC (where the MiVoice 5000 and the SBC co-exist on the same machine) is the following:



In this model, the public address IP1 is configured on the machine's physical LANB port, without the need for NAT on the Internet firewall, and the private address IP2=IP3 is configured on the machine's physical LANA port.

The configuration details for this topology are explained in Chapter 6 of this document.

Another alternative configuration model is possible (private IP1 address and IP NAT on Internet firewall). Please refer to the Mitel documentation:

https://swdlgw.mitel.com/swdlgw/download.xhtml?token=bec9f6d7-ca9e-485c-bc3d-841126622a8b

2.4.2 Prerequisites

In order to establish the connection with public interface of Orange A-SBC, several preliminary configuration steps have to be performed. These involve the following:

- Public IP address assignment
- Public DNS record
- Public DNS relay configuration
- NTP configuration
- Firewall updates
- Certificate updates
- TLS v1.2 v1.3 cipher suites compliance
- SRTP encryption
- Supported codecs on BTol

2.4.3 Publique IP address assignment

The certified solution requires the use of a public IP address configured directly on the SBC integrated in the Mivoice 5000 and placed in the DMZ.

No NAT must be performed between the interface of the embedded SBC that carries the public IP address and the BTalk infrastructure.

2.4.4 Public DNS record

The Orange A-SBC is accessible via a Fully Qualified Domain Name (FQDN) with an SRV or A-type record created on a public DNS server.

The Mitel Integrated SBC requires a record on a public DNS server to be accessible via FQDN over public Internet access.
BTalk over Internet supports both public IP and type A records for DNS resolution.

2.4.5 Public DNS relay

For the DNS resolution of the Orange ASBCs, necessary for outgoing calls from the Mitel IPBX to the BTalk over Internet infrastructure, it is necessary to configure one or two public DNS relays in the Mitel SBC, or one or two private DNS servers that will relay the DNS requests to Internet.

2.4.6 NTP configuration

It is recommended that an NTP server be implemented on the Mitel Mivoice 5000 to ensure that the clock of the embedded SBC is kept accurate. This is necessary for the validation of certificates issued to it.

2.4.7 Firewall updates

In order to accommodate the traffic between the Mitel Integrated SBC and the Orange A-SBC, it is necessary to update the firewall rules to open the ports for this traffic.

BTalk over Internet – port matrix				
IP Source	Ports Source	IP Destination	Ports Destination	Protocole
Public @IP of Integrated SBC	TCP - Any port	Public @IP of Orange A-SBC	TCP - 5061	SIP TLS Signalisation
Public @IP of Orange A-SBC	TCP - Any port	Public @IP of Integrated SBC	TCP - 5061	
Public @IP of Integrated SBC	UDP - 6000-38000	Public @IP of Orange A-SBC	UDP - 6000-38000	SRTP media
Public @IP of Orange A-SBC	UDP - 6000-38000	Public @IP of Integrated SBC	UDP - 6000-38000	
Public @IP of Integrated SBC	UDP – Any port	Public client DNS relay	UDP - 53	DNS

2.4.8 Certificates

In order to ensure secure traffic, public root and intermediate certificates must be exchanged between the Mitel Integrated SBC and the Orange A-SBC.

The Mitel SBC requires an identity certificate signed by a root certificate from a public certificate authority (including any intermediate certificates involved in the chain of trust).
The customer must provide the Orange BTalk team with the public root and intermediate certificates of the same public certification authority, in PEM (X509 V3) format.

In the event that the public root and intermediate certificates used by Orange (Digicert) to sign the Orange ASBC identity certificates are different, the customer must retrieve them and upload them to the Mitel SBC.

Note that in MV5000 release <R8.1 it is not possible to generate a Certificate Signing Request (CSR) file directly on the integrated SBC (MiVzoice 5000).
Therefore, the customer must generate the CSR file himself and then have it signed by a public Certificate Authority.
After the certification authority has approved the Mitel SBC identity certificate, it must be loaded onto the integrated SBC (MiVoice 5000).

2.4.9 TLS Mutual Authentication Mechanism Support regarding public certificate Extended Key Usage (EKU)

Since mid-2026 public Certificate Authorities (CA's) have progressively issued TLS certificates with the **Server Authentication Extended Key Usage only (EKU),** removing Client Authentication EKU by default, in all end-entity public certificate.

This change follows the **Google Chrome Root Program requirement** (decision made in last October 2024) that publicly **trusted TLS x.509 certificates must no longer support both Server Authentication and Client Authentication purposes, leaving only Server Authentication EKU in.**

Some CAs, such as DigiCert, offer a **grace period** during which End- Entity certificates with both Server Authentication and Client Authentication EKUs can still be requested. By default, DigiCert issues certificates with Server Authentication EKU only. This dual-EKU option is available on request until 1 March 2027. After that date, only Server Authentication EKU will be included.

Source: https://knowledge.digicert.com/alerts/sunsetting-client-authentication-eku-from-digicert-public-tls-certificates

Please check your CA provider policy:

1. Grace period available: dual-EKU certificates remain supported for a limited period of time
2. No grace period: both the Orange aSBC and the customer SBC/IPBX must use Server Authentication–only certificates.

In the 2nd scenario, where both endpoints use public certificates with the Server Authentication EKU only, **Orange validates mutual TLS interoperability through testing**.

The impact on mutual authentication may depend on:

- which endpoint acts as the TLS client or TLS server.
- and the vendor capabilities for handling certificates without the Client Authentication EKU

Case 1: Mitel 5000 with integrated SBC initiates the TLS handshake.

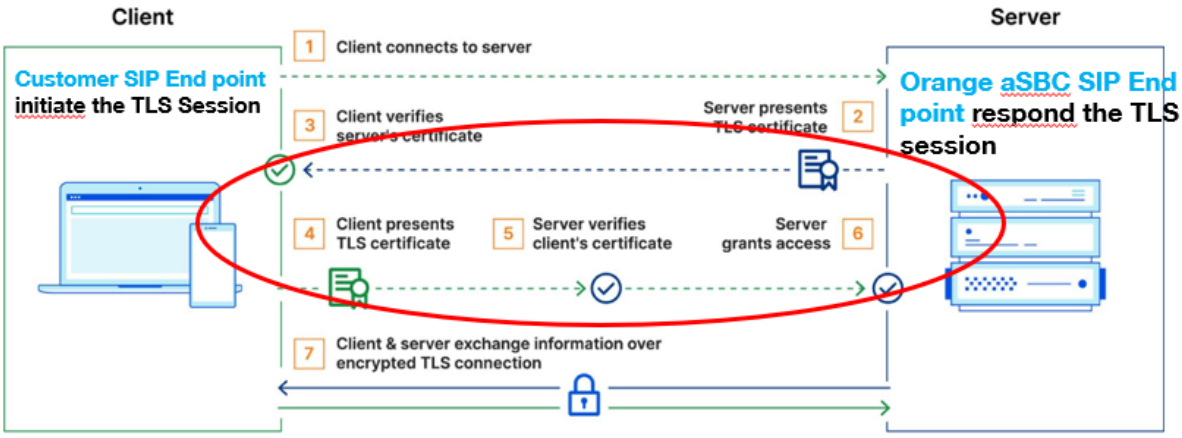
In this scenario:

- The Mitel 5000 with integrated SBC acts as the TLS client.
- The Orange aSBC acts as the TLS server.
- The Mitel 5000 with integrated SBC initiates the TLS handshake.

The Orange aSBC requests a certificate from the Mitel 5000 with integrated SBC in order to perform mutual TLS authentication.

TLS handshake sequence

1. The Orange aSBC requests the customer certificate (TLS message “Certificate request”)
2. The Mitel 5000 with integrated SBC presents its certificate with Server Authentication (serverAuth) EKU only [4].
3. The Orange aSBC verifies the certificate [5] and grants access [6].



Result: Mutual TLS continues to work when the Mitel 5000 with integrated SBC initiates the connection, even if the customer public certificate contains the serverAuth EKU only.

No specific Mitel 5000 with integrated SBC configuration change is required for this scenario.

Case 2: Orange aSBC initiates the TLS

In this scenario:

- The Orange aSBC acts as the TLS client.
- The Mitel 5000 with integrated SBC acts as the TLS server.
- The Orange aSBC initiates the TLS handshake.

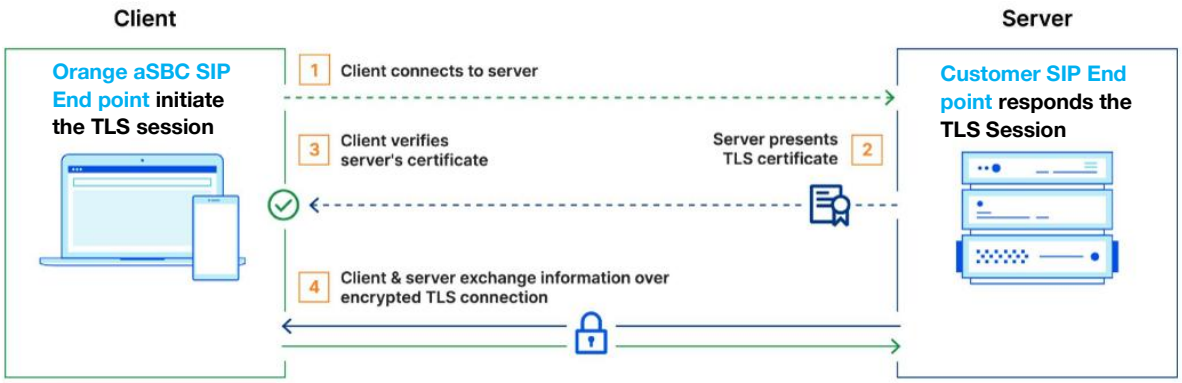
The Mitel 5000 with integrated SBC performing mutual TLS authentication requests a certificate from Orange in order to perform mutual TLS authentication. Orange presents its public certificate containing the serverAuth EKU only.

Default behavior — TLS handshake failure
By default, the Mitel 5000 with integrated SBC requires a certificate presented by a TLS client to include the clientAuth EKU. It therefore rejects the Orange certificate.
As a result, mutual TLS authentication fails and the TLS handshake cannot be completed.

Configuration required to ensure a successful TLS handshake
To allow Orange certificates containing serverAuth EKU only, the customer must disable mutual TLS authentication.
With this setting, the Mitel 5000 with integrated SBC will not request the Orange certificate.
Please go to **§ 6.4 Integrated SBC configuration** for Orange TLS context configuration details.

TLS handshake sequence after the configuration change

1. The Mitel 5000 with integrated SBC does not request the Orange aSBC certificate.
2. The Mitel 5000 with integrated SBC completes the TLS handshake without client certificate verification [4].



Security consideration: Please note this specific Mitel 5000 with integrated SBC configuration option reduce customer security concern with Orange: End customer Mitel 5000 with integrated SBC security heavily change by completing TLS handshake without verification of client certificate and must be accepted by End Customer.

2.4.10 TLS v1.2 and TLS v1.3 cypher suites compliance

The cypher suites supported by the Orange A-SBC for TLS v1.3 (recommended version by Orange) are shown below:

- TLS_AES_256_GCM_SHA384 (0x1302)
- TLS_AES_128_GCM_SHA256 (0x1301)
- TLS_CHACHA20_POLY1305_SHA256 (0x1303)

The cypher suites supported by the Orange A-SBC for TLS v1.2 (alternative version) are shown below:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

For TLS v1.3, the integrated Mitel SBC supports, among other things, the following cryptographic suites. The three suites supported by BTalk over Internet are highlighted in bold:

- **TLS_AES_256_GCM_SHA384 (0x1302)**
- **TLS_CHACHA20_POLY1305_SHA256 (0x1303)**
- **TLS_AES_128_GCM_SHA256 (0x1301)**
- TLS_AES_128_CCM_SHA256 (0x1304)

For TLS v1.2, the integrated Mitel SBC supports, among other things, the following cryptographic suites. The two suites supported by BTalk on the Internet are highlighted in bold:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)**
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 (0xc0af)
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad)
- TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05d)
- TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)**
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae)
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xc0ac)

- TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 (0xc05c)
- TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)

The Mitel integrated SBC and Orange A-SBC will negotiate the most secure matched cipher suite (TLS_AES_256_GCM_SHA384) to establish TLS connection.

On the MiVoice 5000 solution, it is important to note that an "Encryption" licence is required to activate the encryption of flows by the integrated SBC.

2.4.11 SRTP encryption on BTalk over Internet

AES_CM_128_HMAC_SHA1_80 suite is recommended for media encryption.

2.4.12 Supported codecs on BTalk over Internet

Supported codec is G.711A (20ms) for BTalk over Internet.
G.711u (20ms) can be requested on specific case.

3 Parameters to provide by customer to Orange Business for the connection to the service

Below are the parameters (in red) that the customer must provide to Orange Business to connect its IPBX to the service.

Several types of architecture are supported.

3.1 Mivoice 5000 direct SIP trunk architecture on Business VPN

Central site architecture	Level of service	Customer IP addresses used by the service
ARCHITECTURE 1: NO REDUNDANCY		
Single MiVoice 5000 platform (Call server or Mitel gateway)	No redundancy	MV5000 IP@
ARCHITECTURE 2: DUPLICATED SERVERS		
Duplicated MiVoice 5000 Call Servers	Local redundancy (active/passive)	Virtual Call Server IP@
ARCHITECTURE 3: SPATIAL REDUNDANCY		
Spatial redundant MiVoice 5000 Call Servers	Redundancy on 2 different physical sites (active/passive)	Virtual Call Server IP@
ARCHITECTURE 4*: DUAL-HOMING - 1 NUMBERING PLAN		
2 MiVoice 5000 platforms (active/active) in nominal /backup mode for a group of users (1 numbering plan). The MiVoice 5000 platforms can be hosted on the same site or on 2 different physical sites. Each MiVoice 5000 platform (MV5000-1 and MV5000-2) has its own SIP trunk but the MV5000-2 SIP trunk is only used as a backup. Both platforms are independent but considered as being part of one central site. - Nominal mode: All users register on MV5000-1 platform - Backup mode: All users re-register on MV5000-2 platform A MiVoice 5000 platform can be a Call server (or duplicated or spatial redundant Call servers) or a Mitel gateway.	User registration survivability (IP phones only) **Rerouting at Orange SBC level**	Nominal MV5000-1 platform (MV5000-1) IP@ And Backup MV5000-2 platform (MV5000-2) IP@

Central site architecture	Level of service	Customer IP addresses used by the service
ARCHITECTURE 5*: DUAL-HOMING - 2 NUMBERING PLANS		
2 MiVoice 5000 platforms (active/active) hosted on 2 different physical sites (HQ1 et HQ2). Each platform manages a range of users (2 numbering plans). Each platform (MV5000-1 and MV5000-2) has its own SIP trunk and each manages its own group of users in nominal mode. **- In Nominal mode:** All HQ1 users register on HQ1 MV5000-1 platform All HQ2 users register on HQ2 MV5000-2 platform **- In Backup mode:** In case of HQ1 MV5000-1 platform crash, all HQ1 users re-register on HQ2 MV5000-2. In case of HQ2 MV5000-2 platform crash, all HQ2 users re-register on HQ1 MV5000-1. Warning : Access capacity of both HQ sites has to be sized adequately. The 2 HQ sites have to be both connected via MOVACS for example. A MiVoice 5000 platform can be a Call server (or duplicated or spatial redundant Call servers) or a Mitel gateway.	**MV5000-1 HQ1** User registration survivability (IP phones only) **Rerouting at BTalk service level**	HQ1 MV5000-1 IP@
	MV5000-2 HQ2 User registration survivability (IP phones only) **Rerouting at BTalk service level**	HQ2 MV5000-2 IP@

Remote Site (RS) architecture Any Remote site architecture can be associated to any Central site Architecture listed above	Level of service	Customer IP addresses used by the service
Remote site without Mitel gateway	No survivability	N/A
Remote site with Mitel gateway	Local survivability for the remote site hosting the gateway in case of non-access to Central site – Via PSTN only	N/A
Remote site with Mitel gateway + Backup SIP trunk	Local survivability for the remote site hosting the gateway in case of non-access to Central site. SIP trunk used as backup solution for incoming and outgoing traffic.	Gateway IP@

3.2 SIP trunk « SBC Enterprise» architecture on Business VPN

Central site architecture	Level of service	Customer IP addresses used by the service
1 enterprise SBC	No redundancy	Enterprise SBC IP@
2 enterprise SBC In nominal/backup mode	Local redundancy or on 2 different physical sites	Nominal enterprise SBC IP@ And Backup enterprise SBC IP@
2 enterprise SBC In load sharing mode	Local redundancy or on 2 different physical sites	Virtual IP@ of enterprise SBCs
2 enterprise SBC In High Availabilty (HA) mode	Local redundancy or on 2 different physical sites	Virtual IP@ of enterprise SBCs

Remote Site (RS) architecture Any Remote site architecture can be associated to any Central site Architecture listed above	Level of service	Customer IP addresses used by the service
Remote site without Mitel gateway	No survivability	N/A
Remote site with Mitel gateway	Local survivability for the remote site hosting the gateway in case of non-access to Central site – Via PSTN only	N/A

3.3 SIP trunk Mitel « integrated SBC» architecture over Internet

Central site architecture	Level of service	Customer IP addresses used by the service
ARCHITECTURE 1: NO REDUNDANCY		
Single MiVoice 5000 platform with integrated SBC (Mitel Call server or EX gateway)	No redundancy	Integrated SBC public FQDN DNS type A or type SRV
ARCHITECTURE 2: DUPLICATED SERVERS		
Duplicated MiVoice 5000 Call servers with integrated SBC	Local redundancy (active/passive)	Integrated SBC public FQDN DNS type A or type SRV
ARCHITECTURE 3: SPATIAL REDUNDANCY		
Spatial redundant MiVoice 5000 Call servers with integrated SBC	Redundancy on 2 different physical sites (active/passive)	Integrated SBC public FQDN DNS type A or type SRV

Central site architecture	Level of service	Customer IP addresses used by the service
ARCHITECTURE 4*: DUAL-HOMING - 1 NUMBERING PLAN		
2 MiVoice 5000 platforms with integrated SBC (active/active) in nominal /backup mode for a group of users (1 numbering plan). The MiVoice 5000 platforms can be hosted on the same site or on 2 different physical sites. Each MiVoice 5000 platform (MV5000-1 and MV5000-2) has its own SIP trunk but the MV5000-2 SIP trunk is only used as a backup. Both platforms are independent but considered as being part of one central site. - Nominal mode: All users register on MV5000-1 platform - Backup mode: All users re-register on MV5000-2 platform A MiVoice 5000 platform can be a Call server (or duplicated or spatial redundant Call servers) or a Mitel gateway.	User registration survivability (IP phones only) **Rerouting at Orange SBC level**	Integrated SBC public FQDN DNS type A or type SRV of the nominal MV5000-1 platform (MV5000-1) And Integrated SBC public FQDN DNS type A or type SRV of the backup MV5000-2 platform (MV5000-2)
ARCHITECTURE 5*: DUAL-HOMING - 2 NUMBERING PLANS		
2 MiVoice 5000 platforms (active/active) hosted on 2 different physical sites (HQ1 et HQ2). Each platform manages a range of users (2 numbering plans). Each platform (MV5000-1 and MV5000-2) has its own SIP trunk and each manages its own group of users in nominal mode. **- In Nominal mode:** All HQ1 users register on HQ1 MV5000-1 platform All HQ2 users register on HQ2 MV5000-2 platform **- In Backup mode:** In case of HQ1 MV5000-1 platform crash, all HQ1 users re-register on HQ2 MV5000-2. In case of HQ2 MV5000-2 platform crash, all HQ2 users re-register on HQ1 MV5000-1. Warning : Access capacity of both HQ sites has to be sized adequately. The 2 HQ sites have to be both connected via MOVACS for example. A MiVoice 5000 platform can be a Call server (or duplicated or spatial redundant Call servers) or a Mitel gateway.	**HQ1 MV5000-1** User registration survivability (IP phones only) **Rerouting at BTalk service level**	Integrated SBC public FQDN DNS type A or type SRV of the nominal HQ1 MV5000-1 platform (MV5000-1)
	HQ2 MV5000-2 User registration survivability (IP phones only) **Rerouting at BTalk service level**	Integrated SBC public FQDN DNS type A or type SRV of the nominal HQ2 MV5000-2 platform (MV5000-2)

Remote Site (RS) architecture Any Remote site architecture can be associated to any Central site Architecture listed above	Level of service	Customer IP addresses used by the service
Remote site without Mitel gateway	No survivability	N/A
Remote site with Mitel gateway	Local survivability for the remote site hosting the gateway in case of non-access to Central site – Via PSTN only	N/A

4 BTalk/BTalk over Internet certified MiVoice 5000 versions

Orange supports the last two major versions of the MiVoice 5000 solution when they are still supported by Mitel, and ensures that the infrastructure evolutions of its Business Talk service continue to interact correctly with these supported versions and the associated architectures.

For more details on the Mitel Mivoice 5000 release lifecycle, please refer to the WEB page https://pcm.mitel.com/Default.aspx (Mitel MiAccess).

4.1 Mitel Mivoice 5000 IPBX versions supported with BTalk/BTalk over Internet

Mitel MiVoice 5000 IPBX – Software versions			
Product and versions reference	✓: Certified by validation ✓: Compatible by technical analyse NS : Not Supported		Comments/restrictions
Mivoice 5000	**Orange Services**		
	BTalk	**BTalk over Internet**	
R8.3 SP2 AH00	✓	✓ Via Mitel integrated SBC	
R8.3 SP1 AG00	✓	✓ Via Mitel integrated SBC	
R8.3 AE00	✓	✓ Via Mitel integrated SBC	
R8.2 SP3 B400	✓	✓ Via Mitel integrated SBC	
R8.2 SP1 AG00	✓	✓ Via Mitel integrated SBC	
R8.1 SP1 B204	✓	✓ Via Mitel integrated SBC	
R8.1	✓	✓ Via Mitel integrated SBC	
R8.0 SP1	✓	✓ Via Mitel integrated SBC	

4.2 Mitel Mivoice 5000 endpoints and applications supported with BTalk/BTalk over Internet

Mitel MiVoice 5000 IPBX – Endpoints and applications				
Product reference		Minimum supported Software product release NA: Not Applicable	✓: Certified ✓: Not certified NS : Not Supported	Comments
Mitel SIP phones	Refer to Mitel documentation (MiVoice 5000 release notes) to find the list of products and components that Mitel MiVoice 5000 supports.	Refer to the Product Compatibility Matrix application available on the https://pcm.mitel.com/Default.aspx to find for each Mitel product, the software releases compatible with Mitel MiVoice 5000 release. This application uses the Mitel MiAccess Single Sign On mechanism.	✓	Please refer to the manufacturer's website, MiAcces -> Compatibility Matrix, to check the compatibility of the versions of these products with the MiVoice 5000 versions.
Mitel SIP-DECT				
Other Mitel Phones				
Mitel Unified Communication & mobility				
	Unify Phone	NA	NS	Unify Phone is not compatible with BTalk over Internet SIP service.

Mitel MiVoice 5000 IPBX – Endpoints and applications				
Product reference		Minimum supported Software product release NA: Not Applicable	✓: Certified ✓: Not certified **NS** : Not Supported	Comments
Mitel Media gateways	Refer to Mitel documentation (MiVoice 5000 release notes) to find the list of products and components that Mitel MiVoice 5000 supports.	Refer to the Product Compatibility Matrix application available on the https://pcm.mitel.com/Default.aspx to find for each Mitel product, the software releases compatible with Mitel MiVoice 5000 release. This application uses the Mitel MiAccess Single Sign On mechanism.	✓	Please refer to the manufacturer's website, MiAcces -> Compatibility Matrix, to check the compatibility of the versions of these products with the MiVoice 5000 versions.
Fax	Analog fax on EX/GX Gateway	Refer to the Product Compatibility Matrix application available on the https://pcm.mitel.com/Default.aspx to find for each Mitel product, the software releases compatible with Mitel MiVoice 5000 release. This application uses the Mitel MiAccess Single Sign On mechanism.	✓	T.38 and G.711 inband fax are enabled on the BTalk network without an end-to-end guarantee. Orange cannot certify the reliability of fax interoperability that may occur at interconnection points with terminating carriers.
	Analog fax on TA710xi Gateway			
	Analog fax on AG4172 Gateway			

5 Parameters to configure to connect Mivoice 5000 solution to BTalk on BVPN

This section describes the minimum configuration to be applied to the MITEL MiVoice 5000 solution to ensure interoperability with the BTalk infrastructure.

5.1 SIP trunk creation

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Network>Trunk group>Names (4.2.1.1) Create un trunk group for the SIP trunk.	
Parameter	*Value*	Comments
Trunk group N°x	*Trunk group name*	Choose a trunk group numberand a trunk group name (example : « SIP-BTalk »).

5.2 SIP trunk configuration

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Network>Trunk group>Characteristics (4.2.1.2) Select the trunk group previously created.	
Parameter	*Value*	Comments
Signaling characteristics :	---	---
Physical type	VOICE IP	
Nature	BOTHWAY	
Signalling type	SIP	
Subtype	STANDARD	
Characteristics :	---	2 edition modes exist : - « basic » mode accessible via the button : - « advanced » mode accessible via the button : The parameters shown below in *italics* and highlighted in grey are only visible via the "advanced" mode.
Signalling type	SIP	
Subtype	STANDARD	
Link state	CONNECT.	
Company	STE0	Company name configured on the IPBX.
Department	SERV 0	Department name configured on the IPBX.
Protocol	UDP	
Proxy N°1	A-SBC IP@	IP address of the nominal A-SBC
- port	5060	
Proxy N°2	A-SBC IP@	IP address of the secondary A-SBC
- port	5060	
Domaine / realm		Not used
Local proxy	NO	Not used

Proxy checking	.....	Not used
Identifier		Not used
Registering		Not used. Not to check
Authentification		Not used. (Default value : SIP CLIENT)
Client account :	---	---
- login		Not used
- password		Not used
Public name of SIP access point		*Not used*
Audit during speech	*Checked*	
- speech audit management	*MSG UPDATE*	*Used to choose the type of SIP request sent during communication, depending on the next field (Audit frequency), to ensure the availability of the remote device.*
- audit frequency (sec)	*1200*	
Audit out of speech (OPTIONS)	Checked	IPBX sends regularly an OPTIONS message to the Orange A-SBC.
- audit frequency (sec)	300	
- status	ACCEPTED	Status of audit out of speech
- next audit at HH:mm:SS	---	---
Compelled release of trunks	*Unchecked*	
Redirected numbers emission	*DIVERSION*	
Identity sending management:	---	---
- call identifier (From)	*IID/AID*	
- number (From) in E.164 format	*Checked*	
- presentation/restriction	*P-Asserted-ID*	
- call identifier (PAI)	*IID/AID*	
- number (PAI) in E.164 format	*Checked*	
- sending anonymous into From	*Checked*	
- update of name/number (UPDATE)	*Unchecked*	
- number (To) in E.164 format	*Checked or Unchecked*	
Identity reception management:	---	---
- calling id. in	*PAI or PPI or RPID*	
N° without external prefix	*Unchecked*	
Name management	*Unchecked*	
Forwarding management:	---	---
- on busy / immediate forward	*Unchecked*	
- forward on no answer	*Unchecked*	
Call Sending type (internal/external)	*Unchecked*	
Voice mail	*Unchecked*	
Local generation of tones	*Checked*	*Announcements/tones are managed by MIVOICE 5000*
Support PRACK (100rel)	*Checked*	
Tones management before answer	*180+SDP+P-Early-Media*	
- support P-Early-Media	*Checked*	
Re-invite without SDP allowed	*Checked*	
Reject T.38	*415 Unsupported Media Type*	Default value. Regardless of T.38 and G.711 Fax support.

REFER sending	*Unchecked*	
Support of video	*Unchecked*	
Support of T.38	*Unchecked*	Default value. Regardless of T.38 and G.711 Fax support.
Support of other medias (IM, etc..)	*Unchecked*	
Bearer type incoming	*CCBT+CCBNT*	
Calls from	RESEAU	
Priority calls if transit	*Unchecked*	
Search DID numbers	---	---
- incoming digit translator number		Enter in this field the incoming digit translator number. To be filled in only if configured and if it is necessary to translate the number received from the network into an internal number.
- reject of numbers not assigned	*Unchecked*	
Pre-answering message, caller charged	---	---
- if called party free or busy 1	Unchecked	
- if called party busy 2	*Unchecked*	
- if number not assigned	*Unchecked*	
Transf. acc. to called pty compt-dept	*Unchecked*	
Transfer to	SV OP1	Name of the operator service configured on the IPBX.
Listening intervention allowed	Unchecked	
Trunk group id (tel. record)	*0*	
Trunk group monitoring	*Checked*	
Max. nb of simultan. Calls allowed		Not used
CAC IP address	A-SBC IP@	Field configured automatically filled according to the IP address of A-SBC.
Centre – CAC class		Field configured automatically filled according to the CAC configuration.
G711 forced in mode FAX/Modem	*Unchecked*	Default value. Regardless of T.38 and G.711 Fax support.

5.3 Additional configuration: DCF parameters

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>System>Expert>DCF settings (2.7.3) Enter a DCF number to configure « Number (in decimal) of the DCF » then click on the button « Select the item ».	
Parameter	*Value*	Comments
Number (in decimal) of the DCF	282	
Value in decimal	2	
Value in hexadecimal	0002	
Number (in decimal) of the DCF	460	
Value in decimal	1	
Value in hexadecimal	0001	

5.4 Coding laws configuration: network calls

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Quality of service>Voice over IP coding law (4.4.2) Select the « Call type » then the « Set type » and click on « Select the item ».	
Parameter	*Value*	Comments
Priority 1, law:	G711	Coding law set in priority 1.
at type 1:	A LAW (or MU LAW)	G711Ulaw can be supported in option.
duration of packets (ms):	20	
Priority 2, law:	G729	Coding law set in priority 2.
at type 1:	G729A	
at type 2:	G729	
duration of packets (ms):	20	

This configuration has to be applied to the whole call types below :

- **Call type:** NETWORK
- **Direction:** …… (not mandatory)

- **Call type:** TONES
- **Messages type:** NETWORK

5.5 Coding laws configuration: If G729 codec only used for network calls

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Quality of service> Voice over IP coding law (4.4.2) Select the « Call type » then the « Set type » and click on « Select the item ».	
Parameter	*Value*	Comments
Priority 1, law:	G729	Coding law set in priority 1.
at type 1:	G729A	
at type 2:	G729	
duration of packets (ms):	20	
Priorité 2, loi:	……	
Priorité 3, loi:	……	

This configuration apply to the whole call types below :

- **Call type:** NETWORK
- **Direction:** …… (not mandatory)

- **Call type:** TONES
- **Messages type:** NETWORK

- **Call type:** VOICE MAIL

6 Parameters to configure to connect Mivoice 5000 solution to BTalk over Internet

This section describes the minimum configuration to be applied to the MITEL MiVoice 5000 solution to ensure interoperability with the BTalk over Internet infrastructure.

6.1 Public DNS relay configuration

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>System>Configuration>Cards>IP board settings (2.3.4.3) Apply the configuration below.	
Parameter	*Value*	Comments
DNS 1 address	DNS 1 IP@	Configure a 1st public DNS relay or a 1st private DNS server that will relay DNS requests to the Internet.
DNS 2 address	DNS 2 IP@	Configure a 2nd public DNS relay or a 2nd private DNS server that will relay DNS requests to the Internet.

6.2 NTP configuration

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>System>Info>Date and time (2.1.1) Apply the configuration below.	
Parameter	*Value*	Comments
Network synchronisation	Checked	If this box is checked, the system updates its DATE and TIME settings at regular intervals according to the values retrieved from the NTP server(s) defined in the next field.
- time server 1	IP address of the time server 1	DNS name or IP address of the considered NTP server.
- time server 2	IP address of the time server 2	DNS name or IP address of the considered NTP server.
Time zone : - region - town	 Ex : EUROPA Ex : Berlin	The time zone is set by selecting a region and then a city within that region.

6.3 Certificates process

Equipment	MiVoice 5000 IPBX IPBX		
Configuration path	Telephony service>System>Security>Certificates management (2.4.2) Apply the configuration below.		
Parameter		*Value*	Comments
« Generate certificate signing request (CSR)» tab		---	Available in MV5000 release ≥R8.1
Common name			FQDN assigned to a public IP address configured directly on the SBC integrated in the Mivoice 5000.
Company / Organization			Example : « Company ».
Department / Unit			Example : « Company Unit ».
Locality / City			Example : « City ».
Province / Region / State			Example : « State ».
Country code (2 letters)			Example : « FR».
Alternate names*			Not used.
Create CSR			Create and download CSR file used to generate a Mitel SBC identity certificate from a certification authority.
« Certificates» tab		---	Available in MV5000 release ≥R8.1
Action		Add CERTIFICATE (PEM)	Select and download the file with Identity certificate.
Root certificate			Select and download the file with root certificate.
Intermediate certificate (if available)			Select and download the file with intermediate certificate.
Private key (PEM). Leave empty if you used the CSR			This field must remain empty.
Name			Enter the name for this certificate.
Comment			Optional.
« Certificates» tab		---	Recommended only in MV5000 release <R8.1
Action		Add CERTIFICATE	Select the file and click on Download. Please note that this certificate must be in PKCS 12 format (include the certificate, private key and certification chain).
Shared secret		XXXX	This Shared secret field appears to allow you to enter the passphrase (secret phrase) used when generating the pkcs12.

		This field is required to complete the import of the pkcs12 file. The passphrase is a string of alphanumeric characters indicating the password to decrypt the certificate file. The number of characters entered must be between 4 and 20. The characters are displayed in clear text during input and then replaced by ******* when the field is validated. List of characters allowed to be entered for this field: o 0 to 9 o A to Z o a to z o " # ' ( ) - _ @ + = % * > < , . ; / :
Name	XXXX	Enter the name for this certificate. This field is pre-filled with the name of the imported pkcs12 file (only if this file name does not yet exist among the already installed certificates).
Comment	XXXX	This Comment field is optional and will be attached to the certificate to help the operator to identify the certificate in case of multi-import followed by late assignments.
« Servers certificates assignment » tab	---	---
Available certificates	XXXX	Select the name of the imported certificate.
Inter-site link	Unchecked	
WebAdmin	Unchecked	
User Portal	Unchecked	
Internet Gateway	Checked	
LDAP server	Unchecked	
« Certification authorities » tab	---	---
Action	Add CERTIFICATE	Import and download the public root and intermediate certificates used by Orange to sign the Orange ASBC identity certificates.

6.4 Integrated SBC configuration

Equipment	MiVoice 5000	
Configuration path	Telephony service>Network and links>Internet gateway (4.6)	
Parameter	*Value*	Comments
Service INTERNET GATEWAY	START	
Mode	Standard	
Secured interface	Checked	
Both way (MTLS)	Unchecked	This field must be Unchecked as there is no option allowing mTLS support requested by Mitel 5000 with integrated SBC to accept TLS client BTalk over Internet SIP trunk infrastructure certificate requested regardless of whether the client Auth EKU is present or not.
Working mode	SBC TRUNK	
OTT terminals allowed	Unchecked	
Public protocols	TLS	
NAT on public interface	Unchecked	
- public interface	Public IP@ of the integrated SBC	IP1 address in the figure of the section 2.4.
- secured port (TLS)	5061	
Private protocols	TLS	
private interface	Private IP@ of the integrated SBC	IP2 address in the figure of the section 2.4.
- secured port (TLS)	5064	
NAT on private interface	Unchecked	
- iPBX address or FQDN	IP@ of the IPBX	IP3 address in the figure of the section 2.4.
- secured port (TLS)	5061	
SBC port range:		
- minimum RTP port	6000	
- maximum RTP port	38000	
Modification of RTP port on renegotiation	Unchecked	
Support of symetric RTP	NO	
Apply the network topology hiding	Checked	

Equipment	MiVoice 5000	
Configuration path	Telephony service>System>Configuration>Services (2.3.1)	
Parameter	*Value*	Comments
Service INTERNET GATEWAY	START	

6.5 SRTP support

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Quality of service>Ciphering and IP settings (4.4.5) Select « Ciphering » tab	
Parameter	*Value*	Comments

Signalling and voice ciphering	---	---
Voice ciphering	Checked	

6.6 SIP trunk creation

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Network>Trunk group >Names (4.2.1.1) Create un trunk group for the SIP trunk.	
Parameter	*Value*	Comments
Trunk group N°x	*Trunk group name*	Choose a trunk group number and a trunk group name (example : « SIP-BTol »).

6.7 SIP trunk configuration

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Network>Trunk group>Characteristics (4.2.1.2) Select the trunk group previously created.	
Parameter	*Value*	Comments
Signaling characteristics :	---	---
Physical type	VOICE IP	
Nature	BOTHWAY	
Signalling type	SIP	
Subtype	STANDARD	
Characteristics :	---	2 edition modes exist : - « basic » mode accessible via the button : - « advanced » mode accessible via the button : The parameters shown below in *italics* and highlighted in grey are only visible via the "advanced" mode.
Signalling type	SIP	
Subtype	STANDARD	
Link state	CONNECT.	
Company	STE0	Company name configured on the IPBX.
Department	SERV 0	Department name configured on the IPBX.
Protocol	TLS	
- with TLS profile		*Not used.*
- SIPS support	*Unchecked*	
Proxy N°1	FQDN of the nominal A-SBC	FQDN of the nominal A-SBC.
- port	5061	
Proxy N°2	FQDN of the backup A-SBC	FQDN of the backup A-SBC.
- port	5061	
Domaine / realm		Not used.
Local proxy	PROXY NAT SBC	

- adress	IP@ of the IPBX	IP3 address in the figure of the section 2.4.
- port	5064	
Proxy checking	IP ADDRESS	
identifier		Not used.
Registering		Not used.
Authentification		Not used. (Default value: SIP CLIENT).
Client account:	---	---
- login		Not used.
- password		Not used.
Public name of SIP access point		*Not used.*
Audit during speech	*Checked*	
- speech audit management	*MSG UPDATE*	
- audit frequency (sec)	*1200*	
Audit out of speech (OPTIONS)	Checked	
- audit frequency (sec)	300	
- status	ACCEPTED	Audit satus out of conversation.
- next audit at HH:mm:SS	---	---
Compelled release of trunks	*Unchecked*	
Redirected numbers emission	*DIVERSION*	
Identity sending management:	---	---
- call identifier (From)	*IID/AID*	
- number (From) in E.164 format	*Checked*	
- presentation/restriction	*P-Asserted-ID*	
- call identifier (PAI)	*IID/AID*	
- number (PAI) in E.164 format	*Checked or Unchecked*	
- sending anonymous into From	*Checked*	
- update of name/number (UPDATE)	*Unchecked*	
- number (To) in E.164 format	*Checked or Unchecked*	
Identity reception management:	---	---
- calling id. in	*PAI or PPI or RPID*	
N° without external prefix	*Unchecked*	
Name management	*Unchecked*	
Forwarding management:	---	
- on busy / immediate forward	*Unchecked*	---
- forward on no answer	*Unchecked*	
Call Sending type (internal/external)	*Unchecked*	
Voice mail	*Unchecked*	
Local generation of tones	*Checked*	
Support PRACK (100rel)	*Checked*	
Tones management before answer	*180+SDP+P-Early-Media*	
- support P-Early-Media	*Checked*	
Re-invite without SDP allowed	*Checked*	
Reject T.38	*415 Unsupported Media Type*	Default value. Regardless of T.38 and G.711 Fax support.
REFER sending	*Unchecked*	
Support of video	*Unchecked*	

Support of T.38	*Unchecked*	Default value. Regardless of T.38 and G.711 Fax support.
Support of other medias (IM, etc..)	*Unchecked*	
SRTP support	*SRTP preferred*	
Bearer type incoming	*CCBT+CCBNT*	
Calls from	RESEAU	
Priority calls if transit	*Unchecked*	
Search DID numbers	---	---
- incoming digit translator number		Enter in this field the incoming digit translator number. To be filled in only if configured and if it is necessary to translate the number received from the network into an internal number.
- reject of numbers not assigned	*Unchecked*	
Pre-answering message, caller charged	---	---
- if called party free or busy 1	Unchecked	
- if called party busy 2	*Unchecked*	
- if number not assigned	*Unchecked*	
Transf .acc. to called pty compt-dept	*Unchecked*	
Transfer to	OP GP1	Name of the operator service configured on the IPBX.
Trunk group id (tel. record)	*0*	
Trunk group monitoring	*Checked*	
Max. nb of simultan. Calls allowed		Not used.
CAC IP address	Public IP@ of the integrated SBC	Field configured automatically filled according to the IP address of A-SBC.
Centre – CAC class		Field configured automatically filled according to the CAC configuration.
G711 forced in mode FAX/Modem	*Unchecked*	Default value. Regardless of T.38 and G.711 Fax support.

6.8 Additional configuration: DCF parameters

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>System>Expert>DCF settings (2.7.3) Enter a DCF number to configure « Number (in decimal) of the DCF » then click on the button « Select the item ».	
Parameter	*Value*	Comments
Number (in decimal) of the DCF	282	
Value in decimal	2	
Value in hexadecimal	0002	
Number (in decimal) of the DCF	460	
Value in decimal		
Value in hexadecimal	FFFF	

6.9 Coding laws configuration: network calls

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Quality of service>Voice over IP coding law (4.4.2) Select the « Call type » then the « Set type » and click on « Select the item ».	
Parameter	*Value*	Comments
Priority 1, law:	G711	Coding law set in priority 1.
at type 1:	A LAW	
duration of packets (ms):	20	

This configuration has to be applied to the whole call types below :

- **Call type:** NETWORK
- **Direction:** …… (not mandatory)

- **Call type:** TONES
- **Messages type:** NETWORK

7 Parameters to be configured common to sections 5 and 6

7.1 Routes configuration

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>network and links> Network > Routes (4.2.2) Then click on « Advanced characteristics … » and keep the default values.	
Parameter	*Value*	Comments
For routing code	Ex : CODE0_HQ	Select the route code configured on the site (depends directly on the client IPBX configuration).
To direction	NATIONAL	Select the appropriate direction.
Via route type	DIRECTE 0	Select the appropriate route (route = routing priority)
On trunk group	« trunk group name »	Select the SIP trunk group created previously. Example : « SIP-BT».
Tone type	DTMF	Default value.
Transmit type	MF DTMF	Default value.
Dial tone	NO	Default value.
1st serie of digits to insert		Default value.
Second tone	NO	Default value.
2nd serie of digits to insert		Default value.
Third tone	NO	Default value.
Outgoing digit translator number		Enter in this field the outgoing digit translator number. To be filled in only if configured and if it is necessary to translate the number to send to the network into another number.
Charge indication	NO	Default value.
Limiter nb. Of C code rerouting	NO	Default value.
OFF NET carrier	……	Default value.

NOTE: The configuration of the routes may be specific to the customer's IPBX configuration, and has no direct link to the BT or BTalk over Internet SIP trunk configuration. This part is therefore mentioned only as a reminder: a route must be created in order to use the SIP trunk created for BT or BTalk over Internet.

7.2 Outgoing calls handling: IID configuration

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Network>AID handling>IID (4.2.6.5) Configure a IID number.	
Parameter	*Value*	Comments
IID 0 : internal plan	PLAN 1	Select the plan.
or direction	……	Or select a direction.
number		Enter the required IID number
restricted presentation	NO	

NOTE : The IID/AID configuration is specific to the customer's IPBX configuration and has no direct link to the BTalk SIP trunk configuration.

7.3 Outgoing calls handling: Outgoing handling configuration

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony Service> Network and links> Network>AID handling>Outgoing handling (4.2.6.7)	
Parameter	*Value*	Comments
By plan	……	Do not select a plan
And by direction	LOCAL	Select LOCAL direction
And the requested plan	PLAN 1	
On trunk group	« SIP trunk group name »	Select the trunk group.
Fallback present	YES	
- inhibit sending of IID and AID	NO	
- send IID	NON DID EXT	
- AID completed with IID	YES	
- AID set using DID number	YES	
- digit translator number		Enter in this field the outgoing digit translator number for calling party number. To be filled in only if configured and if it is necessary to translate the calling party number send to the network.
- IID number		Enter the IID number created previously.
- inter-plan forwarding	NO	

NOTE: The configuration of outbound handling is specific to the customer's IPBX configuration and has no direct link to the BTalk or BTalk over Internet SIP trunk configuration.

7.4 General settings configuration

Equipment	MiVoice 5000 IPBX	
Configuration path	Telphony service>Subscribers>Rights>General settings (1.4.1)	
Parameter	*Value*	Comments
« Subscriber » tab	---	---
Functions available to extensions	---	---
- external name display	Checked	
« System » tab	---	---
Subscriber forwarded to exterior	---	---
- Charging	CALLING	
- send ident.	CALLING NUMBER	
« Rights » tab	---	---
Transfer authorization	---	---
- TK TK	Checked	
- TK TL	Checked	
« Network » tab	---	---
IP settings :		
- Handling of FAX T.38 communications	Unchecked	Default value. For fax configuration, please refer to § 7.9 Fax configuration with Mitel MiVoice 5000.
- DTMF handled into:	RTP PACKET	

header value (RFC 2833)	101	

7.5 Subscribers characteristics configuration

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Subscribers>Rights>Feature class (1.4.3) Select the feature class to configure by its name.	
Parameter	*Value*	Comments
External forwarding allowed	Checked	
Network rerouting allowed	Checked	
Id sent to public network	A.I.D	The value « ..... » is used to activate the identity restriction.
Id sent to private network	A.I.D	The value « ..... » is used to activate the identity restriction.

7.6 Coding laws configuration: local calls

The coding laws/codecs configuration for local calls may differ depending on the client IPBX configuration. It does not concern network calls using SIP trunk.

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Quality of service>Voice over IP coding law (4.4.2) Select the « Call type » then the « Set type » and click on « Select the item ».	
Paramètre	*Value*	Comments
Priority 1, law:	G722	Coding law set in prority 1.
Duration of packets (ms):	20	
Priority 2, law:	G711	Coding law set in prority 2.
at type 1:	A LAW	
at type 2:	.....	
Duration of packets (ms):	20	
Priority 3, law:	G729	Coding law set in prority 3.
at type 1:	G729A	
at type 2:	G729	
Duration of packets (ms):	20	

This configuration has to be applied to the whole call types below :

- **Call type:** INTERNAL
- **Set type:** IP PROPRIETARY, SIP-DECT IP
- **Call type:** TONES
- **Messages type:** EXTENSION
- **Call type:** CONFERENCE CIRCUITS, VOICE MAIL

7.7 Configuration marquage DSCP

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Quality of service>Ciphering and IP settings (4.4.5) Select « QoS »	
Parameter	*Value*	Comments
DSCP telephony signalling (decimal)	40	
DSCP voice (décimal)	46	

NOTE: MiVoice 5300 IP Phones, Mitel 6800 SIP Phones, Mitel 6900 SIP Phones mark all voice frames at level 3. The DSCP marking setting is broadcast by the MiVoice 5000 Call Server or Mitel 5000 Gateways IPBXs when the terminal is connected.

7.8 CAC configuration

Equipment	MiVoice 5000 IPBX	
Configuration path	Telephony service>Network and links>Quality of service>CAC and localisation>CAC server settings (4.4.4.1)	
Parameter	*Value*	Comments
Server configuration	MAIN	
Available services	---	---
- geographic location	Checked	
- calls controls	Checked	
Control based on class	Checked	
Audio/Video separation	Unchecked	
Saturation before alarm (en %)	80	Configure the required value between 0 and 100.

NOTE: The CAC (Call Admission Control) setup is specific to each customer site and must be customized for their IPBX, independent of BTalk or SIP trunk configurations.

7.9 Fax configuration with Mitel MiVoice 5000

7.9.1 T.38 Fax

Equipment	MiVoice 5000	
Configuration path	Telephony service >Subscribers> Rights> General settings>Network (1.4.1)	
Parameter	*Value*	Comments
Handling of FAX T.38 communications	Checked	

Equipment	MiVoice 5000	
Configuration path	Telephony service>Subscribers>Subscriptions>Create (1.2.1)	
Parameter	*Value*	Comments
Type	INTERNAL	
First directory number	XXXX	Declare the number of the subscriber
Requested number	2	
User password	0000	Default password

Equipment	MiVoice 5000	
Configuration path	Telephony service>Subscribers>Subscriptions>Characteristics Select the new fax entry (identified by its directory number [here "XXXX"]).	
Parameter	*Value*	Comments
DID DN PLAN 1	XXXX	Select the last 4 digits of the SDA to assign
Feature class	FAX	Set the feature class to which the fax belongs.

Equipment	MiVoice 5000	
Configuration path	Telephony service>Subscribers>Subscriptions>Characteristics>Directory	
Parameter	*Value*	Comments
Name	XXXX	Attribute a name to fax
Firstname	XXXX	Attribute a firstname to fax

Equipment	MiVoice 5000

Configuration path	Telephony service>Subscribers>Subscriptions>Characteristics>Terminals	
Parameter	*Value*	Comments
Phys. terminal type 1	SIP	

7.9.2 G.711 Inband Fax

For G.711 inband fax transmission, customers may implement any inband fax configuration, including, but not limited to, autonomous mode, passthrough mode, and voice mode. V.152 is explicitly excluded and is not supported.

Customers are solely responsible for configuring their own fax equipment. Orange does not recommend any specific G.711 inband fax configuration, as fax transmission performance may depend on the behaviour of fax gateways and on any transcoding operations performed within the core network.

Consequently, Orange does not provide technical support for issues related to G.711 inband fax transmission.