Business Talk & BTIP for Alcatel-Lucent Enterprise OmniPCX Enterprise (OXE)

versions addressed in this guide : R101.x

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

Latest edition: 19/10/2026

Table of contents

1. Goal of this document 3
2. Certified architectures 4
2.1. Introduction to architecture components and features 4
2.2. SIP trunk on OXE over BVPN 5
2.3. SIP trunk on OTSBC over BVPN 7
2.4. SIP trunk on OTSBC over Internet 9
2.5. Architecture with Rainbow WebRTC gateway 10
3. Parameters to be provided by customers to access to the service 11
4. BTalk & BTIP certified versions 13
4.1. Global Release Policy 13
4.2. Alcatel-Lucent Entreprise IPBX and SBC 13
4.3. Alcatel-Lucent Entreprise endpoints and applications 13
5. OXE SIP trunking configuration checklist 15
5.1. Common parameters 15
5.2. Fax configuration with OXE 25
5.2.1. G.711 Fax Passthrough 25
5.2.1. T.38 Fax 25
5.3. BTalk French customers and BTIP DROM architectures 26
6. OXE + OTSBC SIP trunking configuration checklist 27
6.1 SBC - IP Network configuration 27
6.1.1 Core Entities 27
6.2 SBC - OXE LAN side configuration 28
6.2.1 Coders & Profiles 28
6.2.2 Core entities 29
6.2.3 Message Manipulation 30
6.3 SBC - BTIP/BTalk side configuration over BVPN (unencrypted flows) 33
6.3.1 Coders & Profiles 33
6.3.2 Core Entities 34
6.3.3 Message Manipulation 35
6.3.4 SBC - IP-to-IP Routing 36
6.4 SBC - BTIP/BTalk side configuration over Internet (encrypted flows) 37
6.4.1 TLS context 37
6.4.2 Certificate 38
6.4.3 TLS Mutual Authentication regarding public certificate Extended Key Usage (EKU) 38
6.4.4 Media Security 42
6.4.5 Coders & Profiles 42
6.4.6 Core Entities 43
6.4.7 Message Manipulation 45
6.4.8 SBC - IP-to-IP Routing 46
Glossary 48

1. Goal of this document

This document defines the technical requirements for ensuring interoperability between the Alcatel-Lucent Enterprise IPBX and Orange Business's Business Talk (BTalk) International and Business Talk IP (BTIP) France services, collectively referred to hereafter as the "Service."

2. Certified architectures

2.1. Introduction to architecture components and features

This document describes “only” the main supported architectures either strictly used by our customers or that are used as reference to add specific usages often required in enterprise context (specific ecosystems, redundancy, multi-codec and/or transcoding, recording…).

Fax flows are supported by both BTIP and BTalk:

- With BTIP (France only), G.711 inband fax passthrough is available by default. T.38 is available upon request.
- With BTalk, both G.711 inband fax passthrough and T.38 are available by default.

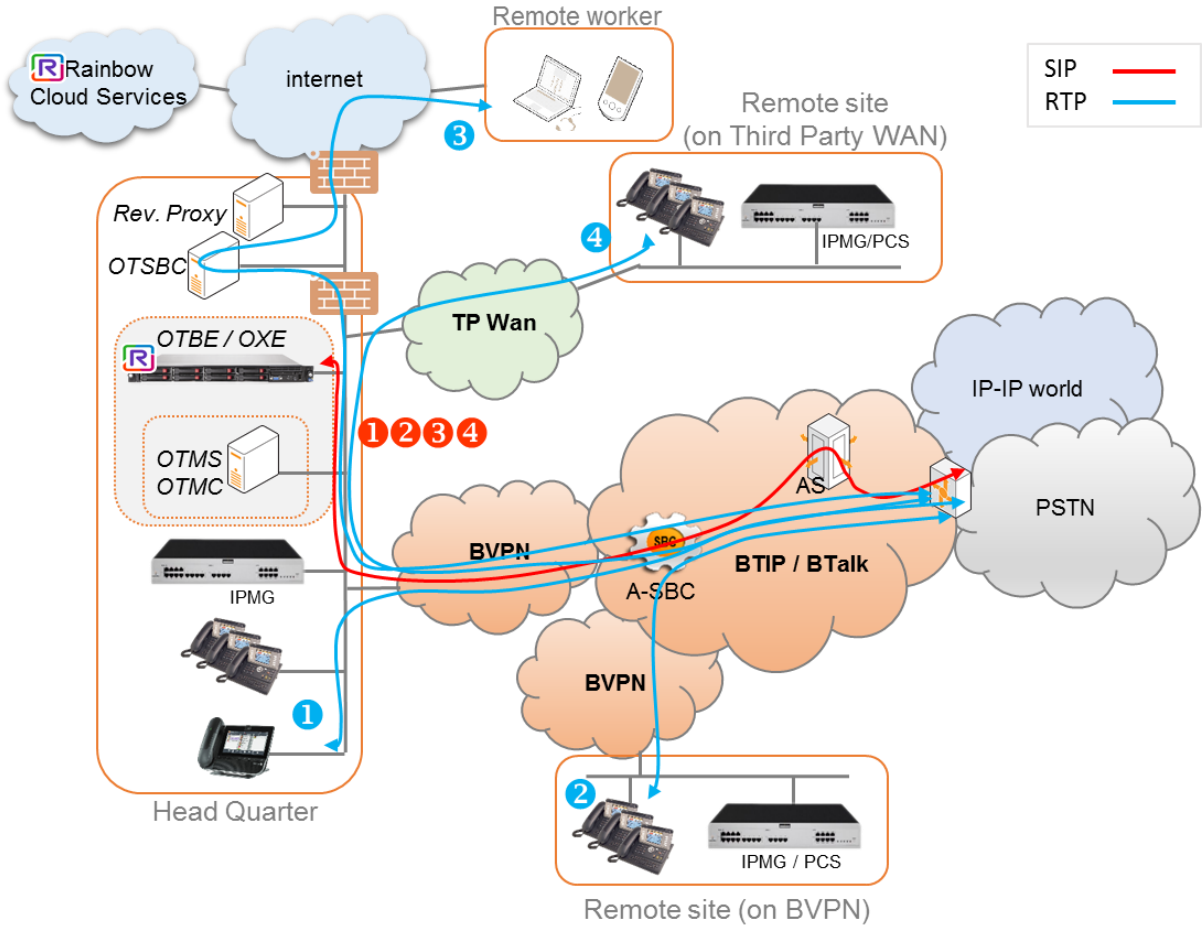
T.38 and G.711 inband fax are enabled on BTIP and BTalk networks without an end-to-end guarantee. Orange cannot certify the reliability of fax interoperability that may occur at interconnection points with terminating carriers.

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

BTIP in French overseas departments are also supported. Dedicated aSBC pairs in Caribbean and Indian Ocean zones are deployed for local calls. For a trunking point of view, the mechanism is similar to “BTalk French customers”, the IPBX must support international dial plans and route local calls to the dedicated local aSBC pair.

*cf QoS parameters in the “Configuration Checklist → IP / IP Quality of Service Category”. This value applies to IP phones, IP boards, IP domains and SIP messages from the OXE Communication Server.

2.2. SIP trunk on OXE over BVPN



Notes :

- in the diagram above, the SIP, proprietary and Rainbow internal flows are hidden.
  - ❶ call from/to head quarter
  - ❷ call from/to remote site (on Business VPN)
  - ❸ call from/to remote worker (on Internet)
  - ❹ call from/to remote site (on Third Party WAN)
- call flows will be the similar with or without OXE Call Server redundancy (duplicated or spatial)

In this architecture :

- all 'SIP trunking' signaling flows are carried by the OXE server and routed on the main BVPN connection.
- Media flows are direct between endpoints and the BTalk/BTIP but IP routing differs from one site to another :
  - For the Head Quarter site, media flows are just routed on the main BVPN connection
  - For Remote sites on BVPN, media flows are just routed on the local BVPN connection (= distributed architecture),

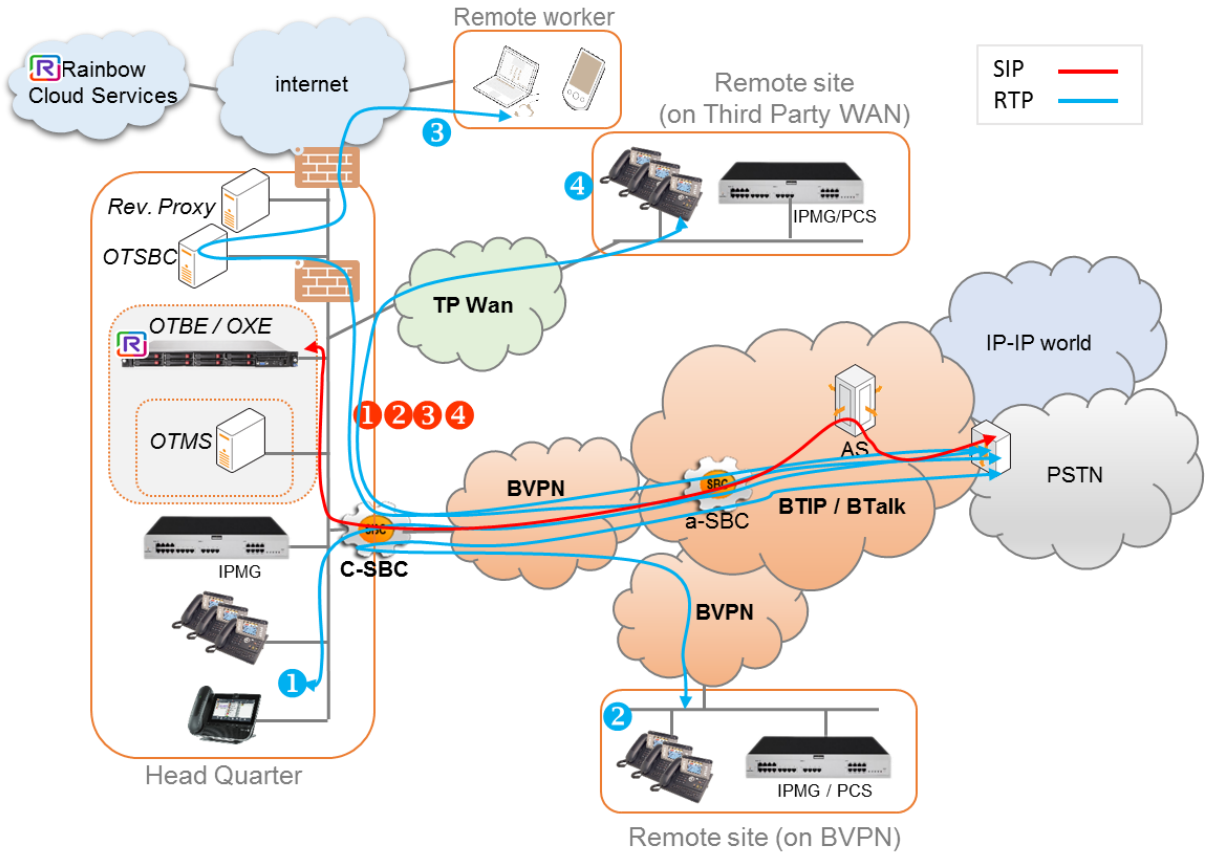
- For Remote sites on Third Party WAN, media flows are routed through the Head Quarter (but not through the IPBX) and use the main BVPN connection (= centralized architecture, cf sizing below).

Here below a table with a few sizing elements :

Call scenario	nb of voice channels/media resources used		
	IPBX	WAN router*	BTIP
1 offnet call from/to the head quarter (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 TPWan **1** in RS TPWan	0 in HQ **1** in RS
1 offnet call from/to a remote site **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 **after transfer/forward to BTIP**	0 in HQ **0** in RS	0 in HQ **0** in RS	0 in HQ **2** in RS
1 **forced onnet** call **from head quarter to a remote site** (= through BTalk 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 on OTSBC over BVPN



Notes :

- in the diagram above, the SIP, proprietary and Rainbow internal flows are hidden :
  - ❶ call from/to head quarter
  - ❷ call from/to remote site (over Business VPN)
  - ❸ call from/to remote worker (over Internet)
  - ❹ call from/to remote site (over Third Party WAN)

In this architecture, both 'SIP trunking' and RTP media flows between endpoints and the BTalk/BTIP are anchored by the enterprise SBC* :

- for the Head Quarter site, media flows are routed through the SBC and the BVPN access
- for Remote Sites either on BVPN or Third Party WAN, media flows transit **through the Head Quarter SBC** and use the central BVPN connection (= **centralized architecture**, cf sizing below).

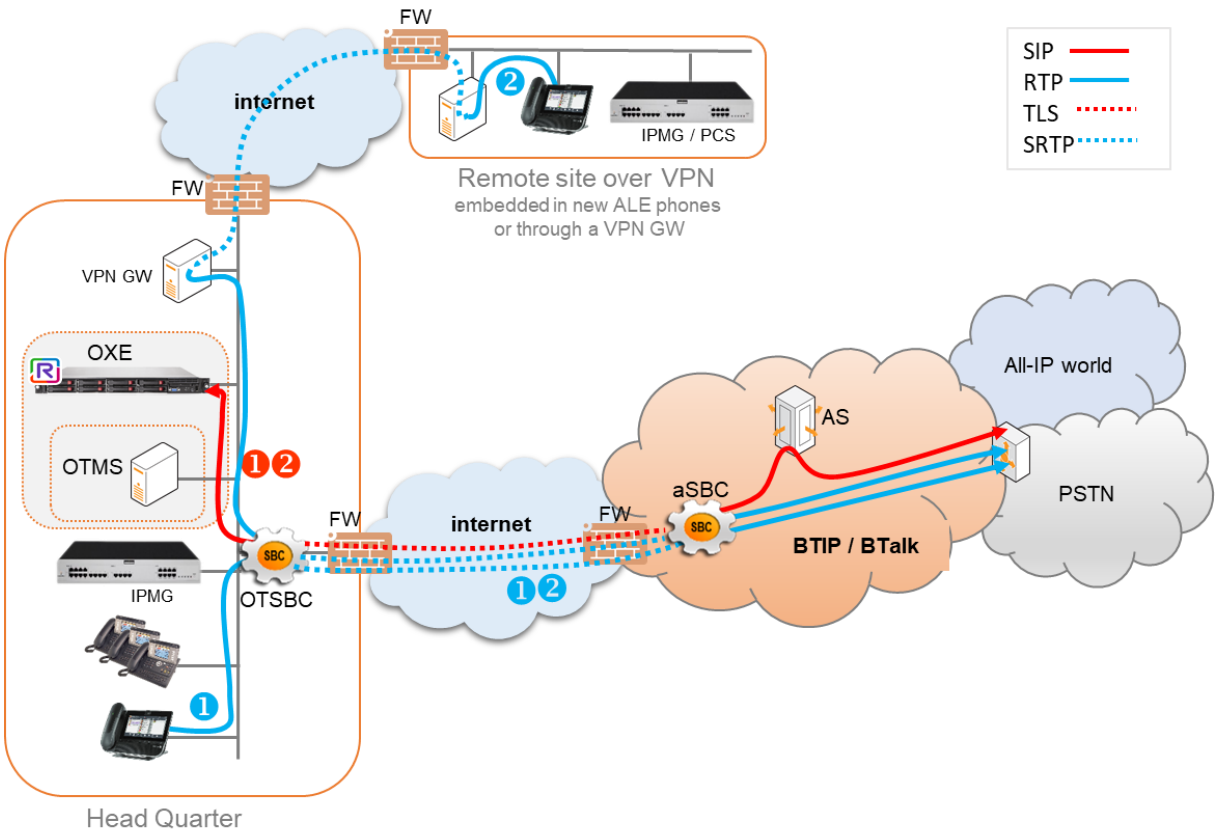
*AudioCodes Mediant (VE or appliance versions) and Alcatel OTSBC are standard, so don't need any other specific implementation request.

Warning : with an enterprise SBC architecture, site access capacity has to be sized adequately on the Head Quarter. Here below a table with a few sizing elements :

Call scenario	nb of voice channels/media resources used		
	IPBX	WAN router*	BTIP
1 offnet call from/to the head quarter (HQ)	**1** for HQ	**1** in HQ	**1** in HQ
1 offnet call from/to a remote site (RS) on BVPN	0 for HQ **1** for 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 TPWan **1** in RS TPWan	0 in HQ **1** in RS
1 offnet call from/to a remote site **with put on hold**	**1** for HQ **1** for RS	**3** in HQ **1** in RS	0 in HQ **1** in RS
1 offnet call from/to a remote site **after transfer/forward to BTIP**	0 for HQ **0** for RS	0 in HQ*/3 in HQ** **0** in RS	0 in HQ **2** in RS
1 **forced onnet** call **from head quarter to a remote site** (= through BTalk infrastructure)	**2** for HQ **2** for 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 cSBC ***if media release is not activated on the cSBC

2.4. SIP trunk on OTSBC over Internet



Notes : in the diagram above, the SIP, proprietary and Rainbow internal flows are hidden

❶ call from/to head quarter

❷ call from/to remote site over Internet (with the VPN client embedded in the ALE phones or with a VPN gateway)

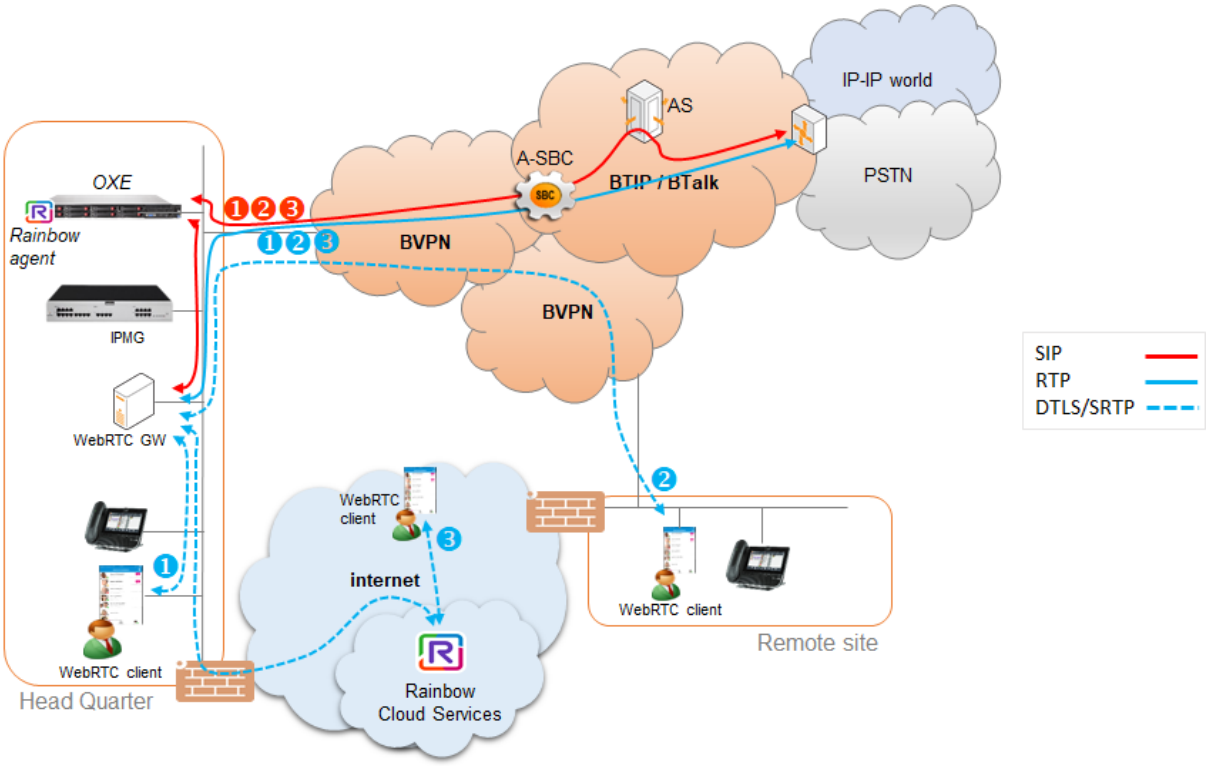
SIP TLS + Secured RTP: all SIP messages and media packets are encrypted on the public internet between Orange and the customer endpoints. This is the level of encryption recommended by default by Orange to ensure security & privacy. Refer to the dedicated configuration section chapter 6.4 for more details.

In this architecture, both 'SIP trunking' and RTP media flows between endpoints and the BTalk/BTIP are anchored by the enterprise SBC* :

- for the Head Quarter site, media flows are routed through the SBC and the Internet access
- for Remote Sites either on Internet, media flows transit **through the Head Quarter SBC** and use the BTIP/BTalk connection (= **centralized architecture**).

* Alcatel OTSBC and AudioCodes Mediant (VE or appliance versions) are standard, so don't need any other specific implementation request.

2.5. Architecture with Rainbow WebRTC gateway



Notes :

- in the diagram above, data flows (HTTPS/XMPP/Jingle/REST) between the clients/OXE/WebRTC GW and Rainbow services on the internet are hidden :
  - ❶ call from/to head quarter
  - ❷ call from/to remote site (over Business VPN)
  - ❸ call from/to remote worker (over Internet)

Since OXE R12.4 MD4, architectures with WebRTC media gateway support the direct RTP feature (with codec G711 only).

Prior to that version media flows to/from BTalk/BTIP are anchored on an IPMG. In that case, IPMG resources have to be sized adequately on the Head Quarter. There isn't any impact on BTalk/BTIP.

3. Parameters to be provided by customers to access to the service

IP addresses marked in red have to be indicated by the Customer, depending on Customer architecture scenario

Head Quarter (HQ) **– architecture without OTSBC**	**Level of Service**	**@IP used by service**	
Single Call Server	No call server redundancy	call server @IP	
Duplicated Call Server	Local call server redundancy	call server @IP (virtual)	
Spatial Redundancy **warning:** - Site access capacity to be sized adequately on the site carrying the 2nd call server - DNS server feature must be activated on both CS (OXE)	Site redundancy: 2 call servers (active/standby) hosted by 2 different physical sites	nominal call server @IP	backup call server @IP
Remote Site (RS) – architecture without OTSBC	**Level of Service**	**@IP used by service**	
Remote site without survivability	No survivability, no trunk redundancy	N/A	
PCS for one remote site	Local user survivability and SIP trunk redundancy for the remote site hosting the PCS in case of non-access to HQ	PCS @IP	
PCS for several remote sites **warning:** Site access capacity to be sized adequately on the site carrying the PCS	Local user survivability and SIP trunk redundancy for the remote site hosting the PCS in case of non-access to HQ	PCS @IP	

Head Quarter (HQ) **– architecture with OTSBC over BVPN**	**Level of Service**	**@IP used by service**	
1 Customer SBC	No redundancy	OTSBC @IP	
2 Customer SBC Nominal / Backup mode	- **Local redundancy**: both SBC are hosted on the same site OR - **Geographical redundancy** both SBC are hosted on 2 different sites	OTSBC1 @IP	OTSBC2 @IP
2 Customer SBC HA mode	- **Local redundancy:** both SBC are hosted on the same site OR **- Geographical redundancy** both SBC are hosted on 2 different sites **warning:** Link level 2 between SBC with max delay 50ms required for geo-redundancy	OTSBC VIP @IP	
Remote Site (RS) **– architecture with OTSBC over BVPN**	**Level of Service**	**@IP used by service**	
SBC on Head Quarter – all modes (see above)	No redundancy	N/A	

Head Quarter (HQ) **– architecture with OTSBC over Internet**	**Level of Service**	**@IP used by service**	
1 customer SBC	No redundancy	OTSBC public FQDN(1) DNS type A	
2 customer SBC Nominal / Backup mode (DNS resiliency model)	- **Local redundancy**: both SBC are hosted on the same site OR - **Geographical redundancy** both SBC are hosted on 2 different sites	OTSBC public FQDN(1) DNS type SRV	
2 customer SBC Nominal / Backup mode (SIP resiliency model)	- **Local redundancy**: both SBC are hosted on the same site OR - **Geographical redundancy** both SBC are hosted on 2 different sites	OTSBC1 public FQDN(1) DNS type A	OTSBC2 public FQDN(1) DNS type A
2 customer SBC HA mode (IP resiliency model)	- **Local redundancy:** both SBC are hosted on the same site OR **- Geographical redundancy** both SBC are hosted on 2 different sites **warning:** Link level 2 between SBC with max delay 50ms required for geo-redundancy	OTSBC public FQDN(1) DNS type A	
Remote Site (RS) **– architecture with OTSBC over Internet**	**Level of Service**	**@IP used by service**	
SBC on Head Quarter – all modes (see above)	No redundancy	N/A	

(1) FQDN is mandatory for BTIP over Internet (France), while public IP or FQDN is supported for Busines Talk over Internet (International)

Refer to the 'BTalk IP over Internet pre-requesites' document provided by your sales team for more details about the encrypted architecture, the certificate management, the firewall rules, etc…

In the TLS context, the full chain Root and Intermediate Certificate (PEM format) must be transmitted to Orange

4. BTalk & BTIP certified versions

4.1. Global Release Policy

Orange supports the last 2 major IPBX versions and will ensure BTalk and BTIP infrastructure evolutions will rightly interwork with the related architectures. Orange will assist customers running supported IPBX versions and facing issues.

Please refer to the latest Alcatel-Lucent MLV Release Policy Information and MLE Cross Compatibility documents for more details about the supported versions:

- 'MLV_ReleasePolicy_PhaseOutProduct_April_2026_Ed57a' or more recent
- 'MLE_CrossCompatibility_April_2026_Ed49b' or more recent

4.2. Alcatel-Lucent Entreprise IPBX and SBC

ALE IPBX & SBC – software versions

Reference product	Software version	Certification	Certified "Loads"
OmniPCX Enterprise OpenTouch Business Edition	**OXE R101**	✓	n3.320.9b (TR), n3.321.2a (MD1), n3.321.4 (MD2), n3.510.7a (MD3), n3.521.8a (MD4), n3.521.10a (MD5), n3.521.11a (MD6), n3.521.12 (MD7), n3.521.13 (MD8), n3.521.14a (MD9), n3.521.15 (MD10), n3.521.16 (MD11), n3.521.17.a (MD12), n3.521.18 (MD13), **N3.521.19.a (MD14)**
	OXE R101.1	✓	n4.205.19 (TR), n4.205.36a (MD1), n4.205.38 (MD2), n4.524.2 (MD4), n4.524.5 (MD5), n4.524.6 (MD6), N4.524.7.a (MD7), **N4.524.8 (MD8)**
	OXE R101.2	✓	n5.212.13.b (TR), n5.212.15 (MD1), **n5.212.16.a (MD2)**
OpenTouch SBC or AudioCodes Mediant VE generic version	**OTSBC 7.4**	✓	7.40A.500.017, 7.40A.500.781, **F7.40A.600.203**
	OTSBC 7.6	✓	**F7.60A.200.158**

4.3. Alcatel-Lucent Entreprise endpoints and applications

ALE IPBX - endpoints and applications

Reference product		Software version	Certification	OXE version	Comments
Attendant	Visual Automated Attendant	-	Not tested		
	4059 EE	2.4.6 min	✓	R101/R101.1	
Voice Mail	4645	-	✓	R101/R101.1	
	OTMC	2.6 min	Not tested		End of Life
Mobility	Desk Sharing	-	Not tested		
	OTSBC	7.4	✓	R101/R101.1	Remote workers with NGInx reverse proxy
UC	Open Touch MS	2.6.1	Not tested		End of Life
	Open Touch Fax Center	9.0	✓	R101/R101.1	
	Rainbow / Cloud Connnect	-	✓	R101/R101.1	call control only. No voice impact
	Rainbow WebRTC GW	3.0 min	✓	R101/R101.1	
Recording	OmniPCX Record	2.5 min	NA	R101/R101.1	No impact
Call Center	OTCC Standard	10.15 min	✓	R101/R101.1	CCAgent
	Business Contact	-	Not tested	R101/R101.1	Customer specific (ALE Professional Services)

ALE IPBX - endpoints and applications

Reference product		Software version	Certification	OXE version	Comments
Alcatel-Lucent endpoints	Pleiades Enterprise series Pleiades Essential series 80x8s/80x8/80x9 series	-	✓	R101/R101.1/R101.2	Refer to ALE release policy
	IP-DECT xBS AP + handsets	-	Not tested		
	IP Desktop Softphone	13 min	✓	R101/R101.1/R101.2	
	ALE softphone (ALES) for PC	2.5 min	✓	R101/R101.1/R101.2	
	8135S Conference phone	2.0.10 min	Not tested		'SIP device' mode
Third-party endpoints & applications	AudioCodes GW MP11x	MP11x v07 ≧ 6.60.x	✓	R100.x	Voice gateway to be declared as 'SIP device'
	ISI-COM Interact	8.x	Not tested		Contact Center
	Conecteo Kiamo	8.x	Not tested		Contact Center
	Fortigate 30E/60F VPN Gateways	-	Not tested		For remote users over internet
	Others		On demand		
Fax	Open Touch Fax Center	-	Not certified		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 ALE IPMG (SLI-x, MIX-x, Z-x)	-	Not certified		

5. OXE SIP trunking configuration checklist

The checklist below presents all the **required** configuration parameters for interoperability between BTalk/BTIP and IPBX OXE. New parameters since the previous edition are highlighted.

5.1. Common parameters

Menu	Value
MEDIA PARAMETERS	
Media Gateway > "select an instance MGw" Média Gateway > "sélectionner une instance MGW"	Law has to be set to Default Loi de quantification doit être configurée à Défaut
System > Timers Installation > Temporisations	Timer 42 should be set to 5 Timer 299 can be set up to 150 in case of DTMF detection issue only Temporisation 42 devrait être configurée à 5 Temporisation 299 peut être augmentée jusqu'à 150 en cas de problème de détection des DTMF uniquement
System > Other System Param. Installation > Autres param. Install.	DTMF on Alert has to be False No End of Dialing has to be set to True DTMF on Alert doit être configuré à Non Pas de fin de numérotation doit être configuré à Oui
System > Other System Param. > System Parameters > Law Installation > Autres param. Install. > Paramètres Système > Loi de quantification	Law has to be set to A Law Loi de quantification doit être configurée à Loi A
System > Other System Param. > Compression Parameters Installation > Autres param. Install. > Paramètres Compression	Voice Activity Detect (Comp Bds) has to be False Voice Activity Detection on G711 has to be set to False Compression Type has to be set to G729 Suppression Silence (Cartes Comp.) doit être configuré à Non Suppression Silence sur G711 doit être configuré à Non Type de compression doit être configuré à G729
System > Other System Param. > SIP Parameters Installation > Autres param. Install. > Paramètres SIP	Packetization times per codec has to be set to False Via Header Inbound Calls Routing has to be set to True Enhanced codec renegotiation has to be set to Network type SIP diversion info for incoming has to be set to True Packetization time par codec doit être configure à Non Entête Via pour appels entrants doit être configure à Oui Négociation optimisée des codecs doit être configuré à Type réseau Sip diversion pour appels entrants doit être configuré à Oui
System > Other System Param. > Signaling String Installation > Autres param. Install. > Signalisation, para. non num	Country Code has to be configured with the Country Code of site Préfixe international doit être configuré avec le code pays du site

Menu	Value
System > Other System Param. > External Signaling Parameters Installation > Autres param. Install. > Paramètres Signalisation Externe	NPD for external forward has to be set to a value different from -1 except in Multivendor / Hybrid or non-ABC architectures NPD pour renvoi extérieur doit être configuré à une valeur différente de -1 sauf dans une architecture Multivendeur / Hybrid ou non-ABC
Users > TSC IP Users > "select a user" Usagers > Usagers TSC IP > "sélectionner un usager"	Voice Coding Algorithm has to be set to Default Algorithme de codage doit être configuré à Défaut
IP > IP Parameters IP > Paramètres IP	Fast Start has to be set to True G711 VOIP Framing has to be set to 20 ms G729 VOIP Framing has to be set to 20 ms Round trip delay request has to be set to False Fast Start doit être configuré à Oui Framing VOIP pour G711 doit être configuré à 20 ms Framing VOIP pour G729 doit être configuré à 20 ms Délais round trip requis doit être configuré à Non
IP > IP Quality Of Service COS IP > Catégorie Qualité Service IP	TOS/Diffserv has to be set to 46 *(default value)* SIP Diff. Service can be set to 40 *(default value)* TOS/DiffServ doit être configuré à 46 *(valeur par défaut)* SIP Diff. Service peut être configuré à 40 *(valeur par défaut)*
IP > IP Domain IP > Domain IP	Intra domain bandwidth has to be set to High bandwidth Extra domain bandwidth has to be set to High bandwidth FAX/MODEM Intra domain call transp has to be set to Yes FAX/MODEM Extra domain call transp has to be set to Yes Bande-passante intra domaine doit être configuré à Large Bande Bande-passante extra domaine doit être configuré à Large Bande FAX/MODEM Appel Intra domain trans doit être configuré à Oui FAX/MODEM Appel Extra domain trans doit être configuré à Oui
IP > IP Domain > IP Domain Address IP > Domain IP > Zone de domaine IP	IP addresses have to be set for: ▪ IP Address Low ▪ IP Address High ▪ IP NetMask Les adresses IP suivantes doivent être configurées : ▪ Adresse IP basse ▪ Adresse IP haute ▪ NetMask IP

If UDP lost is manage IP > IP Quality of Service COS > "select CoS QoS number 0" IP > IP Domain > "select an IP Domain" Shelf > Board > Ethernet Parameters > "select an INTIP or GD/GA board" Si UDP lost est géré IP > Catégorie de qualité de service IP > "sélectionner l'instance CoS QoS 0" IP > Domain IP > "sélectionner un Domaine IP" Alvéole > Carte-Interface > Paramètres Ethernet > "sélectionner une carte INTIP ou GD/GA"	 **UDP Lost** should be set to **45s** **IP Quality of Service** has to be set to **0** **IP Quality of Service** has to be set to **0** **UDP Lost** devrait être configuré à **45s** **Qualité de service IP** doit être configurée à **0** **Qualité de service IP** doit être configurée à **0**
Call Allowance Control (CAC)	
IP > IP Domain > "Select an IP Domain" IP > Domain IP > "sélectionner un Domaine IP"	**Domain Max Voice Connection** has to be set to a limitation call number (–1 is the default value = no limitation) **Nb Max de connexions / domaine** doit être configuré avec un nombre limite d'appel (–1 est la valeur par défaut = aucune limitation)
Diversion parameter for Remote Extension users	
Applications > Remote Extension Parameter > Redirecting IE number available Applications > Paramètres Remote Extension > No de réacheminement EI dispo.	Redirecting IE number available has to be set to YES **No de réacheminement EI dispo.** doit être à **OUI**

ROUTE MECANISM ON OXE Off-net calls	
SIP > SIP Gateway SIP > Passerelle SIP	Cac SIP-SIP has to be set to True Cac SIP-SIP doit être configuré à Oui *Note: for BTalk, the session timers, dynamic payload and SDP in 180 are now managed in the SIP External gateways* *Note : pour BTIP les timers de sessions, de payload dynamique et de SDP dans les 180 sont maintenant gérés dans passeerelles SIP externes*
SIP > SIP Proxy SIP > Proxy	SIP initial time-out has to be set to 500 Retransmission number for INVITE has to be set to 4 TCP when long messages has to be set to False Only authenticated incoming calls has to be set to True Tempo. initiale doit être configurée à 500 Retransmission number for INVITE doit être configurée à 4 TCP lors de longs messages doit être configurée à non Seulement appel arriv. Authentifié doit être configuré à oui
Private SIP Trunk Group (for internal SIP gateway): Trunk Groups Faisceau privé pour passerelle SIP interne: Faisceaux	Trunk Group Type has to be set to T2 T2 Specification has to be set to SIP Q931 Signal variant has to be set to ABC-F Type faisceau doit être configuré à T2 Spécificité T2 doit être configurée à SIP Variante signalisation Q931 doit être configurée à ABC-F
Public SIP Trunk Group (for external SIP gateways): Trunk Groups Faisceaux publiques pour passerelles SIP externes: Faisceaux	Trunk Group Type has to be set to T2 T2 Specification has to be set to SIP Q931 Signal variant has to be set to ISDN all countries Type faisceau doit être configuré à T2 Spécificité T2 doit être configurée à SIP Variante signalisation Q931 doit être configurée à RNIS tout pays
Trunk Groups > *"select a SIP Trunk Group ID"* > Trunk Group Faisceaux > "*sélectionner le faisceau SIP*" > Faisceau	Entity Number has to match to Entity of site Trunk COS has to be set to 31 IE External Forward has to be set to Diverting leg info No Entité doit correspondre à l'Entité du site Classe de service ARS doit être configuré à 31 Transfert Externe IE doit être configuré à Diverting leg info
Trunk Groups > Trunk Group > Virtual accesses for SIP > "select a Trunk Group ID" Faisceaux > Faisceau > Accès Virtuel pour SIP > "sélectionner le faisceau SIP"	Number of SIP Accesses has to be define between 2 (=60 simultaneous calls) and 32 (=960 simultaneous calls) Nombre d'accès SIP à définir entre 2 (=60 appels simultanés) et 32 (=960 appels simultanés

Public numbering plan *(by default/par défaut):* Translator > External Numbering Plan > Numbering Plan Description (NPD) > "select a NPD identifier" Traducteur > Plan de numérotation externe > Description de plan de num. > "sélectionne un identificateur de description"	**Calling Numbering Plan ident.** has to be set to **NPI/TON ISDN international** **Install. number source** has to be set to **None used** **Default number source** has to be set to **None used** **Called DID identifier** has to be set to **0** **Identifiant plan de num appellant** doit être configuré à **Plan/Type num RNIS international** **Origine num. installation** doit être configuré à **Aucun** **Numéro par défaut** doit être configuré à **Aucun** **Numéro de SDA pour appelé** doit être configuré à **0**
Private numbering plan *(optional/en option):* Translator > External Numbering Plan > Numbering Plan Description (NPD) > "select a NPD identifier" Traducteur > Plan de numérotation externe > Description de plan de num. > "sélectionner un identificateur de description"	**Install. number source** has to be set to **None used** **Default number source** has to be set to **None used** **Origine num. installation** doit être configuré à **Aucun** **Numéro par défaut** doit être configuré à **Aucun**
Translator > External Numbering Plan > DID Numbering Translator Traducteur > Plan de numérotation externe > Traducteur numéro SDA	**DID num. transl. Identifier** has to be set to **0** **Numéro de traducteur SDA** doit être configuré à **0**
Translator > External Numbering Plan > DID Numbering Translator > DID Number Translator rules Traducteur > Plan de numérotation externe > Traducteur numéro SDA > Traducteur SDA : règles	**First External Number** has to be set to **CCNSN** (international number), **First Internal Number** has to match the **private short number** (if private numbering used) **1er numéro extérieur** de la tranche doit avoir le format 33ZABPQMCDU **1er numéro intérieur** de la tranche doit avoir le **format de numéro privé** (si plan de num privé utilisé)
Trunk Groups > Trunk group NPD selector > "select a Trunk Group ID" Faisceaux > Sélecteur de Plan de Num Faisceau > "sélectionner le faisceau SIP"	**Public NPD ID** has to match the **NPD identifier** **Management Mode** has to be set to **Normal** **No Desc.Plan.Num public** doit correspondre à l'**identificateur de description** **Mode de gestion** doit être configuré à **Normal**
External Services > Trunk COS > "select a Trunk Group COS" Services extérieurs > Catégories de joncteurs > "sélectionner la classe de service ARS du faisceau"	**Overflow Timer on No Answer** should be set to **300** (default value). Could be reduced for remote sites without Media Gateway using the BTIP/BT DTO mechanism. **Timer T310** has to be set to a value **greater than 110 (>11s)** to wait for the Ring Back Tone. For example: **200 (=20s)** **Débordement sur non-réponse** devrait être configuré à **300** (valeur par défaut). Cette valeur pourrait être réduite pour des sites distants sans Media Gateway et utilisant le mécanisme de DTO BTIP. **Tempo. T310** doit être configuré avec une valeur **plus grande que 110 (>11s)** pour attendre le retour de sonnerie. Par exemple : **200 (=20s)**.

SIP > SIP Ext Gateway	Remote domain has to match IP address of the BTalk SBC (or OTSBC for BTalk over internet) PCS IP Address should to be set to 255.255.255.255 SIP Port Number has to be set to 5060 Transport Type has to be set to UDP […] Supervision timer has to be set to 380 Trunk group number has to match the public SIP trunk Gp […] RFC 3325 supported by the distant has to be set to True […] SDP in 18x has to be set to False Minimal authentication method has to be set to None […] Contact with IP address has to be set to True Dynamic Payload type for DTMF has to be set to 101 Outbound Calls 100 REL has to be set to Supported Incoming Calls 100 REL has to be set to Not Requested Gateway Type has to be set to Standard Type Re-Trans No. for REGISTER/OPTIONS has to be set to 4 P-Asserted-ID in Calling Number has to be set to False Trusted P-Asserted-ID header has to be set to True Trusted From header has to be set to False Diversion Info to provide via has to be set on Diversion Support Re-Invite without SDP has to be set to True Proxy identification on IP address has to be set to False Outbound calls only has to be set to False SDP relay on Ext. Call Fwd should be set to 180 only RFC 5009 supported/Outbound call has to be set to Mode1 Nonce Caching activation has to be set to False DNS SRV/Call retry on busy server has to be set to 0 Unattended Transfer for RSI has to be set to No Redirection functionality has to be set to No Attended Transfer has to be set to No Support Redirection Response has to be set to No OPTIONS required has to be set to YES Support UTF8 characters has to be set to YES Support CSTA User-to-User should be set to YES (!!! If license subscribed only !!!) DDI destination number has to be set to ReqURI UPDATE in Allow header/INIVTE has to be set to Mandatory RFC 4904 supported has to be set to No RFC3264 m-line has to be set to False *(for Fax T.38 support)* Sendonly for Hold has to be set to False In Band DTMF has to be set to No SIP Trunk Recording has to be set to No Send user name in SIP has to be set to User name else nuber

	Session Timer should be set to **21499** (but can be reduced to non-multiple of 1800) **Min Session Timer** has to be set to **900** **Session Timer Method** has to be set to **RE_INVITE** **Allow Direct RTP** has to be set to **YES** **IP Domain** must be configured according to the location of MGW resources (domain number to force, or **-1 by default)** **P-ANI header** has to be set to **None** ***(not used by BTalk)*** **Support G722** has to be set to **YES** **Support G711** has to be set to **YES** **Support G729** has to be set to **YES**

SIP > Passerelles Externes	**Domaine distant** doit correspondre à l'**adresse IP du SBC BTIP** ou de l'**OTSBC** dans le cas de BTIP sur Internet **Adresse IP PCS** devrait être configuré à **255.255.255.255** **Numéro de port** doit être configuré à **5060** **Type de transport** doit être configuré à **UDP** […] **Timer de supervision** doit être configuré à **380** **Numéro de faisceau** doit correspondre au **faisceau SIP public** [...] **RFC 3325 supporté par le distant** doit être configuré à **Oui** […] **SDP dans 18x** doit être configuré à **Non** **Authentification minimale** doit être configurée à **Aucun** […] **Contact avec adresse IP** doit être configuré à **Oui** **Type de payload dynamique (dtmf)** doit être configuré à **101** **Outbound Calls 100 REL** doit être configuré à **Supporté** **Incoming Calls 100 REL** doit être configuré à **Non demandé** **Type de Gateway** doit être configuré à **Type standard** **Re-Trans No. for REGISTER/OPTIONS** doit être configuré à **4** **P-Asserted-ID dans No Appelant** doit être configuré à **Non** **Entête P-Asserted-ID certifié** doit être configuré à **Oui** **Entête From certifié** doit être configuré à **Non** **Info. de renvoi ext. fourni par** doit être configuré à **Diversion** **Supporte le Re-invite sans SDP** doit être configuré à **Oui** **Identificat. Proxy sur Adresse IP** doit être configuré à **Non** **Spécialisé Départ** doit être configuré à **Non** **Relai SDP sur renvoi ext.** devrait être configuré à **180 seulement** **Transparence DSP en Transit** doit être configuré à **Non** **RFC5009 supporté/Appels sortants** doit être configuré à **Mode1** **Activation du Nonce Caching** doit être configuré à **Non** **DNS SRV/Réemission sur Serveur OCC** doit être configuré à **0** **Transfert non supervisé pour RSI** doit être configuré à **Non** **Fonctionnalité de Redirection** doit être configuré à **Non** **Transfert supervisé** doit être configuré à **Non** […] **Envoi OPTIONS** doit être configuré à **Oui** **Support des caractères UTF8** doit être configuré à **Oui** **Support User-to-User CSTA** devrait être configuré à **Oui (!!!** si licence souscrite uniquement !!!) **Numéro de destination** doit être configuré à **ReqURI** **UPDATE présent dans Allow/INIVTE** doit être configuré à **Obligatoire** **RFC 4904 supporté** doit être configuré à **Non** **RFC3264 m-Line** doit être configuré à **Non** (pour le Fax T.38 **Sendonly sur mise en garde** doit être configuré à **Non** **DTMF dans la Bande** doit être configuré à **Non** **Enregistrement Trunk SIP** doit être configuré à **Non**

	Envoi du Nom Utilisateur en SIP doit être configuré à **1 (Nom d'usager sinon numéro)** **Session Timer** devrait être configuré à **21499** (mais peut être réduit à une valeur non-multiple de 1800) **Min Session Timer** doit être configuré à **900** **Session Timer Méthode** doit être configuré à **RE_INVITE** **Autoriser RTP direct** doit être configuré à **Oui** **Domaine** doit être configuré **en fonction de la localisation des ressources MGW (n° de domaine** pour forcer**, ou -1** par défaut) **P-ANI header** doit être configuré à **Aucun** *(non utilisé par BTIP)* **Support G722** doit être configuré à **Oui** **Support G711** doit être configuré à **Oui** **Support G729** doit être configuré à **Oui**
Translator > External Numbering Plan > Numbering Discriminator > Discriminator Rule > "select a Discriminator No." Traducteur > Plan de numérotation externe > Discrimination numérotation > Règle de discrimination > "sélectionner un numéro de discrimination"	**ARS Route List Number** has to match the **ARS Route for SIP Trunking** **Number of Digits** has to be set to the **exact expected number** **No Table De Routage ARS** doit correspondre à la **Route ARS pour SIP Trunking** **Nombre de chiffres** doit être configuré avec **le nombre exact de chiffres attendus**
Translator > Automatic Route Selection > ARS Route list > ARS Route > "select an ARS Route list" Traducteur > Tables de routage ARS > Table de routage ARS > Routage ARS > "sélectionner une table de routage ARS"	**Trunk Group** has to match the **public SIP Trunk** **Numbering Command Table. ID** has to match a **SIP External Gateway** **Quality** has to be set to **Speech and Fax** **Faisceau** doit correspondre au **faisceau SIP public** **No table commande num.** doit correspondre à une **Passerelle Externe** **Qualité** doit être configurée à **Voix et Télécopie**
Translator > Automatic Route Selection > ARS Route list > Time-based Route List > "select an ARS Route list" Traducteur > Tables de routage ARS > Table de routage ARS > Liste des routes temporelles > "sélectionner une table de routage ARS"	**In ARS Route menu, 2 routes have to be created:** ▪ **1 (route SIP to nominal BTIP/BT aSBC)** ▪ **2 (route SIP to backup BTIP/BT aSBC)** **Dans le menu Routage ARS, 2 routes doivent être créées:** ▪ **1 (route SIP vers l'aSBC BTIP/BT nominal)** ▪ **2 (route SIP vers l'aSBC BTIP/BT secours)**
Translator > Automatic Route Selection > ARS Route list > Numbering Command Table > "select a Numbering Command Table" Traducteur > Tables de routage ARS > Table commande num. > "sélectionner une table de commande num."	**Carrier Reference** has to be set to **0** (=not used) **Associated Ext SIP gateway** has to match the **SIP Ext Gateway associated for SIP Trunking.** The parameter **Command** has to be configured to **"I" ([I]nsert).** **Réf.Opérateur réseau** doit être configurée à **0** (=non utilisé) **Gateway SIP associée** doit correspondre à la **Passerelle Externe associé pour SIP Trunking.** Le paramètre **Commande** doit être renseigné à **"I" ([I]nsert).**
Translator > Prefix Plan Traducteur > Plan des préfixes	**Prefix Meaning** has to be set to **Local Features** **Local Features** has to be set to **PCX address in DPNSS** **Signification préfixe** doit être configurée à **Exploitations en local** **Exploitations en local** doit être configuré à **Adresse PABX en DPNSS**

Overflow through PSTN (optional)	
Translator > Automatic Route Selection > ARS Route list > Time-based Route List > "select an ARS Route list" Traducteur > Tables de routage ARS > Table de routage ARS > Liste des routes temporelles > "sélectionner une table de routage ARS"	In ARS Route menu, a third route have to be created: ▪ 1 (route SIP to nominal BTIP/BT aSBC) ▪ 2 (route SIP to backup BTIP/BT aSBC) ▪ 3 (route to PSTN - only if T0/T2 on the site) Dans le menu Routage ARS, une 3eme route doit être créée: ▪ 1 (route SIP vers l'aSBC BTIP/BT nominal) ▪ 2 (route SIP vers l'aSBC BTIP/BT secours) ▪ 3 (route vers le PSTN – seulement si T0/T2 sur le site)
Passive Communication Server configuration (optional)	
Keep only one nominal SIP External Gateway and one backup SIP External Gateway for all sites, which will be used for all CS and PCS. The same ARS will be also used for all. Ne garder qu'une seule passerelle externe SIP nominale et une seule passerelle externe SIP de secours pour l'ensemble des sites, elles seront utilisées pour l'ensemble des CS et PCS. De même, une seule ARS sera utilisée pour chacune des 2 passerelles SIP externes.	
SIP > SIP Ext Gateway > "select the SIP external gateway" SIP > Passerelles Externes > "sélectionner la passerelle Externe"	PCS IP Address has to be set with the "Global IP Address" ➔ 255.255.255.255 Configurer le champ Adresse IP PCS avec l'adresse IP globale ➔ 255.255.255.255
Spatial redundancy configuration (optional)	
Note: Internal OXE DNS resolver must be enabled: netadmin -p yes. Note: La résolution de nom DNS doit être active sur l'OXE: netadmin -p yes.	
4645 Voice Mail configuration	
IP > IP Parameters > G711 VOIP Framing for 4645 IP > Paramètres IP > Framing VOIP pour G711 (4645)	Parameter has to be set to 20 ms (only supported for Appliance Server. For CS (Commun Hardware), parameter has to remain in the default configuration (30ms) Ce paramètre doit être configuré à 20 ms (seulement supporté pour Appliance Server). Pour CS (Hardware Commun), ce paramètre doit resté dans la configuration par défaut (30ms)
4059 Attendant configuration	
Attendant > Attendant sets Opératrice > Postes Opératrices	Tone Presence has to be set to YES Présence tonalité doit être configurée à Oui
System > Timers Installation > Temporisations	Timer 102 has to be set to value different to 0 to have a welcome guide (else 0) Temporisation 102 doit être configurée à une valeur différente de 0 pour avoir un guide d'accueil (sinon 0)
Security configuration	
! Important ! As of R101, trusted hosts including the Btalk SBCs must also be declared in the OXE firewall through the 'Restricted Access Configuration' of netadmin. ! Important ! A partir de la version R101, les @IP de confiance incluant les SBCs BTIP doivent aussi être declarées dans le firewall de l'OXE via le menu 'Configuration d'Accès Restreint' de netadmin.	
SIP > Trusted IP Addresses SIP > Adresses IP de Confiance	Create IP Addresses of each SIP external eco-system including the BTalk SBC). killall sipmotor command must be used to validate the creation. Créer les adresses IP de chaque application externe SIP y compris les SBC BTIP. La commande killall sipmotor doit être utilisée pour valider la création.

5.2. Fax configuration with OXE

5.2.1. G.711 Fax Passthrough

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.

Configure following OXE parameters to enable G.711 Fax Passthrough transmission over SIP trunk.

OXE configuration	
SIP > SIP Ext Gateway SIP > Passerelles Externes	Fax Procedure Type has to be set to G711 only Type procédure FAX doit être configuré à G711
IP > Fax Parameters -> Inhibit the T38 negotioation • true IP > Paramètres Fax -> Inhiber la negociation T38 • true	Enable checkbox Inhibit the T38 negotiation Cocher la case Inhiber la negociation T38
IP > Fax Parameters -> T38 only • false IP > Paramètres Fax -> T38 • false	Disable checkbox T38 only Décocher la case T38

5.2.1. T.38 Fax

Configure following OXE parameters to enable T.38 Fax transmission over SIP trunk.

OXE configuration	
SIP > SIP Ext Gateway SIP > Passerelles Externes	Fax Procedure Type has to be set to T38 only Type procédure FAX doit être configuré à T38
IP > Fax Parameters -> Inhibit the T38 negotioation • false IP > Paramètres Fax -> Inhiber la negociation T38 • false	Disable checkbox Inhibit the T38 negotiation Décocher la case Inhiber la negociation T38
IP > Fax Parameters -> T38 only • true IP > Paramètres Fax -> T38 • true	Enable checkbox T38 only Cocher la case T38

5.3. BTalk French customers and BTIP DROM architectures

For a trunking point of view, mechanism is similar for both 'BTalk French customers' and 'BTIP DROM' (French overseas departments), the IPBX must support international dial plans (example: CC = +262 for La Réunion instead of +33 for France) and route local calls to the dedicated aSBC pair.

"BTIP hors de France" / "BTIP DROM" additional configuration on OXE	
Add SIP External Gateway for BT SBC SIP > SIP Ext Gateway Ajouter les Passerelles SIP Externes pour les aSBC BTalk / BTIP DROM SIP > Passerelles Externes	Please refer to ROUTE MECANISM ON OXE On-net calls off-net calls Voir ROUTE MECANISM ON OXE On-net calls off-net calls
Translator > External Numbering Plan > Numbering Discriminator > Discriminator Rule > "select a Discriminator No." Traducteur > Plan de numérotation externe > Discrimination numérotation > Règle de discrimination > "sélectionner un numéro de discrimination"	ARS Route List Number has to match the ARS Route for SIP Trunking Number of Digits has to be set to the exact expected number No Table De Routage ARS doit correspondre à la Route ARS pour SIP Trunking Nombre de chiffres doit être configuré avec le nombre exact de chiffres attendus
Translator > Automatic Route Selection > ARS Route list > ARS Route > "select an ARS Route list" Traducteur > Tables de routage ARS > Table de routage ARS > Routage ARS > "sélectionner une table de routage ARS"	Trunk Group has to match the public SIP Trunk Numbering Command Table. ID has to match a SIP External Gateway Quality has to be set to Speech and Fax Faisceau doit correspondre au faisceau SIP public No table commande num. doit correspondre à une Passerelle Externe Qualité doit être configurée à Voix et Télécopie
Translator > Automatic Route Selection > ARS Route list > Time-based Route List > "select an ARS Route list" Traducteur > Tables de routage ARS > Table de routage ARS > Liste des routes temporelles > "sélectionner une table de routage ARS"	In ARS Route menu, 2 or 3 routes have to be created: ▪ 1 (route SIP to nominal BTIP/BT aSBC) ▪ 2 (route SIP to backup BTIP/BT aSBC) ▪ 3 (route to PSTN - optional - only if T0/T2 on the site) Dans le menu Routage ARS, 2 ou 3 routes doivent être créées: ▪ 1 (route SIP vers l'aSBC BTIP/BT nominal) ▪ 2 (route SIP vers l'aSBC BTIP/BT secours) ▪ 3 (route vers le PSTN – optionnel – seulement si T0/T2 sur le site)
Translator > Automatic Route Selection > ARS Route list > Numbering Command Table > "select a Numbering Command Table" Traducteur > Tables de routage ARS > Table commande num. > "sélectionner une table de commande num."	Carrier Reference has to be set to 0 (=not used) Associated Ext SIP gateway has to match the SIP Ext Gateway associated for SIP Trunking. The parameter Command has to be configured to "I" ([I]nsert). Réf.Opérateur réseau doit être configurée à 0 (=non utilisé) Gateway SIP associée doit correspondre à la Passerelle Externe associé pour SIP Trunking. Le paramètre Commande doit être renseigné à "I" ([I]nsert).

6. OXE + OTSBC SIP trunking configuration checklist

The aim of this chapter is to provide steps to configure an Alcatel-Lucent OTSBC / AudioCodes Mediant SBC for interworking between the OXE and BTIP/BTalk service.
This guide shows only the settings to be checked or changed. The other settings can remain at their default values.
The "Index" values are given as example because they can be different if a configuration already exists.

On OXE, the SIP External Gateway should point to the OTSBC instead of the BTIP/BTalk SBC.
Even if the public SIP trunk between OTSBC and BTIP/BTalk is encrypted, the local SIP trunk between OXE and OTSBC can be in clear or in native encrypted mode. Only the unencrypted mode is described here and parameters are the same as those already listed in chap. 5.

Warning ! The VIA header is used to determine the origin of incoming calls when other headers do not match with the remote domain (BTIP/BTalk infrastructure) of the SIP External Gateway (OTSBC). So, as a NAT is done by the OTSBC, that parameter must be activated:
/System/Other System Param./SIP Parameters/VIA Header_ Inbound Calls Routing +True

6.1 SBC - IP Network configuration

6.1.1 Core Entities

1. Check or create the ethernet Groups:

   - GROUP 1: that corresponds to the physical (or virtual) interface on OXE side (LAN) or also called "south" side
   - GROUP 2: that corresponds to the physical (or virtual) interface on BTIP/BTalk side (WAN) or also called "north" side

2. Check or create two Ethernet Devices:

   - LAN_Dev : that corresponds to GROUP1
   - WAN_Dev : that corresponds to GROUP2

3. Check or create two IP Interfaces:

   - LAN_IF : Associated to OXE, used for Media, SIG and Management (depends on customer architecture, could be a dedicated interface for management)
   - WAN_IF : Associated to BTIP/Btalk, used for Media and SIG

6.2 SBC - OXE LAN side configuration

6.2.1 Coders & Profiles

Create new Coder Groups through the following menu:
SETUP > SIGNALING&MEDIA > CODERS & PROFILES > Coder Groups

Configure **AudioCodersGroups_0** as follow:

Parameter	Value
AudioCodersGroup_0	
Coder Name	G722
Packetization Time	20
Rate	64
Payload Type	9
Silence Suppression	Disabled
Coder Name	G711A-law (or G711µ-law depending on countries)
Packetization Time	20
Rate	64
Payload Type	8
Silence Suppression	Disabled
Coder Name	G729 (optional, depending on customer request)
Packetization Time	20
Rate	8
Payload Type	18
Silence Suppression	Disabled

Create new IP Profile through the following menu:
SETUP > SIGNALING&MEDIA > CODERS & PROFILES > IP Profiles

Create an IP Profile for OXE as follow:

Parameter	Value
General	
Name	OXE_IPProfile
SBC Media	
Extension Coders Group	AudioCodersGroups_0
RFC2833 DTMF Payload Type	101
SBC Signaling	
Remote Update Support	Supported Only After Connect
Remote re-INVITE	Supported
Media security	
SBC Media Security Mode	RTP
SBC Media	
Extension Coders Group	AudioCodersGroups_0

6.2.2 Core entities

No changes are required on the SRDs.
SETUP > SIGNALING&MEDIA >CORE ENTITIES>SRDs

Parameter	Value
Index	1
Name	defaultSRD (#1)
Sharing Policy	Shared
SBC operation mode	B2BUA
User Security mode	Accept All

Create a Media Realm through the following menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Media Realms

Parameter	Value
Index	1
Name	OXE_MRealm
Topology location	Down
IPV4 interface name	LAN_IF
Port range start	*6000* (depends on customer)
Number of media session legs	*100* (depends on customer)
Default media realm	Yes

Create a SIP Interface through the menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > SIP Interface

Parameter	Value
General	
Name	OXE_SIPint
Topology Location	Down
Network Interface	LAN_IF
UDP Port	5060
TCP Port	0
TLS Port	0
Enable TCP Keepalive	Disable
Media	

Create a new Proxy Set through the menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Proxy Sets

Parameter	Value
Index	1
Name	OXE_PSet
SBC ipv4 SIP interface	OXE_SIPint
Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive time	300
Proxy Hot swap	Disable

Once the OXE Proxy Set created, navigate to the **Proxy Set addresses** parameters.

For OXE, create one proxy address that contain OXE IP address or the hostname in case of spatial redundancy (DNS client must be enable on the OTSBC):

Parameter	Value
General	
Proxy Address	*<OXE_@IP or hostname>*:5060
Transport Type	UDP

Create a new IP Group through the following menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > IP Groups

Parameter	Value
Index	1
Name	OXE_IPgrp
Topology location	Down
Type	Server
Proxy Set	OXE_PSet
IP profile	OXE_IPProfile
Media Realms	OXE_MRealm
Classify by proxy	Enable
Inbound Message Manipulation Set	1
Outbound Message ManipulationSet	3

6.2.3 Message Manipulation

SETUP > SIGNALING&MEDIA > MESSAGE MANIPULATION > Message Manipulations

The manipulation Set ID must be mentioned in "**Inbound message manipulation Set**" on the **"IP Groups"** menu above.

A message manipulation has to be created to carry out properly the OXE user-agent in the BTIP/BTalk network. It will be concatenated with the SBC user-agent:

Parameter	Value
General	
Name	User-agent_OXE
Manipulation Set ID	1
Row Role	Use Current Condition
Match	
Message Type	any
Condition	header.user-agent exists and header.user-agent regex (.*)
Action	
Action Subject	var.session.agent
Action Type	Modify
Action Value	$1

The manipulation **Set ID** must be mentioned in "**Outbound message manipulation Set**" on the "**IP Groups**" menu above.

1. Topology hiding modifies "From host" part with SBC IP address.

Parameter	Value
General	
Name	Hide IP From
Manipulation Set ID	3
Row Role	Use Current Condition
Match	
Message Type	any
Condition	header.from.url.host !contains 'Anonymous'
Action	
Action Subject	header.from.url.host
Action Type	Modify
Action Value	header.via.host

2. Topology hiding: modifies "To host" part with remote proxy IP address.

Parameter	Value
General	
Name	Hide IP To
Manipulation Set ID	3
Row Role	Use Current Condition
Match	
Message Type	any
Condition	
Action	
Action Subject	header.to.url.host
Action Type	Modify
Action Value	param.message.address.dst.ip

3. Topology hiding: modifies "Request-URI" host part with remote proxy IP address.

Parameter	Value
General	
Name	Hide IP Request-URI
Manipulation Set ID	3
Row Role	Use Current Condition
Match	
Message Type	any.request
Condition	
Action	
Action Subject	header.request-uri.url.host
Action Type	Modify
Action Value	param.message.address.dst.ip

4. Topology hiding: modifies "Diversion host" part with SBC IP address.

Parameter	Value
General	
Name	Hide IP Diversion

Manipulation Set ID	3
Row Role	Use Current Condition
Match	
Message Type	any
Condition	header.diversion exists
Action	
Action Subject	header.diversion.url.host
Action Type	Modify
Action Value	header.via.host

6.3 SBC - BTIP/BTalk side configuration over BVPN (unencrypted flows)

For the SBC - BTIP/BTalk side configuration **over Internet** with encrypted flows, refer to the next chapter.

6.3.1 Coders & Profiles

Coder Groups are common on both sides OXE and BTIP/Btalk.

Create new **Allowed Audio Coder Group** through the following menu:
SETUP > SIGNALING&MEDIA > CODERS & PROFILES > Allowed Audio Coder Groups

Parameter	Value
General	
Name	BTIP

Click on **Allowed Audio Coder 0 item** and click on "**+New**" to add the coders in the right order :

Parameter	Value
Index	Coder
0	G722
1	G711 A-law (or G711 µ-law depending on country)
2	G729

Create new BTIP/BTalk IP Profile through the following menu:
SETUP > SIGNALING&MEDIA > CODERS & PROFILES > IP Profiles

Parameter	Value
General	
Name	BTIP_IPProfile
Media security	
SBC Media Security Mode	RTP
SBC Remove Crypto LifeTime in SDP	No
SBC Media	
Extension Coders Group	AudioCodersGroups_0
RFC2833 DTMF Payload Type	101
Quality of Service	
RTP IP DiffServ	46
Signalling DiffServ	46

6.3.2 Core Entities

Note: Please do not use Index 0, if so you may encounter some configuration issues!

Create a BTIP Media Realm through the following menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Media Realms

Parameter	Value
General	
Name	BTIP_MRealm
Topology Location	UP
IPv4 Interface Name	WAN_IF
Port Range Start	*6000* (depends on customer, authorized range on BTIP or BTalk is 6000-20000)
Number of media session legs	*100* (depends on customer)
Default Media Realms	NO

Create a new SIP Interface through the following menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > SIP Interface

Parameter	Value
General	
Name	BTIP_SIPInt
Topology Location	UP
Network Interface	WAN_IF
UDP Port	5060
TCP Port	0
TLS Port	0
Media	
Media Realm	BTIP_MRealm

Create a new Proxy Sets through the following menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Proxy Sets

Parameter	Value
General	
Name	BTIP_PSet
SBC IPv4 SIP Interface	BTIP_SIPInt
Keep alive	
Proxy Keep-Alive	Using Options
Proxy Keep-Alive Time	300
Redundancy	
Proxy Hot swap	Enable
Redundancy mode	*Homing* (depends on customer architecture)

Once the BTIP Proxy Set created, navigate to the **Proxy Set addresses** parameters.
For BTIP, create 2 proxy addresses one for the nominal SBC and one for the Backup SBC:

Parameter	Value
General	
index	1
Proxy Address	*<BTIP_Nominal_SBC @IP>*:5060
Transport Type	UDP
index	2
Proxy Address	*< BTIP_Backup_SBC @IP >*:5060
Transport Type	UDP

Create a new IP Group through the following menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > IP Group

Parameter	Value
General	
Name	BTIP_IPgrp
Topology Location	UP
Proxy Set	BTIP_PSet
IP Profile	BTIP_IPProfile
Media Realm	BTIP_Mrealm
Inbound Message Manipulation Set	-1
Outbound Message ManipulationSet	2

6.3.3 Message Manipulation

A message manipulation has to be created to carry out properly the user-agents in the BTIP/BTalk network. Both OXE and SBC user-agents are concatenated with a '+' :
SETUP > SIGNALING&MEDIA > MESSAGE MANIPULATION > Message Manipulations

Parameter	Value
General	
Name	User-agent_SBC
Manipulation Set ID	2
Row Role	Use Current Condition
Match	
Message Type	any
Condition	header.user-agent regex (.*)
Action	
Action Subject	header.user-agent
Action Type	Modify
Action Value	var.session.0 + '+' + $1

The manipulation Set ID must be mentioned in "Outbound message manipulation Set" on the **"IP Groups"** menu above.

6.3.4 SBC - IP-to-IP Routing

Create 3 IP-to-IP routing rules through the following menu:
SETUP > SIGNALING&MEDIA > SBC > Routing > IP-to-IP Routing

1) For OPTIONS messages:

Parameter	Value
General	
Name	Options
Match	
Request Type	OPTIONS
Action	
Destination Type	Dest Address
Destination Address	internal

2) For OXE to BTIP

Parameter	Value
General	
Name	OXE-to-BTIP
Action	
Destination Type	IP Group
Destination IP Group	BTIP_IPgrp
Match	
Source IP Group	OXE_IPgrp

3) For BTIP to OXE

Parameter	Value
General	
Name	BTIP-to-OXE
Action	
Destination Type	IP Group
Destination IP Group	OXE_IPgrp
Match	
Source IP Group	BTIP_IPgrp

6.4 SBC - BTIP/BTalk side configuration over Internet (encrypted flows)

6.4.1 TLS context

The encrypted architecture requires the usage of an encryption Key and Ciphers present in a TLS context in order. A specific Orange TLS Context have to be created.

This SIP signaling will be configured to be compliant with Orange BTalk specification :

- For encrypted BTIP/BTalk SIP Trunk architecture we need to configure: **TLS v1.3 (recommended)** or TLS 1.2 (alternative)
- TLS **Mutual authentication** activated
- **Key size = 2048**
- Cipher list is supported as **Cipher Client/Server** :

  TLS 1.3 (recommanded):

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

  Create the security context using the menu:
  SETUP > IP Network > SECURITY > TLS Contexts

Parameter	Value
General	
Name	Orange
TLS version	TLSv1.3
Cipher Server TLS 1.3	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
Cipher Client TLS 1.3	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
DH Key Size	2048

TLS 1.2 (alternative):

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

Create the security context using the menu:
SETUP > IP Network > SECURITY > TLS Contexts

Parameter	Value
General	
Name	Orange
TLS version	TLSv1.2
Cipher Server	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
Cipher Client	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
DH Key Size	2048

6.4.2 Certificate

The TLS Context need a Certificate signed. To obtain this Certificate Authority (CA) you must generate your CSR based on the information of the SBC and Company with **SHA-256** encryption.

Create a CSR using the menu:
SETUP > IP Network > SECURITY > TLS Contexts and select the Orange TLS context previously created and click on "**Change Certificate".** Fill in the customer information in the **Certificate Signing Request** form and Click "**Create CSR**".

After creating the CSR, copy the text (including the BEGIN/END lines) and send it to your Certification Authority for signing and **get a fullchain Certificate Authority (CA) –including both Root and Intermediate CA-.**

When you have the CA files (p7b and bundle), please load it on the TLS Context just created. Only Base64 (PEM) encoded X.509 certificates can be loaded to the ALE OTSBC / Audiocodes SBC.
For that, import the certificate using the menu:
SETUP > IP Network > SECURITY > TLS Contexts and select the Orange TLS context previously created and click on "**Change Certificate".**

Scroll down to the **Upload certificates** files from your computer group, click the **Browse** button corresponding to the '**Send Device Certificate...**' field, navigate to the **cert.txt** file, and then click **Load File**.

After the certificate successfully loaded into the device, save the configuration with a device reset.

At this step the fullchain **Root and intermediate Certificate (PEM format) must be transmitted to Orange BTIP/BTalk team.**

Reversaly, as mutual authentication is used between both parties, you must import the **Root and the Intermediate Orange CA** included in the DigiCert CA by following the procedure described below. Connect to the Digicert site : https://www.digicert.com/digicert-root-certificates.htm then download and import (pem format):

- the Root CA: **DigiCert Global Root CA**
- the Intermediate CA: **DigiCert TLS RSA SHA256 2020 CA1**

  *Note: the previous intermediate CA 'DigiCert SHA2 Secure Server CA' **is no longer used***

Import the **Root and the Intermediate Orange CA** certificates using the menu:
SETUP > IP Network > SECURITY > TLS Contexts and select the Orange TLS context previously created and click on "**Trusted Root Certificates"**. Import certificates.

6.4.3 TLS Mutual Authentication 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:

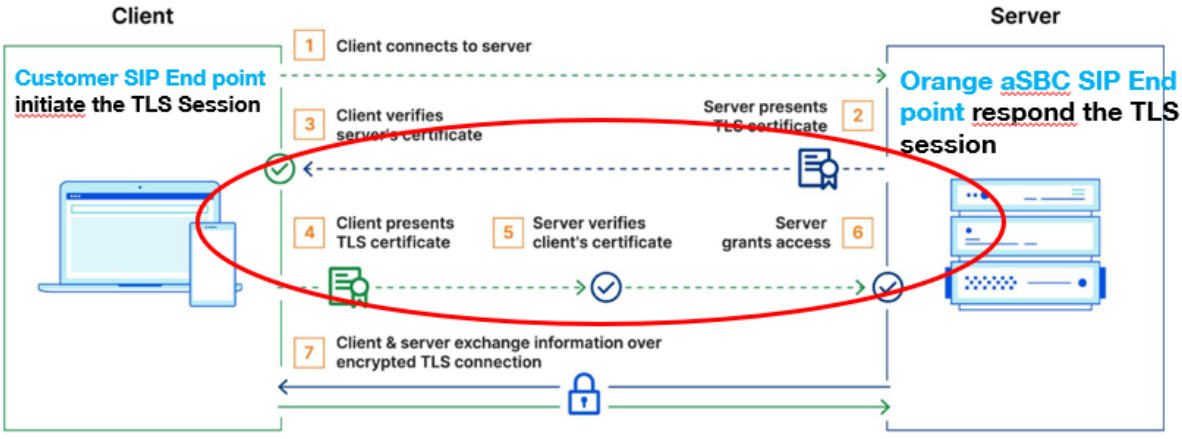
- which endpoint acts as the TLS client or TLS server.
- and the vendor capabilities for handling certificates without the Client Authentication EKU

Alcatel OTSBC TLS Handshake behaviour

Case 1 - Alcatel OTSBC initiates the TLS handshake

The Alcatel OTSBC acts as the TLS client, and the **Orange aSBC SIP Endpoint** acts as the TLS server.

1. The Orange aSBC requests the customer certificate (TLS message “Certificate request”)
2. The Alcatel OTSBC 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 Alcatel OTSBC initiates the connection, even if the customer public certificate contains the serverAuth EKU only.

No specific OTSBC configuration change is required for this scenario.

Case 2: mTLS supported by Audiocodes eSBC without considering missing Client Auth EKU in Orange SBC public certificate.

In this scenario:

1. The Orange aSBC acts as the TLS client.
2. The Audiocodes eSBC acts as the TLS server.
3. The Orange aSBC initiates the TLS handshake.

The Alcatel OTSBC 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 Alcatel OTSBC 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.

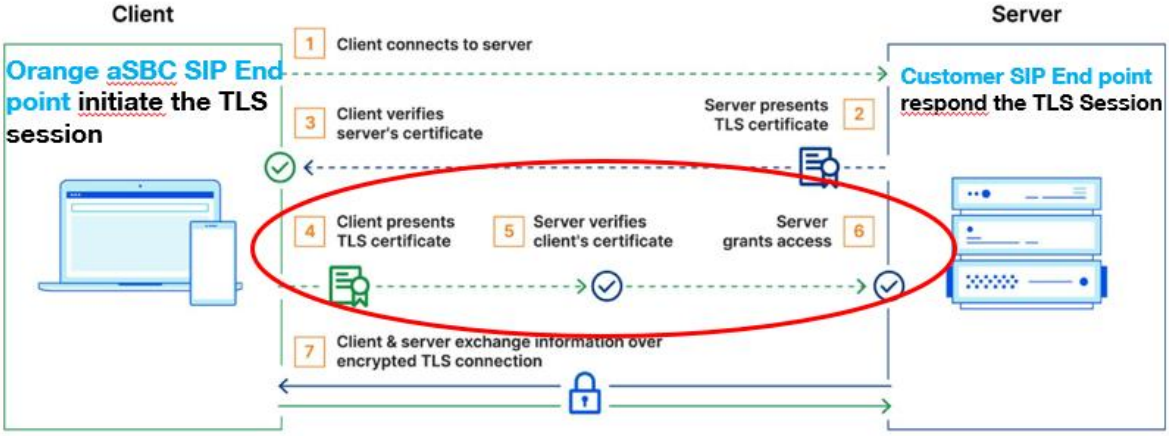
Configuration required to restore mutual TLS
Starting from Audiocodes SBC version 7.40A.600.627 LTS, Audiocodes provides the parameter **"Allow Client Auth Key Usage".** To allow Orange certificates containing serverAuth EKU only, the customer must set this parameter to **"Always"**

'Allow Client Auth Key Usage' `client-auth-key-usage-mode` [AllowClientAuthKeyUsage]	Defines whether the device accepts or rejects client TLS certificates based on the presence of the 'clientAuth' value in the Extended Key Usage (EKU) field. ■ [0] **Always** = The device accepts client certificates regardless of whether the clientAuth EKU is present or not. ■ [1] **According to EKU extension rules** = (Default) The device accepts client certificates only if they include the clientAuth EKU (and rejects certificates that lack the value). **Note:** Certificate Authorities (CAs) such as DigiCert and GlobalSign are gradually discontinuing the issuance of TLS certificates that include the clientAuth EKU.

With this setting, the Alcatel OTSBC accepts the Orange certificate even when the clientAuth EKU is not present.

TLS handshake sequence after the configuration change

1. The Alcatel OTSBC requests the Orange aSBC certificate.
2. The Orange aSBC presents its certificate with Server Authentication (serverAuth) EKU only [4].
3. The Alcatel OTSBC verifies the certificate, accept it regardless of whether the Client Authentication (clientAuth) EKU is not present [5] and grants access [6].



Security consideration: Please note this specific Alcatel OTSBC configuration option reduce customer security concern with Orange: End customer Alcatel OTSBC security heavily change by accepting Orange aSBC certificate without taking into considerations Orange public certificates EKU's in and must accept by End Customer.

Disable client certificate EKU verification:

SETUP > IP Network > Security > TLS Contexts

Parameter	Value
General	
Name	Orange
Allow Client Auth Key Usage	Always

Enable TLS Mutual Authentication and TLS Client Verify Server Certificate through the following menu:

SETUP > IP NETWORK > SECURITY > Security Settings

Parameter	Value
General	
TLS Mutual Authentication	Enable
TLS Client Verify Server Certificate	Enable

6.4.4 Media Security

Enable the media encryption through the following menu:

SETUP > SIGNALING&MEDIA > MEDIA > Media Security

Parameter	Value
General	
Media Security	Enable
Media Security Behavior	Preferable
Offered SRTP Cipher Suite	All

Note: OTSBC Media Security feature is disabled after upgrade from version 7.40 to 7.60.

Configuration of OTSBC after upgrade and restart and then uploading the new license key for version 7.60:
Setup -> Signaling & Media -> Media -> Media Security -> Media Security: Disabled

The Media Security must be enabled again.

Another solution is:
Loading the new license key for 7.60 before upgrading to version 7.60.

Then afer OTSBC software upgrade and restart the Media Security remains enabled.

6.4.5 Coders & Profiles

Create new **Allowed Audio Coder Group** through the following menu:
SETUP > SIGNALING&MEDIA > CODERS & PROFILES > Allowed Audio Coder Groups

Parameter	Value
General	
Name	BTIP

Click on **Allowed Audio Coder 0 item** (index "0" is an example and depends on the current configuration) and click on "**+New**" to add the coders in the right order :

Parameter	Value
Index	Coder
0	G711 A-law (or G711 µ-law depending on country)

Note : only G711 codec is supported with BTIP/BTalk over internet at this time

Create new BTIP/BTalk IP Profile through the following menu:
SETUP > SIGNALING&MEDIA > CODERS & PROFILES > IP Profiles

Parameter	Value
General	
Name	BTIPol_IPProfile
Media security	
SBC Media Security Mode	Secured
SBC Remove Crypto Lifetime in SDP	Yes

SBC Media	
Allowed Audio Coders	BTIP
Allowed Audio Coders Mode	Restriction
RFC2833 DTMF Mode	Extend
RFC2833 DTMF Payload Type	101
Use Silence Suppression	Remove
RTP Redundancy Mode	Disable
Quality of Service	
RTP IP DiffServ	46
Signalling DiffServ	46
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote 3xx Mode	Handle Locally
SBC Signaling	
Diversion Header	As is

6.4.6 Core Entities

Note: Please do not use Index 0, if so you may encounter some configuration issues!

Create a BTIP Media Realm through the following menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Media Realms

Parameter	Value
General	
Name	BTIP_MRealm
Topology Location	UP
IPv4 Interface Name	WAN_IF
Port Range Start	*6000* (depends on customer, authorized range on BTIPoI or BToI is 6000-38000)
Number of media session legs	*100* (depends on customer)
Default Media Realms	NO

Note : on Audiocodes SBC, the RTP UDP port spacing is “10”. It means that for example 5 SIP sessions SIP, 5*10 ports RTP from 6000 to 6050 will be reserved.

Create a new SIP Interface through the following menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > SIP Interfaces

Parameter	Value
General	
Name	BTIP_SIPInt
Topology Location	UP
Network Interface	WAN_IF
UDP Port	0
TCP Port	0
TLS Port	5061
Classification	
Classification Failure Response Type	0
Security	
TLS Context Name	Orange
TLS Mutual Authentication	Enable

Media	
Media Realm	BTIP_MRealm

Create a new Proxy Sets through the following menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > Proxy Sets

Parameter	Value
General	
Name	BTIP_PSet
SBC IPv4 SIP Interface	BTIP_SIPInt
TLS Context Name	Orange
Keep alive	
Proxy Keep-Alive	Using Options
Proxy Keep-Alive Time	300
Redundancy	
Proxy Hot swap	Enable
Redundancy mode	*Homing* (depends on customer architecture)

Select the "**BTIP_PSet**" Proxy Set" just created and click on "**Proxy Address 1 items**" (index 1 can be different, it depends on your current configuration). Once the For BTIP over Internet, create 2 proxy addresses one for the nominal SBC and one for the backup SBC.

Parameter	Value
General	
index	1
Proxy Address	*<BTIP_Public FQDN_Nominal>*:5061
Transport Type	TLS
index	2
Proxy Address	*<BTIP_Public FQDN_Backup>*:5061
Transport Type	TLS

Note : The Public FQDN (Type A or SRV) set in the "Proxy Address" is the "**Public FQDN**" provided by Orange for the SIP trunk BTIP/BTalk. We recommend to use primarily ours Public FQDN which required **DNS Servers must be configured in "Public" network interface.**

Create a new IP Group through the following menu:
SETUP > SIGNALING&MEDIA > CORE ENTITIES > IP Group

Parameter	Value
General	
Name	BTIP_IPgrp
Topology Location	UP
Proxy Set	BTIP_PSet
IP Profile	BTIPoI_IPProfile
Media Realm	BTIP_Mrealm
Inbound Message Manipulation Set	-1
Outbound Message ManipulationSet	2

6.4.7 Message Manipulation

SETUP > SIGNALING&MEDIA > MESSAGE MANIPULATION > Message Manipulations

The manipulation **Set ID** must be mentioned in "**Outbound message manipulation Set**" on the "**IP Groups**" menu above.

Implement following message manipulations:

5. To carry out properly the user-agents in the BTIP/BTalk network. Both OXE and SBC user-agents are concatenated with a '+' :

Parameter	Value
General	
Name	User-agent_SBC
Manipulation Set ID	2
Row Role	Use Current Condition
Match	
Message Type	any
Condition	header.user-agent regex (.*)
Action	
Action Subject	header.user-agent
Action Type	Modify
Action Value	var.session.0 + '+' + $1

6. Topology hiding modifies "From host" part with SBC IP address.

Parameter	Value
General	
Name	Hide IP From
Manipulation Set ID	2
Row Role	Use Current Condition
Match	
Message Type	any
Condition	header.from.url.host !contains 'Anonymous'
Action	
Action Subject	header.from.url.host
Action Type	Modify
Action Value	header.via.host

7. Topology hiding: modifies "To host" part with remote proxy IP address.

Parameter	Value
General	
Name	Hide IP To
Manipulation Set ID	2
Row Role	Use Current Condition
Match	
Message Type	any
Condition	
Action	
Action Subject	header.to.url.host
Action Type	Modify

Action Value	param.message.address.dst.ip

8. Topology hiding: modifies “Request-URI” host part with remote proxy IP address.

Parameter	Value
General	
Name	Hide IP Request-URI
Manipulation Set ID	2
Row Role	Use Current Condition
Match	
Message Type	any.request
Condition	
Action	
Action Subject	header.request-uri.url.host
Action Type	Modify
Action Value	param.message.address.dst.ip

9. Topology hiding: modifies “P-Asserted-Identity host” part with SBC IP address.

Parameter	Value
General	
Name	Hide IP PAI
Manipulation Set ID	2
Row Role	Use Current Condition
Match	
Message Type	any
Condition	header.p-asserted-identity exists
Action	
Action Subject	header.p-asserted-identity.url.host
Action Type	Modify
Action Value	header.via.host

10. Topology hiding: modifies “Diversion host” part with SBC IP address.

Parameter	Value
General	
Name	Hide IP Diversion
Manipulation Set ID	2
Row Role	Use Current Condition
Match	
Message Type	any
Condition	header.diversion exists
Action	
Action Subject	header.diversion.url.host
Action Type	Modify
Action Value	header.via.host

6.4.8 SBC - IP-to-IP Routing

Create 3 IP-to-IP routing rules through the following menu:
SETUP > SIGNALING&MEDIA > SBC > Routing > IP-to-IP Routing

1. For OPTIONS messages:

Parameter	Value
General	
Name	Options
Match	
Request Type	OPTIONS
Action	
Destination Type	Dest Address
Destination Address	internal

2. For OXE to BTIP

Parameter	Value
General	
Name	OXE-to-BTIP
Action	
Destination Type	IP Group
Destination IP Group	BTIP_IPgrp
Match	
Source IP Group	OXE_IPgrp

3. For BTIP to OXE

Parameter	Value
General	
Name	BTIP-to-OXE
Action	
Destination Type	IP Group
Destination IP Group	OXE_IPgrp
Match	
Source IP Group	BTIP_IPgrp

Glossary

- ALE : Alcatel-Lucent Enterprise International
- OXE : OmniPCX Enterprise
- OTBE : OpenTouch Business Edition
- OTMS : OpenTouch Multimedia Services
- OTMC : OpenTouch Messenging Center
- OTSBC : OpenTouch Session Border Controller
- OTFC : OpenTouch Fax Center
- IPMG : IP Media Gateway
- PCS : Passive Communication Server
- WebRTC GW : Rainbow WebRTC gateway
- BVPN : Business Virtual Private Network (Orange Business Services)
- BTIP : Business Talk IP (France) over BVPN
- BTalk : Business Talk (International) over BVPN
- BTIPoI : Business Talk IP over Internet (France)
- BToI : Business Talk over Internet (International)
- A-SBC : access Session Border Controller (Orange Business Services infrastructure)
- C-SBC : enterprise Session Border Controller on customer side (“C-SBC” for “Customer SBC”)
- AS : Application Server BTalk / BTIP
- TP WAN : Third Party WAN (on customer side)
- CAC : Call Admission Control