Alcatel-Lucent OmniPCX Enterprise Purple Native Encryption

Software encryption of communications and hardened platform against cyberattacks

Digitalisation has been underway for some time. Today, employees can collaborate wherever they wish with the ability to communicate in real-time. But not all communication tools provide the necessary framework to address **continuous availability**, **security**, **confidentiality** and **compliance**.

Alcatel-Lucent Enterprise (ALE) has been working with organisations and customers worldwide to understand the new challenges they face and to provide **secure unified communications solutions** that enable people to work from anywhere, with any device.

In this document we describe how **ALE protects your communications from cyberattacks**, with a secure-by-design communication platform, open to the cloud with a hybrid architecture, with native best-of-breed encryption mechanisms, providing full control to your IT team and compliance with your security policies and best practices.

Alcatel·Lucent
Enterprise

Today's cybersecurity landscape

The switch to a digital environment has led to a rapid increase in phishing and ransomware attacks. This is a serious concern for the increasing numbers of remote workers in the space, and all organisations (public and private). With cyber threats on the rise, companies need to work harder than ever to protect their employees and their customers.

One important aspect is the fact that moving to the cloud increases the "attack surface", meaning hackers could exploit non-secure openness to cloud-based services or Software as a Service (SaaS). Stringent requirements from the IT team are necessary for provider and vendors' Service Level Agreements (SLAs).

ALE security-by-design approach

Taking a comprehensive look at the current landscape allows companies to determine the protection strategies they need for their IT assets. For instance, ALE offers companies solutions they need to be compliant with regional or vertical regulations and standards, such as General Data Protection Regulation (GDPR), HDS or HIPAA (for healthcare market), and future NIS2 in European countries.

ALE also offers secure connectivity in the cloud, with mutual authentication and encryption elements, better communications confidentiality in meetings, as well as data privacy and control within the cloud. An end-to-end solution to cover the evolving business security environment ensures that teams can safely thrive in any new environment.

Privacy and reliability of cloud services are sometimes questioned. ALE cloud services offer a strict data privacy policy with data centres in different locations for a worldwide service coverage. ALE has points of presence in privacy conscious countries such as France, Germany, USA, Canada, Singapore and Australia. Under the terms of the contract, personal user data is not used for any commercial or marketing purposes, and ALE ensures compliancy with local data privacy regulations such as GDPR in European countries. ALE cloud services are also certified ISO 27001 for information security management and CSPN from french regulator ANSSI.

ALE cloud services can also leverage the customer's communication servers. Customers can keep critical business communication systems on premises and connect to the cloud for innovative collaboration applications and services.

Unified communications hybrid architecture

The collaboration and unified communications platform is an important foundational tool for the company. However, the return on investment only becomes evident with the enrollment of each working group. To make this happen, the stakeholders must be consulted, and their concerns considered and addressed, including the IT team in charge of the security policies.

Too often, security measures hamper the regular use of innovative new services. When it comes to collaborative work, the user experience must remain intuitive. On the administration side, it is important to verify platform compatibility based on environments approved by the IT department, including for example, the allowance of mobile apps for Android and IOS smartphones and tablets. In addition, the collaborative solution and the communication server must dialogue through open APIs to facilitate the management and control of telephone services and exchanges in real-time. This evolution is leading IT teams to more upstream control.

Alcatel-Lucent Enterprise provides comprehensive **on premises** and **cloud-based communication and collaboration** solutions to address digital transformation. ALE communication solutions enable call continuity from anywhere, in any situation and from any device.

ALE key features to protect communications:

- **Secure connectivity** between on premises ALE communication system (IP-PBX and phones) and the cloud infrastructure operated by ALE, with mutual authentication, encryption and Session Border Controller (SBC) to secure the public network access and remote workers equipped with SIP clients and devices
- **Seamless connection** inside and outside the organisation. The underlying communication infrastructure connects hybrid workers to back-office and front-line employees, whatever their device, through a variety of standard technologies such as PSTN, TDM, IP, SIP, VoWiFi and DECT and provides metrics for IT to monitor the Quality of Service (QoS)
- **High availability** reaching 5x9s with spatially redundant architectures, deployed on customer's premises or hosted in a private cloud, 100% software-based and fully virtualised, with protection against denial of service (DoS) attacks, built-in security with hardened devices and operating systems
- **Data privacy and protection** with role-based access control and encryption of stored data. This ensures all the crucial data gathered in the evolving business environment is fully protected from end-to-end and under your control.
- **Communications confidentiality** with strong encryption mechanisms based on industry standards natively implemented into the solution, without any impact on voice quality and performance, delivering the experience customers and employees expect

Communications are susceptible to being intercepted and listened to by anybody, over the corporate network (LAN or WLAN) and even more so over the public Internet. Multiple counter measures at the network infrastructure level minimise the risk of interception (switched LAN environment, VLAN segmentation, management of ACLs between VLANS, protection against ARP spoofing or flooding), but the only way to ensure complete protection is to have the conversation fully encrypted on transit: Even if intercepted by a malicious person the voice conversation will remain inaudible because de-ciphering is not possible.

Alcatel-Lucent OmniPCX® Enterprise Purple (OXE Purple) provides built-in **Native Encryption** to ensure complete encryption for any communications over the network (private and public Internet).

OXE Purple Native Encryption principles

OXE Purple offers business communications designed for the digital age. It connects the entire Enterprise and provides organisations the **freedom**, **agility** and **security** to grow their business with trust.

OXE Purple delivers the:

- **Freedom** to connect any time with customers and colleagues. It lets them connect in the office, in industrial buildings, on the road, or at home, using a smartphone, a computer, or a dedicated phone.
- **Agility** to automate business communications operations using a private cloud and integrate real-time interactions into business processes
- **Security** for any interactions inside and outside the organisation whether connecting with a colleague, a partner, a customer or a contact centre agent. Interactions can take place over the phone, on an application on the computer or smartphone, in video conferences and from a secure messaging system in the cloud.

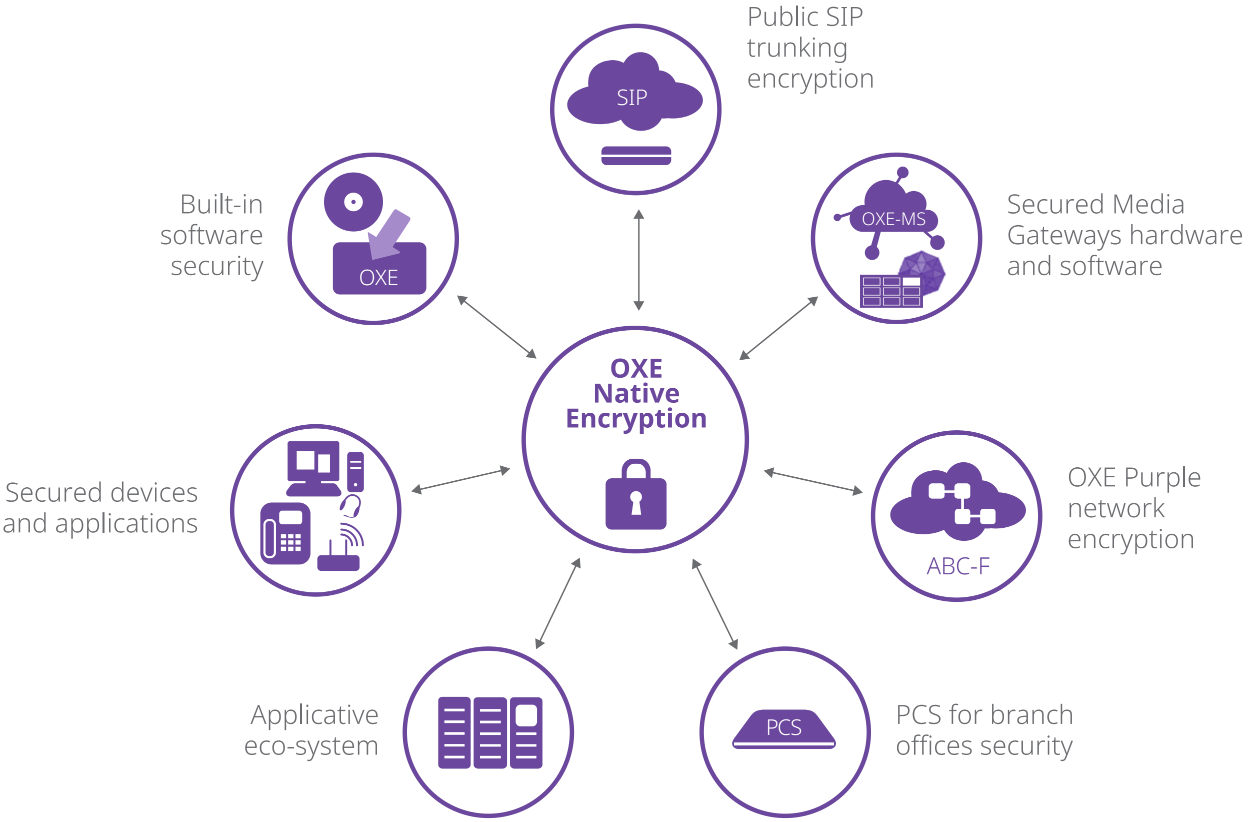
This technology can be securely deployed in any environment: On premises or hosted in private cloud. It is **100% software-based**, supports **virtualisation**, and delivers **5x9s high availability** with hot redundancy of the core components.

It provides confidentiality with state-of-the-art encryption standards with complete encryption in transit for all conversations whatever the device or the software application. It has a flexible architecture, allowing it to target sensitive users among all employees using IP or non-IP devices.

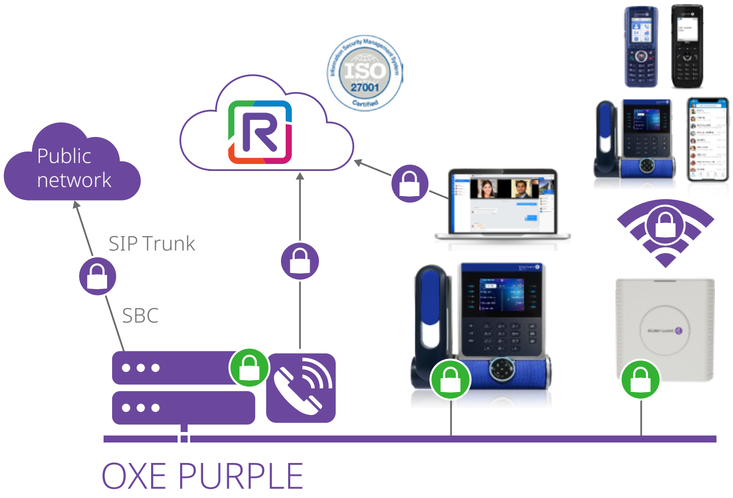
OXE Purple Native Encryption components

OXE Purple Native Encryption offers:

- **Signalling flow encryption** using the Datagram Transport Layer Security (DTLS) or Transport Layer Security (TLS) protocols. This applies to signalling flows exchanged between the OXE Purple Communication Server and DTLS/TLS compatible IP devices and applications.
- **Voice flow encryption** using the SRTP protocol. This applies to voice flows exchanged between DTLS compatible IP devices and applications.
- **Mutual authentication** as an option between server and devices/clients
- **Secured IP Media Gateways** (based on pure software or proprietary hardware) for encrypted media processing including non-IP phones connected to hardware boards (digital and analogue)
- **Encryption of the communications** to the public network through the Public SIP Trunk up to the Service Provider border element using SIP TLS
- **Encryption of conversations** using the Rainbow client application (on desktop, web, android and iOS smartphone) through the Rainbow WebRTC gateway for internal communications (to a device or other application managed by the OXE Purple Communication Server) or to the public network
- **Encryption of the communications** in a network of OXE Purple Communication Servers
- **Support of the geo-redundancy** of the OXE Purple Communication Server and of the Passive Communication Server (PCS) for secure branch office in survivability mode
- **Embedded Certificate Authority (CA) and Trust Store** for certificate-based authentication with a possibility for the customer to customise the certificate with an external Public Key Infrastructure (PKI) for a complete privacy


Public SIP trunking encryption
SIP
Built-in software security
OXE
Secured Media Gateways hardware and software
OXE-MS
OXE Native Encryption
Secured devices and applications
OXE Purple network encryption
ABC-F
Applicative eco-system
PCS
PCS for branch offices security

OXE Purple Native Encryption supports most of the IP devices and applications connected to the Communication Server (including desk phones, softphones and IP DECT base stations). It also supports complete encryption in transit for a user equipped with non-IP equipment (for example an analogue or digital phone) connected to a hardware media gateway managed by the OXE Purple Communication Server. In addition, the feature supports the cloud-based Rainbow™ by Alcatel-Lucent Enterprise collaborative application.

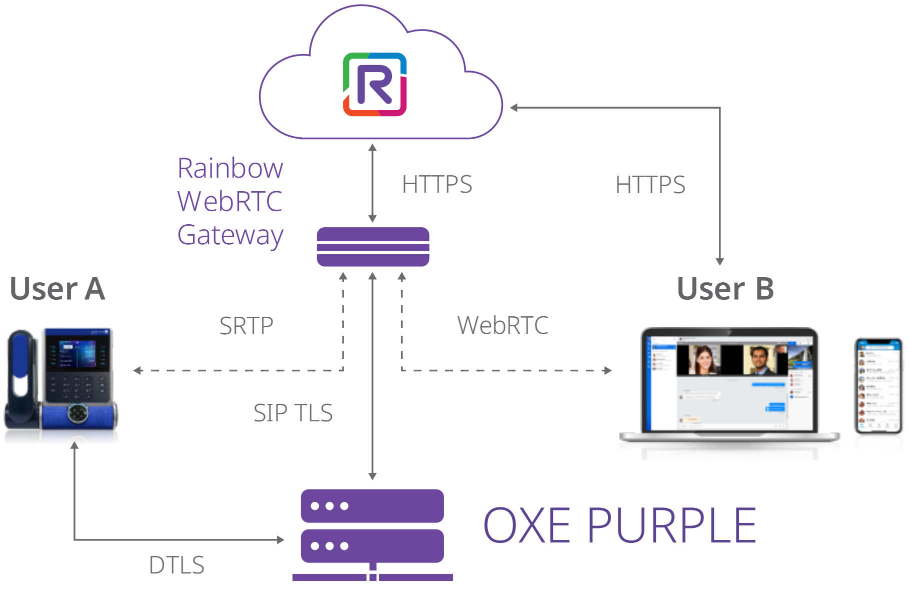


The connection between the OXE Purple Communication Server and the Rainbow cloud services is ensured by the Rainbow WebRTC Gateway software component.

The Rainbow WebRTC Gateway generates an asymmetric key pair and exports a certificate signing request (CSR) to be signed by a certificate authority (CA) that can be the OXE Purple Communication Server embedded certificate authority (CA) or an external public key infrastructure (PKI). The Rainbow WebRTC Gateway identity is controlled by the OXE Purple Communication Server during the TLS handshake using the certificate trust list (CTL) in its Trust Store.

As illustrated in the diagram below, Voice media is encrypted in transit between User A on a desk phone and User B equipped with the Rainbow client application, on PC/Mac/Web or smartphone. The Rainbow WebRTC Gateway performs the real-time relay of the SRTP flow between User A and User B.

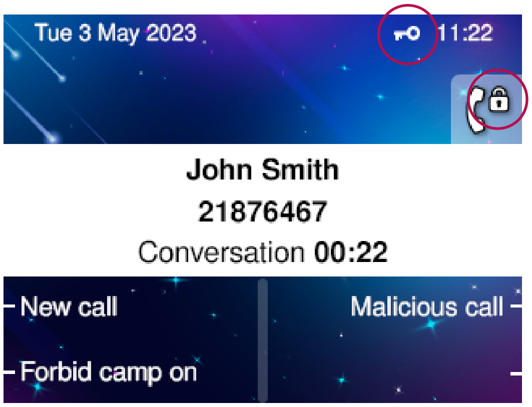
The Rainbow WebRTC Gateway is a full software component that is virtualised, supports duplication and load balancing for more scalability.



Encryption icon on ALE phones and softphone applications

When a communication is encrypted, a shield or padlock icon appears on the phone screen or in the softphone application. This mechanism provides end-users with confidence in the confidentiality of the conversation.

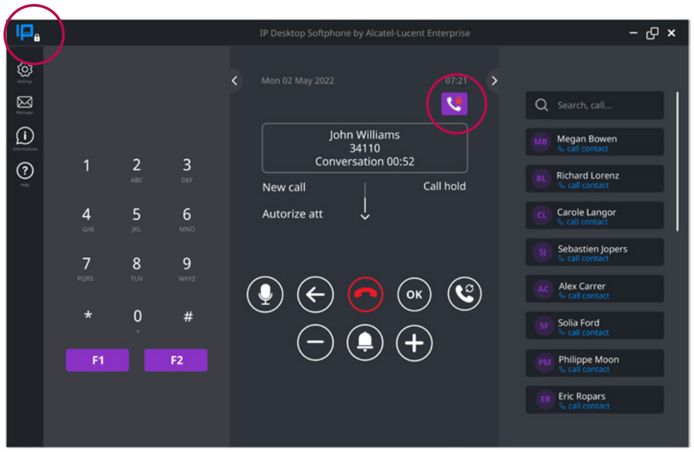
Phones



Tue 3 May 2023 11:22

John Smith
21876467
Conversation 00:22

Softphones



IP Desktop Softphone by Alcatel-Lucent Enterprise

Mon 02 May 2022 07:21

John Williams
34110
Conversation 00:52

Settings
Message
Informations
Help
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
0 +
#
F1
F2
New call
Call hold
Autorize att
OK
Search, call...
MB Megan Bowen call contact
RL Richard Lorenz call contact
CL Carole Langor call contact
SJ Sebastien Jopers call contact
AC Alex Carrer call contact
SF Solia Ford call contact
PM Philippe Moon call contact
ER Eric Ropars call contact

IP Desktop Softphone

Features and benefits

Features	Benefits
Client/device confidentiality (signalling protocol and media)	Prevent from malicious attacks, IP phone spoofing and communications eavesdropping
Mutual authentication and integrity of call control signalling (ensuring that messages have not been modified) with the option of personalising certificates	Protect business communications from denial of service attacks
Support of DTLS 1.2 with AES 256 and SRTP with AES 128: • 100% software-based • 4096 bits SHA2 certificate authentication • ALE Enterprise and Essential DeskPhones (IP), IP Desktop Softphone, compatible with ALE Premium DeskPhones S-series • GD4-XL / GD4/GD3/INTIP3/OMS and PCS • IP-XBS DECT encryption	State-of-the-art ciphering mechanisms to ensure the highest level of protection and confidentiality for all conversations whatever the hardware device or software application used by the employee
Support TLS 1.2 with AES 256 and SRTP with AES 128: • ALE Enterprise DeskPhones in SIP mode, ALE-2 and ALE-3, ALE SoftPhone • SIP trunks • Rainbow WebRTC Gateway encryption	Protect conversations inside and outside the corporate network, including public network access using SIP Trunks
Encryption icon on the phone and in the softphone application to indicate the call is encrypted and secure	End-user confidence in the confidentiality of the conversation
Call encryption in transit with the Rainbow application through the Rainbow WebRTC Gateway	Ensure confidentiality of conversation for employees using the Rainbow client application on PC/Mac, Web, Android smartphone and iPhone
Call recording encryption with Alcatel-Lucent OmniPCX® RECORD Suite	Ensure confidentiality of recorded conversations
Built-in software-based encryption feature for OmniPCX Enterprise Purple solution	Implement high-grade security processes without impacting the manageability of the communication system
Zero impact on Quality of Service (QoS) settings and network configuration	Simple deployment and configuration without the need for changes at the network infrastructure level
Geographic redundancy and local branch office survivability support	Business continuity in all situations without compromise on confidentiality in case of network, server or data centre failures

ALE recommendations and best practices

All organisations (public and private) are significant targets for cyberattacks. Implementing the most secure equipment available is essential. Integrated management tools must allow security supervision across all elements.

Additionally, mobile devices are transforming the communications landscape and heightening the need for security as cyber attackers exploit the increasing volumes of code contained at every point of access. Defense-grade encryption, data privacy and protected communications environments require a secure and highly available infrastructure that is efficient and easy to manage.

ALE recommends you:

Update and monitor your communication system:

- System updates are critically important in terms of cybersecurity. This keeps your communication system up to date with protection against software vulnerability.
- Enable monitoring of your communication system to track suspicious activities by configuring use thresholds and alarms in the network management system

Authenticate and encrypt:

- Enable mutual authentication between all devices (phones and gateways) and the communication server with personalised certificates in the most sensitive environments
- Signalling must be encrypted to prevent protocol poisoning attacks and man in-the-middle attacks
- IP communications must be encrypted to avoid eavesdropping

Make your communication system redundant and add a security component:

- Risk can never be equal to zero. If a gateway or the main communication system is down, a back-up system can take over seamlessly when there is spatial redundancy
- Add the necessary components to protect your communication system, such as a Session Border Controller (SBC) or a Reverse Proxy (RP), while notification servers are used to alert the necessary people

Educate:

- Educate users and administrators; apply best practices within your teams including, reminders for updating passwords, train users on how to fight cybercrime and how to recognise an encrypted call with the shield or padlock icon on the phone

For more information, check out our additional resources:

OmniPCX Enterprise Purple Brochure

OmniPCX Enterprise Purple Datasheet

Securing unified communications and collaboration solutions

Alcatel·Lucent Enterprise